Journal of Law, Market & Innovation

ISSUE 2/2025

Journal of Law, Market & Innovation

2/2025

Editors: ***Riccardo de Caria – Antonio Davola - Cristina Poncibò***

Journal of Law, Market & Innovation
Vol. 4 - Issue 2 - 2025
ISSN 2785-7867
Journal of Law, Market & Innovation

TABLE OF CONTENTS

Riccardo de Caria - Antonio Davola - Cristina Poncibò

FOREWORD TO ISSUE 2/2025

COMPLIANCE & ENFORCEMENT TECHNOLOGIES

The present issue of the Journal of Law, Market & Innovation covers a set of strategic topics that can be traced to the role that emerging technologies can play for compliance and enforcement, and to the subsequent regulatory challenges they raise.

This theme emerges from the acknowledgement that the rapid evolution of digital technologies has fundamentally transformed the landscape of regulatory compliance and enforcement, creating both unprecedented opportunities and complex challenges for legal systems worldwide.

The digital transformation of regulatory frameworks has accelerated dramatically in recent years, particularly within the European Union's expanding digital governance ecosystem. As new technologies like artificial intelligence, blockchain, and automated data analytics become increasingly integrated into compliance and enforcement mechanisms, they promise to bridge traditional enforcement gaps while simultaneously introducing novel regulatory complexities. This technological convergence is particularly evident in the implementation of the EU Digital Acquis, where emerging regulations form an interconnected web of digital governance requirements.

Hence, the concept of compliance and enforcement technologies encompasses a broad spectrum of digital tools designed to promote *ex-ante* compliance with legal frameworks and enhance *ex-post* enforcement capabilities.

These technologies leverage automation, artificial intelligence, and sophisticated data analytics to address enforcement challenges across different jurisdictions, offering the potential to create more consistent, effective, and scalable regulatory oversight. However, their implementation also raises fundamental questions about the balance between technological efficiency and legal certainty, the preservation of due process rights, and the maintenance of democratic accountability in regulatory enforcement.

Accordingly, the contributions to this special issue reflect the multifaceted nature of enforcement and compliance technologies, spanning from environmental regulation to digital market governance, from supply chain transparency to decentralised enforcement mechanisms.

Each article addresses different aspects of how technology can enhance regulatory compliance while grappling with the inherent tensions between innovation and legal stability.

The issue opens with Benjamin Amram, Yehuda Leibler, Romi Listenberg, and Dov Greenbaum's examination of compliance and ethical challenges in carbon trading, defending how technology can strengthen global frameworks for market integrity and sustainability. This contribution illustrates the critical role that digital tools play in environmental governance, where traditional enforcement mechanisms often struggle with the scale and complexity of global carbon markets. Then, Gianluca Sisto's contribution on blockchain applications in agrifood supply chains provides a compelling case study of how distributed ledger technology can achieve sustainability and traceability objectives under the UN 2030 Agenda. This work exemplifies the potential of blockchain technology to create immutable records of supply chain activities, enabling more effective enforcement of food safety regulations and environmental standards.

The third contribution encompasses a legal analysis by Gianfranco Alfano and Ludovica Vairo, focused on digital tools and their role in ensuring compliance with the Digital Markets Act (DMA), drawing from gatekeepers' reports to provide practical insights into regulatory implementation. As major technology companies are adapting their practices to comply with new digital market regulations, both technological and conventional approaches are to be integrated to achieve effective compliance. Alessandro Piovano, Cristina Poncibò, and Carlo Federico Vescovo examine the effective enforcement of the DSA's provisions, addressing one of the most significant challenges in contemporary digital regulation. Their analysis explores how enforcement mechanisms can be designed to address the unique characteristics of digital services while maintaining proportionality and effectiveness across different market contexts. Following, contribution by Balázs Bodó and Stefanie Boss presents a fascinating case study of decentralised law enforcement through Ethereum's proof of stake mechanism for moderation practices. This analysis explores how blockchain-based governance systems can serve as models for regulatory enforcement, offering insights into how decentralised technologies might reshape traditional approaches to legal compliance and enforcement, raising relevant questions about the relationship between technological governance and non-state-based regulatory systems.

Finally, Valeria Comegna's examination of AI and blockchain integration for transparent and secure regulatory compliance and enforcement cooperation addresses the convergence of multiple emerging technologies. This contribution explores how the combination of artificial intelligence and blockchain technology can create more robust and transparent enforcement mechanisms, while addressing the challenges of ensuring accountability and preventing technological lock-in in regulatory systems.

The contributions presented in the issue collectively demonstrate that enforcement and compliance technologies should not be understood as mere procedural tools but,

rather, as strategic and structural components of evolving regulatory architectures, highlighting the need for legal frameworks that can accommodate technological innovation while preserving core principles of rule of law, democratic accountability, and individual rights protection.

Looking forward, the variety and relevance of the different contributions presented exemplifies how the intersection of compliance and enforcement technologies with fundamental legal principles constitutes – and will be even more, in the future – a pivotal standpoint for scholarly attention and policy development. In such sense, the articles in this issue provide valuable insights into both the opportunities and challenges that lie ahead, offering a foundation for future research and policy development in this rapidly evolving field.

The editors believe that this collection of contributions will serve as a valuable resource for scholars, policymakers, and practitioners seeking to understand the complex dynamics of technological enforcement and compliance in contemporary legal systems. As digital technologies continue to transform the landscape of regulatory governance, the insights provided by these authors will be relevant for addressing the ongoing challenges of maintaining effective, fair, and accountable enforcement mechanisms in an increasingly digital world.

R.d.C., A.D., C.P.

Gian Marco Solas *

INNOVATION LETTER

INTERRELATION OF HUMAN LAWS AND LAWS OF NATURE? CODIFICATION OF SUSTAINABLE LEGAL SYSTEMS

'It is mathematically impossible to build a just world without measuring and representing human laws like the other laws of nature'

Abstract

The aim of this Innovation Letter is to raise the problem of the interrelation between human laws and the laws of nature and to propose the codification of sustainable legal systems to measure and potentially foster human progress in universal mathematical terms. It does this initially by providing a brief theoretical and mathematical introduction about key legal and physics-based frameworks, as a way to begin their unification. Followed by outlining simple applications for the codification of sustainable legal systems, with a view to calculate the unexpressed value of legal systems and to potentially optimise it with a public-private Intitial Public Offering (hereinafter IPO)-type of process powered by modern technologies.

JEL CLASSIFICATION: A10, B10, B15, B40, B50, C00, C02, C32, C60, C71, C80, D30, D41, F00, K40, N01, 010, O30, P11, Q01, Q40, R00

SUMMARY

* Italian / EU qualified lawyer. Leading Expert at BRICS Competition Law & Policy Centre (Higher School of Economics, Moscow). Ph.D.[2] (Maastricht Law School, Economic Analysis of Law; University of Cagliari, Comparative Law) – LL.M. (College of Europe, EU Law). Over ten years' experience in global litigation funds, national and international law firms and at the EU Commission. Private investor in and inventor of algorithm 1love.works© and related legal technology (phenography©, phenocurrency©, fractal cross-pollination©) for the codification of sustainable legal systems.

The Author could not have done this research without the grace of the Lord and of the Virgin Mary, and without the patience and support from his parents Antioco and Lorena. To them go the most heartfelt thanks and life devotion through work. The Author also wishes to thank his previous supervisors prof. Aldo Berlinguer and prof. Michael Faure for encouraging this research, and the colleagues at the BRICS Competition Law & Policy Center for freedom of research and support, all of them and particularly Alexey Ivanov, Nicolo' Zingales and Ettore Lombardi. Heartfelt thanks also to Gianluca Pittoni, physicist and mayor of Masainas, for the availability and warm welcome, and to the Opus Dei for spiritual support.

DOI 10.13135/2785-7867/12266

1 Introduction

The idea that there is an interrelation between human laws and the laws of nature is as old as human society, often recurred in history, and particularly in crucial moments for the development of science and legal orders.[1] The problem has again gained traction in the last decades and in different spheres of human knowledge, the questions are many but can in fact be summarised by the philosophical problem as to whether human laws "fit" or "contrast" the laws of nature or otherwise whether and how the latter can be used to measure – and potentially build "more just" - legal systems. The first part of the problem is mainly legal in nature: can we, for instance, defy gravity or thermodynamics by contract or international treaty? Or what is the hierarchical relationship between human laws and the laws of physics? The questions appear pivotal as - in a moment of high uncertainty and the crumbling of international law - universal mathematical laws provide objective criteria for resolution of conflicts and to potentially support the (re)construction of legal orders. The second part of the problem also has an economic and technological nuance. It relates to the potential engineering of sustainable legal systems where fundamental rights enshrined in the United Nations Sustainable Development Goals (UN SDGs) would be effectively implemented. On this basis, the Innovation Letter proposes the codification of sustainable legal systems to both raise and potentially tackle the said problem(s). To do so, paragraph 2 briefly reports on the main and most recent legal and physics-based theoretical frameworks, as well as on their interrelation, also in simple mathematical terms. Paragraph 3 proposes a basic model for the codification of sustainable legal systems to test such interrelation with modern technologies, to measure, and potentially foster human progress in universal mathematical terms. It concludes that such an approach may bring at least one socio-economic improvement, ie the calculation of unexpressed real economic value and on this basis, prompt for legal system optimisation with a public-private IPO-type of process powered by modern technologies.

[1] There is evidence that the concept has been studied by Socrates, Plato and pre-Socratics, but also in previous civilisations, for instance on Eastern, African and Indian philosophy, although evidence is limited by the availability of material records. In Ancient Rome, Seneca discussed natural law in relation to meteorology in *Naturales Quaestiones*. This work is about taking 'measure of God' (1.17), to 'walk through the universe' (*mundum circuire*; 3.1), to celebrate the works of the Gods (3.5), and to free us from fear induced by natural events (6.4). See Seneca, in Edward N Zalta and Uri Nodelman (eds), *Stanford Encyclopedia of Philosophy* (Stanford 2007), <https://plato.stanford.edu/entries/seneca/#PhyThe> accessed 19 May 25. Other authors who have discussed the problem are, for instance, Hobbes and Locke. The first, in his famous *Leviathan* of 1651, starting from a mechanistic understanding of human beings and their passions, wondered what life would be like without government, a condition which he calls the 'state of nature'. In that state, each person would have a right, or license, to do everything to anyone, which would lead to a 'war of all against all' or men to be a 'wolf of other men' (*bellum omnium contra omnes* or *homo homini lupus*). Locke in his Second Treatise of Government of 1689 described property rights as natural rights of the individual, although linked mainly to labour. In France, Montesquieu analysed – in his *Esprit des Lois* of 1748 – the role that geographical conditions have in the shaping of human law. In the United States, the Constitution of 1787 was said to be Newtonian in design, with its carefully crafted 'checks and balances', structured ideally like a 'machine that would go of itself' potentially to meet the crises of the future. See Michael Kammen, '*A Machine That Would Go of Itself: The Constitution in American Culture*' (New York, Alfred A Knopf 1986). See also Laurence Tribe, 'The Idea of the Constitution: A Metaphor-morphosis' (1987) 3(2) Journal of Legal Education 170.

2 Interrelation between human laws and the laws of nature?

Several recent contributions in both the domains of law and physics have discussed the idea that there is an interrelation between human laws and the laws of nature. One of the first modern papers addressing the topic directly is Professor Tribe's, edited by the young future President Obama, on the 'curvature of the constitutional space'[2]. The paper is an interesting attempt to reflect on how legal decisions, in particular judicial ones, can be explained by physics, namely with Einstein's theory of general relativity and the space-time curvature. A more robust attempt was made more recently by Professor Bin[3], who recalls that most continental European orders are influenced by the Kelsenian Pure Theory of Law, central to which there is the notion of a 'basic norm (*Grundnorm*)' - a hypothetical general and abstract norm, presupposed by the theory. From this norm - in a hierarchy of empowerments - all 'lower' norms in a legal system, from constitutional law downward, are understood to derive their validity, hence their authority or binding effect. The Pure Theory is intended as rigorous legal positivism, so that 'legal science' for Kelsen is to be separated from legal politics, must be developed as an autonomous discipline, seemingly supporting a 'Newtonian view of the law', and as something ontologically separated from the rest. Bin concludes that this view must be surpassed as the law cannot be detached from its authors and interpreters, like judges, who not only interpret but also confer validity to the law. This perspective somehow mirrors the debate in physics where, for Einstein, in understanding physical reality the "background" cannot be abstracted from the "foreground": "when a body moves, or a force acts, it affects the curvature of space and time -- and in turn the structure of space-time affects the way in which bodies move and forces act"[4]. From this angle, the point raised appears to be particularly interesting because today's physics seems to be divided between theories 'of the very big… and the theory of the very small... The problem is that they stand in conflict with each other. They are based on two different principles, two different mathematics, and two different philosophies'[5].

Can the interrelation of human law and the laws of nature allow to unify the main theoretical frameworks and, if yes, what are the implications and socio-economic improvements? To test this assumption, let us first recall Newton's famous formula,

$$F = MA \qquad [1]$$

Whereby the force (F) applied to a body equals the mass (M) multiplied by the acceleration (A). Let us take a case where Mark is driving his car and comes to a stoplight

[2] Laurence H Tribe, 'The Curvature of Constitutional Space: What Lawyers Can Learn from Modern Physics' (1989) 103 Harvard Law Review 1.
[3] Roberto Bin, '*A discrezione del Giudice, Ordine e Disordine, una prospettiva quantistica*' (Franco Angeli 2013).
[4] Stephen Hawking, *'A Brief History of Time: From the Big Bang to Black Holes'* (Bantam Press 1988) 29, 33.
[5] Michio Kaku, *'The God Equation. The Quest for a Theory of Everything'* (New York, Doubleday 2021).

of the legal system X signalling red. In such a case, the law ('λ')[6] of X expressed in the stoplight stops the motion of the mass 'Mark+car'. The equation describing the case can be written as follows:

$$\overrightarrow{MA} = \overleftarrow{F\lambda_X} \qquad [2]$$

where the arrow signals a vectorial force indicating the direction of the legal force and of the mass in acceleration. Let us now represent the red $\overleftarrow{F\lambda_X}$ or the green $\overrightarrow{F\lambda_X}$ at the stoplight, using a typical Cartesian graph for simplification, to show how the municipal law expressed in the stoplight curves the velocity of the car in the real-world space-time to maintain order in X.

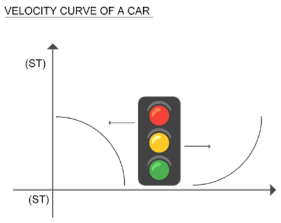


Figure 1

This simple example allows consideration of the idea that legal systems can be treated as complex systems, recently explored, for instance, in *The Physics of the Law*[7] or in *The Ecology of Law*[8] and many others, and that human law is also a law of nature. On applicative and experimental levels, it could allow, for instance, the measurement of legal pressure, weight, friction or inertia, or its thermodynamic effects in specific cases and via evolutionary and cause-effect pathways, as well as its quantum dimension. That is of interest from both a legal and economic perspective. In a recent publication it was proposed using the interdisciplinary methodology to measure markets with a view to fostering global competition litigation[9]. Faced with a practical obstacle that a market could not be calculated with the traditional tools of economics, the article adopted some concepts from history and physics – namely from fluid mechanics and thermodynamics - to better understand its state, limits, and potential for innovation. It suggested that such an approach could help practitioners and authorities improve decision-making, with possible improvements for legal systems in terms of competitiveness and potential optimisation. Such considerations prompt reflection as to whether and to what extent it

[6] λ was first used as a probabilistic factor to evaluate risk of legal claims in Gian Marco Solas, *'Third Party Funding. Law, Economics & Policy'* (Cambridge University Press 2019) Chapter 5.

[7] Pierpaolo Vivo, Daniel Martin Katz and JB Ruhl (eds), *'The Physics of the Law: Legal Systems Through the Prism of Complexity Science'* (Lausanne, Frontiers Media SA 2022).

[8] Fritjof Capra, Ugo Mattei, *'The Ecology of Law: Toward a legal system in tune with nature and community'* (Berrett-Koehler Publishers 2015).

[9] Gian Marco Solas, 'Third Party Funding, new technologies and interdisciplinary methodology in global competition litigation' (2025) 1 Global Competition Litigation Review 17.

is possible to measure human laws like other laws of nature and potentially "engineer more just legal systems" relying on the said interrelation, for instance, using modern technologies for a contemporary codification of legal systems.

3 Codification of sustainable legal systems

Codifications are widely experimented legal processes to reorganise human law and legal systems following the periods of socio-economic turmoil. Examples of codifications are the Constitution of Solon[10], the Iustinianus codification[11], the Napoleonic codification(s)[12], the EU Treaties[13] and all the Charters on human rights or the constitutions[14]. Codifications of the law have occurred in most of the legal systems worldwide, the civil law jurisdictions, distinguishing them from those of common law where instead the *stare decisis* jurisprudential rules prevail[15]. To begin testing the said interrelation, let us model codifications in physical terms as progressive "historical cycles" identifying the spatio-temporal positions of each codification and the hypothetical volume (V) of legal (λ) work (W) to shape all the mass (M) and energy (E) in legal systems.

[10] The Solonian constitution was enacted by Solon in the early 6th century BC in Ancient Greece. At the time of Solon, the Athenian State was almost falling to pieces in consequence of dissensions between the parties into which the population was divided. He promulgated a code of laws embracing the whole of public and private life to revise or abolish the older laws of Draco. Under these reforms, all debts were abolished and debt-slaves freed. He reduced the power of aristocracy and citizens were divided based on their land production.

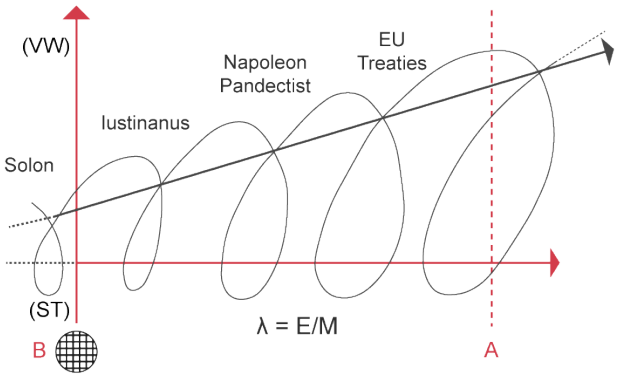
[11] The *Corpus Juris Civilis* ('Body of Civil Law'), which is the modern name for a collection of fundamental works in jurisprudence, enacted from 529 to 534 by order of Justinian I, Byzantine Emperor, to 'repair' the legal order. The work was planned in three parts: the *Code* (*Codex*) is a compilation of imperial enactments; the *Digest* or *Pandects* is an encyclopedia composed of mostly brief extracts from the writings of Roman jurists; and the *Institutes* (*Institutiones*), a student textbook mainly introducing the *Code*. All three parts, even the textbook, were given force of law. They were intended to be, together, the sole source of law; reference to any other source, including the original texts from which the *Code* and the *Digest* had been taken, was forbidden. Nonetheless, Justinian found himself having to enact further laws and today these are counted as a fourth part of the Corpus, the *Novellae Constitutiones* (*Novels*, literally *New Laws*).

[12] The Napoleonic Code (In French, *Code Napoléon* or *Code civil des Français*, normally referred to as *Code civil*) is the French civil code entered into force during the French Consulate, on 21 March 1804 and still in force, although frequently amended, as way to create a clear rational legal order after the tumult of the French revolution. The code, with its stress on clearly written and accessible law, was also a major step in replacing the previous disordered patchwork of feudal laws. It is regarded as one of the few documents that have influenced the whole world, working as model for most civil law jurisdictions.

[13] Among the many, it is worth recalling the Treaty of Paris (1951) establishing the European Coal and Steal Community, or the Treaty of Rome (1957) establishing the EU internal market.

[14] Amongst many of these, it is worth recalling the Universal Declaration of Human Rights adopted by the UN in 1948 and the EU Charter of Fundamental Rights entered into force in 2009.

[15] Ugo Mattei and Luca Pes, 'Civil Law and Common Law: Toward Convergence?' in Gregory Caldeira, Daniel Kelemen and Keith Whittington (eds), *The Oxford Handbook of Law and Politics* (online edition, 2008; Oxford Academic 2009).



PATTERN OF CODIFICATIONS OF THE LAW IN CIVIL LAW JURISDICTIONS (NON EXHAUSTIVE).

Figure 2

Let us take the model and pattern for simplicity as a relatively objective way of describing the history and progress of legal systems. We acknowledge that in each codification the technology available allowed larger and larger access to legal systems and the economy: from wax tablets to papyrus to mass printed civil codes and computer coded legal texts. To explain the application of the model we recall the famous formula of Einstein's special theory of relativity

$$E = MC^2 \qquad [3]$$

where 'E' is energy, 'M' is the mass and 'C^2' the universal mathematical constant representing the speed of light squared as the ratio between all E and M in the universe. Let us recall the above legal factor λ. Interestingly enough, λ is also present in Einstein's theory of general relativity as the cosmological constant, then used to explain the expansion of the universe, as well as to represent wavelengths. We shall consider how it could serve the "expansion of our universe" with an experimental process of codification. That means to write the existing law in code with modern technologies with a view to measure and represent it like other laws of nature, and to potentially engineer and build ordered and sustainable legal systems. In this experiment, we use the law as light, as the beacon of science, as a tool to understand what we cannot, can or must do in specific legal frames of reference, based on applicable law and including the UN SDGs as a universal benchmark for sustainability. We express this assumption in the following equation

$$\lambda = C^2 \qquad [4]$$

Now assume cutting a section of the spiral in Figure 2 (dotted line A), we will obtain section (B) representing hypothetically the global legal system(s). Let us take a fraction of it, a simple city, which we call again X, a system that would look like Figure 3 and that we can model for simplicity and transferability like in figure 4.

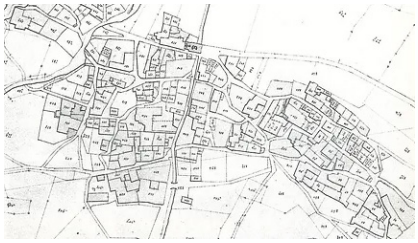


Figure 3

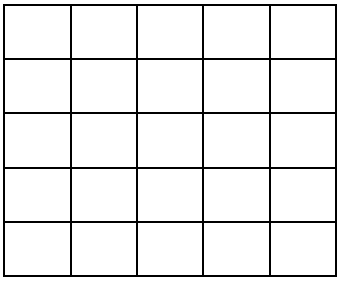


Figure 4

We assign individuals and assets of X a colour depending on the *lato sensu* biological and physical situation, like the stoplight in Figure 1 above:

- We identify in green every legal fraction (asset) of X or individual that are in 'optimal state' according to the applicable law and UN SDGs, the 'active life' or 'energy' of the system. That means for instance a private house or a public building well maintained, a business doing well, or an individual being healthy, in relatively good conditions, working or studying etc.;
- in yellow we identify those situations that are 'so-so', 'inertial', those that need some work or attention: it could be a private or a public building not well maintained but still performing a function (like a house guesting people), a business surviving but not thriving or an individual living through difficult conditions. In other words, those that raise some sustainability issues and that are slowly degrading unless taken care of;
- in red we measure those situations that are chaotic or abandoned, the "entropy", the "end cycle" or "waste", like a totally abandoned building or land plot, a bankrupted business, criminal or homeless individuals, etc.[16]; situations that normally require resolving disputes or otherwise entail legal complexity and that clearly raise sustainability issues and public policy concerns.
-

Figure 5

[16] Nicholas Georgescu-Roegen, *The Entropy Law and the Economic Process* (Harvard University Press, Cambridge 1971).

In this measurement, we obviously include standard economic markers such as consumption and production, as well as strengths of X, like outstanding natural, cultural or historical resources or agricultural or manufacture productions and such. Anything that makes the system unique and "attractive", that has "gravitational-like effects". On this basis, recalling [3] and [4], we propose the following equation for the codification of any legal system (town, municipality, or aggregations thereof, like provinces, regions, states etc).

$$\lambda_X = \frac{E_X}{M_X} \qquad [5]$$

which suggests using the applicable law and the UN SDGs as "rules of the game", to measure the unexpressed mass, the 'entropy', to then transform it into 'new energy' or 'life' for the system via smart contracts, legal claims and administrative decisions. The codification as such allows to then design and measure competitive legal processes, with a view to potentially expressing the full potential and to reach an ideal relativistic equilibrium as in the following figures.

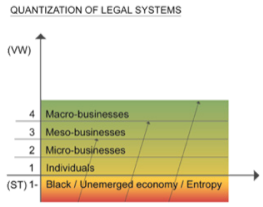


Figure 6

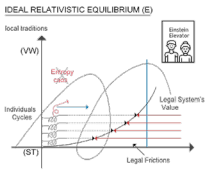


Figure 7

Figure 8

The model in Figure 4 suggests the "quantisation of legal systems". While it is not the purpose of this paragraph to discuss quantum physics, it is important to recall some of its concepts to explain its application to a legal system. One is "quantum entanglement", the phenomenon of a group of particles being generated, interacting, or sharing spatial proximity in such a way that the quantum state of each particle of the group cannot be described independently of the state of the others[17]. The other interesting concept is the "quantum jump", the transition of a system from one energy level to another[18]. In quantum physics, when the system absorbs energy, there is a transition to a higher energy level; when the system loses energy, there is a transition to a lower energy level. For the codification, we use model 4 to first approximately classify entangled mass and energy as above. Then, recalling the idea that money can be considered as energy[19], to fund the

[17] Yunpeng Tao, 'Quantum entanglement: Principles and research progress in quantum information processing' (2024) 30 Theoretical and Natural Science 1, 263-274.

[18] Mazen Khoder, 'A Concept of Universal Quantum Jump' (2020) 44 (LXX) Matematichki Bilten 1, 37-51.

[19] Sergey Rashkovskiy, 'Economic Thermodynamics' [2022] ARxIV <https://arxiv.org/abs/2106.08964> accessed 15 June 2025; Sergey Rashkovskiy, 'Thermodynamics of Markets' [2021] ARxIV <https://arxiv.org/abs/2010.10260> accessed 15 June 2025.

effort to reach the ideal equilibrium projected by every system, systematising life and work cycles according to empirical measurements and the applicable law like in figure 5 and 6. The models will not be explained further at this stage but rather proposed as analogical or even just metaphorical tools to test the said interrelation in specific legal systems, while continuing their conceptual and mathematical development for future publications[20].

4 Conclusions

This Innovation Letter aimed at raising the problem of interrelation between human laws and the laws of nature, namely with a brief report of the main legal and physics-based theoretical frameworks and with some simple examples and mathematical equations. To test the improvements of such an interrelation, it proposed the codification of sustainable legal systems to measure and potentially foster legal systems' progress in universal and mathematical terms. That means, in practice, once the unexpressed or abandoned mass ("entropy") is measured in specific systems, to put in place an IPO-type of process for legal systems, entailing the tokenisation of assets for fundraising and governance of codified legal systems; as well as the usage of empirical data powered artificial intelligence machine learning, predictive, generative tools for markets to emerge, and to enforce the law.

Sample of a real case study analysed, Masainas, a small town of roughly 1,000 inhabitants by the sea in Sardinia famous for its artichokes

The calculation of unexpressed "entropic" mass reveals assets or potential like on the left of the column below in Figure 7, that need capital to be built and/or started as per column right. The potential for 10 businesses in agriculture, manufacturing and services related to the artichoke value chain of Figure 9 below, and energy production calculated with AI tools based on the strengths of X, as well as on (part of) the production that could be internalised based on consumption. The hypothetical tokenisation of the assets would allow for regulating ownership, usage and/or governance according to the applicable law, like in the example of Figure 8 below, as well as to "gamify" legal systems and provide transparency and certainty about economic and legal data. N.B.: the calculation is approximate and subject to further empirical analysis. The token distribution and governance proposal are hypothetical and subject to agreement by concerned parties.

[20] The problem will be treated in a forthcoming essay, G M Solas, "De Lege et Amore – Theory of Interrelation & Sustainability", as well as in other publications.

ASSETS / POTENTIAL	***CAPITAL NEEDED***
10 businesses in the artichoke value chain	*2,000,000 EUR*
100 buildings or land units	*30,000,000 EUR*
2 energy plants	*2,000,000 EUR*
Legal costs	*1,000,000 EUR*
Total	***35,000,000 EUR***
Total token	***100,000 x 350 EUR***
Token: *rights to products from companies; property or use of buildings; energy; or dividends from sale*	

Figure 9

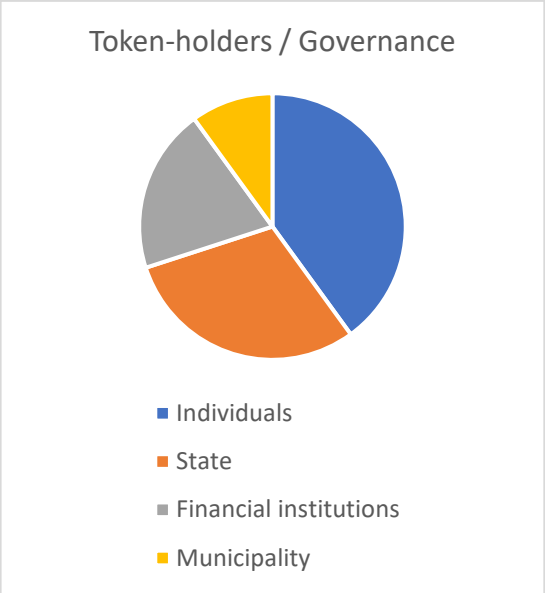


Figure 10

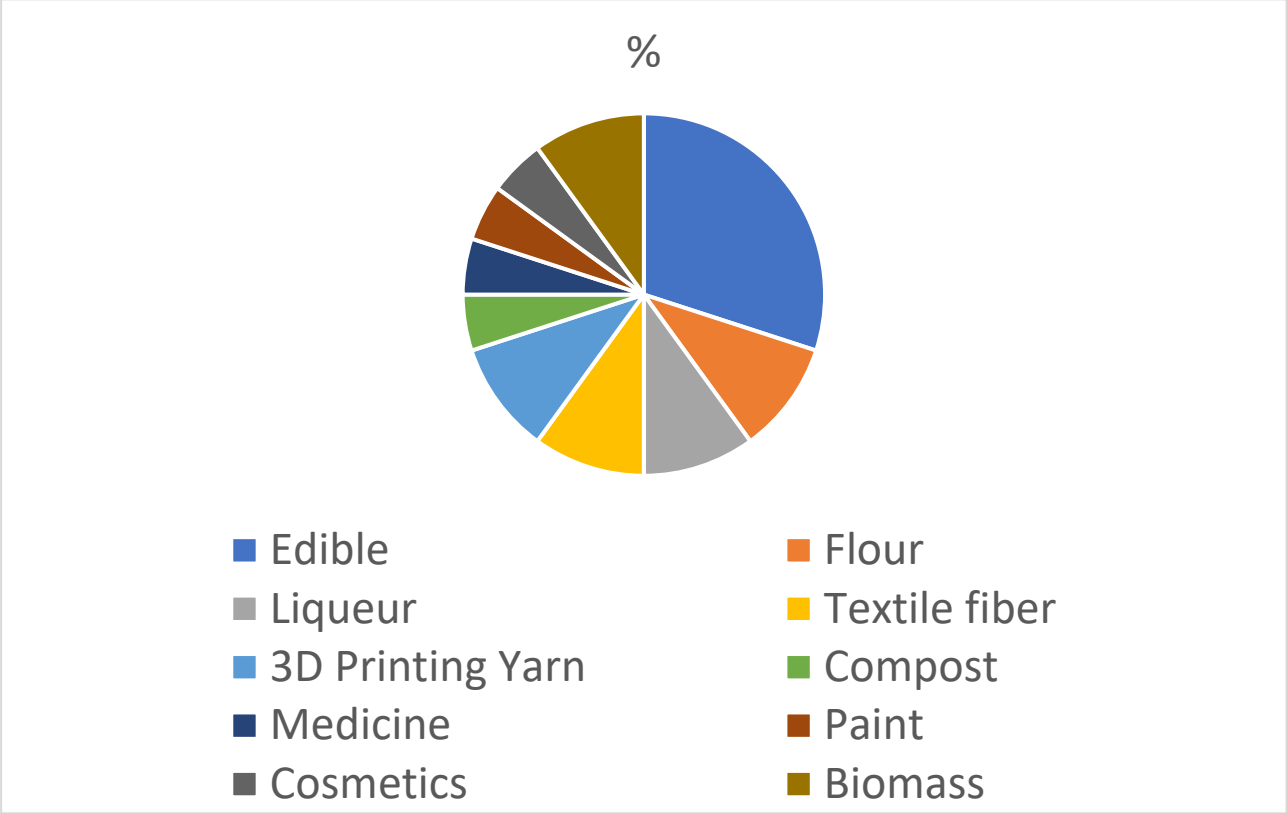

%
Edible
Flour
Liqueur
Textile fiber
3D Printing Yarn
Compost
Medicine
Paint
Cosmetics
Biomass

Figure 11

Benjamin Amram, Yehuda Leibler, Romi Listenberg, and Dov Greenbaum[*]

SPECIAL SECTION

NAVIGATING COMPLIANCE AND ETHICAL CHALLENGES IN CARBON TRADING: STRENGTHENING GLOBAL FRAMEWORKS FOR MARKET INTEGRITY AND SUSTAINABILITY

Abstract

Anthropogenic climate change represents an unprecedented existential threat to global ecological systems and human civilisation, necessitating urgent and comprehensive mitigation strategies. This paper provides a critical analysis of specific regulatory, verification, and ethical challenges that currently undermine carbon trading markets as useful climate change mitigation mechanisms. We argue that current implementations of carbon trading systems largely fail to mitigate climate change. They often create the illusion of progress. Our examination focuses on documented issues in existing markets: regulatory inconsistencies that create enforcement gaps, verification deficiencies that compromise credit integrity, and persistent questions about additionality and double-counting. We identify how these structural flaws create problematic incentives that may discourage actual emissions reductions while enabling lower-quality credits to proliferate. The analysis further addresses the ethical dimension of carbon markets, documenting how the burden of emissions mitigation falls disproportionately on developing countries, particularly in the Global South, despite their historically minimal contributions to global emissions. We examine specific documented cases where political misalignment, energy injustices, and the prioritisation of carbon sequestration over development have undermined both climate goals and sustainable development. The paper concludes by evaluating how emerging technologies and governance approaches could potentially address these documented challenges, while acknowledging the limitations of technological solutions absent broader structural reforms.

JEL CLASSIFICATION: K32, Q54, O31

[*] Benjamin Amram - Zvi Meitar Institute for Legal Implications of Emerging Technologies, Reichman University; Yehuda Leibler - Zvi Meitar Institute for Legal Implications of Emerging Technologies, Reichman University; Romi Listenberg - Zvi Meitar Institute for Legal Implications of Emerging Technologies, Reichman University; Dov Greenbaum - Harry Radzyner School of Law Reichman University, Dina Recanati School of Medicine Reichman University, Zvi Meitar Institute for Legal Implications of Emerging Technologies, Reichman University; Biomedical Informatics and Data Science, Yale University.

DOI 10.13135/2785-7867/12268

SUMMARY

1 Introduction and Background – 1.1 Introduction – 1.2 Climate Change and Net Zero - 1.3 The Concept of Carbon Credits - 1.4 Types of Carbon Credits – 1.5 The Current Regulatory Landscape - 2 Challenges and Concerns – 2.1 An Incentive Not to Reduce 2.2 Lack of Scalability – 2.3 Incentivising Lower Credit Quality – 2.4 Issues with Supply, Demand and Markets - 3 Compliance Markets Dilemmas: Fraud, Efficacy, Efficiency, & Ethics – 3.1 Greenwashing - 3.2 Additionality - 3.3 Leakage - 3.4 Double counting - 3.5 VAT Fraud and Money Laundering - 3.6 Ethical Concerns and the Global South - 4. Emerging Trends and Technologies - 4.1 Technological Innovation in Service of Monitoring - 4.2 Blockchain and Distributed Ledger Technologies - 4.3 21st Century Carbon Markets: Transparency, Efficacy, & Effectiveness - 4.4 Reconceptualising Carbon Assets and Liabilities - 4.5 Networked Market Architectures - 4.6 Implementation and Technical Challenges - 4.7 Policy Recommendations for Carbon Market Reform - 4.8 Addressing potential counterarguments - 5 Conclusions and future outlook

1 Introduction and background

1.1 Introduction

Carbon trading markets suffer from at least three critical structural flaws that significantly compromise their effectiveness as climate change mitigation mechanisms. Although market-based instruments have theoretical promise and have proliferated globally, they largely fail to deliver meaningful emissions reductions due to serious design deficiencies that require substantial reform. We argue that carbon markets are not inherently doomed to failure, but their current implementations reflect fundamental shortcomings that must be addressed through coordinated regulatory, technological, and ethical interventions. This paper provides a critical analysis of these interconnected challenges—misaligned incentive structures, verification deficiencies, and equity concerns—examining how they undermine both environmental outcomes and social justice. Moreover, the disproportionate policy focus on carbon market solutions represents significant opportunity costs. This diverts attention and resources from more direct and proven emissions reduction strategies such as regulatory standards, public infrastructure investment, and fundamental economic transformation.

Rather than abandoning market mechanisms entirely, we propose that comprehensive reforms across regulatory harmonisation, technological integration, and ethical reorientation could potentially transform these markets from potentially exploitative financial instruments into more effective tools for climate mitigation. The urgency of the climate crisis demands that we either fundamentally redesign carbon trading systems to eliminate their structural contradictions or significantly diminish their role in our collective climate response.

This paper analyses these interconnected challenges through an interdisciplinary lens that integrates legal, economic, and ethical perspectives. By examining documented cases of market dysfunction across varied jurisdictions, we demonstrate how these problems

are not merely implementation difficulties but fundamental design flaws requiring structural reform.

We evaluate how emerging technologies, particularly distributed ledger systems like blockchain, might address transparency and verification challenges, while also acknowledging the limitations of technological solutions absent broader governance reforms. Our analysis reveals that effective carbon market reform requires coordinated intervention in at least three domains: regulatory harmonisation, technological integration, and ethical reorientation. By identifying specific pathways toward more transparent, effective, and equitable carbon trading mechanisms, this paper contributes to the urgent project of transforming these markets from structurally flawed market instruments into genuine tools for climate justice and environmental protection.

This paper adopts an interdisciplinary approach integrating legal analysis, economic literature, and ethical frameworks to examine structural flaws in global carbon trading markets. Drawing on case studies and documented examples from the European Union, United States, and voluntary markets in the Global South, we explore how carbon markets function not just as regulatory instruments but as emergent financial ecosystems marked by verification failures, regulatory fragmentation, and structural inequities. Our methodology employs documentary analysis, collecting evidence from regulatory frameworks, market implementation studies, and ethical impact assessments to systematically evaluate carbon trading across jurisdictional, operational, and ethical dimensions.

The analysis proceeds across three key dimensions: First, we establish the conceptual foundations of carbon credits, exploring their types and regulatory frameworks. Second, we identify critical market challenges including misaligned incentives that discourage actual emissions reductions, limited scalability, quality issues, governance gaps enabling market manipulation, and verification problems (examining additionality failures, leakage effects, and measurement inconsistencies through published case studies). Third, we evaluate both compliance dilemmas (greenwashing, verification failures) and ethical concerns regarding the disproportionate burden placed on developing nations, using an environmental justice framework to assess the implications of carbon offset projects in these regions. While emerging technologies such as digital Monitoring, Reporting, and Verification (MRV) systems, AI-powered verification, and distributed ledger technologies offer promising solutions, we argue that technical innovations alone are insufficient without parallel reforms in regulatory design and ethical accountability. The paper concludes with policy recommendations for transforming carbon markets into more transparent, effective, and equitable climate mitigation mechanisms, emphasising that market legitimacy and effectiveness require aligning market mechanisms with transparent verification, equitable burden-sharing, and enforceable legal standards.

1.2 Climate change and net zero

Climate change has become a pressing threat to the international community. Between 1880 and 1981, Earth's temperature rose by 0.08°C per decade; the pace of this increase accelerated to 0.18°C per decade in the 1980s.[1] Carbon credits, a form of tradable certificates that give entities a right to emit a preset amount of greenhouse gas (GHG), have emerged as potential solutions for addressing the emissions problem that has led in part to the temperature rise.[2] The popularity of these assets as a substitute for actual carbon reduction continues to increase dramatically.

Today, almost 200 nations have agreed to reduce their greenhouse gas emissions, aiming for zero emissions by 2050.[3] Furthermore, the number of companies with zero-emission pledges has increased from 500 to 1,000 during the period between 2019 and 2020.[4] However, the achievement of these ambitious goals remains a daunting task. Some emissions, such as those involving chemical reactions in the cement sector, cannot be completely eradicated.[5] Consequently, carbon credits have become an attractive strategy for offsetting emissions by funding sustainability projects.

1.3 The concept of carbon credits

Carbon markets attempt to correct market failures by pricing negative externalities associated with greenhouse gas emissions, but structural design flaws often undermine this theoretical promise.[6] By introducing a cap-and-trade mechanism—where regulators set an overall emissions limit (cap) and allow companies to buy and sell emission allowances (trade)—they create scarcity in emissions rights, thereby enabling market-based price discovery for carbon. Empirical studies have affirmed that emissions trading systems (ETSs), such as the EU ETS, function efficiently by allowing emitters to reallocate abatement efforts based on marginal cost differentials, reducing compliance costs while maintaining environmental targets.[7] Carbon allowances exhibit variable but often high tradability and liquidity—characteristics typically associated with mature commodity

[1] Rebecca Lindsey and Luann Dahlman, 'Climate Change: Global Temperature' (*Climate.gov*, 18 January 2023) <http://www.climate.gov/news-features/understanding-climate/climate-change-global-temperature> accessed 15 November 2024.
[2] Justin D Macinante, *Effective Global Carbon Markets: Networked Emissions Trading Using Disruptive Technology* (Edward Elgar Publishing 2020).
[3] ibid.
[4] Geoff Bertram and Simon Terry, *The Carbon Challenge: New Zealand's Emissions Trading Scheme* (Bridget Williams Books 2021).
[5] Christopher Blaufelder, Charlotte Levy, Patrick Mannion, and Dickon Pinner, *A Blueprint for Scaling Voluntary Carbon Markets to Meet the Climate Challenge* (McKinsey Report 2021). <https://www.mckinsey.com/capabilities/sustainability/our-insights/a-blueprint-for-scaling-voluntary-carbon-markets-to-meet-the-climate-challenge> accessed 21 January 2025.
[6] Qingyang Wu, Siyu Ren, Yao Hou, Zaoli Yang, Congyu Zhao, and Xusheng Yao, 'Easing financial constraints through carbon trading' (2024) 67 Empirical Economics 655.
[7] Denny A Ellerman, Frank J Convery, and Christian De Perthuis, *Pricing carbon: the European Union emissions trading scheme* (Cambridge university press 2010); Lawrence H Goulder and Andrew Schein, "Carbon taxes vs. cap and trade: A critical review" [2013] NBER Working paper 19338.

markets—despite their regulatory origin.[8] In fact, trading volumes and market depth in the EU ETS rival those in traditional commodities like natural gas or electricity, reinforcing the argument that carbon credits constitute a "real" market.[9] And, like other commodities, carbon prices reflect supply-demand dynamics, but with added policy-driven volatility.[10] Nevertheless, price signals from carbon markets have demonstrably influenced investment in low-carbon technologies,[11] highlighting their function as instruments of both cost efficiency and long-term decarbonisation.[12]

The idea behind carbon trading can be traced back to the Kyoto Protocol, which established the national quotas for emitting carbon dioxide for each of the signatories.[13] The Kyoto Protocol imposes binding emission reduction obligations exclusively on Annex I Parties, with each assigned a quantified emissions limitation and reduction objective (QELRO) under Annex B. These legally binding commitments were enforced through a compliance mechanism including potential penalties for non-compliance, establishing Kyoto as a top-down legal instrument grounded in international treaty law.[14]

In contrast, the Paris Agreement's Article 6 establishes voluntary cooperative mechanisms: Article 6.2 facilitates bilateral transfers of mitigation outcomes (ITMOs), while Article 6.4 introduces a centralised crediting mechanism governed by the United Nations Framework Convention on Climate Change (UNFCCC); neither imposes mandatory participation or reduction targets. The legal obligation under Article 6 arises only upon a Party's decision to use these mechanisms, at which point it must adhere to the procedural rules agreed in the Article 6 rulebook.[15] This reflects a shift from the top-down compliance model of Kyoto to the bottom-up, facilitative architecture of Paris. Accordingly, references to carbon market "obligations" under Paris must distinguish between treaty-

[8] Boquiang Lin and Chenchen Huang, 'Analysis of emission reduction effects of carbon trading: Market mechanism or government intervention?' (2022) 33 Sustainable Production and Consumption 28, 37; Idris A Adediran and Raymond Swaray, 'Carbon trading amidst global uncertainty: The role of policy and geopolitical uncertainty' (2023) 123 Economic Modelling 1.

[9] Ralf Martin Mirabelle Muuls, Laure B de Preux and Ulrich J Wagner, 'Industry compensation under relocation risk: A firm-level analysis of the EU emissions trading scheme' (2014) 104 (8) American Economic Review 2482.

[10] Lin and Huang (n 8); Adediran and Swaray (n 8).

[11] Qianqian Hong, Linhao Cui and Penghui Hong, 'The impact of carbon emissions trading on energy efficiency: Evidence from quasi-experiment in China's carbon emissions trading pilot' (2022) 110(C) Energy Economics 106025; Wei Zhang, Guoxiang Li, and Fanyong Guo, 'Does carbon emissions trading promote green technology innovation in China?' (2022) 315 Applied Energy 1.

[12] Dazhi Linghu, Xinli Wu, Kee-Hung Lai, Fei Ye, Ajay Kumar, and Kim Hua Tan, 'Implementation strategy and emission reduction effectiveness of carbon cap-and-trade in heterogeneous enterprises' (2022) 248 International Journal of Production Economics 1.

[13] Jorge Gonçalves and Manuel Luís Costa, 'The political influence of ecological economics in the European Union applied to the cap-and-trade policy' (2022) 195 Ecological economics 1; John C Cole, 'Genesis of the CDM: The Original Policymaking Goals of the 1997 Brazilian Proposal and Their Evolution in the Kyoto Protocol Negotiations into the CDM' (2010) 12(1) International Environmental Agreements: Politics, Law and Economics 41.

[14] Daniel Bodansky, 'The History of the Global Climate Change Regime' in Urs Luterbacher and Detlef F Sprinz (eds), *International Relations and Global Climate Change* (MIT Press 2001) 23, 40.

[15] Lavanya Rajamani, Louise Jeffery, Niklas Höhne, Frederic Hans, Alyssa Glass, Gaurav Ganti, and Andreas Geiges, "National 'fair shares' in reducing greenhouse gas emissions within the principled framework of international environmental law" (2021) 21(8) Climate Policy 983, 1004; Michael A Mehling, Gilbert E Metcalf, and Robert N Stavins, 'Linking climate policies to advance global mitigation' (2018) 359(6379) Science 997, 998.

based participation and conditional procedural duties, ensuring legal terminology aligns with the instruments' formal status under international law.

Under Kyoto, countries that exceeded their quotas could buy carbon credits from those with surplus allowances. Over time, this instrument has expanded significantly, with regions like the European Union[16] and 11 US states having adopted the programme.[17]

A decision regarding the implementation of Article 6 of the Paris Agreement at COP26, which gave rise to a crediting mechanism, provided countries with a mechanism for buying voluntary carbon credits as well.[18] In this situation, the market of voluntary credits is expected to display dramatic growth in the near future. Voluntary carbon credits, driven by non-governmental and private organisations, form an increasingly important market due to their financial incentives. In 2020, voluntary carbon credits that were retired accounted for the reported offset of around 95 million tons of carbon dioxide, which indicates a more than 100% increase in comparison with the data from 2017.[19]

Having examined the fundamental principles and historical development of carbon credits, we now turn to the diverse typology of these instruments and how their various forms serve different market functions.

1.4 Types of carbon credits

Carbon credits can be divided into either mandatory or voluntary categories. Voluntary credits depend on particular projects and often involve either avoidance or removal projects. Avoidance projects focus on avoiding GHG emissions via varied efforts such as a large-scale wetland prevention programme or a local initiative aimed at changing diets for beef to reduce methane emissions.[20]

Removal projects seek to capture greenhouse gases and remove them from the atmosphere.[21] Considering that removal projects are believed to have a more significant impact on the environment, their credits are typically traded at a premium.[22]

Voluntary markets are often leveraged as part of broader corporate social responsibility (CSR) strategies, enabling firms to pursue carbon neutrality, enhance brand reputation,

[16] European Commission, 'EU Emissions Trading System (EU ETS)' (September 2022) <https://climate.ec.europa.eu/eu-action/eu-emissions-trading-system-eu-ets_en> accessed 22 October 2024.
[17] Richard Schmalensee and Robert N Stavins, 'The Design of Environmental Markets: What Have We Learned from Experience with Cap and Trade?' (2017) 33(4) Oxford Review of Economic Policy 572.
[18] Lin Chen, Goodluck Msigwa, Mingyu Yang, Ahmed I Osman, Samer Fawzy, David W Rooney, and Pow-Seng Yap, 'Strategies to Achieve a Carbon Neutral Society: A Review', (2022) 20 (4) Environmental Chemistry Letters 2277, 2310.
[19] Chirstopher Blaufelder, Joshua Katz, Cindy Levy, Dickon Pinner, and Jop Weterings, 'How the Voluntary Carbon Market Can Help Address Climate Change' (McKinsey & Company 2020) <https://www.mckinsey.com/capabilities/sustainability/our-insights/how-the-voluntary-carbon-market-can-help-address-climate-change> accessed 19 February 2025.
[20] Michael Wara, 'Is the Global Carbon Market Working?' (2007) 445 Nature 595.
[21] Macinante (n 2).
[22] Blaufelder and others (n 5).

and meet growing consumer expectations for environmentally responsible practices.[23] Moreover, voluntary carbon markets play a critical role in financing climate resilience initiatives, particularly in regions and ecosystems vulnerable to the impacts of climate change.[24]

As described herein, despite their potential, voluntary markets are subject to ongoing scrutiny regarding the credibility and efficacy of carbon offsets in the absence of uniform regulatory oversight. Consequently, ensuring the legitimacy of voluntary carbon credits requires rigorous verification protocols and adherence to recognised standards.[25] Transparency, third-party certification, and long-term monitoring are thus essential to building and sustaining trust in the voluntary carbon market framework.[26]

In contrast, compliance carbon markets, or mandatory markets, are regulatory mechanisms established by governments to enforce greenhouse gas (GHG) emission reductions. These markets are embedded within legal frameworks that impose binding obligations, typically targeting high-emission sectors such as energy, manufacturing, and aviation. The European Union Emissions Trading System (EU ETS)[27] serves as a leading example, operating on a cap-and-trade basis: a fixed emissions cap is set, and companies must hold allowances equivalent to their emissions, either allocated or purchased. Surplus allowances can be traded, creating financial incentives to reduce emissions.

Other significant compliance schemes include California's Cap-and-Trade Program[28] and China's National Emissions Trading Scheme.[29] These systems aim to align industry behaviour with national or regional climate targets through enforceable limits and penalties for non-compliance.

The principal distinction between compliance and voluntary carbon markets lies in regulation. Compliance markets are mandatory for specific sectors, while voluntary markets are driven by corporate sustainability initiatives and offer participants greater flexibility in credit procurement. Cost structures differ as well—compliance markets

[23] Andrea Von Avenarius, Thattekere Settygowda Devaraja, and Rüdiger Kiesel, 'An empirical comparison of carbon credit projects under the clean development mechanism and verified carbon standard' (2018) 6(49) Climate 1; Jianhu Cai and Feiying Jiang, 'Decision models of pricing and carbon emission reduction for low-carbon supply chain under cap-and-trade regulation' (2023) 264 International Journal of Production Economics 1.

[24] Andrei Marcu and Federico Cecchetti, 'The trading of carbon' in M Hafner and G Luciani (eds), *The Palgrave Handbook of International Energy Economics* (Palgrave Macmillan, Cham 2022) 439, 469; Rana Elkahwagy, Vandana Gyanchandani, and Dario Piselli, 'UNFCCC Nationally Determined Contributions: Climate Change and Trade' Working Paper 2017-02 (Center for Trade and Economic Integration 2017).

[25] Kenneth R Richards and Grant Eric Huebner, 'Evaluating protocols and standards for forest carbon-offset programs, Part B: leakage assessment, wood products, validation and verification' (2012) 3(4) Carbon Management 411, 425.

[26] Jianfu Wang, Shiping Jin, Weiguo Bai, Yongliang Li, and Yuhui Jin, 'Comparative analysis of the international carbon verification policies and systems' (2016) 84 Natural Hazards 381, 397.

[27] ibid 16.

[28] California's Cap-and-Trade Program site <https://ww2.arb.ca.gov/our-work/programs/cap-and-trade-program> accessed 20 June 2025.

[29] Progress Report of China's National Carbon Market (2024) <https://www.mee.gov.cn/ywdt/xwfb/202407/W020240722528850763859.pdf> accessed 20 June 2025.

typically involve higher expenses due to legal and administrative requirements, whereas voluntary credits are generally cheaper, though prices vary by project and location.[30]

Compliance markets tend to, albeit, sometimes inefficiently,[31] achieve more substantial environmental outcomes as they are central to binding climate commitments,[32] such as those under the Paris Agreement. They drive systemic change by placing a price on carbon and encouraging innovation in low-emission technologies.[33]

Nonetheless, challenges persist. Carbon pricing in these markets is sensitive to political and economic conditions, affecting market stability.[34] Regulatory complexity can burden companies, and cap-and-trade systems may enable continued emissions if entities can afford to purchase credits, potentially undermining climate objectives.[35]

Another classification groups carbon credit offsets into groups such as nature-based gas sequestration, actual reduction of emissions, technology-based removal of greenhouse gases from the atmosphere, and avoidance of nature loss.[36]

Carbon Credits that are offset by technology-based removal of greenhouse gases and removal of additional emissions have the potential for significant growth in supply over the next decades.[37] Nature-based sequestration and avoiding nature loss projects are also likely to increase dramatically in the near future, but their supply is expected to be concentrated in developed countries.[38]

While developing and least developed states might struggle with meeting the demand for these assets, the voluntary carbon credit market is likely to continue growing globally.[39]

1.5 The current regulatory landscape

Carbon credit markets operate under fragmented regulatory frameworks without a single governing body. This regulatory fragmentation creates significant challenges for market oversight, as inconsistencies between different jurisdictions' approaches can

[30] Zhijie Jia and Boqiang Lin, 'Rethinking the choice of carbon tax and carbon trading in China' (2020) 159 Technological Forecasting and Social Change 1.
[31] Yi-Fan Chen, 'Cap-and-trade system, firm selection, and emission intensity' (2025) 145 Energy Economics 1.
[32] Cameron Hepburn, 'Carbon trading: A review of the Kyoto mechanisms' (2007) 32 Annual Review of Environment and Resources 375, 393.
[33] Xing Chen and Boqiang Lin, 'Towards carbon neutrality by implementing carbon emissions trading scheme: Policy evaluation in China' (2021) 157 Energy Policy 1.
[34] Thomas D Jeitschko, Soo Jin Kim, and Pal Pallavi, 'Curbing price fluctuations in cap-and-trade auctions under changing demand expectations' (2024) 139 Energy Economics 1.
[35] Yonghong Zhao, Fu-Wei Huang, Ching-Hui Chang, and Jyh-Jiuan Lin, 'Domestic and foreign cap-and-trade regulations, carbon tariffs, and product tariffs during international trade conflicts: A multiproduct cost-efficiency analysis' (2024) 140 Energy Economics 1.
[36] Axel Michaelowa, Igor Shishlov, and Dario Brescia, 'Evolution of international carbon markets: lessons for the Paris Agreement' (2019) 10(6) Wiley Interdisciplinary Reviews: Climate Change 1.
[37] Blaufelder and others (n 5).
[38] Bertram and Terry (n 4).
[39] Hepburn (n 32).

create opportunities for regulatory arbitrage and undermine the environmental integrity of carbon trading

The European market of carbon credits, which is the largest cap-and-trade scheme in the world,[40] is regulated by the European Union Emissions Trading System (EU ETS) for EU states as well as Norway, Liechtenstein, and Iceland. The scheme covers 40% of GHG emissions in the European Union and limits emissions of approximately 10,000 installations in the manufacturing, aviation, and power sectors. The EU ETS is monitored by financial regulators, including ESMA, which recently found that the EU carbon market functioned without major deficiencies.[41] In the United Kingdom, the UK Emissions Trading Scheme (UK ETS) was adopted in 2021 to replace the EU ETS through the Greenhouse Gas Emissions Trading Scheme Order 2020.[42] In the United States, the White House, U.S. Department of Treasury, U.S. Department of Energy, and U.S. Department of Agriculture issued a joint policy statement in May 2024 that contains the principles for guiding voluntary market conduct.[43]

Additionally, the Carbon Border Adjustment Mechanism (CBAM) adopted by the European Union on October 1, 2023 forms yet another mechanism of regulating the carbon markets, particularly by imposing requirements on global manufacturers and exporters such as those in China.[44]

The United Nations Framework Convention on Climate Change (UNFCCC) operates a Carbon Offset Platform that allows companies and individuals to purchase carbon credits.[45] The organisation certifies environmentally friendly projects in developing countries using certified emission reductions. Following the landmark decision at COP26, the organisation was further tasked with regulating the trading of carbon credits by countries that aim at meeting their emission reduction goals.[46] COP26 also birthed the Article 6 rulebook that guides how countries trade carbon credits in efforts to reduce greenhouse gas emissions and meeting individual climate goals.[47]

[40] Cap and Trade is a market-based regulatory system designed to reduce greenhouse gas emissions. It sets a **"cap"** on the total amount of emissions that industries can produce, while allowing companies to **"trade"** emission allowances with each other.

[41] European Securities and Markets Authority, "ESMA Publishes Its Final Report on the EU Carbon Market" (ESMA 2022) https://www.esma.europa.eu/press-news/esma-news/esma-publishes-its-final-report-eu-carbon-market accessed 20 June 2025.

[42] Department for Energy Security & Net Zero and Department for Business, Energy & Industrial Strategy, "Participating in the UK ETS" (GOV.UK 2025) <https://www.gov.uk/government/publications/participating-in-the-uk-ets/participating-in-the-uk-ets> accessed 20 June 2025.

[43] U.S. Dep't of the Treasury, "U.S. Department of the Treasury Releases Joint Policy Statement and Principles on Voluntary Carbon Markets" (U.S. DEP'T OF THE TREASURY 2024) <https://home.treasury.gov/news/press-releases/jy2372> accessed 20 June 2025.

[44] Jiezhong Chang, 'Implementation of the EU Carbon Border Adjustment Mechanism and China's Policy and Legal Responses' (2025) 110 Env't Impact Assessment Review 1.

[45] United Nations Online Platform for Voluntary Cancellation of Certified Emission Reductions (CERs), "United Nations Carbon Offset Platform" [2023] <https://offset.climateneutralnow.org/> accessed 20 June 2025.

[46] Chen and others (n 18).

[47] Michele Stua, Colin Nolden, and Michael Coulon, 'Climate Clubs Embedded in Article 6 of the Paris Agreement' (2022) 180 Resources, Conservation and Recycling 1.

UNFCCC also monitors compliance with the Kyoto Protocol and the Paris Agreement. Moreover, there are numerous bodies that verify the contributions of sustainability projects that sell carbon credits. For instance, S&P Global Platts collects data on projects that are certified by such standards as Verified Carbon Standard, Climate Action Reserve, and the Gold Standard.[48] Verified Carbon Standard (Verra) is currently the most widely used programme for certifying greenhouse gas credits. Verra is a non-government organisation specialising in providing certification for voluntary carbon markets. Despite its focus on voluntary credits, Verra's certifications are often acknowledged in some mandatory compliance markets, such as the carbon markets of Colombia and South Africa.[49]

This certification ecosystem raises important questions about accountability and governance in voluntary markets. Unlike compliance markets with clear regulatory oversight, the authority of voluntary certification bodies derives primarily from market acceptance rather than legal mandate. This hybrid public-private governance structure creates complex jurisdictional questions regarding the enforcement of standards, particularly in cross-border transactions.

While this regulatory patchwork represents earnest attempts to govern carbon markets, significant structural challenges have emerged that threaten both market integrity and environmental outcomes, as we explore in the following sections.

2 Challenges and concerns

This section examines four interconnected challenges that undermine carbon market effectiveness: misaligned incentives, limited scalability, quality issues, and market structure problems.

2.1 An incentive not to reduce

One of the major challenges associated with the carbon credit system is that it gives countries and entities an incentive not to actually reduce their GHG emissions in practice. This fundamental tension between financial incentives and environmental outcomes represents a classic principal-agent problem, where the objectives of market participants may not align with the ultimate goal of emissions reduction. The mechanism provides companies and individuals with an opportunity to offset rather than take practical measures to reduce emissions, as documented extensively in the literature.

[48] "Specifications Guide for Carbon Markets" (S&P Global, August 2023), <https://www.spglobal.com/commodityinsights/PlattsContent/_assets/_files/en/our-methodology/methodology-specifications/method_carbon_credits.pdf> accessed 20 June 2025.
[49] Verra, "Verified Carbon Standard" <https://verra.org/programs/verified-carbon-standard> accessed 8 March 2025.

For example, Cao and others discovered that there is a statistically significant relationship between the carbon trading price and carbon emission reduction levels.[50] Han and others[51] showed that a reduction in transaction costs resulted in a greater loss to residents, something that was not expected by the researchers. Song and Moura share a controversial opinion that carbon credits for forest preservation "may be worse than nothing".[52] Zhao and others[53] argue that introducing renewable energies is currently a much more expensive option for Chinese companies than buying carbon credits.

In some contexts, carbon trading, particularly when carbon prices are low or allowances are perceived as cheap relative to innovation costs, can create a "crowding-out effect" on corporate R&D investment in green technology. High-polluting enterprises may find it cheaper to purchase carbon quotas than to invest in higher-cost, riskier green technology innovation, especially in the short term or in early-stage markets with ample quotas. This diverts funds away from investments that could lead to deeper, technology-driven emission reductions towards simply purchasing the right to emit, potentially perpetuating less efficient practices.[54]

Despite this criticism, some researchers are optimistic that the price of offsetting will eventually increase over time such that the incentive to offset instead of practical reduction is reduced.[55] This assumption relies on the capability of the market to "fix itself". In line with many standard economic theories, the invisible hand of efficient markets self-corrects and self regulates to limit market failures, hence closing the gaps and correcting the key abnormalities.[56]

For example, research by BloombergNEF shows that the prices of carbon offsets could eventually reach a figure between $47 and $120 per ton.[57] The exact price of these assets will depend on numerous supply-related and demand-related factors. Alternatively, one possible scenario is that a significant increase in the price of carbon credits is unlikely in the future owing to the oversupplied nature of the market.[58] Another scenario views the

[50] Kaiying Cao, Xiaoping Xu, Qiang Wu, and Quanpeng Zhang, 'Optimal Production and Carbon Emission Reduction Level under Cap-and-Trade and Low Carbon Subsidy Policies' (2017) 167 Journal of Cleaner Production 505.
[51] Jiayuan Han, Lingcheng Kong, Wenbin Wang, and Jiqing Xie, 'Motivating Individual Carbon Reduction with Saleable Carbon Credits: Policy Implications for Public Emission Reduction Projects' (2022) 122(5) Industrial Management & Data Systems 1268.
[52] Lisa Song and Paula Moura, 'An (Even More) Inconvenient Truth: Why Carbon Credits for Forest Preservation May Be Worse Than Nothing' (*ProPublica*, 22 May 2019) <https://features.propublica.org/brazil-carbon-offsets/inconvenient-truth-carbon-credits-dont-work-deforestation-redd-acre-cambodia/> accessed 20 June 2025.
[53] Fuquan Zhao, Feiqi Liu, Han Hao, and Zongwei Liu, 'Carbon Emission Reduction Strategy for Energy Users in China' (2020) 12(16) Sustainability 6498.
[54] Zhang and others (n 11).
[55] Rohit Jindal, Brent Swallow, and John Kerr, 'Forestry-Based Carbon Sequestration Projects in Africa: Potential Benefits and Challenges' (2008) 32 Natural Resources Forum 116.
[56] Evangelos Pournaras, Mark Yao, and Dirk Helbing, 'Self-Regulating Supply–Demand Systems' (2017) 76 Future Generation Computer Systems 73.
[57] BloombergNEF, "Global Carbon Market Outlook 2022: Bulls Trump Bears" (*Bloomberg*, 31 October 2022) <https://www.bloomberg.com/professional/blog/global-carbon-market-outlook-2022-bulls-trump-bears/> accessed 20 June 2025.
[58] Blaufelder and others (n 5).

possibility where markets will tighten their requirements towards these assets.[59] For example, regulatory measures like the Clean Development Mechanism requires parties to adhere to emission reductions requirements, hence limiting the types of acceptable offset credits.[60] Still, most voluntary markets lack rigid verification and validation procedures, resulting in criticisms of their accuracy and effectiveness of their validation methodologies.[61] While the introduction of stricter requirements may seem justifiable, it is likely to cause a further increase in project prices owing to higher project costs and their reduced number.

Beyond these problematic incentive structures, carbon markets face fundamental operational challenges. These limitations restrict market scalability despite growing demand and climate urgency.

2.2 Lack of scalability

Lack of scalability is a major challenge in carbon trading. The scalability challenge reflects broader issues in market design, as carbon markets must balance the competing demands of economic efficiency, environmental integrity, and administrative feasibility.

Scalability challenges arise from unpredictable supply and demand dynamics in carbon credit markets,[62] while at the same time ensuring that necessary market liquidity levels are attained for satisfying the needs of stakeholders. As such, companies are likely to shift to early purchases of carbon credits for their high-emission projects.[63] Rawuf believes that firms "will increasingly start offsetting their emissions as they begin work, rather than waiting until year-end".[64] It is currently unclear whether suppliers will be able to meet this growing demand.

The literature offers numerous insights into ways to ensure scalability in carbon trading. For example, a recent report by McKinsey proposes the use of digital verification and standardised standards for carbon credits definition, contracting, and trading infrastructure.[65] Still, the achievement of these goals remain challenging due to an absence of a consensus on terminologies of carbon credits as well as technical difficulties

[59] Marc N Conte and Matthew J Kotchen, 'Explaining the Price of Voluntary Carbon Offsets' (2010) 1(2) Climate Change Economics 93.
[60] United Nations Climate Change, "The Clean Development Mechanism" <https://unfccc.int/process-and-meetings/the-kyoto-protocol/mechanisms-under-the-kyoto-protocol/the-clean-development-mechanism> accessed 6 September 2023.
[61] Charlotte Streck, 'How Voluntary Carbon Markets Can Drive Climate Ambition' (2021) 39(3) Journal of Energy & Natural Resources Law 367.
[62] Jeitschko and others (n 34).
[63] Abdul Rawuf, "Transparency and Scalability: Two Keys to Unlocking Carbon Markets' Potential" (*Arabian Business*, 30 May 2022) <https://www.arabianbusiness.com/opinion/transparency-and-scalability-two-keys-to-unlocking-carbon-markets-potential> accessed 20 June 2025.
[64] ibid.
[65] Blaufelder and others (n 5).

related to the creation of such an ambitious solution.[66] Furthermore, shared principles and standardised protocols might be inconsistent with the current trading practices in most voluntary markets.[67] Despite the proposed enhancement measures, scalability remains challenging.

2.3 Incentivising lower credit quality

One of the most problematic features of existing carbon trading regimes is the presence of perverse incentive mechanisms that actively encourage the proliferation of low-quality credits.[68] This fundamental market design flaw undermines the environmental integrity that carbon markets are intended to promote. Typically, companies pursue ways to attain their corporate social responsibility (CSR) goals while maximising profits.[69] Such companies buy cheap carbon credits that confer a reputational gain without ensuring any real emission reduction in practice.[70] Furthermore, voluntary markets have very little regulation, so firms can buy practically useless credits regarding global warming with minimal scrutiny.[71] Solving this problem calls for a public awareness that discourages firms from buying low-quality credits, perhaps via shaming.[72] Additionally, building stricter validation and verification frameworks to make sure that carbon offsets are actually effective may help to ensure a sufficient quality of all the carbon credits in both voluntary and mandatory markets.[73] Still, some of the low-quality credits may be introduced via unethical actors, and therefore outright fraudulent.[74] Others may be used for money laundering rather than bona fide efforts to reduce emission.[75]

2.4 Issues with supply, demand and markets

The incentive model embedded in the carbon trading markets also faces challenges from mismatches between demand and supply. Buyers from different industries have

[66] Enas Al Kawasmi, Edin Arnautovic, and Davor Svetinovic, 'Bitcoin-Based Decentralized Carbon Emissions Trading Infrastructure Model' (2014) 18(2) Systems Engineering 115.
[67] Fangyuan Zhao and Wai Kin (Victor) Chan, 'When Is Blockchain Worth It? A Case Study of Carbon Trading' (2020) 13(8) Energies 1980.
[68] Hepburn (n 32).
[69] Morteza Khojastehpour and Raechel Johns, 'The Effect of Environmental CSR Issues on Corporate/Brand Reputation and Corporate Profitability' (2014) 26(4) European Business Review 330.
[70] Matthew Lockwood, 'The economics of personal carbon trading' (2010) 10(4) Climate Policy 447.
[71] Blaufelder and others (n 5).
[72] Brilé Anderson and Thomas Bernauer, 'How Much Carbon Offsetting and Where? Implications of Efficiency, Effectiveness, and Ethicality Considerations for Public Opinion Formation' (2016) 94 Energy Policy 387.
[73] Tse-Lun Chen, Hui-Min Hsu, Shu-Yuan Pan, and Pen-Chi Chiang, 'Advances and Challenges of Implementing Carbon Offset Mechanism for a Low Carbon Economy: The Taiwanese Experience' (2019) 239 Journal of Cleaner Production 1.
[74] Deloitte, "Carbon Credit Fraud: The White Collar Crime of the Future" <https://tomaswell.files.wordpress.com/2015/02/carbon_credit_fraud.pdf> accessed 21 March 2025.
[75] Ed King, "Interpol Warns of Criminal Focus on $176 Billion Carbon Market" (*Climate Home News*, 8 May 2013) <https://www.climatechangenews.com/2013/08/05/interpol-warns-of-criminal-focus-on-176-billion-carbon-market/> accessed 20 June 2025.

unequal incentive structures for purchasing credits.[76] For example, high-emission industries such as mining rely more heavily on offsets than players in other sectors.[77] A significant challenge arises from the fragmentation of carbon trading across multiple marketplaces, resulting in inconsistent standards, verification practices, and pricing mechanisms. This regulatory patchwork creates opportunities for arbitrage and undermines market transparency, as different trading platforms may apply varying levels of scrutiny to similar carbon reduction projects.[78]

This multitude of voluntary markets also makes integration more complex, as new verification methods may increase costs and discourage participation.[79] Furthermore, some buyers could be confused by the rigid procedures of new markets and the unprecedentedly high level of competition that they will face. This information asymmetry between sophisticated market participants and newer entrants threatens market efficiency and potentially undermines the confidence necessary for robust trading

Another problem stems from the fact that carbon markets are based on controversial ideas such as the existence of a linear relationship between emissions and offsets. Thus, many projects cannot credibly measure their environmental impacts, and this makes the entire concept of offsetting questionable regarding their effectiveness.[80] As such, companies that are serious about their sustainable activities might stop the use of face-value offsetting credits and concentrate on reducing the emission of their greenhouse gases.

3 Compliance markets dilemmas: fraud, efficacy, efficiency & ethics

Inadequate verification systems compromise the fundamental integrity of carbon credits through persistent problems of additionality, leakage, and measurement inconsistency. Without robust standards to ensure emissions reductions are genuine, additional, and permanent, carbon trading becomes vulnerable to credits representing fictional or exaggerated climate benefits. This verification crisis threatens the environmental value proposition of the entire carbon market system.

New, unregulated markets often provide fertile ground for fraudulent activity. The legal literature has extensively documented how regulatory vacuums in novel markets create ideal conditions for various forms of manipulation, with carbon markets being

[76] Jonathan Otto, 'Precarious Participation: Assessing Inequality and Risk in the Carbon Credit Commodity Chain' (2018) 109(1) Annals of the American Association of Geographers 187.
[77] Song and Moura (n 52).
[78] Song Xu, Kannan Govindan, Wanru Wang, and Wenting Yang, "Supply chain management under cap-and-trade regulation: A literature review and research opportunities' (2024) 271 International Journal of Production Economics 109199; Jeitschko and others (n 34); Xuelian Li, Wei Zhou, Tang-Yun Lo, and Jyh-Horng Lin, 'International climate policy dilemmas: Examining effective carbon tariff and cap-and-trade regulation from a sustainable insurance perspective' (2024) 134 Energy Economics 1.
[79] Al Kawasmi, Arnautovic and Svetinovic (n 66).
[80] Benjamin K Sovacool, 'Four Problems with Global Carbon Markets: A Critical Review' (2011) 22(6) Energy & Environment 681.

particularly vulnerable due to their intangible nature and complex verification requirements.[81] The nascent carbon trading market is still evolving and therefore lacks uniform standards of measurements and verification.[82] Since there is no standard measurement of a "high quality carbon credit" and some factors that are used such as: additionality, leakage, double counting, verification and transparency remain unregulated.[83] Fraud, money-laundering and criminal activity can heavily affect the efficiency and trust of the carbon market leading to reduced trading and increasing price per unit.[84] This imbalance led to an emissions market reliant on the integrity of countries and corporations to present accurate data of emissions levels.[85] As a result, organisations and countries are operating in the unregulated carbon market as America's old Wild West.

Among the most prevalent forms of market manipulation in carbon trading is greenwashing, which represents not merely a procedural concern but a fundamental threat to market credibility.

3.1 Greenwashing

Many regard the carbon market as a 'greenwashing scam' that enables polluters to avoid emissions restrictions. Greenwashing describes practices by organisations that falsely appear to be environmentally friendly rather than actually engaging in sustainable practices. "Corporations and even organised crime groups may purchase carbon offsets to finance "green" projects as fronts for other activities. These "green fronts" can apply to receive emission reduction credits which can then be sold directly to companies or traded on carbon markets generating large revenues.[86] At COP 27, The International Organization for Securities Commissions (IOSCO) has outlined the actions it undertakes to protect investors by mitigating greenwashing in financial markets, to contribute to promote well-functioning carbon markets.[87] For example, the multinational energy companies may present themselves as "progressive" and environmentally responsible to legitimise their

[81] Xihan Xiong, Zhipeng Wang, Tianxiang Cui, William Knottenbelt, and Michael Huth, 'Market Misconduct in Decentralized Finance (DeFi): Analysis, Regulatory Challenges and Policy Implications' [2023] *arXiv* <*arXiv:2311.17715*> accessed 20 June 2025; Sebeom Oh, "Market Manipulation in NFT Markets", MPRA Paper No. 116704 (University Library of Munich, Germany 2023).

[82] PWC, 'How to Assess Your Green Fraud Risks' <https://www.pwc.co.uk/assets/pdf/greenfraud.pdf> accessed 6 September 2023.

[83] IOSCO, 'Voluntary Carbon Markets Discussion Paper' CR/06/22 (The International Organization of Securities Commissions 2022) <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD718.pdf> accessed 20 June 2025.

[84] Regina Betz and others, *The Carbon Market Challenge: Preventing Abuse Through Effective Governance* (Cambridge University Press 2022).

[85] Heidi Bachram, 'Climate Fraud and Carbon Colonialism: The New Trade in Greenhouse Gases' (2004) 15(4) Capitalism Nature Socialism 5.

[86] Clifford Curtis Williams, 'A Burning Desire: The Need for Anti-Money Laundering Regulations in Carbon Emissions Trading Schemes to Combat Emerging Criminal Typologies' (2013) 16 Journal of Money Laundering Control 298.

[87] IOSCO, 'IOSCO Outlines Regulatory Priorities for Sustainability Disclosures, Mitigating Greenwashing and Promoting Integrity in Carbon Markets' (The International Organization for Securities Commissions 2022) IOSCO/MR/33/2022 <https://www.iosco.org/news/pdf/IOSCONEWS669.pdf> accessed 20 June 2025.

forms of energy production. These companies however, arguably make no actual environmental change while being able to keep polluting without any consequences.[88]

In another example, in 2021, carbon offset credits purchased by a vehicle manufacturer were inexplicably about five times larger than their 2020 purchases.[89]

Credit Suisse's 2022 Sustainability Report acknowledges significant challenges in ESG data quality, third-party verification, and climate-related disclosures, which may undermine the reliability of some sustainability claims in the market.[90]

The geographic concentration of carbon trading mechanisms reveals a troubling equity crisis in global climate finance. Despite Least Developed Countries (LDCs) and Small Island Developing States (SIDS) prominently featuring renewable energy projects in their Nationally Determined Contributions (NDCs), their participation in the Clean Development Mechanism (CDM) remains severely limited. Over 80% of CDM projects cluster in a few large developing economies—primarily China and India—while Africa's representation is minimal despite hosting 54 countries. [91] This imbalance stems from structural barriers including prohibitive project costs, political instability, inadequate infrastructure, and limited technical capacity in the poorest nations. This reflects a "carbon colonialism," where emissions mitigation burdens shift disproportionately to those least responsible historically for carbon emissions.

Though LDCs possess substantial renewable energy potential and land-based mitigation opportunities in forestry and agriculture, these assets remain largely untapped due to market barriers. This systemic exclusion from carbon market benefits contradicts the Paris Agreement's principle of common but differentiated responsibilities while perpetuating global climate inequities that disproportionately harm the world's most vulnerable populations.[92]

In April 2021, a report analysed 100 certified offset programs and found significant performance failures. The analysis revealed that 90% of the projects either failed to offset their claimed emissions reductions or actually caused local environmental damage.

[88] Steffen Boehm and Siddharta Dabhi, *Upsetting the Offset: The Political Economy of Carbon Markets* (MayFly Books 2009); Akshat Rathi, Natasha White and Demetrios Pogkas, "Junk Carbon Offsets are What Make These Big Companies Carbon Neutral" (*Bloomberg*, 21 November 2022) <https://www.bloomberg.com/graphics/2022-carbon-offsets-renewable-energy/?> accessed 20 June 2025.

[89] Josh Gabbatiss, "Analysis: How some of the world's largest companies rely on carbon offsets to 'reach net-zero'" (*Carbon Brief*, 28 September 2023) <https://interactive.carbonbrief.org/carbon-offsets-2023/> accessed 20 June 2025; Nina Lakhani, 'Corporations invested in carbon offsets that were 'likely junk', analysis says' *The Guardian* (London, 30 May 2024) <https://www.theguardian.com/environment/article/2024/may/30/corporate-carbon-offsets-credits> accessed 20 June 2025.

[90] Credit Suisse Group AG, "Sustainability report 2022" <https://www.responsibilityreports.com/HostedData/ResponsibilityReportArchive/c/NYSE_CS_2022.pdf> accessed 20 June 2025.

[91] Avenarius and others (n 23).

[92] Hepburn (n 32).

Similarly, another investigation found that airline companies' offsetting schemes have made emission predictions that exaggerated success.[93]

Overall, we increasingly see companies make statements regarding carbon credit transactions. However, they often employ climate terms such as “net zero” in ways that could potentially indicate greenwashing if not outright fraud.

To mitigate the growing problem of greenwashing—where companies exaggerate or misrepresent their environmental efforts—some experts propose tightening the conditions under which carbon offset credits can be used. Specifically, it would be best if large corporations should only be allowed to access offset markets after they have made verifiable and reasonable efforts to reduce their direct and indirect emissions through internal measures such as energy efficiency improvements, process optimisation, or a shift to renewable energy. This approach prioritises actual emissions reductions over symbolic offset purchases and ensures that offsets serve as a complementary, not primary, tool in a company’s decarbonisation strategy. By enforcing such a hierarchy—first reduce, then offset—regulators and stakeholders can discourage superficial climate pledges and promote more meaningful climate action.[94] And even when companies have good intentions, they often lack the understanding and in-depth knowledge to pick a suitable project that will actually make a difference. Selecting high-quality carbon credits is inherently challenging due to systemic flaws in how carbon markets are designed and operate. Many protocols and standards, particularly for forest-based offsets, suffer from deep-rooted weaknesses in core areas like additionality, permanence, leakage, and verification. These shortcomings are often due to vague guidelines or misunderstandings of how markets function. The verification process, intended to ensure credibility, is undermined by conflicts of interest and limited technical expertise—verifiers may only assess compliance with inadequate rules, rather than conducting a truly independent evaluation. Compounding this, project developers are incentivised to exploit these weaknesses, sometimes manipulating estimates or reporting to maximise profits, especially when oversight is weak. As a result, many projects underperform or would have occurred even without the carbon market mechanism, meaning their credits do not reflect real, additional emissions reductions.[95] These structural and behavioural issues—not merely poor judgment by credit buyers—make it difficult to confidently identify projects that deliver meaningful climate impact.

Ultimately, if companies claim that they are reducing carbon emissions, they must be able to demonstrate as such to investors and regulators.[96] The legal enforceability of carbon reduction claims requires robust verification mechanisms that can withstand

[93] Emmy Hawker, ‘Can a New Sheriff Tame Carbon Markets’ Wild West?’ (*ESG Investor*, 19 January 2022) <https://www.esginvestor.net/can-a-new-sheriff-tame-carbon-markets-wild-west/> accessed 6 September 2023.
[94] ibid.
[95] Richards and Huebner (n 25).
[96] Patrick Temple-West, ‘Critics Take Aim at “Wild West” Carbon Offset Market’ *Financial Times* (London, 8 June 2022) <https://www.ft.com/content/9b02fcf7-9e04-4b71-ad14-251552d5a78e> accessed 8 June 2022.

judicial scrutiny, a standard that many current verification procedures fail to meet under close examination.

3.2 Additionality

Assessing additionality, as described in the Kyoto Protocol[97] is a key part of all baseline-and-credit schemes. It determines whether a project leads to real emissions reductions that wouldn't have happened without the incentive. The baseline serves as a reference, showing what emissions would have been without the project. Any such project reduces emissions from sources or enhances removals by carbon sinks—natural systems like plants, oceans, and soil that absorb more carbon than they release. Ensuring additionality is important because it prevents credit schemes from rewarding reductions that would have occurred anyway. However, since additionality involves predicting future scenarios, it can never be determined with complete certainty.[98]

Scarcity plays a crucial role in ensuring the integrity of baseline-and-credit schemes by limiting the supply of credits to only truly additional projects. [99] In offsetting programmes, this scarcity is created by distinguishing eligible activities from those that do not meet the additionality criteria, ensuring that only projects leading to genuine emissions reductions receive credits. The Kyoto Protocol mandates additionality but does not specify how to determine the baseline, the reference point for measuring reductions.

To address this, the UNFCCC developed tools to minimise the risks associated with counterfactual data and to require project developers to establish precise baseline measurements. Accurate and consistent measurement is essential, as errors can lead to the issuance of invalid credits, undermining the credibility of the carbon market. [100] By controlling the supply of credits, additionality helps maintain the scarcity necessary for an effective and trustworthy offset system.

Assessing additionality is challenging because it relies on counterfactual scenarios that cannot be definitively proven. There is no accurate and standardised methodology to calculate additionality because there is no certainty about what would happen without the project.[101] Furthermore, fraudulent measurement of emissions can be created by tampering with measurement devices or reporting misstatements.[102] In a 2023 report, the

[97] 'Kyoto Protocol to the United Nations Framework' Article 12, paragraph 5(c) <https://unfccc.int/resource/docs/convkp/kpeng.pdf> accessed 20 June 2025.
[98] Australian Government Climate Change Authority, 'Coverage, Additionality and Baselines - Lessons from the Carbon Farming Initiative and Other Schemes: CCA Study' (CCA 2014) <https://www.climatechangeauthority.gov.au/publications/coverage-additionality-and-baselines-lessons-carbon-farming-initiative-and-other-schemes> accessed 6 September 2023.
[99] Michael Gillenwater and others, 'Policing the Voluntary Carbon Market' (2007) 1 Nature Climate Change 85.
[100] Tanguy du Monceau and Arnaud Brohé, 'Briefing Paper "Baseline Setting and Additionality Testing within the Clean Development Mechanism (CDM)"' (London 2011) <https://climate.ec.europa.eu/system/files/2017-02/additionality_baseline_en_0.pdf> accessed 20 June 2025.
[101] ibid.
[102] Deloitte (n 74).

Guardian newspaper revealed that more than 90% of rainforest carbon offsets are worthless. The research into Verra, a large voluntary carbon credit registry, found that the majority of the credits do not represent genuine carbon reductions. According to the investigation, only a couple of Verra's rainforest projects showed evidence of deforestation reductions. Another study by the University of Cambridge found that 32 projects out of 40 scenarios of forest loss appeared to be overstated by approximately 400%.[103] This uncertainty provides the opportunity to manipulate the process or make false claims about the project. Players in the market have an incentive to provide biased information that will increase their chances of being qualified as an additional project.[104]

Ensuring additionality in carbon offset programs is complex. First, these programmes rely on obtaining accurate data from field actors, but regulators often face **asymmetric information—w**here those involved in offsetting have incentives to exaggerate their program's impact to gain approval. Both credit sellers and buyers benefit when a program is deemed "additional," which can undermine the integrity of the carbon market.

Moreover, additionality is influenced by multiple factors. Activities vary in function and are shaped by diverse variables, making additionality standards inherently **subjective.** Additionally, the **most expensive projects** are often the most likely to qualify as additional, which may lead investors to artificially inflate costs to meet the criteria.

Another key challenge is that additionality depends on **context-specific factors**—such as project circumstances, risk levels, and investor behaviour. However, existing frameworks largely **overlook these complexities,** leading to projects that appear "additional" on paper but fail to contribute meaningfully to net-zero goals.

Policymakers and regulators must recognise that as additionality assessments become more stringent, the risk increases that **fewer projects will be developed**, potentially limiting the effectiveness of carbon offset initiatives.

3.3 Leakage

Carbon reduction projects must also prevent leakage, which occurs when emissions increase outside a project's boundary as a result of the project's intervention. For example, protecting a section of the Amazon rainforest may simply push logging activities to another area, undermining the intended environmental benefits. Leakage risks are higher when regulations and incentives apply to only a portion of the relevant resources or stakeholders.

Leakage can occur at different levels: on-site leakage happens when emissions unexpectedly rise within the project area, while off-site leakage occurs beyond it. Off-

[103] Patrick Greenfield, 'Revealed: More than 90% of Rainforest Carbon Offsets by Biggest Certifier Are Worthless, Analysis Shows' *The Guardian* (London, 18 January 2023) <https://www.theguardian.com/environment/2023/jan/18/revealed-forest-carbon-offsets-biggest-provider-worthless-verra-aoe> accessed 7 September 2023.
[104] Gillenwater and others (n 99).

site leakage may be international, where emissions shift from a regulated country to one with fewer restrictions, or subnational, where a country's policy regulates only certain sectors, allowing emissions to move to unregulated industries. To ensure meaningful emissions reductions, policymakers must design comprehensive frameworks that anticipate and mitigate leakage risks.

Emissions Trading System (ETS) leakage occurs when businesses relocate production to countries with less stringent emission regulations to avoid the costs associated with carbon pricing. This shift can actually lead to an overall increase in global emissions, undermining the effectiveness of carbon reduction policies. The EU Emissions Trading System (EU ETS) recognises this risk, particularly in industries that are energy-intensive and exposed to international competition. To mitigate ETS leakage, the EU allocates a higher share of free allowances to sectors most vulnerable to relocation, ensuring they remain competitive while still incentivising emission reductions within the regulated jurisdiction.[105]

The main challenge with leakage is that it is not directly observable but rather estimated using economic data and modelling. Due to variations in leakage rates and the uncertainty of these measurements, leakage can undermine the integrity of offset programs.[106] Additionally, leakage highlights a broader issue—wealthy countries often displace emissions to developing nations, exacerbating global environmental inequalities. To minimise leakage, emissions reductions and removals must be carefully quantified, with appropriate adjustments made for estimated leakage to ensure the credibility of offset programme.[107]

3.4 Double counting

Another concern is that traded credits may be "double-counted", meaning carbon emissions removal units are counted more than once. For example, the same credit can be sold and resold to different buyers.[108]

In fact, double counting can appear in many different forms and result from different situations[109] such as: double issuance, if more than one unit is issued for the same emissions; double claiming, if the same emission reductions are accounted for the same mitigation pledges usually in the context of transferring units from developing to

[105] Commission Delegated Decision (EU) 2019/708 of 15 February 2019 supplementing Directive 2003/87/EC of the European Parliament and of the Council concerning the determination of sectors and subsectors deemed at risk of carbon leakage for the period 2021 to 2030 [2019] OJ L120/62.
[106] W Aaron Jenkins, Lydia P Olander and Brian C Murray, 'Addressing Leakage in a Greenhouse Gas Mitigation Offsets Program for Forestry and Agriculture' (Nicholas Institute for Environmental Policy Solutions 2009) <https://nicholasinstitute.duke.edu/sites/default/files/publications/offsetseries4-paper.pdf> accessed 20 June 2025.
[107] Blaufelder and others (n 5).
[108] United Nations Framework Convention on Climate Change (adopted 12 December 2015) (UNFCC) art 6(2) - further 'Paris Agreement'.
[109] Lambert Schneider, Anja Kollmuss and Michael Lazarus, 'Addressing the Risk of Double Counting Emission Reductions under the UNFCCC' (2015) 131 Climatic Change 473.

developed countries; "double selling", counted once by the country of origin when reporting its emissions and again by the receiving country or entity and lastly double purpose, the unit is also used for financial or technology purposes.[110]

Another significant fraud risk in carbon markets is the sale of non-existent or misrepresented carbon credits, including those that have already been claimed by someone else. Since carbon credits exist only as digital records in registries, they can be vulnerable to forgery or duplication. The global nature of carbon trading further complicates tracking and preventing such fraudulent activities.[111] To ensure unique ownership and prevent double counting, it is essential to establish clear verification mechanisms that confirm ownership rights. Each credit must be assigned to a single entry in a registry and permanently retired once used, preventing the circulation of recycled carbon units and maintaining the integrity of the market.[112]

The credibility of the EU ETS has also been impacted by fraud, including the theft of €7 million in emission permits from the Czech Republic's carbon registry.[113] Similarly, the Clean Development Mechanism (CDM) has faced fraudulent activities, such as Chinese companies deliberately producing greenhouse gases to generate credits and then destroying them, the sale of fake forestry credits, and the reuse of credits by EU states. To address these issues, experts are advocating for a global registry to track and log all voluntary carbon market (VCM) projects and credits, ensuring greater transparency and accountability.[114]

3.5 VAT fraud and money laundering

Carbon credits are highly susceptible to fraud due to their intangible nature, high market value, and the ease with which they can be traded on spot markets. Unlike physical commodities such as corn or gold—where volume and delivery can be readily verified—carbon offsets lack a physical form, making it difficult for purchasers to independently confirm that the claimed emissions reductions have actually taken place. This reliance on unverifiable assumptions, combined with limited oversight mechanisms, renders the carbon market vulnerable to manipulation and fraudulent activity.[115]

[110] Lambert Schneider and others, 'Double Counting and the Paris Agreement Rulebook' (2019) 366 Science 180.
[111] IOSCO (n 83).
[112] Brian Preston, 'Climate Change Litigation (Part 1)' (2011) 5 Carbon & Climate Law Review 3.
[113] Fred Pearce, (2011, January 20). 'Black market steals half a million pollution permits' (*New Scientist*, 20 January 2011) <https://www.newscientist.com/article/dn20012-black-market-steals-half-a-million-pollution-permits/> accessed 20 June 2025.
[114] Frédéric Hache, '50 Shades of Green: The Rise of Natural Capital Markets and Sustainable Finance – Part I. Carbon' (Green Finance Observatory 2019) <https://greenfinanceobservatory.org/wp-content/uploads/2019/03/50-shades-carbon-final.pdf> accessed 20 June 2025.
[115] Alex Fredman and Todd Phillips, 'The CFTC Should Raise Standards and Mitigate Fraud in the Carbon Offsets Market' (Center for American Progress 2022) <https://www.americanprogress.org/article/the-cftc-should-raise-standards-and-mitigate-fraud-in-the-carbon-offsets-market/> accessed 7 September 2023.

This vulnerability has not only enabled manipulation within the carbon credit system itself but has also facilitated large-scale financial fraud schemes. One prominent example involves the exploitation of value-added tax (VAT) systems, where fraudulent actors leverage the ease of carbon credit transfers to evade tax obligations on a massive scale.[116]

VAT is a tax applied to imported goods and services. There are two main types of VAT fraud, one of which is "missing-trader" fraud. This occurs when a buyer acquires emission allowances from a country where VAT is exempt, then sells them domestically while charging VAT but failing to remit the tax to local authorities. The term “missing-trader” refers to the fact that the seller typically disappears before the fraud is detected. This scheme is estimated to cost revenue authorities approximately 50 billion euros annually in lost tax revenue.[117]

The second, more complex type of VAT fraud is known as "carousel frauds". Allowances are transferred along a network of interconnected companies located in different countries within the same carbon market. In each trading cycle, the trader does not return the VAT to the local tax authority.[118] The EU ETS has experienced VAT fraud involving large sums of money. In 2009, the UK arrested seven people for executing a 38 million pounds carbon credit VAT fraud. The French authorities similarly suspected a 156 million euros VAT fraud. The effects of VAT fraud are mainly large losses of tax revenues in the countries where the goods are "carouseled". In 2018, 36 people in France were convicted of €385 million carbon VAT fraud scheme.[119] Europol estimates that in 2009 VAT fraud on the EU ETS reached roughly 5 billion euros.[120]

In addition to facilitating tax evasion, carbon offset markets are increasingly vulnerable to exploitation for money laundering, especially in developing countries where regulatory oversight is limited or inconsistently enforced. Thus, carbon credit markets, particularly emissions trading schemes (ETS), have emerged as lucrative yet vulnerable platforms for money laundering. In particular, the absence of robust anti-money laundering (AML) safeguards during the initial development of mechanisms like the EU ETS left them open to criminal exploitation.[121] Emission allowances and credits can be traded much like traditional financial instruments, yet without equivalent regulatory oversight. This parallel to traditional securities markets, combined with international variability in enforcement standards, creates jurisdictional blind spots that money launderers can

[116] Katherine Nield and Dr Ricardo Pereira, ‘Fraud on the European Union Emissions Trading Scheme: Effects, Vulnerabilities and Regulatory Reform’ (2011) 20 European Energy and Environmental Law Review 255.
[117] ‘MTIC (Missing Trader Intra Community) Fraud’ (*Europol*, 2022) <https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/economic-crime/mtic-missing-trader-intra-community-fraud> accessed 7 September 2023.
[118] Betz and others (n 84).
[119] Maria Cronin, Craig Hogg and Kirsten Stewart, ‘Carbon Credit Fraud: COP27 and Policing the Wild West’ (*The European Business Review*, 27 November 2022) <https://www.europeanbusinessreview.com/carbon-credit-fraud-cop27-and-policing-the-wild-west/> accessed 7 September 2023.
[120] Nield and Pereira (n 116).
[121] Curtis Williams, ‘A burning desire: The need for anti-money laundering regulations in carbon emissions trading schemes to combat emerging criminal typologies’ (2013) 16(4) Journal of Money Laundering Control 298.

exploit. Criminals may layer illicit proceeds through carbon transactions, eventually integrating them into the financial system with a veneer of legitimacy.

Moreover, the global scale of environmental crime—estimated by the Financial Action Task Force (FATF) to generate up to $281 billion annually—underscores the importance of using AML enforcement as a countermeasure.[122] Europol has estimated losses from such frauds at over €5 billion, with 90% of trading volume during peak years attributed to illicit activity. These operations not only deprive governments of tax revenues but also distort carbon markets, eroding trust and reducing their efficacy as tools for climate mitigation.[123]

Carbon offset projects, especially in regions with limited regulatory infrastructure, can serve as entry points for illicit capital under the guise of climate finance. For example, fraudsters might establish sham offset projects or manipulate emissions data to generate tradable credits backed by little or no actual emissions reduction. This misuse distorts market integrity, undermines climate goals, and diverts legitimate climate finance. As carbon markets expand globally, experts stress the need to integrate AML mechanisms from the outset, including rigorous verification, beneficial ownership transparency, and international cooperation. Without these safeguards, carbon markets may unintentionally facilitate financial flows that enable environmental degradation rather than its mitigation.[124]

3.6 Ethical concerns and the global south

Current carbon market structures create disproportionate burdens on developing nations while enabling industrialised economies to outsource their climate responsibilities. The documented pattern of implementing offset projects in the Global South without adequate safeguards for local communities raises fundamental questions of climate justice and global equity. Carbon trading mechanisms must address these ethical contradictions to serve as legitimate climate solutions.

Developed countries increasingly implement decarbonisation projects in developing nations to offset emissions. They use mechanisms such as the Clean Development Mechanism (CDM)[125] and the Warsaw Framework for REDD+.[126] Reducing Emissions from Deforestation and Forest Degradation (REDD+) is a global initiative aimed at incentivising forest conservation in developing countries. REDD+ seeks to mitigate climate change by

[122] Chiara Sophia Oberle, 'Greening White-Collar Crime: Transforming Anti-Money Laundering Enforcement into an Instrument Against Environmental Crime' (Master thesis, University of Geneva 2022).
[123] Katherine Nield and Ricardo Pereira, 'Financial crimes in the European carbon markets' in Stefan E Weishaar (ed), *Research Handbook on Emissions Trading* (Edward Elgar Publishing 2016) 195.
[124] Deloitte (n 74).
[125] Hepburn (n 32).
[126] Kanako Morita and Ken'ichi Matsumoto, 'Challenges and lessons learned for REDD+ finance and its governance' (2023) 18(8) Carbon Balance and Management 1; John Parrotta, Stephanie Mansourian, Nelson Grima, and Christoph Wildburger (eds), 'Forests, climate, biodiversity and people: assessing a decade of REDD+' (IUFRO World Series Volume 40, Vienna 2022).

providing financial compensation to governments, communities, and private actors for preserving forests, thus preventing deforestation and associated carbon emissions. However, scholars have raised significant ethical concerns about these projects, particularly their impact on local populations.

These concerns include the risk that carbon offset projects may come at the expense of economic prosperity in developing countries,[127] misaligned political motivations that prioritise external interests over local needs, and increased energy injustices that exacerbate existing inequalities.[128] Additionally, these initiatives can disrupt local communities' welfare by displacing people or limiting their access to resources,[129] while the absence of robust institutional structures often fosters corruption, especially in regions such as Africa and Latin America. [130] These challenges highlight the need for stronger regulatory oversight and greater inclusion of local stakeholders in the decision-making process.

The disproportionate burden of climate change on developing countries remains one of the major challenges in the world today. Climate change is predominantly caused by the wealthiest of the world's population who contribute disproportionately to about 40 percent of the released emissions.[131] However, climate change consequences will disproportionately affect the world's poorest countries.[132] The paradox is that the Global South has the most to lose from both climate change and the economic transition to decarbonisation.[133] While climate change affects their natural resources[134] the poorest also suffer the greatest from rising energy prices[135] which result from carbon credit and taxation policies exacerbating inequality through an inaccessibility to energy.

This paradox highlights a fundamental tension in international climate law between the right to development and climate protection obligations. Article 4.7 of the UNFCCC explicitly acknowledges that economic and social development and poverty eradication are 'first and overriding priorities' for developing countries.[136] However, carbon market mechanisms often fail to adequately balance these competing legal principles, creating

[127] Peter Newell, Marcus Power, and Harriet Bulkeley, "Rising Powers, Lowering Emissions?" (IDS 2016).
[128] ibid.
[129] Baimwera Bernard, David Wang'ombe, and Ernest Kitindi, 'Carbon Markets: Have They Worked for Africa?' (2017) 6 (2) Review of Integrative Business & Economic Research 90.
[130] Wim Carton, Adeniyi Asiyanbi, Silke Beck, Holly J Buck, and Jens F Lund, 'Negative Emissions and the Long History of Carbon Removal' (2020) 11 (6) Wiley Interdisciplinary Reviews: Climate Change 1.
[131] Bill Gates, *How to Avoid a Climate Disaster: The Solutions We Have and the Breakthroughs We Need* (Diversified Publishing 2021).
[132] Intergovernmental Panel on Climate Change (IPCC), "Climate Change 2022 - Mitigation of Climate Change: Working Group III Contribution to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change" (Cambridge: Cambridge University Press 2023).
[133] Matt Ridley, *The Rational Optimist: How Prosperity Evolves* (Harper Collins, 2011).
[134] Arild Angelsen and others, 'Environmental Income and Rural Livelihoods: A Global-Comparative Analysis' (2014) 64(1S) World Development S12; World Food Programme (WFP), "Climate Change in Southern Africa" (2021).
[135] Samuel Asumadu Sarkodie and Samuel Adams, 'Electricity Access, Human Development Index, Governance and Income Inequality in Sub-Saharan Africa' (2020) 6 Energy Reports 455.
[136] Lukas Hermwille, Wolfgang Obergassel, Hermann E Ott, and Christiane Beuermann, 'UNFCCC before and after Paris: What's necessary for an effective climate regime?' (2017) 17(2) Climate Policy 150.

what some scholars describe as 'carbon colonialism' where climate mitigation burdens are disproportionately placed on those least responsible for the problem.[137] Nevertheless, global emissions reduction by each and every country is necessary in order to achieve carbon neutrality. Ludena and others wed how global conformity of negative carbon solutions is required to achieve carbon neutrality.[138] However, the carbon market policies enacted in the Paris Climate Agreement of 2015 arguably force economic burdens on developing nations to take financial responsibility for increasing energy use, for the purposes of poverty eradication.[139] Carbon market policies create economic burdens on developing nations while denying them prosperity, despite the fact that climate change was primarily caused by industrialised countries. This arrangement is potentially unethical and incongruent with the United Nations Sustainable Development Goals (SDGs).[140]

Political misalignment is another significant ethical concern in carbon offset projects, including REDD+. These include fundamental tension between development and climate goals,[141] ongoing tensions between more inclusive, participatory approaches and the dominant logic of market-based governance focused on commodification, standardisation, and profit accumulation,[142] lack of policy harmonisation and institutional fragmentation,[143] and equity, burden shifting, and international tensions.[144]

However, critics argue that these projects often continue despite mistreatment of local communities and politically or commercially driven motivations.[145]

Asiyanbi and Lund question the "persistence and tentative stability" of REDD+ initiatives, highlighting how political and private sector interests can overshadow the needs of affected populations. Similarly, Alusiola and others conducted a meta-analysis of conflicts arising from REDD+ forest projects to understand their causes, mechanisms, and consequences. Their study identified six key conflict catalysts: (1) injustices and restrictions on full access to and control over forest resources, (2) the creation of new forest governance structures that alter stakeholder relationships, (3) the exclusion of community members from meaningful participation, (4) failure to meet high project expectations, (5) changes in land tenure policies driven by migration, and (6) the exacerbation of historical land tenure disputes. These findings highlight the socio-political

[137] Heidi Bachram, 'Climate fraud and carbon colonialism: the new trade in greenhouse gases' (2004) 15(4) Capitalism nature socialism 5.
[138] Carlos Ludeña, Carlos J De Miguel, and Andrés Ricardo Schuschny, 'Climate Change and Carbon Markets: Implications for Developing Countries' (2015) 116 CEPAL Review 62.
[139] Bernard, Wang'ombe, and Kitindi (n 129).
[140] UN SDG, 'The 17 Goals' <https://sdgs.un.org/goals> accessed 28 December 2022.
[141] Gonçalves and Costa (n 13).
[142] Parrotta and others (n 126).
[143] Li and others (n 78).
[144] Christoph Böhringer, Jan Schneider, and Emmanuael Asane-Otoo, 'Trade in carbon and carbon tariffs' (2021) 78 Environmental and Resource Economics 669.
[145] Adeniyi Asiyanbi, and Jens Friis Lund, 'Policy persistence: REDD+ between stabilization and contestation' (2020) 27(1) Journal of Political Ecology 378, 380.

complexities of REDD+ and emphasise the need for more inclusive, transparent, and locally driven approaches to forest conservation and carbon offsetting.[146]

Another ethical concern arises from the risk that carbon offsetting projects may be implemented at the expense of economic prosperity in developing countries. REDD+ initiatives, for instance, often impose restrictions on forest access, disproportionately affecting vulnerable populations who depend on these resources for their livelihoods. The history of carbon sequestration projects also reveals a pattern of motivations that do not always align with genuine climate solutions. Carton and others argue that some countries have supported these projects primarily as a means to justify continued fossil fuel consumption while outsourcing their emissions reductions to developing nations.[147] This is evident in the strong backing for carbon sinks from countries that have historically obstructed progress in climate negotiations or have fossil-fuel-dependent economies.[148] For example, Norway has been a major proponent of carbon neutrality through offsets, as it allows the country to continue oil and gas extraction while compensating for emissions through forest conservation abroad.[149]

Structural and economic disparities further exacerbate the challenges of carbon trading. REDD+ which was founded by economists has nevertheless led to "underestimation of social and political obstacles to implementation."[150] This economic perspective led to many project failures by overlooking "contextual dynamics"[151] of local environments and situations leading to the exploitation of locals and exacerbating societal inequalities. Beyond this, possible economic gains from forest sequestration projects are rerouted back to the northern hemisphere.[152] While local livelihood is disrupted, energy prices rise due to carbon pricing, climate change exacerbates food and water insecurities, and local labour wages stagnate, this creates a "dissonance between expensive carbon and cheaper local inputs [which] creates both an obstacle and an opportunity".[153]

If the *wrong* decarbonisation policies and projects are implemented in the southern hemisphere, the local people may be exploited in multiple ways. In South Africa and Mozambique, for example, the unequal distribution of energy infrastructure throughout both countries causes *energy injustices*: social and economic gaps caused by unequal

[146] Rowan Alumasa Alusiola, Janpeter Schilling, and Paul Klär, 'REDD+ Conflict: Understanding the Pathways between Forest Projects and Social Conflict' (2021) 12(6) Forests 1.
[147] Carton and others (n 130).
[148] Martina Jung, 'The History of Sinks - an Analysis of Negotiating Positions in the Climate Regime' HWWA Discussion Paper No 293 (Hamburg Institute of International Economics 2004) 12.
[149] McDermott, Constance, Bhaskar Vira, Judith Walcott, Maria Brockhaus, Matthew Harris, Eric Mensah Kumeh, and Carolina de Mendonça Gueiros, 'The evolving governance of REDD+' in *Forests, Climate, Biodiversity and People: Assessing a Decade of REDD+* (IUFRO, Vienna 2022) 21.
[150] ibid 13.
[151] ibid 7.
[152] Bernard, Wang'ombe, and Kitindi (n 129).
[153] Frank Ackerman, 'Carbon Markets and Beyond: The Limited Role of Prices and Taxes in Climate and Development Policy' G-24 Discussion Paper Series No 53 (UNCTAD 2008) 8 <https://unctad.org/system/files/official-document/gdsmdpg2420084_en.pdf> accessed 20 June 2025.

access and accessibility due to costs of energy.[154] Disrupting local environments causes "marginalisation and rights abuses across many carbon forestry projects",[155] "maltreatment of indigenous peoples and their environment"[156], such as violent engagements, as seen in Uganda twice.

Lastly, corruption in combination with weak government structures creates adverse risk for investors and makes CDM projects unattractive, as well as hindering economic potential.[157] Due to all of this adverse risk, financing in African projects has been significantly limited.[158] This exacerbates challenges to creating ethical and meaningful decarbonisation strategies such as implementing renewable technologies and investments.

While these ethical dilemmas represent significant challenges to the legitimacy of carbon markets, emerging technological innovations offer potential pathways toward more transparent, efficient, and equitable trading systems.

4 Emerging trends and technologies

While emerging technologies may address certain transparency and verification challenges in carbon markets, they cannot resolve the fundamental incentive misalignments and ethical contradictions that plague these systems without radical structural reforms technologies offer promising but incomplete solutions to carbon market dysfunctions. Distributed ledger technologies, artificial intelligence, and advanced monitoring systems can enhance verification processes and market transparency, but must be integrated within robust regulatory frameworks and ethical standards. The fundamental challenge lies not in technological capability but in governance design that aligns market incentives with genuine climate protection.[159]

4.1 Technological innovation in service of monitoring

Digital technologies are widely considered essential for improving carbon trading market efficiency. Monitoring, reporting, and verifying (MRV) carbon emissions consumes significant time and results in the inflation of asset prices.[160] From a legal perspective, these verification challenges create fundamental questions about whether carbon credits

[154] Newell, Power, and Bulkeley (n 127).
[155] Carton and others (n 130) 12.
[156] Bernard, Wang'ombe, and Kitindi (n 129).
[157] ibid.
[158] Least Developed Countries Group and UN Climate Change Negotiations, "Least Developed Countries Group Calls for COP23 to Be a COP of Finance and Support," (*LDC Climate Change*, 2 November 2017) <https://www.ldc-climate.org/media_briefings/media-briefing-least-developed-countries-group-calls-for-cop23-to-be-a-cop-of-finance-and-support/> accessed 20 June 2025.
[159] Nicolò Barbieri, Alberto Marzucchi, Ugo Rizzo, 'Green technologies, interdependencies, and policy' (2023) 118 Journal of Environmental Economics and Management 1.
[160] Yadav Sapkota and John R White, 'Carbon Offset Market Methodologies Applicable for Coastal Wetland Restoration and Conservation in the United States: A Review' (2020) 701 Science of the Total Environment <https://www.sciencedirect.com/science/article/pii/S0048969719344882> accessed 7 September 2023.

represent legally enforceable claims to atmospheric resources. Verification difficulties undermine not only market efficiency but the legal standing of carbon credits as property rights, raising complex questions about liability for verification failures that current regulatory frameworks inadequately address.[161] Moreover, verification margin of error can reach nearly 100%, while conflicts of interest between auditors and project developers threaten the credibility of the entire process.[162]

A recent study by the World Bank concludes that the "widespread adoption of digital MRV systems – and the simplification of MRV process this enables – will greatly increase the efficiency of future carbon markets"[163] since they are superior to the current methods, which "can be costly, error-prone, and time-consuming, often relying on manual processes and in-person surveys".[164] The most evident area for applying digital technologies is the collection and verification of data. Simultaneously, digital MRV systems also could be linked to global or national registries to ensure compliance with reporting requirements. Many countries already use pilot systems to regulate their carbon markets.[165]

The available evidence provides a compelling reason to believe that digital technology has been revolutionising carbon markets; simultaneously, the adoption of digital MRV systems is still fragmentary and inconsistent owing to the diversity of various solutions. Sylvera, for example, is known as a universal framework for providing credible carbon credit ratings owing to the reliance on satellite and LiDAR data and modern artificial intelligence tools.[166]

Kazakhstan and Jordan use an alpha-version of the system for renewable energy designed by the EU Bank of Reconstruction and Development that utilises cloud computing and smart sensors to conduct the acquisition and processing of data in real time and automate verification procedures.[167]

Various countries are currently experimenting with digital systems, but none have adopted a single MRV system that would automate all the relevant processes across the carbon market infrastructure.[168]

---

[161] Jianfu Wang, Shiping Jin, Weiguo Bai, Yongliang Li, and Yuhui Jin, 'Comparative analysis of the international carbon verification policies and systems' (2016) 84 Natural Hazards 381.
[162] Richards and Huebner (n 25).
[163] Lucas Belenky, 'Carbon Markets: Why Digitization Will Be Key to Success' (*World Bank Blogs*, 16 August 2022) <https://blogs.worldbank.org/climatechange/carbon-markets-why-digitization-will-be-key-success> accessed 7 September 2023.
[164] World Bank, 'Digital Monitoring, Reporting, and Verification Systems and Their Application in Future Carbon Markets' (World Bank Group 2022) ii <http://hdl.handle.net/10986/37622> accessed 7 September 2023.
[165] ibid.
[166] Raúl C Rosales and others, 'Voluntary Carbon Markets in ASEAN: Challenges and Opportunities for Scaling Up' (Imperial College Business School 2021) <https://eprints.soas.ac.uk/35781/1/Green_Finance_COP26_Universities_Network_Policy_Report.pdf> accessed 20 June 2025.
[167] John C Shideler and Jean Hetzel, *Introduction to Climate Change Management: Transitioning to a Low-Carbon Economy* (Springer Nature 2021).
[168] Stephanie Mansourian, Amy E Duchelle, Carlos Sabogal and Bhaskar Vira, 'REDD+ Challenges and Lessons Learnt' in John Parrotta, Stephanie Mansourian, Christoph Wildburger and Nelson Grima (eds), *Forests, Climate, Biodiversity and People: Assessing a Decade of REDD+* (IUFRO, Vienna 2022).

Unfortunately, however, the integration of digital technologies into carbon markets occurs in an inconsistent manner. The World Bank cites various MRV systems, including those focusing on mitigation action, support, or monitoring of GHG emissions over time. The development of holistic digital MRV systems is currently inhibited by numerous barriers, such as high costs of technologies, the lack of capacity for adopting new technologies, and concerns related to the capture of highly sensitive data.[169] The successful implementation of innovative technologies could help address most problems faced by carbon markets and ensure automated reporting, reliable monitoring, and streamlined verification. However, it seems that most stakeholders are currently not prepared for the wide-scale implementation of digital MRV systems.

The carbon trading market has been embracing an increasing number of other innovative technologies as well. Many of them are connected with artificial intelligence (AI) and satellite imagery. For example, the company Albo Climate monitors and measures performance of carbon sequestration sustainability projects with the help of deep learning.[170] The scalability of carbon removal offered by the startup could lower the costs of monitoring and potentially make the monitoring process more efficient. Pachama and NCX, in turn, are creating AI-powered carbon offset markets focusing on forestation projects by estimating carbon offsets and ensuring credibility of projects via sensors, aerial imagery, and computer vision.[171] AI applications also are used to track the overall material embodied carbon emissions, something that is hard to estimate manually; moreover, they are often utilised to optimise the use of machinery on project sites and monitor emissions produced by equipment.[172] As a result, companies can determine their needs for carbon offsets based on credible emission data. Watson recently reported that S&P Global Platts plans to launch AI-driven carbon credit indices to increase transparency of the market and simplify the evaluation of projects' co-benefits.[173] The examples above illustrate that AI and other technologies have been revolutionising carbon credit markets, contributing to transparency and efficiency.

4.2 Blockchain and distributed ledger technologies

The carbon market challenges detailed in previous sections—from fraud and double counting to verification difficulties and lack of transparency—highlight the need for

[169] World Bank (n 164).
[170] Albo Climate official site <https://www.albosys.com> accessed 8 April 2023.
[171] Bob Toews, 'These Are The Startups Applying AI To Tackle Climate Change' (*Forbes*, 20 June 2021) <https://www.forbes.com/sites/robtoews/2021/06/20/these-are-the-startups-applying-ai-to-tackle-climate-change/> accessed 7 September 2023.
[172] Gary Ng and others, 'The Concept of "Carbon Credit" in the Construction Industry: A Case Study of viAct's Scenario Based AI in Carbon Credit Management' (2022) 11 International Journal of Business and Management Invention (IJBMI) 50.
[173] Frank Watson, 'S&P Global Platts to Launch AI-Driven Carbon Credit Indices' (*S&P Global Commodity Insights*, 24 February 2021) <https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/coal/022421-sampp-global-platts-to-launch-ai-driven-carbon-credit-indices> accessed 7 September 2023.

innovative solutions that can enhance market integrity. Distributed Ledger Technology (DLT) has emerged as a promising approach to address many of these fundamental issues simultaneously.

Carbon markets fundamentally operate as information systems that track credits, verify emissions reductions, and facilitate transactions. The core challenges these markets face—lack of transparency, vulnerability to fraud, double counting, and verification difficulties—are precisely the types of problems that distributed ledger technologies were designed to solve. By creating immutable, transparent records that can be verified by all participants without requiring trust in a central authority, DLT offers a technological foundation that aligns with the requirements of effective carbon trading.

Before examining the application of DLT to carbon markets, it is important to understand its fundamental principles. At its core, DLT refers to a digital system that records transactions of assets and their details in multiple places simultaneously. Unlike traditional databases controlled by a single entity, DLTs distribute identical copies of the ledger across a network of computers (nodes), with each participant maintaining their own copy that is updated through consensus.

Blockchain is the most well-known type of DLT. It organises data into digital blocks that are cryptographically linked in a chronological digital chain. This structure creates several key characteristics that make it valuable for carbon markets: 1) Immutability: Once recorded, data cannot be altered without changing all subsequent blocks, making fraudulent manipulation extremely difficult. 2) Transparency: All authorised participants can view the entire transaction history, enabling verification without requiring trust in a central authority. 3) Traceability: Every transaction is permanently recorded with timestamps, allowing complete tracking of assets (such as carbon credits) throughout their lifecycle. And, 4) Smart contracts: These are self-executing agreements with terms directly written into code that automatically execute actions when predetermined conditions are met, potentially reducing administrative costs and enabling automated compliance.

When applied to carbon markets, these features can address critical challenges by providing transparent tracking of emissions and credits, preventing double-counting, automating verification processes, and enabling trustworthy peer-to-peer trading without intermediaries. The sections that follow examine how these capabilities can be leveraged to transform carbon market operations at both infrastructural and operational levels.

Given this, in general, DLT applications align well with the transparency and reliability requirements set forth in UNFCCC regulations for climate change action. Grounded in the Paris Agreement, Article 13 mandates enhanced transparency to support the objectives of Article 2, which aims to limit global temperature rise to well below 2 degrees Celsius.[174]

[174] 'Transparency of Support under the Paris Agreement' (*United Nations Framework Convention on Climate Change (UNFCCC)*) <https://unfccc.int/topics/climate-finance/workstreams/transparency-of-support-ex-post/transparency-of-support-under-the-paris-agreement> accessed 16 March 2023; Macinante (n 2); 'Key Aspects of the Paris Agreement'

The Conference of the Parties (COP) created the Capacity-building Initiative for Transparency (CBIT).[175]

During COP21, three primary objectives were established: **(1)** strengthening national institutions for transparency-related activities in alignment with national priorities, **(2)** providing relevant tools, training, and assistance to meet the transparency provisions outlined in Article 13 of the Paris Agreement, and **(3)** facilitating the continuous improvement of transparency over time.[176] However, this push for enhanced transparency must not come at the expense of national rights and sovereignty. Unfortunately, the Kyoto Protocol fell short of Article 13's expectations,[177] as the International Transaction Log (ITL) has been criticised for its lack of public accessibility and the presence of legal loopholes that have been exploited for financial gain across markets.[178]

The core principles of any effective carbon market should be: (1) to ensure and enhance the transparency of climate change data including the carbon market while not imposing on national sovereignty in accordance with Article 13;[179] (2) transparency of data measured by Measurement, Reporting and Verification (MRV) processes should include its location, disclosure, and accessibility[180] which will enhance the efficacy and security of

(*United Nations Framework Convention on Climate Change (UNFCCC)*) <https://unfccc.int/most-requested/key-aspects-of-the-paris-agreement> accessed 16 March 2023; 'Financial Intermediary Funds (FIFs)' (*The World Bank*, 2023) <https://fiftrustee.worldbank.org/en/about/unit/dfi/fiftrustee/fund-detail/cbit> accessed 16 March 2023.

[175] Macinante (n 2).

[176] 'Financial Intermediary Funds (FIFs)' (n 174).

[177] Macinante (n 2).

[178] Alastair Marke, Max Inglis and Constantine Markides, 'Emerging Technologies and Their Applicability to Solving Challenges in the Carbon Markets: An Overview' in Alastair Marke, Fabiano de Andrade Correa and Michael Mehling (eds), *Governing Carbon Markets with Distributed Ledger Technology* (Cambridge University Press 2022) <https://www.cambridge.org/core/books/governing-carbon-markets-with-distributed-ledger-technology/emerging-technologies-and-their-applicability-to-solving-challenges-in-the-carbon-markets-an-overview/3146E5BBD0A13810BC0070367F8BABBF> accessed 16 January 2023; Steffen Boehm and Siddharta Dabhi, *Upsetting the Offset: The Political Economy of Carbon Markets* (MayFly Books 2009) <http://mayflybooks.org/?page_id=21> accessed 6 September 2023; Deloitte (n 74); Gillenwater and others (n 99); Lambert Schneider and others, 'Double Counting and the Paris Agreement Rulebook' (2019) 366 Science 180; Lambert Schneider, Anja Kollmuss and Michael Lazarus, 'Addressing the Risk of Double Counting Emission Reductions under the UNFCCC' (2015) 131 Climatic Change 473; Katherine Nield and Ricardo Pereira, 'Fraud on the European Union Emissions Trading Scheme: Effects, Vulnerabilities and Regulatory Reform' (2011) 20 European Energy and Environmental Law Review 255; 'MTIC (Missing Trader Intra Community) Fraud' (*Europol*, 2022) <https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/economic-crime/mtic-missing-trader-intra-community-fraud> accessed 7 September 2023; Betz and others (n 84).

[179] 'Transparency of Support under the Paris Agreement' (n 174); 'Key Aspects of the Paris Agreement' (n 174); 'Financial Intermediary Funds (FIFs)' (n 174).

[180] Michael A Mehling, 'Governing the Carbon Market' in Alastair Marke, Fabiano de Andrade Correa and Michael Mehling (eds), *Governing Carbon Markets with Distributed Ledger Technology* (Cambridge University Press 2022) <https://www.cambridge.org/core/books/governing-carbon-markets-with-distributed-ledger-technology/governing-the-carbon-market/C8528231958BFAC44975D649143EB9CF> accessed 16 January 2023.

the carbon markets;[181] (3) lastly, is to ensure the outcomes of implementing a market strategy is aligned with Article 2 and Article 4 of the Paris Agreement.[182]

Today, many carbon markets, including the European Union Emissions Trading System (EU ETS), are considered linked markets, as they operate based on agreements negotiated among 30 participating countries. These negotiations are often lengthy and complex, with evolving national interests influencing the terms. As a result, certain parties may benefit more than others, creating an imbalance in the system.[183]

The applicability of DLT can be analysed from two perspectives: external (infrastructure) and internal (operational).

Externally, DLT, artificial intelligence (AI), and the internet of things (IoT) can create a networked carbon market (NCM) using the structures and models of DLT. The NCM is not an overarching market but rather the infrastructure to allow transparency of trading between markets.

The regulatory framework for a networked carbon market (NCM) consists of five key components as described by Macinante: First, the market infrastructure establishes the foundation for interoperability between carbon markets. Second, clear rules for distributed ledger operations govern the functionality and management of the DLT system. Third, operational mechanisms are required to ensure market efficiency, including a valuation mechanism to account for differences in mitigation efforts across jurisdictions and a transaction mechanism to facilitate seamless exchanges. Fourth, transactional rules provide a regulatory framework to ensure compliance, security, and efficiency in market transactions. Finally, participants operate at different levels, including jurisdictional, cross-jurisdictional, and supra-jurisdictional entities, ensuring broad market participation and governance.[184]

DLT models can effectively mitigate key security risks in carbon markets, as identified by Marke and others.[185] The first major risk, cybercrime, can be addressed through the Doorkeeper Model, which enhances cybersecurity within the EU ETS. Under this model, all servers hosting EU ETS accounts would subscribe to multiple antivirus software solutions on a blockchain, leveraging thousands of scanning engines for collective protection. Unlike traditional bug bounty programs, blockchain enables a collaborative yet competitive

[181] Chunhua Ju and others, 'A Novel Credible Carbon Footprint Traceability System for Low Carbon Economy Using Blockchain Technology' (2022) 19 International Journal of Environmental Research and Public Health 1; Mehling (n 180); Nicholas Scott, Sai Nellore and Alastair Marke, 'DLT and the Voluntary Carbon Markets' in Alastair Marke, Fabiano de Andrade Correa and Michael Mehling (eds), *Governing Carbon Markets with Distributed Ledger Technology* (Cambridge University Press 2022) <https://www.cambridge.org/core/books/governing-carbon-markets-with-distributed-ledger-technology/dlt-and-the-voluntary-carbon-markets/C14F0FA68EAF61E41696804EF4FAAE7E> accessed 18 January 2023.
[182] 'Key Aspects of the Paris Agreement' (n 174).
[183] Macinante (n 2).
[184] ibid.
[185] Marke, Inglis and Markides (n 178).

cyber-protection network by integrating prediction markets with proof-of-work, offering broader and faster coverage against cyber threats.[186]

The second security risk involves fraudulent trading and identity verification, which can be mitigated through the Know Your Customer (KYC) Model. Carbon markets have been exploited for financial gain, notably through VAT fraud schemes like missing-trader fraud, where perpetrators manipulate interjurisdictional trades to receive undue VAT allowances.[187] Implementing a blockchain-based KYC model would enhance user authentication, ensuring that only legitimate participants engage in carbon trading, thereby increasing transparency and reducing the risk of market abuse.[188]

Lastly, the risk of ensuring the fulfilment of contractual obligations can be mitigated through a four-trigger smart contract verification process. When applying DLT to existing Emissions Trading Systems (ETS) to enhance MRV capabilities, these four triggers play a crucial role.

The first trigger integrates with the Know Your Customer (KYC) model to verify that the entity interacting with the blockchain is authorised to conduct a transaction. The second trigger ensures that the party has the necessary resources, such as the required currency, to fulfil the contractual obligations. Once these conditions are validated, the third trigger introduces a security safeguard by delaying contract execution momentarily, allowing artificial intelligence to scan the server for potential threats. Finally, the fourth trigger verifies compliance with both jurisdictional and interjurisdictional regulations to ensure that all transactions adhere to the applicable legal frameworks.[189]

As trading volumes increase, interactive traceability models—which combine off-chain traceability with on-chain verification—will become essential for tracking carbon assets efficiently. Furthermore, blockchain's ability to enhance supply chain visibility will improve CO2 emissions tracing and management.[190] Ultimately, by leveraging DLT, carbon markets can achieve greater transparency, security, and regulatory compliance, fostering a more reliable and equitable system for climate action.

Building on these technological foundations, we can envision a transformed carbon market architecture that addresses the fundamental challenges identified throughout this analysis while creating new opportunities for market evolution.

[186] Marco Zolla, Alastair Marke and Michael A Mehling, 'DLT and the European Union Emissions Trading System' in Alastair Marke, Fabiano de Andrade Correa and Michael Mehling (eds), *Governing Carbon Markets with Distributed Ledger Technology* (Cambridge University Press 2022) <https://www.cambridge.org/core/books/governing-carbon-markets-with-distributed-ledger-technology/dlt-and-the-european-union-emissions-trading-system/ED9E775E0B93E173650FD989CA9D9D62> accessed 16 January 2023.
[187] Betz and others (n 84).
[188] Scott, Nellore and Marke (n 181); Zolla, Marke and Mehling (n 186).
[189] Zolla, Marke and Mehling (n 186).
[190] Pu Wang and others, 'Key Challenges for China's Carbon Emissions Trading Program' (2019) 10(5) WIREs Climate Change 1.

4.3 21st Century carbon markets: transparency, efficacy & effectiveness

The challenges and emerging technologies outlined in the previous sections create an opportunity to redesign our conceptual understanding of carbon pricing and the structure and operations of carbon markets. The carbon market reformation must fulfil the economic, financial, political, social, geographic, and environmental dimensions of climate change in order to be deemed successful.[191] Emissions are conceptually difficult since their environmental consequences cannot be traced to a single source or individual. Furthermore, the catalysts of climate change are dispersed throughout a range of industries and therefore it is important that adaptability and scalability be core principles to any policy solution.[192]

Since carbon markets and offsetting require a well-structured foundation to function effectively, an effective carbon market must incorporate six essential components. First, it must establish an efficient financial market to facilitate carbon trading. Second, it should adhere to sound economic principles that ensure market stability and fairness. Third, incentivising global cooperation and encouraging participation from diverse forms of government is crucial for widespread adoption. Fourth, the market must discourage malicious political behaviour that could undermine its integrity. Fifth, upholding ethical standards is essential, including preventing energy injustices, promoting socioeconomic equality, and aligning with the United Nations Sustainable Development Goals (SDGs).[193] Finally, and most importantly, the market must provide a mechanism for achieving the objectives of Paris Agreement Articles 2 and 4 while ensuring compliance with Article 13, which mandates data transparency without infringing on national sovereignty[194].

4.4 Reconceptualising carbon assets and liabilities

To meet these foundational goals, improvements in monitoring, reporting, and verification (MRV) are necessary. This can be achieved through the application of converging technologies such as the Internet of Things (IoT), artificial intelligence (AI), and DLT. These technologies have the potential to create a networked carbon market (NCM) that would function as a global financial market, enhancing transparency and efficiency.[195] However, a fundamental ambiguity in carbon markets lies in the 209tandardized209tion of carbon itself. The Harvard Business Review has described carbon

[191] Yizhang He and Wei Song, 'Analysis of the Impact of Carbon Trading Policies on Carbon Emission and Carbon Emission Efficiency' (2022) 14(16) Sustainability 1; Macinante (n 2); Gareth Bryant, *Carbon Markets in a Climate-Changing Capitalism* (Cambridge University Press 2019) <https://www.cambridge.org/core/books/carbon-markets-in-a-climatechanging-capitalism/2799AE2678141AC4B9C91027EAD63520> accessed 11 January 2023; Benjamin K Sovacool and others, 'Decarbonization and Its Discontents: A Critical Energy Justice Perspective on Four Low-Carbon Transitions' (2019) 155 Climatic Change 581.
[192] Mehling (n 180).
[193] 'Sustainable Development Goals' (*United Nations Development Programme (UNDP)*) <https://www.undp.org/sustainable-development-goals> accessed 5 April 2023.
[194] 'Key Aspects of the Paris Agreement' (n 174).
[195] Macinante (n 2).

as a liability in one article,[196] while referring to carbon credits as an asset in another,[197] highlighting the inconsistencies in market perception. This discrepancy can be resolved through the deployment of an NCM, which would provide a standardised framework for defining and valuing carbon within financial and regulatory systems.

Networked Carbon Markets were originally introduced by the World Bank Group (WBG) in 2013 to allow interjurisdictional carbon trading without infringing on the nationally and regionally instituted carbon markets. Local carbon markets would be able to "opt in" to the interjurisdictional network with minimal conditions. As the concept of NCMs were ahead of its time, today's contemporary technologies were not mentioned in the WBG report.[198] In 2018, Marke introduced the application of DLT to create a NCM[199] while Macinante in 2020 further developed to suggest the converging power of AI and IoT to this carbon trading web.[200] Our policy proposal for creating optimal carbon markets aligns with the six principles outlined above and have three components: carbon pricing reformation, microgrids, and an interjurisdictional network. Their functioning and operations of these three components require DLT, IoT, and AI technologies to ensure the transparency and efficacy of carbon markets.

Carbon as a traded entity is unique in that carbon emissions are a liability while the carbon credits derived from those emissions are traded as assets.[201] Utilising and furthering this concept allows us to define carbon credits as a financial derivative of carbon. When conceptualising carbon in this way, pricing factors can reflect the *true* value of carbon accounting for the quantity of carbon emissions and mitigated; supply and demand; and socioeconomic, economic, and political factors. The price on carbon is not merely the amount of carbon reduced or emitted in quantity, but the quality of that carbon.

This concept of quantity versus quality of carbon reflected in its price is essential for the optimisation of carbon markets and ethical oversight of its functioning. The quantity looks at carbon as a liability and is established as the value per one ton of carbon dioxide equivalent.[202] The quality of carbon pricing fixed into the derivative value of carbon

[196] Robert G Eccles and John Mulliken, 'Carbon Might Be Your Company's Biggest Financial Liability' [2021] *Harvard Business Review* <https://hbr.org/2021/10/carbon-might-be-your-companys-biggest-financial-liability> accessed 5 April 2023.
[197] Alex Rau and Robert Toker, 'Start Thinking About Carbon Assets—Now' [2008] *Harvard Business Review* <https://hbr.org/2008/09/start-thinking-about-carbon-assets-now> accessed 5 April 2023.
[198] 'Globally-Networked Carbon Markets: 1st Working Group Meeting' <https://www.worldbank.org/content/dam/Worldbank/document/SDN/networked-carbon-markets-WG1.pdf> accessed 5 April 2023.
[199] Alastair Marke (ed), *Transforming Climate Finance and Green Investment with Blockchains* (1st edn, Academic Press 2018).
[200] Macinante (n 2).
[201] Eccles and Mulliken (n 196).
[202] 'Carbon Pricing Dashboard' (*World Bank Group*) <https://carbonpricingdashboard.worldbank.org/what-carbon-pricing> accessed 6 April 2023.

credits integrates: (1) *Social Value of Mitigation Activities* (SVMA),[203] (2) economic condition and a sovereignty's degree of contribution to emissions, (3) reliability and transparency rating of a carbon market's jurisdiction, (4) term and stability of mitigation action,[204] (5) and supply and demand of carbon credits within the jurisdiction. These factors are in alignment with Section 108 of the UNFCCC Paris Agreement which states that the Conference of the Parties, "*Recognizes* the social, economic and environmental value of voluntary mitigation actions and their co-benefits for adaptation, health and sustainable development".[205] The price of carbon at a given jurisdiction can be the result of pure supply and demand while the carbon credits' conversion rate between two jurisdictions will reflect the quality of carbon with the listed factors.

4.5 Networked market architectures

If carbon markets are to be maintained despite their fundamental flaws, networked approaches using DLT applications might at least address certain transparency issues, though they would not resolve the deeper problems of misaligned incentives and global inequity. This framework would enable jurisdictions to participate in the networked carbon market and engage in global credit trading while preserving national sovereignty in accordance with Article 13 of the Paris Agreement. Participation would require only acceptance of the network's basic operational terms rather than complex bilateral agreements between countries.[206] These terms can be enforced through "smart contract-based transactions peer-to-peer, in this case, across jurisdiction".[207] Smart contracts enable a consensus and agreement of the conversion rate mechanisms in order to trade over the network between jurisdictions and peer-to-peer (P2P) increasing the efficacy and volume of carbon trading by removing the intermediaries.

While the carbon pricing conversion rates between microgrids would be seamless and transparent with DLT benefits of decentralised data and smart contracts, a growing focus is on the voluntary market, prosumers, and P2P trading.[208] The adaptability of the global NCM to many carbon markets is crucial to developing a truly sustainable and transparent framework for a financial network with the goal of attaining net zero. While a 2016 World Bank report stated that the three major challenges of creating a NCM are allocating of emissions, allowing 'heterogeneity' in the design of connecting carbon markets, and

[203] Jean-Charles Hourcade, Antonin Pottier and Etienne Espagne, 'Social Value of Mitigation Activities and Forms of Carbon Pricing' (2018) 155 International Economics 8.
[204] Scott, Nellore and Marke (n 181).
[205] 'Paris Agreement' (n 108).
[206] 'Key Aspects of the Paris Agreement' (n 174).
[207] Macinante (n 2) 108.
[208] Ju and others (n 181); Weiqi Hua and others, 'A Blockchain Based Peer-to-Peer Trading Framework Integrating Energy and Carbon Markets' (2020) 279 Applied Energy 1.

challenges to the transparency of data.[209] A DLT structured NCM would neutralise the latter two issues. By having infrastructure in place allowing the conversion of carbon units between jurisdictions based on agreed upon methodologies will enable the allocation of emissions with robust accounting to allow for better market efficiency, and private sector and the evolving prosumer market participation.[210] This would allow any jurisdiction to enter the networked carbon market and trade globally while not infringing on national sovereignty in alignment with Article 13[211] while only agreeing to the terms of use allowing "smart contract-based transactions peer-to-peer, in this case, across jurisdiction".[212]

Under this paradigm, individual carbon markets could continue to evolve and govern themselves while being able to participate in the NCM to trade between jurisdictions. Even though the goal of all carbon markets is unified, their local needs are different in terms of who is participating and the most effective implementation. Whether it is individuals trading on the voluntary market or prosumers connected to smart electrical grids or large sector-varying corporations, it is important that jurisdictions create legislation and carbon markets fitting for the users on that carbon market. He and Song suggested the most effective implementation of carbon markets is per industry.[213] Prosumer markets require different legislation and governance than manufacturers to participate in carbon neutralisation.

Microgrids and jurisdictional trading would be connected by the DLT infrastructure, ensuring transparency, accountability, and efficacy of carbon markets.[214] The NCM must consider the varying carbon accounting (reliability) and carbon valuing practices. The NCM would consist of three levels, including interjurisdictional, which contains the five principles above, jurisdictional, which are the independent carbon markets, and the intra-jurisdictional levels containing individual traders, prosumers, consumers, and organisations. The responsibility of the interjurisdictional ledger is to be a registry holding all information from all jurisdictions with transparent oversight and ensure the agreed upon data reporting. Part of the terms agreed to by participants to join the NCM is "accepting the rules, infrastructural arrangements, and other measures".[215] These terms would be the same for any jurisdiction wishing to participate in the NCM and "the agreement is not between jurisdictions, as such, but rather between the joining jurisdiction and the network."[216] This system serves a multitude of functions: (1) minimising misaligned political motivations and imbalance of power in negotiations, (2)

[209] 'The Networked Carbon Markets Initiative' (World Bank Group Climate Change 2016) <https://thedocs.worldbank.org/en/doc/162841457735232763-0020022016/original/NCMinitiativepitchbook.pdf> accessed 16 March 2023.
[210] Macinante (n 2); Hua and others (n 208).
[211] 'Key Aspects of Paris Agreement' (n 174).
[212] Macinante (n 2) 108.
[213] He and Song (n 191).
[214] Macinante (n 2).
[215] ibid 95.
[216] ibid.

allow flexibility for jurisdictions to leave or enter the network without disrupting the carbon price or functioning of the network, (3) transference of carbon credits would not be necessary and result in less accounting fiascos.

Ideally, the network will be fully distributed throughout all individual participants and allow for full transparency. This means all historical transactions within the jurisdictions across the network would be accessible by all parties and even the public. However, multiple technical challenges occur when attempting a fully distributed system regarding computing, memory, and processing capacity; and the incongruency of updating times between nodes in geographically different places. This last aspect becomes increasingly important as the network grows.[217]

Currently, two solutions to the technological limitations are mentioned. First, is the integration of 6G in the carbon market supply chain, which is expected to be rolled out for commercial use within the decade. Compared to 5G, it would allow for 50x the data rate and 100x the mobile traffic capacity, and large blockchain connected networks to function seamlessly.[218] Another potential solution is to have full transactional histories stored at the administrator or jurisdictional level while at the individual level holds only historical transactions up to a certain backdate[219] or only in the jurisdiction.

NCM is a solution to the current weaknesses inherent in the design of carbon trading and offsetting. By taking advantage of emerging technologies in AI, DLT, and IoT, carbon markets would be able to function independently while interacting seamlessly. Here we further the idea of NCM. The core idea of integrating emerging technologies into the markets is to increase the MRV for transparency.[220]

The process begins with tracking and monitoring carbon emissions and mitigation activities through sensor technology in the IoT. These technologies can be satellite imagery in combination with AI,[221] smart meters, and aerial imagery with computer vision.[222] DLT cannot guarantee the credibility of the data collected, only the security and transparency of what is collected.[223] After collecting reliable data, it is held on the DLT infrastructure to ensure robust accounting. AI will filter information and crosscheck it throughout the tamperproof network in order to avoid double counting and fraudulent activities.[224] Using smart contracts for transactions of carbon credits through different jurisdictions on the DLT will allow track record keeping. Altogether these technologies will enable the next century carbon market and offsetting.

[217] Macinante (n 2).
[218] Dinh C Nguyen and others, '6G Internet of Things: A Comprehensive Survey' (2022) 9 IEEE Internet of Things Journal 359.
[219] Macinante (n 2).
[220] World Bank (n 164).
[221] Rosales and others (n 166).
[222] Toews (n 171).
[223] Marke, Inglis and Markides (n 178).
[224] Mehling (n 180).

Succinctly: The integration of Distributed Ledger Technology, artificial intelligence, and the Internet of Things into carbon markets presents a transformative opportunity to address longstanding challenges in transparency, efficiency, and scalability. NCMs build upon previous efforts by the World Bank Group and recent advancements in emerging technologies to create an interjurisdictional framework that enhances market functionality without infringing on national sovereignty. By establishing a decentralised yet interconnected system, the NCM would enable seamless carbon trading while maintaining jurisdictional autonomy and ensuring robust monitoring, reporting, and verification.

Through smart contracts and decentralised infrastructure, the NCM offers a solution to existing inefficiencies, including political imbalances, fraudulent trading practices, and inconsistent carbon valuation methodologies. The ability to differentiate between carbon as a liability and carbon credits as assets enhances the market's ability to price carbon more accurately based on both quantity and quality. Additionally, the system's adaptability ensures that various stakeholders—from governments and corporations to prosumers and individual traders—can participate effectively.

As carbon markets continue to evolve, the integration of advanced technologies like 6G and AI-driven verification will further enhance market reliability and scalability. By leveraging a fully transparent and tamper-proof DLT infrastructure, carbon markets can transition toward a more accountable, secure, and equitable trading system that aligns with the objectives of the Paris Agreement and the United Nations Sustainable Development Goals (SDGs).

For technological solutions to effectively transform carbon markets, they must be accompanied by coordinated regulatory reforms across three domains. First, standardisation of verification protocols through an international body similar to the IPCC could establish clear, science-based criteria for carbon credit validation. This would include consistent methodologies for establishing baselines, measuring additionality, and quantifying leakage effects across all market mechanisms. Second, harmonised legal frameworks must clarify the legal status of carbon assets, define liability for verification failures, and establish cross-jurisdictional enforcement mechanisms. This requires development of model legislation that countries can adopt with appropriate local modifications while maintaining core principles. Such frameworks should explicitly address the legal status of digitally-verified carbon credits, recognise smart contracts in carbon transactions, and establish clear recourse mechanisms for disputes. Third, governance reforms must shift from purely market-based oversight toward hybrid public-private governance structures with meaningful participation from affected communities. This includes establishing independent verification authorities with proper resources, whistleblower protections for reporting fraud, and transparent processes for challenging credit validity. These reforms should be phased in gradually with appropriate transition

periods to avoid market disruption while ensuring steady progress toward improved integrity.

Beyond these broad regulatory directions, specific governance architectures are needed to operationalise the oversight of technological solutions in carbon markets. Effective implementation of technological solutions requires governance structures specifically designed to align technological capabilities with market integrity goals.

We propose a three-tiered governance framework to ensure technology actually improves carbon market outcomes rather than simply digitising existing problems. At the technical layer, open standards bodies comprising climate scientists, technology experts, and market participants should develop and maintain protocols for monitoring, reporting, and verification. These standards must include rigorous data quality requirements, interoperability specifications, and minimum performance criteria for verification systems. Critical to this layer is the requirement that all verification algorithms be transparent and auditable, avoiding "black box" solutions that obscure decision-making. At the market operation layer, independent certification authorities should evaluate technological solutions against these standards, with rotational oversight to prevent regulatory capture. These authorities would be empowered to suspend non-compliant systems and require regular security audits. Importantly, this layer should include mandatory transparency requirements for all verification decisions, including machine learning audit trails. At the accountability layer, a combination of judicial oversight, civil society monitoring, and affected community representation should provide checks and balances on the entire system. This includes specialised arbitration mechanisms for disputes, regular public reporting requirements, and formal channels for indigenous and local communities to challenge credits that affect their territories. By ensuring technology serves climate goals rather than merely creating new profit centres, this governance framework transforms carbon markets into genuine climate solutions rather than technological shortcuts around fundamental market flaws.

4.6 Implementation and technical challenges

While technological and governance innovations offer promising pathways for carbon market reform, a clear-eyed assessment of their limitations is essential for realistic implementation. Despite their potential, distributed ledger technologies and other digital solutions face significant hurdles that must be addressed through coordinated global action.

Implementation challenges include technical and structural barriers. The energy consumption of proof-of-work blockchain protocols presents an ironic contradiction for climate-focused applications, though newer consensus mechanisms are substantially reducing this footprint. More fundamentally, the "garbage-in, garbage-out" problem persists: while blockchain ensures data immutability, it cannot independently verify the

accuracy of input data from physical monitoring systems. This limitation is particularly relevant for carbon markets where verification of real-world emissions reductions remains problematic.

Regulatory and accessibility barriers further complicate adoption. Significant legal uncertainty persists regarding the status of smart contracts and blockchain-based carbon assets across jurisdictions. Additionally, the infrastructure and technical expertise required for implementation may create new forms of inequality, potentially excluding developing nations with limited digital infrastructure—the very countries that should benefit most from improved carbon market mechanisms. The substantial cost of transitioning existing markets to DLT systems requires coordination among numerous stakeholders with competing interests.

Addressing these challenges demands a comprehensive approach including thoughtful governance frameworks, technical standards development, capacity building initiatives, and regulatory clarity. Success ultimately depends on ensuring that technological solutions enhance market integrity rather than merely digitising existing inequities, while promoting a just and sustainable economic framework for meaningful climate action.

4.7 Policy recommendations for carbon market reform

Based on our analysis of structural flaws in current carbon trading systems, we propose the following concrete policy recommendations for key stakeholders. Drawing on our analysis of carbon market structural deficiencies, we propose targeted interventions across international, national, and private sector domains.

At the international level, we advocate establishing a unified blockchain-based global carbon registry to prevent double-counting, implementing standardised science-based additionality methodologies that accommodate regional contexts, and mandating environmental justice assessments for significant offset projects. National regulators should implement progressively rising carbon price floors (5% annually above inflation) to incentivise direct emissions reductions, create regulatory sandboxes for verifying new monitoring technologies against gold-standard measurements, and develop clear liability frameworks that distribute responsibility proportionally among verifiers, developers, and credit purchasers. For market participants, we recommend adopting tiered disclosure requirements (Platinum/Gold/Silver/Bronze) based on verification strength and co-benefits, committing to phase out low-quality credits by 2027 with clear interim targets, and establishing a technology transfer fund (funded by at least 2% of transaction value) to ensure developing nations can access advanced monitoring capabilities. These recommendations work synergistically to address verification challenges, market integrity concerns, and ethical considerations while recognising stakeholders' differing capacities and responsibilities—ultimately transforming carbon markets into more effective climate mitigation instruments.

4.8 Addressing potential counterarguments

Our analysis has presented a critical assessment of carbon market flaws, but several counterarguments deserve serious consideration. First, proponents may argue that despite their imperfections, carbon markets remain the most politically feasible mechanism for pricing carbon in many jurisdictions. They contend that theoretical perfection should not be the enemy of practical progress, and that incremental improvements within market frameworks are more realistic than wholesale alternatives.

While we acknowledge the political constraints, our analysis demonstrates that flaws in current carbon markets are structural rather than incidental, requiring fundamental reforms rather than mere technical adjustments. Second, some may argue that technological fixes like blockchain-based monitoring can resolve most verification challenges without requiring deeper market restructuring. This techno-optimism, while understandable, underestimates how technological solutions themselves are shaped by existing power dynamics and market incentives. Without corresponding governance reforms, technologies may simply entrench existing inequities with a veneer of digital certainty. Technology can enable verification improvements, but cannot substitute for proper institutional oversight.

Third, defenders of current carbon market frameworks might point to successful emissions reductions in specific sectors or regions as evidence that markets can work effectively. The EU ETS, for instance, has contributed to emissions reductions in the power sector after initial design flaws were addressed. However, these limited successes must be weighed against the broader pattern of verification failures, perverse incentives, and environmental justice concerns documented in our analysis. Sector-specific successes do not negate systemic problems across global carbon markets.

Finally, some economists may contend that market inefficiencies will naturally correct themselves as carbon prices rise and participants demand greater integrity. This view overstates markets' self-correcting capabilities in the context of fundamental information asymmetries, regulatory fragmentation, and power imbalances that characterise current carbon trading systems. The climate crisis demands more deliberate, equity-centred reforms rather than faith in eventual market corrections. By addressing these counterarguments directly, we strengthen our case for comprehensive carbon market reform while acknowledging legitimate concerns about implementation challenges.

The evidence examined in this paper suggests that carbon markets in their current form function primarily as financial mechanisms that enable continued emissions rather than as instruments for meaningful climate action. While technological and governance reforms may improve certain aspects, addressing climate change will require moving beyond market-based approaches to more direct regulatory interventions and fundamental economic transformation. The path forward lies not in abandoning market mechanisms

entirely, but in transforming them from potentially exploitative financial instruments into genuine tools for climate mitigation and environmental justice.

5 Conclusions and future outlook

Current carbon market frameworks exhibit critical structural limitations that compromise their effectiveness as climate change mitigation tools. Our analysis identifies three interconnected challenges undermining market integrity: regulatory fragmentation creating enforcement gaps, verification deficiencies compromising credit quality, and inequitable distributional impacts. These issues represent fundamental tensions between market-driven approaches and environmental imperatives, revealing systemic contradictions that require integrated solutions.

The ethical dimensions of carbon markets are particularly concerning. Our research demonstrates how existing frameworks disproportionately burden developing nations, perpetuating global inequities rather than addressing them. While equity considerations demand that developed countries shoulder a larger share of emissions reductions due to their historical responsibility, environmental effectiveness necessitates broader participation, including from developing nations whose rising emissions are increasingly significant.[225] Carbon offset projects in the Global South often prioritise economic expediency over meaningful environmental progress and social justice, undermining the markets' purported objectives.

Our policy recommendations focus on three essential domains: regulatory harmonisation, technological integration, and ethical oversight. Carbon markets operate at the nexus of environmental science, legal frameworks, market economics, and ethical considerations—with tensions between these domains creating vulnerabilities that compromise effectiveness. The identified regulatory inconsistencies raise fundamental questions about governing atmospheric commons across jurisdictional boundaries, while verification challenges reveal epistemological concerns about measuring counterfactuals in complex socio-ecological systems.

These challenges require a coordinated approach. Regulatory reforms without technological innovation lack enforcement capacity; technological solutions without ethical frameworks risk digitising—rather than resolving—injustice; and ethical considerations without implementation mechanisms remain aspirational. The path forward demands an integrated approach recognising these interdependencies.

Three promising directions for carbon market evolution emerge: First, "nested governance" models connecting local, national, and international regulatory frameworks while respecting sovereignty could address jurisdictional challenges while creating coherent verification standards. Second, advanced monitoring technologies integrated

[225] Daniel Bodansky, Jutta Brunnée, and Lavanya Rajamani, *International climate change law* (Oxford University Press 2017).

with transparent governance frameworks could transform verification processes, creating socio-technical systems where technology enhances rather than replaces human oversight. Third, reconceptualising carbon credits as instruments of climate justice could fundamentally alter market dynamics by incorporating equity and historical responsibility into credit valuation.

Carbon market transformation must be understood within broader sustainable economic transitions. While market mechanisms have roles to play, they require robust governance frameworks aligning financial incentives with environmental and social objectives, moving beyond narrow carbon pricing efficiency toward deeper questions of economic institutions supporting climate stability and global equity.

As climate impacts intensify and net-zero commitments proliferate, the importance of carbon markets will only grow. The critical challenge is ensuring they become instruments of genuine climate action rather than vehicles for environmental commodification. While emerging technologies such as blockchain and AI-enhanced monitoring offer promising tools for improving transparency and efficiency, they cannot substitute for coherent regulation or ethically grounded governance. Policy reform must prioritise enforceable standards, inclusive oversight, and equitable participation—especially for stakeholders in the Global South. Ultimately, the legitimacy of carbon markets will depend on whether they can evolve from transactional instruments into frameworks that balance environmental integrity, global justice, and long-term climate stability.

Gianluca Sisto *

SPECIAL SECTION

BLOCKCHAIN IN AGRIFOOD SUPPLY CHAIN

Achieving traceability and sustainability under the UN 2030 agenda

Abstract

A comprehensive social and regulatory framework could incentivise States to pursue a balanced integration between digital transformation, ecological transition, and agricultural development. Within this context, it is increasingly feasible to design trustless, intermediary-free production chains that reduce critical inefficiencies, foster innovative forms of competition, and promote new models of sustainability.

Blockchain technology emerges as a trusted infrastructure for certification and data storage, providing guarantees of certainty, transparency, and security. These features not only enhance consumer awareness but also provide a potential solution to the persistent issue of counterfeiting.

This study aims to examine how this infrastructure can adapt to the diverse requirements established by European, national, and regional legislators, particularly about food safety, traceability, and eco-sustainability. Rethinking blockchain integration within supply chains could thus mark a turning point in reshaping the current bioeconomy, transitioning from a traditionally linear economic model to a truly circular economy. In such a system, waste materials are either reintegrated into other production cycles or responsibly disposed of in an environmentally responsible manner.

To achieve a genuinely sustainable and circular economy, the integration of blockchain with digital twin technology could enable comprehensive, qualitative tracking and monitoring of products throughout their entire lifecycle — from production to disposal — ensuring their reusability.

While technology can efficiently address challenges related to traceability and counterfeiting, it cannot replace the subjective evaluations required for issuing certifications such as P.D.O. (Protected Designation of Origin) and P.G.I. (Protected Geographical Indication), which remain essential in the context of supply chain economies.

It is important to underscore, however, that certifying a product is not equivalent to certifying its entire supply chain. By enhancing the reliability and efficiency of the information it processes, blockchain could improve supply chain management and overall profitability. In turn, this would promote a more balanced and transparent B2C (business-to-consumer) relationship, reducing informational asymmetries and strengthening contractual trust.

JEL CLASSIFICATION: K13, K15

* PhD in Comparative Private Law at University of Bari - 'A. Moro'.

DOI 10.13135/2785-7867/12269

SUMMARY

1 Digital innovation in the agri-food sector under UN 2030 goals

To promote the sustainability of the agri-food supply chain, the UN 2030 Agenda has set as a goal 2.4, which aims to "...implement resilient agricultural practices that increase productivity and production and that help protect ecosystems...". However, it does not specify the tools needed to achieve these goals; a review of numerous international reports on the point reveals that 'increasing productivity' and 'implementing agricultural practices' are well known concepts[1].

The FAO 2018 report already indicated several preliminary ways to achieve these goals, including precisely the use of distributed ledger-based technologies, which are considered "...a unique opportunity for the agricultural sector".

The potential of this phenomenon could bring unlimited benefits to the agri-food sector through increased information symmetry, certainty in product traceability and easy control of the environmental impact of the entire production chain.

In this regard, last European Union legislative interventions on corporate sustainability have focused precisely on this aspect: the "Corporate Sustainability Reporting Directive" (Directive 2022/2464) addresses corporate sustainability reporting, aiming to improve the transparency of environmental, social, and governance information, ie, ESG rating. This Directive targets the actors involved in the production chain through two distinct action modes: the identification of disclosures along the chain and the dissemination of best practices inspired by sustainability[2], which is expected to have an economic impact as well[3].

In general, technological advances could provide the supply-chain with automation of production lines and productivity gains, giving new life to what has been dubbed 'Industry 4.0'.

[1] For example see: Food and Agriculture Organization of United Nations, International Telecommunication Union, Status of Digital Agricolcture in 18 countries of Europe and Central Asia (ITU Publications 2020) <https://openknowledge.fao.org/server/api/core/bitstreams/29c2830e-8560-48ff-b636-06af2a1bb778/content> accessed 20 June 2025; Word Economic Forum 'Shaping of Global Food Systems: A Scenarios Analysis' (2017) <https://www3.weforum.org/docs/IP/2016/NVA/WEF_FSA_FutureofGlobalFoodSystems.pdf> accessed 20 June 2025; Food and Agriculture Organization of the United Nations, Environmental Sustainability in Agriculture (OEDC 2023) <https://openknowledge.fao.org/server/api/core/bitstreams/32da2942-3854-4736-af19-877b3ab22d35/content> accessed 20 June 2025.

[2] Mia Callegari, 'Sostenibilità, supply chain e intelligenza artificiale' (2024) 5 Giurisprudenza Italiana 1211.

[3] European Parliament and Council Directive (2022/2464) as regards corporate sustainability reporting [2024] OJ L 322/15 paragraph 8.

This trend enables supply chains to achieve significant performance improvements through a multitude of applications. Specifically, by analysing a series of case studies, it emerges that the technologies most commonly used in the agri-food sector are those focused on monitoring and controlling resources — particularly IoT and sensors for data transmission and processing — as well as those involved in product identification and tracking, with blockchain playing a key role in this regard[4]. In this context blockchain could act as a privileged system for certification and archiving, valued for its inherent guarantees of certainty, transparency and security and these qualities must be applied to ensure *end-to-end* traceability, quality assurance and reduction of food waste.

The combination of technology and agriculture finds its concrete application in several projects: in Italy, the three-year framework project 2019-2021 of Mi.p.a.s, together with Microsoft, has created 'AgriDigit'[5], a cloud that enables technological development in agriculture, offering greater capillarity in traceability and giving further guarantees to consumers in terms of food safety and transparency of information; in Spain, the Council of Ministers approved in November 2021, at the proposal of the Ministry of Agriculture, Fisheries and Food (MAPA), investments for the environmental and digital transformation of the agricultural sector between 2021 and 2023, with the aim of adopting structural reforms necessary to promote a change in the agricultural production model that improves its sustainability in environmental, economic and social terms.

2 The role of blockchain in data management and security

Blockchain is a form of Distributed Ledger Technology (DLT) based on a shared, decentralised, distributed and transparent database[6]. It functions as a public ledger of information that is, in principle, irreversible and tamper-proof, where a transaction can only be validated once it has been approved by all nodes in the network. Owing to these features, blockchain can be conceptualised as a "public blackboard" on which all transactions executed up to that point can be read, along with the identities of the asset holders and the traceability of each transfer[7].

This digital architecture is organised into smaller, fixed-size sets of data known as blocks. The link between each block and the next is ensured by a cryptographic function called a 'hash', which compresses information of arbitrary length into a unique alphanumeric code. As the chain grows, each block contains the hash of the previous ones,

[4] Livio Cricelli, Roberto Mauriello, Serena Strazzullo, 'Technological innovation in agri-food supply chains' (2022) 5 British Food Journal 1852.
[5] Agridigit is a project, divided into six sub-projects, which deals with - among other things - testing which technological mechanisms enable greater efficiency in the world of agriculture. To can find out more about what the whole project consists of at: <https://www.crea.gov.it/-/agridigit> accessed 20 June 2025.
[6] Andrea Stazi, *Automazione contrattuale e "contratti intelligenti". Gli smart contract nel diritto comparato* (Giappichelli 2019) 100.
[7] Maria Rosaura Maugeri, *Smart Contracts e disciplina dei contratti* (Il Mulino 2021) 21.

thereby creating an immutable chain—or, more precisely, a chain in which any alteration would immediately reveal evidence of tampering[8].

One of the main issues associated with distributed ledger technology is the management of consensus, which refers to the process by which nodes reach an "agreement" to approve individual transactions. This mechanism serves as a validity guarantee for the ledger among the nodes and is implemented through computational protocols. The most widely used protocol is proof of work, where, to find the solution necessary to validate the transaction, nodes must solve a complex mathematical problem. Once the correct solution is found, for the transaction to be added to the most recent block, other nodes must understand and verify it as quickly as possible, but the system appears efficient because the mathematical problem is extremely difficult to solve, but once the solution is found, it is easily verifiable by anyone[9].

Nowadays, in the European system, the quality of agrifood products is ensured by strict regulations and, for this reason, data from logistics, transportation and product conformity management processes are verified by different bodies, depending on the country and are stored in paper records, centralised databases or non-automated channels. However, as there is still no connection between companies operating in a given product sector, either locally or at EU level, there is no shared *framework for* the digital management of this information[10].

Fragmentary, incomplete or contradictory data do not offer sufficient certainty as to the reliability of each individual product, nor do they allow timely action to be taken in the event of malfunctions, food contamination or more general irregularities.

For this reason, the current major concern of players within the food supply chain has shifted to the problem of integrity, ie, the 'fairness and authenticity of food in food value chains'[11] a challenge that could find fertile ground through the application of blockchain technology. Yet, it should be considered that, in the light of the sectoral regulations in force, it is not possible to replace a state certifying body; at most, the way in which the data processed within the supply chain, which is the subject of subsequent audits, can be improved.

[8] Lorenzo Parola, Paola Merati, Giacomo Gavotti, 'Blockchain e smart contract: questioni giuridiche aperte' (2018) 6 I Contratti 681.
[9] Andrea Visconti, Andra Frisoni, 'Consenso e mining nella blockchain' in Laura Ammanati e Allegra Canepa (eds), *Tech Law. Il diritto di fronte alle nuove tecnologie* (Editoriale Scientifica 2021) 182; Christian Cachin, Marko Vukolic, 'Blockchain Consensus Protocols in the Wild' in 31st International Symposium on Distributed Computing (DISC 2017), Leibniz International Proceedings in Informatics (LIPIcs), Volume 91 (Leibniz 2017) 1:1.
[10] Ministry of Economic Development, 'Blockchain for Made in Italy traceability: Origin, Quality, Sustainability. Case study applied to the textile sector' (2019) <www.mimit.gov.it/index.php/it/normativa/notifiche-e-avvisi/blockchain-per-la-tracciabilita-del-made-in-italy> accessed 20 June 2025.
[11] Eloisa Marchesoni, 'La blockchain per la tracciabilità del made in Italy: Origine, Qualità, Sostenibilità. Caso di studio applicato al settore tessile' (Ministero dello sviluppo economico & Ibm. 2019) <https://www.agendadigitale.eu/documenti/blockchain-per-lagrifood-rivoluzione-smart-contract-ecco-vantaggi-e-limiti/> accessed 20 June 2025.

Having identified the limitations of the current supply-chain system, the key feature of blockchain for the agri-food supply chain is the ability of collecting a substantial amount of information[12].

The blockchain is a type of Distributed Ledger Technologies, characterised by the fact that there is a well-defined sequence of data, in which several pieces of information are linked together in such a way as to form a chain whereby the next block of data is added at the end of the structure itself, in strict chronological order[13].

In this technology, as in all DLT's, there is no central database, which is replaced by the individual nodes of the network forming a decentralised, distributed, encrypted and transparent one, which acts as a public repository of information that tends to be irreversible and incorruptible in which, before a transaction can be added, all nodes must approve it[14] and which, once approved, is 'branded' through *time stamping*[15], thus making it legally enforceable against third parties[16]. At this point, it is straightforward to draw a comparison between a *block-chain* and a *supply-chain* whereby each block could be the representation of a *player* operating within a supply chain and the link between the 'on-chain' and 'off-chain' worlds could be ensured using *smart contracts*.

The characteristics of the blockchain that could guarantee the product traceability and the clarity of information in the supply chain are immutability, secured by the cryptographic hash function and transparency.

Indeed, before data can be considered immutably recorded on the blockchain, at least six subsequent blocks must be validated, as only after this point does any alteration to the most recent block become economically unfeasible for an attacker. This is because one would need to generate a new block containing the exact same hash as the altered block, thereby replicating the computational effort required to validate all preceding blocks.

For this reason, some scholars argue that blockchain should be regarded as "virtually" irreversible. In fact, information could theoretically be modified if consensus for such a change were achieved by a majority of nodes in the network[17].

[12] Most international regulations that have attempted to give a definition of blockchain identify as their starting point exactly the function of DLT, which enables the collection of an immense amount of information. This choice of legal policy seems audacious, since the main and best-known function of blockchain is instead to avoid so-called *double spending* in the exchange of cryptocurrencies.

[13] Kelvin Low, Eliza Mik, 'Pause the Blockchain Revolution' (2020) 69 (1) International & Comparative Law Quarterly 135; Stéphane Blemus, 'Law and the Blockchain: A legal Perspective on Current Regulatory Trends Worldwide' (2017) 4 Revue de Droit Financier 1; Cristina Poncibò, *La blockchain il diritto privato comparato* (Edizioni Scientifiche Italiane 2021); Massimo Giuliano, 'La blockchain e gli smart contracts nell'innovazione del diritto del terzo millennio' (2018) 34 (6) Il diritto dell'informazione e dell'informatica 989, 1100.

[14] Reggie O'Shields, 'Smart Contracts: Legal Agreements for the Blockchain' (2017) 21 (1) Banking Institute Journal 177.

[15] Paolo Lessio, 'Blockchain e tracciabilità della filiera' in Roberto Battaglini, Massimiliano Giordano (eds), *Blockchain e Smart Contract: funzionamento, profili giuridici e internazionali* (Giuffrè Francis Lefebvre 2019) 514.

[16] The cryptographic key used to approve transactions on the blockchain, together with its exact time identification, in fact allows compliance with the digital signature requirements of the European Eidass regulation.

[17] Ettore Battelli, 'Le nuove frontiere dell'automazione contrattuale tra codici algoritmici e big data: gli smart contract in ambito assicurativo, bancario e finanziario' (2020) 4 Giustizia Civile 671; Sara Saberi, Mathab Kouhizadeh, Joseph

Future technological developments could potentially enable a malicious actor to match or surpass the computational power of 50 % +1 of the nodes, thereby gaining control of the entire chain.

Nonetheless, even if data were tampered with, all subsequent blocks would be identifiable, allowing the remaining nodes to detect the manipulation and, crucially, to pinpoint the exact moment at which the fraudulent alteration occurred.

Another potential avenue for modification lies in the blockchain's source code itself. Programmers may assign certain nodes the authority to retroactively cancel or alter transactions. However, while this approach introduces greater flexibility, it simultaneously compromises the security of the system, as an attacker could gain control by accessing only the so-called "privileged nodes"[18].

Read in conjunction, these features ensure the overall integrity of the data[19]: information is connected to other data in a sequential, validated manner that makes it immutable, identified at a given space-time moment and so legally enforceable against third parties. This system allows for the widespread management of all data, transformations or certifications associated with the product. Therefore, *Industry 4.0* refers also to a way of doing business, based on new production paradigms[20], the harmonious use of new technologies, and which tends to improve crop yields and production quality[21].

3 Evolving food traceability. Legal frameworks and challenges from Europe to United States

In Europe, traceability, as a nuance of the principle of food safety, finds its legal basis in European Regulation n 178/2002 which, in Article 18, prescribes the obligation to trace every stage of production, providing for adequate control systems.

The reasoning of this approach is well identified in recital 28 of this Regulation EC/178/2002: '*Experience has shown that the inability to trace food and feed products can jeopardies the functioning of the internal market in these products. It is therefore necessary to establish a general system for traceability of products covering both the feed and food sectors to be able to carry out targeted and accurate withdrawals or to provide information to consumers or control officials, thereby avoiding greater and unjustified inconvenience when the safety of foodstuffs is endangered*'.

Sarkis, Lejia Shen, 'Blockchain technology and its relationships to sustainable supply chain management' (2018) 57(7) International Journal of Production Research 2117.

[18] Nathan Fulmer, 'Exploring the Legal Issues of Blockchain Applications' (2019) 52 (1) Akron Law Review 170.

[19] H L Gururaj, Ravi Kumar, Sam Goundar (eds), *Convergence of Internet of Things and Blockchain Technologies* (Springer 2022) 249.

[20] Wanda D'Avanzo, 'Blockchain e smart contracts per la gestione della filiera agroalimentare' (2021) 1 Diritto Agroalimentare 93.

[21] Claudio Gagliardini, Franz Russo, *I.o.T. e nuovo marketing. Come e perché le aziende devono utilizzare l'internet delle cose nelle loro strategie di marketing* (Dario Flavocchio Editore 2019).

'Traceability' was response to the growing demand from consumers for reliable and transparent information and reflected an increasing information asymmetry between producer and consumer, also due to an expansion of the production chain[22].

In fact, it served as a crucial risk management tool, enabling the swift removal of harmful food products and providing consumers with specific, accurate information about the items they purchase.

Nowadays, the problem is complex from a twofold point of view: on the one hand, there is no traceability obligation for the packaging of agricultural products, even though they form the basis of most processed products; on the other hand, processors of raw materials are hardly ever in a technical position to be able to operate an efficient *tracing* operation[23].

For this reason, the food system had to manage a large amount of information, leading to significant challenges in legal certification, due to the obsolescence of any other traditional system[24].

This system allows industry operators to quickly identify both suppliers and customers, ensuring greater accountability throughout the supply chain[25].

Moreover, thanks to globalisation and the immense lengthening of production chains, the problem of traceability in the agri-food chain has taken on global dimensions, with the need to investigate whether the problems encountered so far can also be found in non-European legal experiences.

In the United States, food safety activities have been defined as those designed to decrease the likelihood of a food causing harm to consumers[26], while traceability of the supply chain is discussed in more detail in terms of the amount of information, the ubiquity of control to which the supply chain is subjected, and the detail of information[27].

In 2011, with the enactment of the *Food Safety Modernization Act* (FSMA)[28], the US food traceability system was fundamentally changed[29].

[22] Defined as 'the ability to trace and follow a food, feed, food-producing animal or substance intended to be, or expected to be incorporated into a food or feed through all stages of its production, processing and distribution' Regulation EC/178/2002, Art 3.

[23] Luigi Costato, 'Le regole di produzione e di commercializzazione dei prodotti alimentari' in Luigi Costato, Paolo Borghi, Sebastiano Rizzioli, Valeria Paganizza, Laura Salvi (eds), *Compendio di diritto alimentare* (8th edn, Wolters Kluwer 2017) 275.

[24] Lessio (n 15) 520.

[25] Isabel Hernandez San Juan, 'The Blockchain Technology and the Regulation of Traceability: The Digitization of Food Quality and Safety' (2020) 15(6) European Food and Feed Law Review 563.

[26] Elis Golan, 'Traceability in the Us Food Supply: Economic Theory and Industries Study. Us Department of Agriculture, Economic Research Service' Washington DC Agricultural Economic Report No 3 (2004).

[27] Diego Souza-Monteiro, Neal Hooker, 'Food safety and traceability' in Walter Armbruster and Ronald Knutson (eds), *US Programs Affecting Food and Agricultural Marketing* (Springer 2013) 249.

[28] The full text of FSMA: <https://www.fda.gov/food/food-safety-modernization-act-fsma/full-text-food-safety-modernization-act-fsma> accessed 20 June 2025.

[29] John Scharff, David Decker, Marc Riedl, *Food Safety Law* (Wolters Kluwer 2020); Neal Fortin, *Food Safety Modernization Act: Law, Policy, and Practice* (Wiley-Blackwell 2018).

The FSMA has imposed a wide range of new food safety obligations on the FDA[30] addressed to food producers, farms, operators and others involved in the supply chain[31].

Section 103 requires all operators in the food chain, with the exception of small establishments, to equip themselves with risk prevention and protection control systems during the production, processing and packaging of the product, with the aim of creating a link between traceability and food safety.

This was implemented through the *Food* Traceability *Final Rule*[32], which established new traceability requirements for persons producing, processing, packaging or holding food, if included in the *Food Traceability List* (FTL), obliging them to maintain records containing key data elements associated with specific critical traceability events and to provide information to the FDA.

Since the *Food Traceability Final* Rule requires entities in the same supply chain to share information with each other, it was felt that the most effective and efficient way to implement this rule was to oblige all stakeholders to comply by the same date, 20 January 2026.

Some states have already begun working on the proper implementation of Section 103 to achieve initial results; one example is the *California Leafty Green Products Handler Marketing Agreement*, which provides for the creation of a state-wide traceability system.

However, this regulatory apparatus has been widely criticised for focusing only on producers, without considering the need to think about an integrated production chain[33].

Also deserving of attention is Section 204, which calls on food control agencies[34] to implement technological systems for collecting and storing data.

From the US perspective, even though it is based on a very different legislative framework, the same challenges faced in Europe can be observed — namely, the difficulty of managing large volumes of information and the challenge of thinking in terms of an integrated production chain.

In both contexts, there is a significant reliance on new technologies. For instance, it would be possible to record information about key stages of the food supply chain on a blockchain, automating agreements between the various stakeholders and achieving substantial cost savings by eliminating electronic data interchange and paper-based systems, while also reducing inefficiencies, vulnerabilities, inconsistencies, and other shortcomings.

[30] The Food and Drug Administration, the most important US federal food safety agency.
[31] Arthur Stansbury, 'U.S. Food Safety Modernization Act: Implications for Exporters of Food to the United States' [2014] LMuR 237.
[32] Miriam Guggenheim, Cory Trio, *FSMA Final Rule on Requirements for Additional Traceability Records for Certain Foods* (IFDA 2020) <https://www.ifdaonline.org/wp-content/uploads/2024/02/IFDA-Manual-on-FSMA-204-Food-Traceability-Rule.pdf> accessed 20 June 2025; Michael Roberts, *Food Safety Modernization Act: A guide for the Food Industry* (CRC Press 2020).
[33] Souza-Monteiro, Hooker (n 27) 253.
[34] See paragraph 7.

In both legal systems under analysis, the quality of agri-food products is safeguarded through distinct regulatory frameworks. Consequently, data related to logistics management, transportation, and product compliance verification are managed by multiple entities—differing from one jurisdiction to another—and are stored using paper-based records, centralised databases, or other non-automated systems.

Nonetheless, in the absence of interoperable systems among businesses operating within a given commodity sector, no unified framework currently exists for the digital management of such information.

Fragmentation, incompleteness, and internal inconsistencies in available data hinder the ability to ensure product reliability and obstruct timely responses in cases of malfunction, contamination, or administrative non-compliance.

As a result, the primary concern among stakeholders in the agri-food supply chain has shifted toward the issue of integrity—understood as the "accuracy and authenticity of food within food value chains"[35].

It is important to emphasise, as we have already said, that under the current sector-specific regulatory framework, blockchain technology cannot serve as a substitute for state-certified authorities. Rather, it is more appropriate to assert that this technology may improve the management of data generated throughout the production chain and subsequently subjected to regulatory audits.

Its adoption could offer substantial benefits, including cost reductions through the elimination of paper-based data exchanges and documentation. Moreover, it has the potential to mitigate inefficiencies, vulnerabilities, inconsistencies, and other structural limitations associated with analogue systems[36].

Indeed, blockchain enables the creation of sequentially linked, validated, and time-stamped data sets that are legally enforceable and technically immutable. This architecture allows for the decentralised management of all product-related information, encompassing not only transformations and processing stages but also certification procedures.

The tracing process—currently constrained by the registration and storage of off-chain data—could be substantially optimised. Owing to its intrinsic characteristics, blockchain guarantees that all legally mandated information is recorded in a secure, transparent, and tamper-proof manner. Each block in the chain contains a complete, time-stamped record of all transactions executed up to that point. This structure effectively functions as a digital "blackboard," enabling the reading of every transaction, its temporal reference, the identity of the asset holders, and the traceability of each transfer. In light of the need

[35] Eloisa Marchesoni, 'La blockchain per la tracciabilità del made in Italy: Origine, Qualità, Sostenibilità. Caso di studio applicato al settore tessile' (Ministero dello sviluppo economico & Ibm. 2019) <https://www.agendadigitale.eu/documenti/blockchain-per-lagrifood-rivoluzione-smart-contract-ecco-vantaggi-e-limiti/> accessed 20 June 2025.

[36] Bharat Bhushan, Abhishek Kumar, Latyar Katiyar, *Security Magnification in Supply Chain Management Using Blockchain Technology, Blockchain Technologies for Sustainability* (Springer 2022) 47.

to adopt an integrated supply chain perspective, blockchain technology may also serve to ensure that all stakeholders operate on the basis of a uniform level of information concerning the validity and provenance of certifications. Moreover, such data would be rendered tamper-proof and resistant to manipulation.

Although current applications of blockchain in supply chain management primarily focus on the agri-food sector—highlighting the technology's capacity to process and secure large volumes of data—the true paradigm shift lies in the convergence of blockchain with the Internet of Things (IoT) and smart contracts[37].

One of the most concrete examples in this regard is the IBM Food Trust[38], which provides all network participants with a safe, intelligent and sustainable food ecosystem that considers food provenance, transaction data, and processing details, thus making the origin of the purchased product, certifications, and quality data available to the customer-consumer within seconds.

Traceability obliges operators to think in terms of an 'integrated chain' approach by implementing a standardised and uniform coding system[39].

However, the integration of blockchain into the agri-food supply chain is not cost-neutral.

On the contrary, the development and deployment of such a system require substantial financial investment on the part of businesses. These expenditures are primarily associated with the technical infrastructure necessary for the creation, validation, and maintenance of a secure and decentralised ledger—ranging from computational power and energy consumption to personnel training and compliance with applicable regulatory frameworks. Unsurprisingly, these operational expenditures are ultimately passed on to the end consumer in the form of higher product prices. Nevertheless, empirical studies[40] suggest that consumers may be willing to absorb such additional costs, provided that they are accompanied by tangible improvements in the perceived quality, safety, and traceability of the product.

That said, when measured against the current level of technological maturity, limited standardisation, and lack of full interoperability of blockchain-based agri-food systems,

[37] Maria Teresa Della Mura 'IoT, AI Blockchain per le Supply Chain: nuova efficienza e nuovi modelli di business' *Il Post* (29 May 2020) <https://www.industry4business.it/industria-4-0/iot-ai-blockchain-per-le-supply-chain-nuova-efficienza-e-nuovi-modelli-di-business/> accessed 15 July 2024.
[38] IBM site <https://www.ibm.com/it-it/products/supply-chain-intelligence-suite/food-trust> accessed 20 June 2025.
[39] Stefano Masini, *Corso di diritto alimentare* (5th edn, Giuffrè Francis Lefebvre 2022) 173. And what does the blockchain look like, if not as a product obtained from the processing of computer code, ontologically uniform and homogeneous, valid for all users who participate in it.
[40] Lorenzo Compagnucci, Dominique Lepore, Francesca Spigarella, Emanuele Frontoni, Marco Baldi, Lorenzo Di Berardino, 'Uncovering the Potential of Blockchain in the Agri-food Supply Chain: An Interdisciplinary Case Study (2022) 65 Journal of Engineering and Technology Management 5.

these added costs may still appear not proportionate to the concrete benefits currently achievable throughout the supply chain[41].

Furthermore, although the regulation prescribes which information[42] must be disclosed to the public authority, eg, in the event of contamination, it leaves it up to individual operators to decide how to collect and store this data.

In the United States as well, the principle of traceability is established by the same legislative act, the Food Safety Modernization Act (FSMA), where it is referred to as traceback. This concept embodies the one step back, one step forward principle, requiring operators to identify not only the entities to which they have distributed the product but also those from whom they have received it. Unlike the European framework, however, the U.S. system is less stringent and is not governed by a dedicated set of regulations.

The *tracing* process, today slowed down by the costly off-chain data recording and storage, would indeed be facilitated using blockchain technology[43].

The intrinsic nature of the 'blockchain' would make it possible to manage all the information that the law prescribes in a certain, transparent and immutable manner: each block of the chain, in fact, keeps a copy of the totality of the transactions executed up to that moment, thanks to which it is possible to read all the transactions, the time at which they were finalised, the owners of the values exchanged and the traces of the passage of these assets[44].

The integration of blockchain technology into the agri-food supply chain cannot, in itself, be regarded as a solution for all systemic inefficiencies or compliance challenges. One of the most critical limitations lies in the fact that the accuracy and reliability of the data entered into the blockchain remain largely dependent on the discretion of individual operators at various stages of the supply chain.

Although the immutability of blockchain ensures that, once recorded, data cannot be altered without detection, it does not guarantee the accuracy or authenticity of the data at the point of entry. This limitation gives rise to what is commonly referred to as the "garbage in, garbage out" problem, whereby inaccurate or fraudulent information, once entered, is perpetuated across the system as if it were valid[45].

Nonetheless, the insertion of erroneous or misleading data does not absolve the responsible operator of legal liability. On the contrary, blockchain's inherent traceability mechanisms may serve to enhance accountability, as every transaction—together with the

[41] Luigi Costato, 'La rintracciabilità degli alimenti' in Luigi Costato, Alberto Germanò, Eva Rook Basile (eds), *Trattato di diritto agrario* (Utet Giuridica 2011) 539; Noila Mohd Nawi, 'Consumers' preferences and willingness-to-pay for traceability systems in purchasing meat and meat products' (2023) 7 Food Research 3.
[42] These are: nature and quantity of raw materials, name and address of suppliers, date of receipt, nature and quantity of products marketed and date of delivery of products.
[43] Pierluigi Gallo, Giovanni Capizzi, Maria Timoshina, 'SeedsBit: Blockchain per la tracciabilità agroalimentare multifiliera' (2021) 2 Federalismi 92.
[44] Maugeri (n 7) 21.
[45] Warwick Powell, Marcus Foth, Shoufeng Cao, Valeri Naraelov, 'Garbage in garbage out: The precarious link between IoT and blockchain in food supply chains' (2022) 25 Journal of Industrial Information Integration 1, 4.

identity (or pseudonym) of the party responsible for generating it—is permanently recorded and subject to audit.

Accordingly, while blockchain can significantly improve transparency, traceability, and auditability within agri-food supply chains, it cannot substitute the need for robust regulatory oversight and human due diligence in the verification and certification of input data[46].

With respect to the need to think in terms of an integrated supply chain, blockchain could also be used to ensure that different *players* share the same level of information on the validity and provenance of certificates and that they are tamper-proof.

However, while in the field of *supply management* the main use cases of blockchain relate to the food supply chain, with specific reference to the blockchain's features concerning the ability to manage large amounts of data, the real key must be read in the light of the combination of blockchain, IoT and smart contracts[47].

According to some studies, the possibility of eliminating the insertion of false data into the blockchain by human agents could be achieved through the use of the Internet of Things, particularly by means of computerised sensors responsible for automatically recording the parameters to be entered into the chain[48].

It is worth pointing out that, indeed, we are faced with two mechanisms that, although useful together, are different from each other: while ensuring greater transparency and capillary traceability in the supply chain is an objective that can be achieved through L.T.D., ensuring real-time data collection, on the other hand, is an operation that must necessarily be performed through the use of the Internet of Thing and Machine Learning.

4 Balancing blockchain governance: public vs private models

A key issue to address is the choice of *governance* model for blockchain to be applied to the business opportunities previously examined. According to its creator, *Satoshi Nakamoto*, the only possible form of *governance* for this technology is a 'public' model- one in which all network participants have free access to the chain, can validate transactions and be custodians of the sequence of the entire chain[49].

However, such a system is ill-suited to the objective of integrity that one would like to achieve, due to the dense regulatory system of public controls that inevitably clashes with the circumstance that, with this type of *governance*, any individual with a computer and an Internet connection could well enter false information into the so-called *permissionless* chain, thus defeating the usefulness of the entire system thus designed.

[46] For further insight into the relationship between external controls and supply chain integrity Cfr infra, par 5.
[47] Della Mura (n 37) accessed 15 July 2025.
[48] Powell and others (n 45) 3.
[49] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' <https://bitcoin.org/bitcoin.pdf> accessed 20 June 2025.

On the other hand, a completely privatised (so-called *permissioned*) system, whose information is not freely accessible, would not be able to guarantee the adequate transparency required and which would instead constitute the main element of the implementation of consumer confidence.

Therefore, the right compromise could be reached using *consortium* platforms, where only a few authorised nodes can execute and approve transactions, but whose information is accessible to all interested parties[50].

A concrete example of the application of this solution is the DIH Agrifood project[51], which utilises a consortium-type blockchain based on Ethereum[52]. In this context, any participant can access the blockchain and verify information related to the products of the food supply chain, such as their origin and journey, simply by scanning the QR codes placed on the products. Each transaction on the blockchain handles basic blockchain-related information, such as the timestamp, digital identity, and signature, as well as specific product-related information, such as the type, harvest region, harvest date and time, and logistics-related information, such as the batch number and product type. The solution also allows for the storage of digital proofs, such as photos of the harvest or delivery, on a related IPFS or Swarm network, along with other rich data, such as certificates, nutritional data, farmer/producer information, agricultural practices data, and environmental footprint data. In this model, however, users do not have the necessary powers to approve transactions but only the ability to observe and verify the information.

5 Smart contracts, the point of contact between real and virtual

It is interesting to explore how the 'off-chain' dimension interacts with the blockchain and the methods through which this connection occurs.

This possibility can be provided by *smart contracts* technology, which consists of code sequences that self-execute according on the predefined patterns they are programmed to follow[53]. Without delving too deeply into an attempt to provide a universally agreed-upon legal definition of smart contract[54], what is truly relevant are its characteristics once it begins operating on the blockchain.

It is important to clarify that, although they function effectively in synergy, smart contracts and blockchain are distinct technologies. While blockchain is a decentralised

[50] Stazi (n 6) 100.
[51] For more information: DIH Agrifood project <https://itc-cluster.com/dih-agrifood/> accessed 20 June 2025.
[52] Ethereum is an open-source, decentralised platform based on blockchain that enables the development and management of smart contracts.
[53] Stazi (n 6) 109.
[54] Florian Möslein, 'Legal Boundaries of Blockchain Technologies: Smart Contracts as Self-Help?' in Alberto De Franceschi, Robert Schulze (eds), *Digital Revolution – New challenges for Law* (Nomos 2019); Maria José Schmidt-Kessen, 'Creating Markets in No-Trust Environments: The Law and Economics of Smart Contract' (2019) 35 (1) Computer Law and Security Review 69, 77; Pierluigi Gallo, 'Dlt, blockchain e smart contract' in Marco Cian, Claudia Sandei (eds), *Diritto del Fintech* (CEDAM 2020) 137; Sara Rigazio, 'Smart contracts e tecnologie basate su registri distribuiti nella L. 12/2019' (2021) 2 Diritto dell'informazione e dell'informatica 369, 374.

ledger, smart contracts are software programs designed to automatically execute transactions.

The idea of integrating smart contracts with blockchain technology was proposed by Nick Szabo, who authored two seminal papers: Formalising and Securing Relationships on Public Networks and The Idea of Smart Contracts. In these works, Szabo compares the operational mechanism of this combined technology to the process of purchasing goods from a vending machine, where the execution of the contract via the insertion of money is, in essence, the transfer of a right through the execution of computer algorithms, contingent upon the fulfilment of a specific condition[55]. Thus, with smart contracts, the aim is to minimise, or even eliminate, human involvement in the creation of contractual conditions and their subsequent execution, using binary language as the fundamental tool[56].

The code used for the drafting of a smart contract, the Boolean language, is capable to meet both the requirements of (im)modifiability, certainty and transparency requirements of the supply chain, as well as flexibility of the agri-food sector's *managing*. It eliminates any ambiguity regarding the origin of goods and ensures that each step in the process is subject to controls that can only be passed if certain predefined conditions are met in advance.

These conditions could concern both the origin of the product, the transformations it has undergone, and the characteristics required for a product to be defined as 'quality', as well as indications concerning sustainability such as soil consumption, use of plant protection products, carbon dioxide production and water impact.

Therefore, *stakeholders* whose goal is to produce a specific type of product, with specific labelling and capable of attracting a significant number of consumers, could equip themselves with as many *smart* contracts as there are critical points in the supply chain, so that the contract code is set up so that each step in the supply chain, starting with the production of raw materials, is subject to a system of conditions designed to arrive at a specific finished product, with characteristics that, acquired throughout the supply chain, are controlled and monitored.

Only that particular product, coming from that territory and having undergone that specific processing, will fulfil the conditions identified from time to time by the Boolean language '*If this/then that*', thus perfecting the different smart contracts, executing them and thus initiating the process of storing data in the blockchain: when the network nodes approve the transaction, it will be added to the last block of data existing up to that point.

[55] Nick Szabo, 'Formalizing and Securing Relationships on Public Networks' (1997) 2(9) First Monday <https://doi.org/10.5210/fm.v2i9.548> accessed 20 June 2025; Nick Szabo, 'The Idea of Smart Contract' (1997) 6 199 <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html> accessed 20 June 2025.

[56] Max Raskin, 'The Law and Legality of Smart Contracts' (2017) 1(2) Georgetown Law Technological Review 305, 315.

This ensures strict adherence to the clauses identified within each contract regulating the supply chain relationship, which, once verified and executed, tends not to be altered[57], and then proceeds to the next stage of the supply chain, where a subsequent smart contract will identify further conditions and so on, until it reaches the final consumer.

The integration of smart contracts within the agri-food supply chain can significantly enhance the traceability and transparency of product data. By automating the execution of predefined contractual conditions through blockchain technology, smart contracts ensure that each transaction or step in the production process is recorded and verified without the need for intermediaries. This automated, immutable data recording guarantees the integrity of the entire supply chain, providing a clear and verifiable audit trail from raw materials to final product.

As a direct consequence of this enhanced transparency and traceability, businesses within the supply chain are better positioned to obtain voluntary product certifications. These certifications, such as those related to sustainability, organic farming, or product origin, often require rigorous documentation and verification to ensure compliance with specific standards. Blockchain, using smart contracts, simplifies and streamlines this process by providing an immutable record of compliance at every step of the supply chain.

Thus, the use of smart contracts not only strengthens the integrity of the agri-food supply chain but also facilitates the acquisition of voluntary certifications by reducing the complexity and cost of verifying compliance. This opens the door for businesses to access premium markets where certification plays a crucial role in consumer decision-making, all while maintaining the credibility and authenticity of the product claims[58].

Such system would not have the strength to replace the system of controls necessary to provide voluntary quality labels, but it would facilitate their acquisition, allowing the supply chain to transmit certain, unchangeable data and reducing the number of intermediaries present, with considerable savings in terms of transaction costs and error recovery, generating greater confidence in the end consumer.

The importance that voluntary product certifications assume in terms of transparency towards the consumer and greater profit for the company is such that mere compulsory product certification is not sufficient for the company to be competitive on the market. BIO, DOP, IGP and STP) that certifies the peculiarities of a product and that - although voluntary - is in any case subject to compliance with specific technical rules, incorporated within legal regulations and therefore binding[59].

[57] Chiara Campagna, 'Intelligenza artificiale e blockchain nel settore agroalimentare: il made in Italy che diventa smart' in Filippo Romeo (ed), *La difesa del made in Italy nel settore agroalimentare fra spinte protezionistiche e crisi pandemica* (Giappichelli Editore 2021) 151.

[58] Emiliano Troisi, 'Blockchain-based Food Supply Chains: the Role of Smart Contract' (2023) Special Issue EJPLT 138, 144.

[59] Giorgia Chiaramonte, 'Crisi Pandemica, certificazioni non obbligatorie dei prodotti agroalimentari e pratiche commerciali sleali alla luce della normativa emergenziale' in Filippo Romeo (ed), *La difesa del made in Italy nel settore agroalimentare fra spinte protezionistiche e crisi pandemica* (Giappichelli Editore 2021) 171.

In this regard, the European Commission, in its Communication No. 2010/C 341/04 'EU Best Practice Guidelines for voluntary certification schemes for agricultural products and foodstuffs' has well specified that' private certification is not necessary to demonstrate compliance with legal requirements. Any private certification scheme in the agri-food sector must remain voluntary. If operators use certification of compliance with minimum requirements to facilitate transactions with other actors in the food chain, it must be clear that this practice cannot be used to differentiate products on the market."

Thanks to the system of signs of quality and origin, an attempt is being made to shift competition from price to quality, thus enabling the market to pursue objectives other than mere corporate profit, such as the inescapable one of sustainability[60], now the *fil rouge* of European and global innovation. In a fully implemented situation, therefore, each contractual relationship within the supply chain could be viewed, verified and executed by several *smart contracts*, while managing to keep corporate confidentiality inviolate[61].

As mentioned, the blockchain/smart contracts system should, however, include, in order to achieve satisfactory result, the implementation of further technologies such as, for example, IoT and QR-code technology, which guarantee greater security and transparency for all players in the food supply chain.

Think of an IoT sensor with which it is possible to measure and certify the agricultural area that the producer has decided to allocate to the P.D.O. or P.G.I. product, to precisely identify cultivated plant varieties, to measure the density of production activity as well as to constantly monitor the processes adopted for the processing and treatment of raw materials.

The QR code, on the other hand, would make it easier to understand the stages of the manufacturing process, the history of each food product, from its genesis to its distribution, i.e. from the origin of the raw materials to their processing, through to transport, storage and warehousing at the point of sale, simply by scanning the code with a smartphone.

6 Liability for blockchain in supply chain networks

It is necessary to ask what happens if, in a system in which the information entered is so secure that it cannot be changed or removed and on which everyone places extreme trust, nodes in the chain were to enter untrue information.

The problem shifts to the responsibility of the nodes[62] and, in particular, to the form of responsibility existing in the person – be it a natural person or a legal entity – who enters the data into the decentralised system and who should guarantee its veracity.

[60] Michail Bitzios, Lisa Jack, Sally-Ann Krzyzaniak, Marl Xu, 'Country-of-Origin Labelling, Food Traceability Drivers and Food Fraud: Lessons from Consumers' Preferences and Perceptions' (2017) 8(3) European Journal of Risk Regulation 541.
[61] Gururaj, Kumar and Goundar (n 19) 247.
[62] Nodes which, at the stage of implementation we are discussing, would be none other than the players in the supply chain.

This issue is not new, as the same question was posed, before the emergence of this new technology, when - with the introduction of the HACCP system - a regulatory burden was placed on the producer/processor/distributor to track a given good, with the aim of causing them to take responsibility[63].

The issue of the fragmentation of responsibilities along the supply chain is a significant one, and it has engaged States in the search for a complex balance between rules concerning the allocation of liability of supply-chain players and the need to manage the risks inherent in production activities that follow different regulatory paths[64].

In general, two distinct approaches can be identified within continental European legal systems. On the one hand, some have decided to impose a series of obligations on producers related to food safety, requiring a high degree of diligence in their compliance. On the other hand, since the adoption of the Directive on defective products, some others have considered extending these rules to operators within the agri-food supply chain.

In Italy, case law[65] has established the principle that an operator in the supply chain must take measures proportional to the characteristics of the product, and in doing so, they are required, under Article 1227, paragraph 2, of the Civil Code, to adopt measures linked to the level of diligence demanded, which is higher than that of a reasonable man[66]. Some authors have attempted to frame this operation within the framework of the strict liability for dangerous activity under Article 2050 of the Civil Code[67] with the assumption that the activities falling within this paradigm are not only those indicated by the Consolidated Law on Public Safety, but also those that could have a significantly greater impact, in terms of public protection, than ordinary situations[68].

In Germany, through the same reasoning, the theory of *Stufenverantwortlichkeit*[69] has developed, according to which the fragmentation of the supply chain translates into adherence to Article 17 of the Regulation 178/2002, whereby each operator is held accountable for any product discrepancies arising from their actions, without a general liability for any potential event. This approach aligns perfectly with the adoption of a technological traceability system, which precisely identifies the steps and interventions of each player involved.

France explicitly affirmed that the liability of food producers could be linked to that outlined in the Directive on defective products. This created an objective standard of protection regarding the identification of unsafe food products, particularly considering

[63] Lessio (n 15) 519.
[64] Giuseppe Toscano, 'Suggestioni del *lebensmittelstraftecht* in vista di una riforma degli illeciti agroalimentari' (2020) 63 (4) Rivista Italiana di diritto e procedura penale 1843.
[65] Cass. n. 5824/2014.
[66] Maria Pia Genesin, 'La responsabilità primaria dell'operatore del settore alimentare in relazione alla food safety' (2018) 3 Responsabilità Civile e Previdenza 809.
[67] Marianna Giuffrida, 'Innovazione tecnologica e responsabilità dell'operatore nel settore alimentare' (2018) 4 Rivista di diritto alimentare 4.
[68] Alessandro Ghiani, *Blockchain: linee guida. Dai casi pratici alla regolamentazione* (Giappichelli Editore 2021) 77.
[69] Gerhard Dannecker, 'Stufenverantwortung - wer haftet wofür?' [2002] ZLR 20.

the direct connection between defective products and the safety expectations of consumers, as defined in the 1985 Directive and continuing to evolve. The adoption of Regulation 178/2002 did not alter this regime, except by highlighting the need to strengthen the system through the establishment of a public agency, the General Service for Consumer Protection, Competition, and the Fight Against Fraud[70].

Therefore, with the advent of the Industrial Revolution 4.0. the problem would not be so much to identify the form of liability, but to establish the criteria for imputing this liability when using blockchain technology.

It is possible to identify two forms of liability attributable to the individual nodes of the network: that based on the failure of the operator who decided to enter incorrect data, or that resulting from the malfunctioning of the computer code underlying the blockchain and smart contracts.

While the regulatory regime applicable to the first form of liability is easy to grasp, as it can follow *sic et simpliciter* the traditional civil law rules[71], for the second the issue is different.

The nature of civil liability for damage caused by an algorithm depends, first and foremost, on its degree of autonomy and, in the case at hand, we are dealing with 'ordinary' algorithms for which, after receiving data, a model established by the programmer is applied in order to obtain a result; in this case, the assumption of liability for damage generated by the malfunctioning algorithm should fall on all those who took part in the chain of its production, with the discipline of defective product damage being applied extensively. This would therefore be, according to part of the doctrine[72], strict liability.

This being the case, programmers are held objectively liable for any defects in the code that has been used to make the system operational, forcing them to bear - in the event of damage being done - such a cost that innovation would be financially unsustainable, with the consequence that the development of Blockchain and Smart Contracts would be discouraged.

Indeed, if the Product Liability Directive were to be applied to the case at hand, in the light of the European defect in the matter, an excessively broad interpretation would be made: Directive 1985/374/EC provides that goods that are movable and tangible fall within the definition of a product, but it is quite clear that a tangible code string is not[73].

To remedy this problem, in some European jurisdictions, tangible software is considered to be tangible at the moment it is incorporated into the movable asset that

[70] Elodie Rouviere, Julie Caswell, 'From punishment to prevention: A French case study of the introduction of co-regulation in enforcing food safety' (2012) 3 Food Policy 246, 254.
[71] Think, from a purely civil law point of view, of the regulation of product liability.
[72] Remo Trezza, *Diritto e Intelligenza Artificiale* (Pacini Giuridica 2022) 54.
[73] Duncan Fairgrieve, Eleonora Rajneri, 'Is Software a Product under the Product Liability Directive?' (2019) 1 IWRZ 24.

will contain it[74], producing the knock-on effect - in terms of liability allocation - of having to involve, in terms of solidarity, not only the creator of the code but also, if different, the manufacturer of the asset[75].

An approach that limits the liability of developers by establishing appropriate standards of conduct could help safeguard and promote technological development; one might expect the software industry to do its best to ensure that algorithms are secure against computer intrusion, but one can never demand certainty[76]. Therefore, the European legislator could develop a liability standard that focuses on reasonable care and best efforts to avoid malfunctions as far as possible[77]. Indeed, it is precisely in this direction that the European institutions are moving, through the proposal for a directive put in place by the European Parliament in September 2022[78] and adopted in November 2024[79].

Notwithstanding possible regulatory developments to meet these regulatory shortcomings, however, the question of qualifying the applicable liability regime remains while relying, in fact, on increasingly automated technologies[80], there is a discrepancy between the attribution of liability to the parties programming these machines and the way in which control over these technologies could take place[81]. Particularly sensitive to the subject has been the German doctrine, which considers that product liability law is an appropriate instrument to regulate the phenomenon, only if the producer continues to be able to exert a certain influence on the damage that the product causes[82].

In the light of all these considerations, it is interesting to observe that, albeit through different interpretations and very different starting points, the conclusion has been reached that, at least with respect to the current state of the art, the discipline around which liability would revolve - both of the planners and of the protagonists of the supply chain - is the one, in some respects now outdated, of product liability, which moreover represents the pivot of the discipline of the liability of the operators of the supply chain.

---

[74] Giovanni Commandè, 'Intelligenza artificiale e responsabilità tra liability ed accountability' (2019) 1 Analisi Giuridica dell'Economia 169, 177.

[75] The main European jurisdictions that favour this hypothesis are Germany and United Kingdom; see, respectively: Ulrich Magnus, 'Product Liability in Germany' in Piotr Machnikowski (ed), *European Product Liability: An analysis of the State of the Art in the Era of New Technologies* (De Gruyter 2018) 245; Eden Miller, Richard Goldberg, *Product Liability* (OUP 2004) par 9.100. However, there is no lack of reflections to the contrary, for example, in Italy: Lavinia Vizzoni, *Domotica e diritto. La smart house tra regole e responsabilità* (Giuffrè Francis Lefebvre 2021) 185.

[76] Predrag Cvetkovic, 'Liability in the Context of Blockchain-Smart Contract Nexus: Introductory Considerations' (2020) 89 Зборник радова Правног факултета у Нишу 83, 85.

[77] Gitta Veldt, 'The New Product Liability Proposal - Fit for the Digital Age or in Need of Shaping Up? An Analysis of the Draft Product Liability Directive' (2023) 12(2) EuCML 24.

[78] The report accompanying the proposal for a directive is available at the following link: <https://eur-lex.europa.eu/resource.html?uri=cellar:b9a6a6fe-3ff4-11ed-92ed-01aa75ed71a1.0013.02/DOC_1&format=PDF> accessed 20 June 2025.

[79] Full text of Directive <*https://data.consilium.europa.eu/doc/document/PE-7-2024-INIT/it/pdf*.> accessed 20 June 2025.

[80] *Smart contracts* operating on blockchain are in fact *self-executing* contracts and once activated there is no way back, unless special chain *fork* or self-destruct functions are provided within the source code.

[81] Cvetkovic (n 76) 93.

[82] Gerhard Wagner, 'Robot Liability' [2018] SSRN <://papers.ssrn.com/sol3/papers.cfm?abstract_id=3198764> accessed 20 June 2025.

The reform deserves credit for attempting to adapt existing regulations to the growing complexity of new digital goods covered by the Directive. This is especially relevant given that these products are not always tangible—consider, for example, software—or, if they are, some of their components may not be, as highlighted in Recital 13 of the Directive.

Article 4, paragraph 1 defines products as any movable goods, even if integrated into or interconnected with other movable or immovable goods. This resolves a practical issue by eliminating the distinction, for proof purposes, between physical goods incorporating or interconnected with software and the software itself[83]. This clarification ensures that stakeholders in the supply chain are subject to the liability regime established by the Directive, even in cases where liability arises due to data manipulation or falsification.

Regarding the definition of "product," the 1985 Directive's concept of "movable goods" remains in place, with digital manufacturing files and software specifically added. However, some scholars[84] argue that separate definitions should be introduced for "digital manufacturing files" and "software" to align them with Directives 770 and 771 of 2019, thereby harmonising the rules on contractual liability for defects in services and extracontractual liability[85].

On the other hand, the European legislator has excluded open-source software acquired for free from the scope of the new Directive, a decision that has raised concerns, especially considering that the previous Directive did not exclude free products from liability coverage[86].

Article 8 of the new Directive is particularly relevant for the food chain, as it establishes the principle of joint liability for all economic operators involved in the production of a defective product, which is especially useful for analysing liability in long, multi-stage supply chains.

Questions may arise when the software causing damage is open source, as seen in public governance blockchains. Recital 14 and Article 2 of the new Directive use the need to protect innovation as a pretext to exclude open-source code, provided it is not part of a commercial activity—defined here as instances where the software is sold, or personal data is exchanged. However, it remains unclear why open-source software should be excluded, given that the previous Directive did not impose such exclusions for free products.

Despite these concerns, an interesting aspect of the reform is the shift in the reference moment for determining liability—from the time of market placement to when the

[83] Tommaso De Mari Casareto dal Verme, *Intelligenza artificiale e responsabilità. Uno studio sui criteri di imputazione* (Editoriale Scientifica 2024) 343.
[84] Izquerdo Grau, 'An Appraisal of the Proposal for a Directive on Liability' (2023) 2(5) EuCML 198; Christiane Wendehorst, 'Product Liability or Operator Liability for Ai – What is the best Way Forward' in S Lohsse, R Schulze, D Staudenmayer (eds), *Liability for AI* (Hart 2023) 99.
[85] Karni Chagal-Feferkorn, 'Am I an Algorithm or a Product? When Products Liability Should Apply to Algorithmic Decision-Makers' (2019) 30 Stanford Law & Policy Review 61.
[86] Andrea Cioni, 'Nuovi pregi e vecchi difetti della proposta di direttiva sulla responsabilità da prodotto difettoso, con particolare riferimento all'onere della prova' (2023) 88(2) Responsabilità civile e previdenza 656, 667.

manufacturer's control over the product ends[87]. While this change was likely aimed at software, it could also apply to any movable goods subject to stringent post-market monitoring, as in the case of food products. However, some argue that post-market controls should apply only to the software component, not the hardware[88].

The recent European reform, despite some limitations, represents a significant attempt to adapt the regulatory framework to the specificities of digital products, ensuring consumer protection while also fostering innovation. However, it will be crucial to monitor the evolution of these regulations to ensure that software developers, especially those working with open-source code, are not penalised, thereby maintaining the balance between accountability and incentives for innovation, but the way is clear: the development of the liability framework must provide a regulatory structure capable of harnessing the full potential of these new technologies, while mitigating their risks. It should outline responsibility not only along the supply chain but also throughout the blockchain[89].

7 Digital food liability law in United States

In the United States, the study of the functioning of digital-supply chain liability necessarily passes through a not insignificant systematic premise.

The rules concerning food safety on the 'new continent' are decidedly more confusing than those on the European scene, also in light of the fact that, on the one hand, the matter is entrusted to state competence and, on the other, that the tasks entrusted to the agencies dealing with food safety - unlike in Europe - include not only the preliminary scientific assessment of the risk, but also its management[90]. Furthermore, there is a further division of state competence concerning the type of foodstuff, with the added difficulty of having to manage different agencies not only in different states, but also according to the different product in question.

This fragmented nature has significant implications for the applicable regulations: even product liability laws, which apply to damages caused by food products, are limited by the jurisdiction of individual states. As a result, this creates considerable inconsistencies, not only in the sanctions imposed but also in the burden of proof the producer must meet to be exempt from liability. In some states, contributory negligence cannot be used as a defence by the manufacturer, while in others, such as Mississippi, it can. Additionally,

[87] Gerhard Wagner, 'Liability Rules for the Digital Age – Aiming for the Brussel Effect' (2022) 13 (3) Journal of European Tort Law 191, 206.
[88] ibid 210.
[89] Callegari (n 2) 1219.
[90] Carolina Magli, *Il danno da alimenti tra responsabilità del produttore e stile di vita del consumatore* (Cedam 2018) 173.

some states have statutes of limitation—time limits within which claims must be made—while others do not, further adding to the complexity[91].

To be able to resolve this composite situation, various solutions have been put forward that aim to achieve the same degree of harmony as the solutions adopted in European systems. First came the *Restatment (Third) of the Tort*, which, however, has no binding force for the Courts of the individual American States; subsequently, various proposals were launched for a *federal product liability*, which, however, Congress never followed up on, also in view of the difficulty in choosing the legislation to be raised to federal discipline[92].

A further solution envisaged by a part of the doctrine aims to avoid the - increasingly constant - phenomenon of the so-called *choice of law* and concerns the enactment of a rule that identifies, depending on the case, which law is applicable[93], creating, where necessary, a *federal pre-emption* of state law, assigning the agencies the task of achieving the much-desired regulatory harmony.

It is essential to establish a form of liability that is independent of the complex and often ambiguous regulatory framework. In the United States, when examining the liability regime for blockchain users, greater emphasis is placed on understanding the operational mechanisms of the technology itself, with a clear distinction made between public and private blockchains.

In permissionless one, liability is thought to be allocable under the theory of 'joint control', which is understood as the outcome of specific decisions made within the context of shared network governance. Instead, in permissioned blockchains, liability would be assigned to the individual node based on its specific level of involvement in the transaction that resulted in harm to a user, following a 'contractual theory'.

According to the theory of joint control[94], the civil liability of blockchain nodes is argued to be based on an analogy with the rules governing joint venture partnerships, equating the relationships between nodes to those between participants in a shared enterprise[95]. The central assumption is that liability is tied to the control exercised by certain actors over the network's organisational structure. Consequently, an inquiry into liability would focus on identifying who controls the structure and who bears its operational risks (and benefits)[96]. However, while the complete decentralisation of decision-making could, in theory, grant all nodes significant influence over one another's

[91] As an illustration, consider that the law of most states imposes disclosure requirements even after the sale, while in some, such as Mississippi, this obligation is not required by law.
[92] Carolina Magli, *La sicurezza alimentare tra norme preventive, obblighi risarcitori ed 'autoresponsabilità' del consumatore. Sistema italiano e statunitense a confront* (D.U. Press 2021) 72.
[93] Russell J Weintraub, 'Methods for Resolving Conflict-of-Law Problems in Mass Tort Litigation' [1989] U Ill Law Review 129, 141.
[94] Dirk Zetzsche, Ross Buckley, Douglas Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2018) 4 U Il L Rev 1361.
[95] Hugh Collins, 'Introduction to Networks as Connected Contracts', Gunther Teubner (ed), *Networks As Connected Contracts* (Hart 2011).
[96] Rainer Kulmsal, 'Blockchains: Private Law Matters' [2020] Sing J Legal Stud 63, 86.

positions, it has already been demonstrated that some users possess the ability to direct the behaviour of others by embedding specific commands in the source code, which in the context of a supply chain could be more easily traced.

In this regard, the theory of joint control faces significant limitations in relation to the principles of causal liability, as it risks extending responsibility to parties that have no direct involvement in the actions leading to the harm[97]. Although this approach attempts to align blockchain dynamics with existing legal frameworks, it fails to adequately account for the fundamental principle that liability—whether joint or several—should be rooted in a clear and direct causal connection between an actor's conduct and the resulting damage. This gap leads to potential uncertainty and inequities in the allocation of risk.

The contractual theory of liability, by contrast, finds fertile ground in blockchains with private governance, which are particularly common in the agrifood sector. This theory shifts the focus to how access to the platform is granted and emphasises the precise identification of the roles of those involved. In this context, a relationship is presumed between the "user-nodes" participating in a transaction and the entity managing the underlying infrastructure, with liability framed within a form of contractual responsibility. The network operator, in accordance with the contractual theory, would be liable for damages resulting from any defect in the infrastructure's operation, while the nodes involved in the transaction would be responsible for damages caused in other ways.

This theory gains further support from the fact that, in the United States, some States[98] have begun to recognise that a digital asset can be considered an object of property rights under two alternative conditions: the existence of specific regulations on the matter or the successful passing of the so-called *Wilberforce test*, the principle born in *National Provincial Bank v Ainsworth*[99]. According to this test, an asset can be subject to property law if it is determinable or identifiable, distinguishable by third parties, permanent, and stable criteria that seem to be met by tokens recorded on the blockchain.

However, attributing contractual liability to the software distributor that provides access to the network could serve as a disincentive to innovation, potentially rendering the model financially unsustainable. A preferable approach would be to limit such liability by setting clear standards of expected diligence, while also providing explicit guidelines for the cybersecurity measures required to safeguard the network[100].

Despite ongoing discussions about how to address these shortcomings, the question of the most suitable liability regime remains unresolved. As automation advances, a clear gap emerges between the assignment of responsibility to those who design such technologies and the practical mechanisms available for exercising control over them[101].

[97] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Elgar 2016).
[98] Arizona, Nevada, Wyoming, Illinois e Delaware.
[99] *National Provincial Bank Ltd v Ainsworth* [1965] AC 1175 (House of Lords).
[100] Cvetkovic (n 76) 100.
[101] ibid 93.

German legal scholarship has been particularly engaged with this issue, maintaining that product liability law offers an effective framework for regulation—provided that manufacturers retain a degree of influence over the harm their products might cause[102].

In Conclusion, it is particularly striking that, despite divergent interpretations and starting points, scholars broadly agree that product liability law remains the central legal framework governing liability for both software developers and supply chain actors. At least given the current state of technological development, this body of law serves as the primary regulatory mechanism for assigning liability across the industry—even beyond Europe.

8 Enhancing supply chain sustainability through blockchain technology

Thanks to the increased protection in the collection of data to facilitate the awarding of quality certifications, the capillarity of product traceability, and the increase in consumer confidence in the product, the supply chain may increase its competitiveness thus being able to pursue other objectives, not strictly related to immediate profit, such as environmental sustainability. This outcome is achieved through the assessment of corporate sustainability measurement via ESG (Environmental, Social, and Governance) ratings, the Sustainable Development Goals (SDGs), and the positive implications that a strong ESG performance can have on a company in terms of external investments[103]; specifically, it has been observed that value chains utilizing blockchain are rated more favourably compared to those that do not, precisely because of the data certification guarantees provided by this technology, which it implements in the aforementioned ways[104]. It can thus be concluded that the integration of ESG metrics has an increasingly significant impact on the economic and financial valuation of companies, linked to enhanced market reputation[105].

In fact, the practical application in which blockchain has been shown to be most conducive to sustainability has been supply chain traceability[106].

[102] Gherard Wagner, 'Robot Liability' in V Mak, T F E Tjong Tjin Tai, A Berlee (eds), *Research Handbook Data Science and Law* (Elgar 2018) 61.
[103] Tai Ming Wut, 'Intangible Assets and Sustainable Development' in Leal Filnho (ed), *Encyclopedia of Sustainability in Higher Education* (Springer 2019).
[104] Roberto Moro-Visconti, 'Fake news and (mis)information asymmetries' [2024] <https://www.researchgate.net/publication/380890830_Fake_news_and_misinformation_asymmetries.> accessed 20 June 2025.
[105] Kalpana Tyagi, 'A Global Blockchain-Based agro-food value chain facilitate trade and sustainable blocks of healthy lives and food for all' (2023) 10(1996) Humanities & Social Sciences Communications 1, 4; Roberto Moro Visconti, 'Rating ESG ed impatto sulla valutazione di marchi, brevetti, intelligenza artificiale e altri intangibili' (2024) 4 Il diritto industriale 386, 397. However, some scholars argue that the intersection between sustainability and profit may distort competition. Ex multis: Andrea Pezzoli, 'Come era verde il mio cartello' (2022) 1 Analisi Giuridica dell'economia 327.
[106] Francisco Luis Benítez-Martínez, Pedro Nuñez-Cacho, Valentin Molina-Moreno, Esteban Romero-Frías, 'Blockchain as a Service: A Holistic Approach to Traceability in the Circular Economy' in S Muthu (ed), *Blockchain Technologies for Sustainability* (Springer 2022) 119.

As companies' sustainability strategies evolve and sustainability reports require a high volume of data, the reliable and secure management of indicators such as water and energy consumption, chemical usage or the CO_2 impact of cultivation is an imperative that only blockchain can address.

Indeed, this technology guarantees the possibility of following a model of economy that is no longer linear, typical of the current supply chain (raw materials, production, distribution, consumption, waste), but circular[107]. This is undoubtedly a matter of primary importance, as the circularity of materials would be reliably and securely tracked, thanks to the peculiarities analysed so far.

Recording this information, however, is important not only in terms of environmental friendliness, but also in terms of corporate profitability: more and more consumers are orienting their purchases according to the sustainability of their choice[108].

Blockchain technology can play a crucial role in advancing a circular economy by enhancing the treatment, reuse, and disposal of waste. Through the transparent and immutable records provided by blockchain, it becomes possible to track the exact nature of waste materials, understand how best to recover them, and determine the most efficient methods for their reintegration into the supply chain. This includes processes such as recycling and reuse, where all previous steps and treatments the materials underwent are fully traceable and verifiable[109].

In addition to improving waste management monitoring, blockchain technology can facilitate more streamlined and efficient systems for managing waste, further supporting the shift towards a circular economy. By enabling the integration of various stakeholders and processes within the supply chain, blockchain systems can promote more sustainable practices such as the recycling of packaging materials and the reduction of waste.

The use of smart contracts and distributed ledgers within this context provides an added layer of efficiency and accountability. Smart contracts, which automate transactions based on pre-set conditions, could be utilised to optimise waste management processes, ensuring timely and accurate actions at each step. These mechanisms significantly enhance transparency, scalability, and operational efficiency across the waste treatment process, making it easier to implement and track circular economy initiatives. Ultimately, blockchain has the potential to create a more sustainable and closed-loop system, reducing waste and maximising resource recovery throughout the entire supply chain[110].

Finally, one of the most interesting aspects to be analysed is the challenge of constantly monitoring sustainability through tokenisation of assets; through this procedure, in fact,

[107] Circular economy in the context of the supply chain can be understood as that system whereby, once the end of the production cycle is reached, resources remain within the economic system so that they can be reused again in the production cycle and realise new value.
[108] On 28 November 2020, the Alliance of Agri-Food Cooperatives and Vodafone signed a cooperation agreement in the field of *smart agriculture* via apps for smartphones and tablets, sensors for monitoring agro-climatic parameters.
[109] Gallo, Capizzi, Timoshina (n 43) 94.
[110] Troisi (n 58) 150.

different stakeholders increase their cooperation and competition in building circular economy environments[111].

In this context, of great interest is the use of the so-called digital twin, ie, the virtual representation of an object, asset or process, which is updated in real time through IoT sensors placed on the actual product that transmit data to its 'digital' version, allowing measurements and simulations to be made in the areas of - among others - environmental impact and maintenance, with a huge reduction in costs[112].

In Spain, with reference to this possibility, a platform has been developed by the start-up Nutrasign2, allowing users to create a unique, secure and immutable digital token of each product, offering traceability from the origin of the raw material to the table.

However, the main problem encountered in this area concerns the absence of a definition of sustainability, which, to date, can only be found in a few *soft-law* texts[113] , the application of which is left to the free choice of the parties, even though it has, as mentioned above, a considerable impact on consumer choices[114].

9 Conclusions

Despite the incredible numbers of benefits that the use of blockchain would bring to the agri-food sector, there is a considerable level of mistrust among stakeholders about the technology, due to its still not optimal reputation, as well as several technical-legal problems that need to be questioned.

The first point concerns the reliability of the data that are stored by the blockchain. In addition to the system of node accountability above, the blockchain can never be sufficient to definitively eliminate fraud in the food chain, although, as more and more data becomes available and is linked to it, it will be easier to detect and trace it, significantly reducing the likelihood of fraudulent information corrupting the system.

It is also important to note that, from a business asset protection perspective, total transparency is not sustainable, because part of the industry's activity has an interest in not being known to the rest of the market[115]. To partially solve this problem, some data could be made available or visible only to certain node-participants, to guarantee corporate confidentiality, without the possibility of tampering. However, the conditions

[111] Benítez-Martínez, Nuñez-Cacho, Molina, Romero-Frías (n 106) 123.
[112] Laura Cappello, *L'evoluzione del consumatore negli ecosistemi decentralizzati. L'impatto della digitalizzazione e della blockchain* (G Giappichelli 2022) 115.
[113] An example is Article 12 of the Italian Code of Self-Regulation for Commercial Communications: "commercial communication claiming or evoking environmental or ecological benefits must be based on truthful, relevant and scientifically verifiable data. Such communication must make it clear to which aspect of the advertised product or activity the claimed benefits relate."
[114] Beatrice La Porta, 'L'etichettatura di sostenibilità nel settore vitivinicolo' in Giuseppina Pisciotta Tosini (ed), *Atti del convegno di comunicazione di sostenibilità e blockchain* (Palermo University Press 2022) 53.
[115] One thinks of the secrecy of information concerning the composition of certain products such as Coca-Cola.

for data access should be planned from the outset, making it complex for a new player to enter the supply chain.

However, the conditions of access to data would have to be planned before the starting of the system, making access to the supply chain complex for a new actor[116].

Before implementing the blockchain in the supply chain, it would be necessary to review the procedures that manage it, undertaking a thorough evaluation of the systemic effects it would have on operational procedures and trying to simplify them as much as possible. The solution, as doctrine has argued[117] , is not to integrate all possible data and documents on the blockchain, but only those considered most important.

Another long-standing issue concerns the environmental energetic impact of *mining*, the operation through which one node of the network, before all others, approves the transaction to be added to the ledger: the node with the highest computational power will be the first to solve the mathematical question necessary to approve the transaction, obtaining a reward for its work, which is usually a crypto-currency.

The problem concerns the increasing of one's computing power, because to do it, it is necessary to use very powerful computers, which consume considerable amounts of electricity, generating a nonsense whereby one tries to promote environmental sustainability through a technology that wastes huge amounts of energy. The solution to this question lies in the possibility of using other transaction approval mechanisms, which already exist, but are little used, such as *proof of stake*, which does not use the computational energy as the preferred criterion, but that of the resources that the individual node has available.

Finally, although the consumer has the computer certainty that a *smart contract* performs certain transactions and verifies certain conditions without being able to be tampered with in any way, he does not understand what these conditions are specifically: the smart contract, in fact, is not only written in a computer language[118] that the consumer does not know, but he does not even have the possibility of reading what conditions have determined its execution.

The lack of intelligibility of smart contracts, which results in a decrease in the trust users place in them, could be stemmed by the use of hybrid language - computer/linguistic idioms - that balances both the requirements of food security and the need for easy-to-read information that food security itself brings; it is no coincidence that the creation of

[116] Eloisa Marchesoni 'La blockchain per la tracciabilità del made in Italy: Origine, Qualità, Sostenibilità. Caso di studio applicato al settore tessile' (Ministero dello sviluppo economico & Ibm. 2019) <https://www.agendadigitale.eu/documenti/blockchain-per-lagrifood-rivoluzione-smart-contract-ecco-vantaggi-e-limiti/> accessed 12 June 2024.
[117] Hernandez (n 25) 567.
[118] Gallo, Capizzi, Timoshina (n 43) 100.

a copy of the smart contract written in natural language is becoming increasingly common in practice[119].

It was thus realised that blockchain technology enables the keeping of an infallible record of information, smart contracts allow, by analysing their content, an understanding of the history of the stored data, while machine learning technologies[120], such as IoT, guarantee real-time monitoring of the supply chain.

In conclusion, the integrity of the agri-food chain could certainly be achieved through these new technologies.

It is equally true, however, that talking about food integrity and food security necessarily leads the discourse towards the problem of subjectivity. Blockchain, in whatever form it takes, would not enjoy the legal subjectivity recognised by the law as a certifying body and, therefore, it would be appropriate to make a distinction between the use of blockchain as a technology capable of 'certifying the product' from a technology capable of 'certifying the supply chain', raising its safety standards, and in this latter concept, the sense of blockchain in the agri-food supply chain.

[119] Damiano Di Maio, Gioacchino Rinaldi, 'Blockchain and the legal revolution of smart contracts' (*Diritto bancario*, 11 July 2016) <https://www.dirittobancario.it/art/blockchain-e-la-rivoluzione-legale-degli-smart-contracts/> accessed 20 July 2025.

[120] With particular reference to artificial intelligence systems, they can play a crucial role in achieving sustainability goals: their computational power enables more precise interoperability and interconnection with the various technologies used within the supply chain. Cfr. Ricardo Vineusa, 'The Role of Artificial Intelligence in Achieving the Sustainable Development Goals' (2020) 233 Nature Communications 11. These studies have also been taken into consideration in the recent AI Act, as evidenced by Recital 4, which suggests that "it can provide key competitive advantages to businesses and lead to favourable social and environmental outcomes" in the agricultural sector. Upon careful reading of these regulations, it emerges, among other things, that these are the exact same indicators used in ESG assessments.

Gianfranco Alfano and Ludovica Vairo[*]

SPECIAL SECTION

TECHNOLOGICAL TOOLS AND TRADITIONAL MEASURES TO COMPLY WITH THE DMA

Legal analysis from gatekeepers' reports under Article 11

Abstract

This paper provides an in-depth examination of the technological and governance tools implemented by companies designated as "gatekeepers" under the Digital Markets Act (DMA) to fulfil the extensive *ex-ante* obligations set forth by the Regulation. Drawing on the (non-confidential summaries of the) compliance reports submitted in 2024 and 2025 by these companies under Article 11, the paper reveals – exploring both legal and technological dimensions – how gatekeepers align with the DMA's requirements. The study thus highlights the interplay between centralised enforcement by the European Commission, sophisticated technological solutions and robust governance measures required by the DMA, shedding light on both the achievements and challenges of maintaining compliance in rapidly evolving digital markets.

JEL CLASSIFICATION: K10, K21, K22, K23

SUMMARY

[*] Gianfranco Alfano is a business law researcher at University of Naples "Federico II". Ludovica Vairo is PhD graduate in economic and business law at University of Naples "Federico II". This paper is the outcome of a unified approach and a shared reflection by both authors. However, paragraphs 1, 2, 2.1, 2.2 and 4 are attributable, in particular, to Gianfranco Alfano while paragraphs 3, 3.1, 3.2, 5 and 6 are attributable, in particular, to Ludovica Vairo.

 DOI 10.13135/2785-7867/12270

1 Introduction

The Regulation (EU) 2022/1925 (Digital Markets Act, hereinafter "DMA")[1] represents a pivotal step towards contestability and fairness in the digital markets. Adopted pursuant to Article 114 TFEU[2], the DMA specifically targets large digital platforms, designated as "gatekeepers" in relation to specific core platform services. It imposes *ex-ante* obligations aimed at preventing anti-competitive behaviour and promoting an open, innovative environment within the digital sector, both in the EU and globally[3].

The DMA not only prescribes substantive obligations but also mandates rigorous reporting to demonstrate adherence. Indeed, a critical component of this regulatory framework is compliance, seen as the interaction between rules and gatekeepers' behaviour[4].

This paper provides a comprehensive analysis of the role of compliance reports, and the synergy between technological and governance strategies that support the broader compliance ecosystem. The research aims to investigate: *i*) the extent to which the compliance reports submitted under Article 11 of the DMA may be considered not only as tools for regulatory enforcement, but also as indicators of a substantive transformation in gatekeepers' business practices and as catalysts for greater transparency and accountability in digital markets; and *ii*) how the technological solutions and internal governance mechanisms adopted by gatekeepers vary across different core platform services in response to the DMA's obligations. The methodological approach adopted is primarily qualitative and legal-analytical, relying on the systematic analysis of all non-confidential compliance reports yearly published by gatekeepers, as available on the European Commission's website.

[1] European Parliament and Council Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.

[2] The choice of legal basis is due to the cross-border nature of digital services, which carries the risk of regulatory fragmentation with a negative impact on the functioning of the single market. See Sophia Catharina Gröf, 'Regulating BigTech: An Investigation on the Admissibility of Article 114 TFEU as the Appropriate Legal Basis for the Digital Markets Act based on an Analysis of the Objectives and Regulatory Mechanisms' [2023] SSNR <https://ssrn.com/abstract=4549209> accessed 9 March 2025; Marco Vargiu, 'Revitalisation of the essential facilities doctrine in EU competition law' (2023) 2(1) JLMI 104, 123.

[3] Fabiana Di Porto, Tatjana Grote, Gabriele Volpi and Riccardo Invernizzi, '"I see something you don't see". A computational analysis of the digital services act and the digital markets act' [2021] Stanford Computational Antitrust 85; Aline Blankertz and Julian Jaursch, 'How the EU Plans to Rewrite the Rules for the Internet' [2020] <https://www.brookings.edu/techstream/how-the-eu-plans-to-rewrite-the-rules-for-theinternet> accessed 9 March 2025; Aviv Gaon and Yuval Reinfeld, 'Advancing fair digital competition: a closer look at the DMA framework' (2024) 3(3) JLMI 358, 374.

[4] See Benjamin van Rooij and D Daniel Sokol (eds), *The Cambridge Handbook of Compliance* (Cambridge University Press 2021) 1,10.

2 Duty of power: the importance of being (designed as) a gatekeeper

The fact that the DMA's rules apply solely to a limited and predefined group of entities (formally designated as "gatekeepers" by the European Commission) leads to at least two types of consequences.

Firstly, and upstream, this affects the definition of the obligations imposed on gatekeepers, which are precise, pre-defined, and highly formalised[5]. In fact, the list of companies subject to this regulation has effectively been established by the European legislator, who then calibrated the size and qualitative thresholds set out in Article 3 of the DMA to "capture" the target companies[6].

Moreover, and downstream, it affects the characteristics of enforcement, allowing for the establishment of a centralised framework, essentially placed in the hands of the Commission alone[7] (which may be supported, in rather vague terms, by national authorities[8]). Both circumstances, as will be seen, contribute to fostering the development of regulatory dialogue spaces between the regulator and the regulated companies, who effectively cooperate in identifying virtuous behaviours and scrutinising the measures adopted within the framework of a process characterised by openness, adaptability, and collaboration.

2.1 Qualitative and quantitative criteria for the designation of gatekeepers. The (formal?) irrelevance of acting as an ecosystem orchestrator

Gatekeepers are designated according to both qualitative and quantitative criteria[9].

[5] See Friso Bostoen, 'Understanding the Digital Markets Act' (2023) 68(2) The Antitrust Bulletin 263, 267 <https://ssrn.com/abstract=4440819> accessed 9 March 2025.

[6] Bostoen (n 5) 274: «the EC had an idea which companies should be captured—in particular the GAFAM (*Google*, *Apple*, *Facebook*, *Amazon*, and *Microsoft*)—and then crafted the thresholds accordingly».

[7] On the contrary, Alberto Bacchiega and Thomas Tombal, 'Agency Insights: The first steps of the DMA adventure' (2024) 12(2) Journal of antitrust enforcement 189, 191, believe that the Commission should not be seen as «a lonely enforcer» of the DMA, as it can rely on mechanisms that ensure the involvement of national competition authorities (*ie,* European Competition Network and High-Level Group).

[8] Although some scholars advocate for a collaborative approach from the NCAs (see Gabriella Muscolo, 'Il rapporto tra applicazione/regolamentazione antitrust e il DMA', in Jacques Moscianese and Oreste Pollicino (eds), *Concorrenza e regolazione nei mercati digitali* (Giappichelli 2024) 110, no significant intervention by these national authorities has been observed during the initial phase of the DMA's application.

[9] Under Article 3(1) of DMA, an undertaking shall be designated as a gatekeeper by the European Commission if it: (a) has a significant impact on the internal market; (b) provides a core platform service which is an important gateway for business users to reach end users; and (c) enjoys an entrenched and durable position in its operations, or it is foreseeable that it will enjoy such a position in the near future. Article 3(2) of DMA provides quantitative thresholds, such as annual EEA turnover equal to or above EUR 7.5 billion or a market capitalisation of at least EUR 75 billion, along with a large base of monthly active end users and yearly active business users. As can be easily inferred from the examination of the European Commission's practice, the quantitative conditions set out in Article 3(2) establish a mere presumption of the fulfilment of the substantive requirements outlined in Article 3(1), which, however, may be proven through other means, following appropriate and more detailed market investigations conducted by the Commission.

Though the DMA itself characterises the quantitative thresholds as indicative rather than definitive, the Commission's «first wave»[10] of designations on September 2023[11] illustrates the considerable weight placed on these numerical benchmarks. Beyond the challenges in identifying a clear demarcation line between qualitative and quantitative criteria[12], the emphasis on quantitative metrics may be excessive, as it may overlook the ability of a platform to wield ecosystem-wide influence even without meeting the precise thresholds. The concept of "ecosystem" is absent in DMA rules: the word "ecosystem" appears only in the recitals[13], while the regulatory framework explicitly revolves around the (sole) notion of "core platform service", as clearly outlined in the wording of Article 3(1), letter b) of the DMA, under which a company may be designated as a gatekeeper if and insofar as it provides a core platform service that constitutes an important gateway for business users to reach end users[14].

Giving more prominence to qualitative considerations could better capture the power of the gatekeeper to be «market makers or orchestrators»[15], who not only govern the architecture of the ecosystem – typically shaped (often at the moment of its creation) to meet their own economic needs – but also have the power to unilaterally modify the operating rules of the same ecosystem[16]. And besides, the «gatekeeper power is not a mere measure of bigness»[17].

However, it «could be a strategic choice»[18] to avoid references to the (vague) concept of a digital ecosystem, to ensure the fulfilment of one of the primary objectives that inspired the very adoption of the DMA, namely, to guarantee swift and effective

[10] Alba Ribera Martínez, 'Full (Regulatory) Steam Ahead: Gatekeepers Issue the First Wave of DMA Compliance Reports' (*Kluwer Competition Law Blog*, 2010) <https://competitionlawblog.kluwercompetitionlaw.com/2024/03/11/full-regulatory-steam-ahead-gatekeepers-issue-the-first-wave-of-dma-compliance-reports/> accessed 9 March 2025.

[11] Commission Decision (2023) C/2023/6100 (*Apple*); Commission Decision (2023) C/2023/6101 (*Alphabet*); Commission Decision (2023) C/2023/6102 (*ByteDance*); Commission Decision (2023) C/2023/6104 (*Amazon*); Commission Decision (2023) C/2023/6105 (*Meta*); Commission Decision (2023) C/2023/6106 (*Microsoft*).

[12] Case T-1077/23 *ByteDance Ltd v. European Commission* [2024] ECLI:EU:T:2024:478, par 40, where it is stated that «it may be difficult, if not impossible, to distinguish between 'quantitative' and 'qualitative' arguments or evidence» and «it may appear artificial to separate one from another and to accept the relevance of the quantitative element alone where it is in fact intended to support an argument of a qualitative nature».

[13] Recitals 3, 32 and 64 of DMA.

[14] Many scholars have suggested – in the discussions preceding the final adoption of the DMA – the addition of the ability to coordinate ecosystems among the criteria for qualifying businesses as gatekeepers: see Alexandre de Streel, Richard Feasey, Jan Kramer and Giorgio Monti, 'Making the Digital Markets Act More Resilient and Effective' (Centre on Regulation in Europe 2021) 17 <https://cerre.eu/wp-content/uploads/2021/05/CERRE_-DMA_European-Parliament-Council-recommendations_FULL-PAPER_May-2021.pdf> accessed 9 March 2025.

[15] Robin Mansell, 'Platforms of power' (2015) 43(1) Intermedia 20, 25.

[16] Michael G Jacobides and Ioannis Lianos, 'Ecosystems and Competition Law in Theory and Practice' (2021) 30(5) Industrial and Corporate Change 1199, 1215.

[17] Alexandre de Streel, 'Gatekeeper Power in the Digital Economy: An Emerging Concept in EU Law' (*Organisation for Economy Co-operation and Development* 22 June 2022) 11 <https://one.oecd.org/document/DAF/COMP/WD(2022)57/en/pdf> accessed 9 March 2025.

[18] Phillip Hornung, 'The Ecosystem Concept, the DMA, and Section 19a GWB' (2023) 12(3) Journal of Antitrust Enforcement 17.

enforcement. And in fact, although formally irrelevant for the designation purposes (as confirmed by the EU case law[19]) some consideration of digital ecosystems seems "implicit" in certain obligations set out in Articles 5-7 of the DMA[20], which aim to fragment the services offered by gatekeepers (for example, preventing access to a core platform service from being conditional on prior registration with another core platform service offered by the same gatekeeper). It is not far-fetched to assert that, in substance, «the DMA has been intended to specifically address the problems related to ecosystems»[21].

The Commission has already demonstrated a willingness to consider non-numerical evidence by opening market investigations to confirm or reject gatekeeper designations[22]. Following the first wave of designations, the Commission soon included *Booking Holding Inc.* (*BHI*) for its accommodation intermediation service *Booking.com* and *Apple*'s *iPadOS*. Notably, *iPadOS* did not meet the quantitative thresholds but was deemed – after a qualitative investigation under Article 17(1) – to constitute an "important point of access" for business users, considering the market power held by *Apple* in the tablet operating systems segment[23].

This decision of the Commission also demonstrates the dynamism of the DMA. In light of the rapidly evolving and complex technological nature of core platform services, in fact, the DMA foresees «regular reviews» of gatekeeper status[24] (as well as of core platform services and obligations, in order to keep pace with the digital sector's rapid transformations)[25]. The Commission is required to adopt a flexible approach, reassessing whether designated gatekeepers continue to meet both quantitative and qualitative conditions at least every three years[26]. This mechanism ensures that the initial designations remain up to date and that newly influential platforms can be brought under the DMA's purview.

[19] Case T-1077/23 (n12), par 132, where it is stated that «no provision or recital of the DMA suggests that, in order to be designated as a gatekeeper, a company must necessarily control a platform ecosystem».

[20] de Streel, Feasey, Kramer and Monti (n 14) 50. See Frédéric Marty and Jeanne Mouton, 'Ecosystem as quasi-essential facilities: should we impose platform neutrality?' (2022) 1(3) JLMI 108, 133.

[21] Giuseppe Colangelo, 'DMA begins' (2023) 11(1) Journal of Antitrust Enforcement 116, 120.

[22] Article 17(1) of DMA.

[23] Commission Decision, C(2023) 4374 final (*The designation of iPadOS*) follows a qualitative investigation (Commission Decision (2023) C/2023/6076). According to European Commission analysis, «iPadOS has been one of the two leading operating systems for tablets in the Union for more than 10 years», and «it is expected that the number of end users and business users of iPadOS, and therefore its importance as a CPS, will continue to grow»; hence, although it does not meet the quantitative thresholds set by the regulation, iPadOS represents an important access point for commercial users to reach end users and must therefore be designated as a gatekeeper.

[24] Recital 30 of DMA.

[25] Recitals 77 and 105 of DMA.

[26] Article 4(2) of DMA. Some authors had suggested setting a longer timeframe (of at least 5 years) for the review of the gatekeeper status: see A de Streel, Feasey, Kramer and Monti (n 14) 87.

2.2 Gatekeepers' obligations under Article 5-7

Under the DMA, gatekeepers must comply with a series of obligations aimed «to ensure contestability and fairness for the markets in the digital sector»[27]. These obligations are numerous and diverse, yet all are intended to address the dysfunctions of digital markets not only in terms of prices, quality, choice, and innovation, but also in relation to abusive behaviours by the gatekeepers[28]. Specifically, some obligations primarily aim at ensuring fairness; others combine fairness with the facilitation of competition; still other obligations are primarily aimed at preventing the strengthening and consolidation of gatekeepers' market power, thereby facilitating the actions of competitors in the core services market or in adjacent markets.

At this point, a clarification is useful. The DMA is adopted based on Article 114 TFEU and aims – at least in principle – to seek objectives distinct from those of antitrust law. Nonetheless, the intention to promote competition in the digital markets overlaps at least partially with the provisions of Articles 101-102 TFEU[29]. The rules contained in the DMA have indeed been described as «*ipso facto* competition rules»[30].

Even in this area, however, the DMA seeks to achieve objectives that antitrust law has chosen not to pursue (or that, in any case, has not pursued adequately), and namely, removing barriers to entry in digital markets and levelling the playing field for businesses operating within them[31]. Many of DMA obligations are therefore aimed at "levelling" the starting conditions for companies operating in the digital sector[32], and can thus be considered as «a new, broader, 'antitrust plus' embodiment of the evolving concept of competition law»[33].

[27] Recital 7 of DMA.

[28] Pietro Manzini, 'Equità e contendibilità nei mercati digitali: la proposta di Digital Market Act' (*Aisdue* 2021) 33-39 <https://www.aisdue.eu/pietro-manzini-equita-e-contendibilita-nei-mercati-digitali-la-proposta-di-digital-market-act/> accessed 9 March 2025.

[29] Some scholars highlight how «the DMA appears to be merely an antitrust intervention vested by regulation»: G Colangelo (n 21) 122; similarly, Natalia Moreno Belloso and Nicolas Petit, 'The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove' (2023) 48 European Law Review 391. On the relationship between DMA and European competition law, see Mario Libertini, 'Il regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza' (2022) 4 Rivista trimestrale di diritto pubblico 1069; Margherita Colangelo, 'La regolazione ex ante delle piattaforme digitali: analisi e spunti di riflessione sul Regolamento sui mercati digitali (Regolamento (UE) 2022/1925 del 14 settembre 2022)' (2023) 2 Le Nuove Leggi Civili Commentate 422, 440.

[30] Oles Andriychuk, 'Do DMA obligations for gatekeepers create entitlements for business users?' (2022) 11(1) Journal of Antitrust Enforcement 123, 125.

[31] According to Giulia Ferrari and Mariateresa Maggiolino, 'Il potere across markets delle GAFAM: come reagire?' [2021] Rivista Orizzonti del diritto commerciale 471, antitrust law does not seek to eliminate barriers to entry; instead, it recognises their presence primarily to assess the potential longevity of the market power enjoyed by firms shielded by such barriers.

[32] Mariateresa Maggiolino, 'Is the DMA (Un)Fair?' (2024) 12(2) Journal of Antitrust Enforcement 267, 271: «the various rules outlined in the DMA can be interpreted as *equity-oriented* measures aimed at promoting *merit* over *meritocracy*».

[33] Andriychuk (n 30) 125.

More specifically, the catalogue of obligations set out in Articles 5-7 – while originating from case law in the area of antitrust[34], which in a *de jure condendo* perspective will also influence the evolution of the aforementioned set of obligations[35] – presents its own peculiarities[36], capable of overcoming some of the challenges encountered in the recent past in the application of antitrust law (particularly regarding abuse of dominance) in digital markets[37].

What emerges is a regulatory framework characterised by the *ex-ante* definition of the *dos & donts* that companies designated as gatekeepers must adhere to[38], following a logic typical of regulatory action[39]. While «competition laws are closer to standard»[40], the prescriptions of the DMA identify the objectives to be pursued by public authorities, define the parameters for identifying relevant subjects for the regulation, and then precisely establish the obligations imposed on them[41], within the pro-competitive perspective of regulatory acts[42].

These obligations, which are exhaustive in nature and thus not subject to broad or analogical interpretation, apply uniformly to all gatekeepers, «irrespective of their different business models»[43]. In doing so, they confer renewed substance to the concept of "special responsibility," long acknowledged as applicable to companies with significant market power[44].

[34] Lyuxing Tao, 'The 'gatekeeper scope' of the Digital Markets Act: An analysis of its soundness and compatibility of 'dominant position' in the competition law' (2024) 10 North East Law Review 108, 114; M Colangelo (n 29) 418. For a critic, see Rupprect Podszun, Phillip Bongartz and Sarah Langenstein, 'The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers' (2021) 10(2) Journal of European Consumer and Market Law 60, 67, according to which «the list of obligations should be closely revised, not with a view to competition law only, but with a broader assessment of market failures related to the activities of digital gatekeepers».

[35] Not only that: the update of the catalogue of obligations and prohibitions also appears "linked" to the evolution of case law in antitrust matters under Articles 101-102 TFEU, as expressly provided under Article 19(1) of the DMA.

[36] Filippo Donati, 'Verso una nuova regolazione delle piattaforme digitali' (2021) 2 Rivista della regolazione dei mercati 238.

[37] In digital contexts, therefore, the difficulties related to the (not always easy) identification of the relevant market in a digital setting and the demonstration of a company's "dominant" position are well known.

[38] According to Aurelio Gentili, 'Le fonti del diritto d'impresa: un tentativo di sistema' (2024) 2 Contratto e impresa 342, 344, «regulatory law performs a corrective function with respect to entrepreneurial autonomy».

[39] Bruno Carotti, 'La politica europea sul digitale: ancora molto rumore' (2022) 2 Rivista trimestrale di diritto pubblico 997, 1003.

[40] Bostoen (n 5) 267.

[41] See Rupprect Podszun, 'From Competition Law to Platform Regulation. Regulatory Choices for the Digital Markets Act' (2022) 17(1) Economics 1, 7: «regulatory law works with rules that are much more specific and prohibit or prescribe exact behavior».

[42] Ginevra Bruzzone, 'Verso il Digital Markets Act: obiettivi, strumenti e architettura istituzionale' (2021) 2 Rivista della regolazione dei mercati 323, 330.

[43] See G Colangelo (n 21) 118, 121, who instead suggests «the definition of obligations tailored to the business model under scrutiny», that «would have safeguarded the economic justification and the regulatory nature of the DMA».

[44] Case C-322/81, *Michelin v Commission* [1983] ECR I-3461, par 10.

The European Commission can apply conduct obligations not only to digital companies that already hold a «gatekeeper power»[45], but also to those that are close to acquiring such a status. In fact, some measures can be applied to so-called emerging gatekeepers, ie, companies that currently do not meet the qualitative and quantitative conditions to be designated as gatekeepers but that «will enjoy an entrenched and durable position in the near future» that «could become unassailable» so as «it appears appropriate to intervene before the market tips irreversibly»[46]. Such emerging gatekeepers may be subject to obligations which are particularly relevant for multi-sided platforms[47].

In any case, for each company subject to the DMA, compliance with the obligations set out in the regulation involves building technical solutions and governance measures (ie, a dedicated compliance function), amending existing mechanisms, and reviewing and revising existing policies. The following pages are dedicated to the analysis of the tools employed by gatekeepers, based on the information derived from the non-confidential summaries of the compliance reports published by the European Commission.

3 "Comply and explain": the role of compliance reports in enforcing the DMA

Gatekeepers have to comply with obligations of a dual nature: on the one hand, they are required, after an initial self-assessment, to align their services and business models with the provisions of the DMA through technical tools and internal governance mechanisms ("substantial obligations"); on the other hand, they must explain the measures they plan to adopt and/or have already adopted to the European Commission and the broader public of stakeholders ("reporting obligations").

One complementary to the other[48], these obligations appear to form an unprecedented "comply and explain" mechanism and provide the interpreter with a regulatory model that places significant emphasis on compliance reporting activities.

Each gatekeeper is required to submit a compliance report to the Commission within six months of designation (by the same deadline set for complying with substantial obligations), and to update it at least annually[49]. A summary of each report (excluding confidential information but still capable of illustrating the ongoing compliance efforts) is shared with the public on the European Commission's website.

[45] de Streel, Feasey, Kramer and Monti (n 14) 3.
[46] See Recitals 26 - 27 and Article 3 of DMA.
[47] Fabiana Di Porto and Annalisa Signorelli, 'Regolare attraverso l'intelligenza artificiale' in Alessandro Pajno, Filippo Donati and Antonio Perrucci (eds), *Intelligenza artificiale e diritto: una rivoluzione? Diritti fondamentali, dati personali e regolazione* (Il Mulino 2022) 627; Caio Mario Da Silva Pereira Neto and Filippo Lancieri, 'Towards a layered approach to relevant markets in multi-sided transaction platforms' (2020) 82(3) Antitrust Law Journal 701; Andrei Hagiu and Julian Wright, 'Multi-sided platforms' (2015) 43 International Journal of Industrial Organization 163.
[48] Anne Witt, 'The Digital Markets Act – Regulating the Wild West' (2023) 60(3) Common Market Law Review 640.
[49] Article 11(1) of DMA.

As some scholars have rightly pointed out, «the starting point of DMA enforcement is the compliance report by the gatekeeper»[50]: in addition to maximising overall transparency in the long term, in fact, the imposition of this reporting obligation allows for tracking the effects of the DMA's application in terms of market contestability and fairness[51], by highlighting the structural changes that various gatekeepers have implemented to comply with the rules[52].

These reports serve several interlocking functions, which can be identified in at least three categories.

The first function – undoubtedly the most evident – pertains to the assessment and control (both external and internal) of the measures implemented by the gatekeeper to ensure compliance with the DMA obligations.

The primary function of the compliance reports (which, in fact, will be examined in greater detail below) is fulfilled in their complete version, which is not subject to publication and is transmitted solely to the Commission. By reviewing these reports, the European authority can evaluate the effectiveness of gatekeepers' strategies, determining whether companies have genuinely adhered to the obligations or if further remedial actions are required.

In this sense, compliance reports thus become a fundamental and irreplaceable tool for reducing the informational asymmetries between the Commission and the gatekeeper company. The information must – in addition to being complete and detailed, as required by Article 11 DMA – be reliable for the Commission. The issue of credibility is central, as «compliance with the DMA cannot be rendered effective if the enforcer does not believe in the gatekeeper's informational disclosure»[53].

Moreover, always from an external perspective, non-confidential public summaries of these reports can be used by third parties (*ie*, competitors, consumers and consumer organisations, and even scholars and other stakeholders) to play a role in "bottom-up surveillance", often encouraged by the Commission itself, which invites experts and other

[50] Jasper van den Boom and Rupprecht Podszun, 'Procedures in the DMA: non-compliance navigation –Exploring the European Commission's space fordiscretion and informality in procedure and decision-making in the Digital Markets Act' [2025] European Competition Journal 4 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5091649> accessed 9 March 2025.

[51] It is therefore entirely understandable the surprise expressed by some scholars when recalling that the provision in Article 11 DMA was not included in the original proposal made by the European Commission in 2020, being added only following the intervention of the European Parliament: Alba Ribera Martínez, 'The Credibility of the DMA's Compliance Reports' (2024) 48 (1) World Competition 6, 7 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4932420> accessed 9 March 2025.

[52] Jacques Crémer, David Dinielli, Paul Heidhues, Gene Kimmelman, Giorgio Monti, Rupprecht Podszun, Monika Schnitzer, Fiona Scott Morton and Alexandre De Streel, 'Enforcing the Digital Markets Act: institutional choices, compliance, and antitrust' (2023) 11(3) Journal of Antitrust Enforcement 315, 325.

[53] Ribera Martínez (n 51) 3.

interested parties to provide feedback on the compliance proposals put forward by one or more gatekeepers[54].

From an internal perspective, however, the process of drafting the report represents a useful opportunity for self-assessment[55] and (consequently) self-correction for the gatekeeper companies[56]. These companies are encouraged to track the techniques employed to ensure compliance with the DMA, to highlight opportunities and risks, with the aim of improving future implementations.

In addition to the functions mentioned, two other perhaps less evident functions emerge, likely unintended – at least according to the legislator's declared intentions – but equally significant.

First and foremost, the public version of the compliance reports often acts as a knowledge-sharing platform, indirectly guiding smaller operators and market entrants on best practices and compliance strategies that might otherwise remain hidden. This can foster the development of a collaborative compliance culture across digital markets, engaging even smaller companies with less market power in a virtuous and spontaneous alignment with some of the behaviours outlined in the DMA.

Along the same lines, there is another function that can be defined as "voice". The significance of these documents may go far beyond the mere public representation of the gatekeeper's efforts to comply with European rules. Public summaries of compliance reports serve as an elective space where gatekeeper companies can present their perspective on the concrete choices made to adhere to the obligations laid out in the DMA (and the more or less participatory processes through which these choices were made[57]).

[54] See European Commission, *Consultation on the proposed measures for requesting interoperability with Apple's iOS and iPadOS operating systems* DMA.100204, 18 December 2024 – 9 January 2025 <https://digital-markets-act.ec.europa.eu/dma100203-consultation-proposed-measures-interoperability-between-apples-ios-operating-system-and_en> accessed 9 March 2025. As stated in the press release accompanying the document, the scope of the European Commission is to seek «feedback from interested third parties on the proposed measures in relation to the iOS features in the scope of these proceedings, namely notifications, background execution, automatic Bluetooth audio switching, high-bandwidth peer-to-peer Wi-Fi connections, AirDrop, AirPlay, close-range wireless file transfers, media casting, proximity-triggered pairing, automatic Wi-Fi connection, and NFC functionality. In particular, the Commission seeks views on the technical aspects of the measures». Among scholars, see Crémer, Dinielli, Heidhues, Kimmelman, Monti, Podszun, Schnitzer and de Streel (n 52) 327, who consider the non-confidential public summaries as «an enforcement tool that can substantially lower the costs to the Commission». This is by no means a minor issue; indeed, it has been noted that *ex-ante* regulation (such as the DMA) «is very costly since it involves mobilizing supervisory agents and efficient administration upstream of any activity» Pierre Bentata, 'Regulating "gatekeepers": predictable "unintended consequences" of the DMA for users' welfare' (*Competition forum,* 2022) 13 <https://competition-forum.com/wp-content/uploads/2022/01/art.-n%C2%B00031.pdf> accessed 9 March 2025.

[55] See Alexandre de Streel, Marc Bourreau, Richard Feasey, Jan Kraemer and Giorgio Monti, 'Implementing the DMA: substantive and procedural principles' [2024] Centre on Regulation in Europe 96.

[56] In the drafting of the compliance report, the head of the compliance function, envisaged under Article 28 DMA, takes on a primary role of responsibility. See Crémer, Dinielli, Heidhues, Kimmelman, Monti, Podszun, Schnitzer and de Streel (n 52) 327.

[57] See Amazon's Compliance Report (2024) 4: «Finally, prior to the launch of new features and consistent with Amazon's usual processes, we conducted user studies on key DMA requirements. The study outcomes helped inform the final

It can be seen as a tool for dialogue – and, in some respects, for marketing purposes[58] – with their users and other stakeholders, undoubtedly valuable given the profound changes that, in many cases, gatekeepers have made to their services and business models specifically to comply with the regulations. In this sense, the voice function of compliance reports would at least partially balance the European legislator's «institutional choice» to impose high penalties in the event of DMA violations, which are capable of attracting «significant media attention and stock market reactions»[59].

Compliance reports published on the European Commission's website provide insight into the guiding principles and strategic direction adopted – and formally declared – by the supervised BigTech companies in relation to the core objectives of the DMA. This approach manifests both in their autonomous initiatives, extending beyond mere compliance with the obligations set forth in the Regulation, and in their adherence to the means and methods established by the European legislator. A notable example in this regard is *Apple*'s Compliance Report, in which the Cupertino company expresses its clear discontent (and concern) regarding the choices made by European institutions, which it believes could «bring greater risks to users and developers» going so far as to declare that «Apple will continue to urge the European Commission to allow it to take other measures to protect its users»[60]. At the same time, it is equally interesting to consider the statements (rather different) accompanying the publication of *Microsoft*'s Compliance Reports, which highlight how the company's business model, based on offering an "open" OS service like *Windows*, has always been consistent with the spirit of the DMA[61].

The choice of venue by the two companies mentioned does not appear to be accidental, precisely because of the publicity that characterises these reports, which can be consulted by industry operators and the broader public of interested stakeholders. Whether and to what extent European institutions will heed these warnings – within the framework of the

customer-facing touch points, and help our customers, our advertising customers, and Sellers to navigate through the experience and understand its impacts and implications. Looking ahead, we have a wide variety of mechanisms for gathering feedback from our stakeholders, including customers, Sellers, and advertising customers, to help us continuously improve our compliance measures». It is noteworthy that *Amazon*, despite highlighting the open dialogue it has with its stakeholders, chose to produce a compliance report (in its public version) that is very concise and far less explanatory than those submitted by other gatekeepers.

[58] As observed by Ribera Martínez (n 10) some gatekeepers (namely: *Apple* and *Amazon*) «only presented a patchwork of marketing-approved statements to satisfy, in appearance, the requirement of submitting a compliance report».

[59] See Umberto Nizza and Cristina Poncibò, 'Antitrust Mega Fines in Digital Markets and Their Impact on Compliance: An Overview of EU and US Approaches' [2024] Stanford-Vienna Transatlantic Technology Forum Working Paper n° 115.

[60] Apple's Compliance Report (2024) 1.

[61] See Chris Nelson, 'Microsoft implements DMA compliance measures' (*Microsoft EU Policy Blog*, 7 March 2024) <https://blogs.microsoft.com/eupolicy/2024/03/07/microsoft-dma-compliance-windows-linkedin> accessed 9 March 2025: «because Windows is designed as an open platform for applications and has been for decades, it complied with many of the key provisions of the DMA even before the act was passed».

DMA review scheduled for 3 May 2026, and every three years thereafter[62] – remains to be seen.

3.1 Compliance reports and gatekeepers dialogue with the European Commission

Compliance reports serve as a vital tool for fostering an ongoing dialogue between gatekeepers and the European Commission.

The reports represent an opportunity for discussion from which positive effects can arise both for the Commission and for the gatekeepers, and ultimately, for the fairness and contestability of the digital markets.

From the Commission's perspective, the reports are an inexhaustible source of information regarding the dynamics of digital markets and the business models adopted by gatekeepers. These reports enable the Commission to attain a more comprehensive and timely understanding – otherwise inherently delayed and partial – of digital markets as a whole, with particular regard to the technical tools and governance measures adopted by gatekeepers. The effects are at least twofold: by having a greater (and more objective) awareness of the gatekeepers' adherence to the DMA's rules, the Commission is able, on one hand, to ensure more precise and comprehensive oversight, taking immediate corrective actions in the event of gaps or deficiencies, and on the other hand, to promote future revisions of the Regulation that would be more aligned with the needs of gatekeepers and digital markets, enhancing their fairness and contestability[63].

In fact, from the gatekeepers' perspective, compliance reports are not merely a means of reporting compliance but can serve as a space for gatekeepers to outline their concerns, approaches, and potential challenges in meeting the obligations. Furthermore, the gatekeeper «can also use it strategically (...) to test the limits of what can be considered compliant»[64].

The space dedicated to dialogue for compliance purposes – in which third parties may also participate[65] – is clearly highlighted by the Commission's practice of organizing specific public workshops dedicated to each gatekeeper[66]. In this context, the Commission

[62] Article 53 of DMA. From a combined reading of that article and Recital 105 of the DMA, it follows that the obligation of periodic review consists in assessing whether the objectives of ensuring fair and contestable markets have been achieved and determining the impacts on commercial users—particularly SMEs—and on end users. This assessment serves as a basis for considering any modifications to both the list of core platform services and the obligations imposed on gatekeepers, while also considering technological and commercial developments. On the evaluation and revision process of the DMA, see Alexandre de Streel, Richard Feasey and Giorgio Monti, *DMA@1: Looking back and ahead* (Centre on Regulation in Europe 2025) 90.

[63] Antonio Manganelli, 'Piattaforme digitali e social network, fra pluralità degli ordinamenti, pluralismo informativo e potere di mercato' (2023) 2 Giurisprudenza costituzionale 883, 886.

[64] Van den Boom and Podszun (n 50) 4.

[65] Namely, civil society representatives such as consumer protection associations, but participation is open to journalists, consultants, external lawyers, and academics or students.

[66] The list of workshops (*ie*: 25 November 2024 - BHI DMA compliance workshop; 26 March 2024 - Microsoft DMA compliance workshop; 22 March 2024 - ByteDance DMA compliance workshop; 21 March 2024 - Alphabet DMA compliance

acts as a "consultant", functioning as an «*amicus*» for the gatekeepers[67]. In particular, Article 8(3) allows gatekeepers to request a *preliminary* opinion from the Commission regarding the effectiveness of the measures they intend to adopt to comply with the obligations set out in the DMA. However, it is worth noting that, even if «it would be beneficial for gatekeepers to discuss its proposed compliance measures with the Commission before the deadline (…) it cannot be obliged to»[68].

It can be stated that «gatekeepers become part of and not just subject to the regulatory design»[69]; this option appears essential for overcoming one of the «weakest points» of the DMA, namely the irrelevance of economic justifications put forward by gatekeepers[70].

The regulatory paradigm underlying the DMA shifts from being a typically reactive mechanism addressing market dysfunctions and suppressing abuses to assuming a preventive and evaluative character[71].

3.2 Compliance reports and European Commission's centralised enforcement

The European Commission – through the joint team involving DG Competition and DG Connect[72] – is responsible for designating gatekeepers, issuing delegated regulations, updating obligations, and proposing amendments to the regulation. Consequently, it may initiate market investigations, conduct inspections, and adopt application guidelines, in the exercise of its monitoring functions. Furthermore, the Commission has investigative and monitoring powers, and acts as the *sole enforcer* of the DMA.

The rationale behind such a centralisation of powers essentially rests on at least two reasons: on one hand, the unprecedented nature of the rules could lead to fragmented

workshop; 20 March 2024 - Amazon DMA compliance workshop; 19 March 2024 - Meta DMA compliance workshop; 18 March 2024 - Apple DMA compliance workshop) is available at <https://digital-markets-act.ec.europa.eu/events_en> accessed 9 March 2025. See Ribera Martínez (n 10); Jasper van den Boom and Sarah Hinck, 'A Week of Workshops: Observations from the DMA Compliance Workshops' (*SCiDA Blog* 27 March 2024), <https://scidaproject.com/2024/03/27/a-week-of-workshops-observations-from-the-dma-compliance-workshops/> accessed 9 March 2025, who highlights that these workshops may be «transformative», since «such an open debate via a public engagement platform on how gatekeepers intend to comply and such direct feedback is a novel development within the EU».

[67] Jacques Moscianese, 'Il Digital Markets Act: oltre l'auto-regolamentazione dei gatekeeper' in Jacques Moscianese and Oreste Pollicino (eds), *Concorrenza e regolazione nei mercati digitali* (Giappichelli 2024) 13, 16.

[68] de Streel, Bourreau, Feasey, Kraemer and Monti (n 55) 103.

[69] Imelda Maher, 'Regulatory design in the EU Digital Markets Act: no solo run for the European Commission' (2024) 12(2) Journal of Antitrust Enforcement 273, 277.

[70] Bostoen (n 5) 288.

[71] Pedro Magalhães Batista and Wolf-Georg Ringe, 'Dynamism in financial market regulation: harnessing regulatory and supervisory technologies' [2021] Stanford Journal of Blockchain Law & Policy 203.

[72] See European Commission, Digital Markets Act, <https://digital-markets-act.ec.europa.eu/index_en#:~:text=The%20European%20Commission%20is%20the,and%20enforcement%20of%20the%20DMA> accessed 9 March 2025.

and contradictory outcomes[73]; on the other hand, the goal of a European digital single market is facilitated by the uniqueness of the oversight system, to avoid gaps and regulatory discrepancies[74]. This is even more significant given the targets of this regulation, identified as a small group of entities with immense power and impact at both the EU level and globally.

In addition to the aforementioned objectives, there may be another, less explicitly stated aim—one that, in certain respects, could be seen as a step towards a "return to the past". This concerns the desire to curb the assertiveness that National Competition Authorities (NCAs) had demonstrated in applying European antitrust law[75], which had been encouraged by the decentralisation process established through Regulation No. 1/2003[76].

The "political decision" to centralise powers within the Commission[77], while facilitating a coherent and efficient interpretation and application of the rules (and avoiding fragmentation of the internal market[78]), also raises some concerns[79]. The centralisation may have a potentially negative impact on the Commission's activities, which are burdened with additional functions[80], leading to a likely insufficiency in the enforcement of the DMA (with the potentially paradoxical effect of «amplifying the privileging of gatekeepers through insufficient DMA enforcement»[81]), especially given the unclear coordinating role that private enforcement can play[82].

[73] Not surprisingly, many scholars emphasise the need for a learning-by-doing approach aimed at gradually harnessing the experience acquired by the Commission itself – and, albeit in a more secondary role, by the NCAs – in enforcing the DMA (thus, Maher (n 69) 279). On this topic, also see Florian Wagner-von Papp, 'Digital antitrust and the DMA: in praise of institutional diversity' (2024) 12(2) Journal of Antitrust Enforcement 338, 344, who highlights the need for «experimentation with new competition tools». As observed by Nicolas Petit, 'The Proposed Digital Markets Act (DMA): A Legal and Policy Review' (2021) 12(7) Journal of European Competition Law & Practice 529, 540, the DMA «is based on very little 'experience' from cases and no feedback from judicial review».

[74] Luisa Torchia, 'I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale' (2022) 4 Rivista trimestrale di diritto pubblico 1101, 1108.

[75] Roberto Pardolesi and Cristoforo Osti, 'Superleague. Il canto di Natale della Corte di giustizia' (2023) 3 Mercato concorrenza regole 487, 498. However, limiting the role of national competition authorities may be seen as a risk, according to Gaon and Reinfeld (n 3) 363.

[76] Petit (n 73) 539, observes that the complex system of governance embodied by the DMA «appears designed in the same way as the governance system of Regulation 17/62». According to Giuseppe Giordano, 'Il Digital Markets Act e la centralizzazione dei poteri in capo alla Commissione europea: quale ruolo per le Autorità antitrust nazionali?' (2022) 3 Comparazione e diritto civile 979, 985, the approach adopted in the DMA contradicts the traditional decentralisation of European law.

[77] Libertini (n 29) 1078.

[78] Oreste Pollicino, 'Diritti, mercati e poteri: il processo di costituzionalizzazione dell'Unione Europea' in Jacques Moscianese and Oreste Pollicino (eds), *Concorrenza e regolazione nei mercati digitali* (Giappichelli 2024) 3, 7, 8.

[79] See Maher (n 69) 277, which highlights the need for the Commission to have «adequate human, financial and technical resources to perform its duties effectively».

[80] See Wagner-von Papp (n 73) 343: «the centralization of the enforcement powers with the Commission was criticized, especially in light of the resource constraints of the Commission, which is to take on the largest and most powerful undertakings in the world with only 80 additional staff».

[81] Jörg Hoffmann, Liza Herrmann and Lukas Kestler, 'Gatekeeper's potential privilege - the need to limit DMA centralization' (2024) 12(1) Journal of Antitrust Enforcement 126, 146.

[82] See M Colangelo (n 29) 435.

The principles of collaboration and cooperation between the Commission, national antitrust authorities[83], national courts[84], and Member States[85], although stated, have a «very weak» substance[86]. Furthermore, the DMA «does not provide many rules that would support such private enforcement»[87] which «may be rare but it can serve as an additional deterrent service»[88].

This institutional framework – which sees the Commission as a sort of "federal regulator for digital gatekeepers"[89] – must be considered alongside the decision to impose significant compliance and transparency burdens on the gatekeepers themselves, as well as the obligation to demonstrate proactively how their internal processes and technological interventions satisfy the DMA's requirements. This serves to mitigate the concerns mentioned above and ensure more precise monitoring of compliance by the European Commission. Indeed, it can be stated that «as part of their special responsibilities, 'gatekeepers' must be proactive in their cooperation with the Commission's scrutiny»[90], both at the designation stage and in the enforcement phase. Consequently, the actual attitude adopted by the gatekeeper can either facilitate or hinder, depending on the degree of cooperation, the Commission's activities[91].

Specifically, it is the gatekeepers who conduct the initial self-assessment and establish appropriate technical tools and internal governance mechanisms – *ie*, a dedicated compliance control function – aimed at ensuring full and continuous compliance with the obligations of the regulation. The reporting function constitutes one of the key governance measures introduced by the DMA, the purpose of which is also to facilitate enforcement by the European Commission.

[83] According to Article 37 of DMA, national competition authorities are required to report to the Commission on any violations of regulatory obligations resulting from their investigations, as well as to coordinate with it for the implementation of antitrust rules, with the aim of aligning their respective actions and avoiding regulatory overlap. The importance of strengthening coordination with national authorities is emphasised by Muscolo (n 8) 110; Gabriella Romano, 'Il ruolo delle ANC nell'implementazione del DMA' in Jacques Moscianese and Oreste Pollicino (eds), *Concorrenza e regolazione nei mercati digitali* (Giappichelli 2024) 43.

[84] According to Article 39 of DMA, national courts are involved in ensuring the «coherent application» of the regulation, mitigating the risk of conflicting judicial decisions with those adopted by the Commission.

[85] Member States (at least three) encourage the Commission to initiate specific investigations when they suspect that a company exceeds the relevant regulatory thresholds for qualifying as a gatekeeper or that violations of obligations exist. See Recital 41 of DMA.

[86] Rupprecht Podszun, 'From Competition Law to Platform Regulation – Regulatory Choices for the Digital Markets Act' (2022) 17(1) Economics 1, 10.

[87] Jirí Kindl, 'Prospects for concurrent private enforcement of the DMA and Article 102 TFEU' (2024) 12(2) Journal of Antitrust Enforcement 241.

[88] Giorgio Monti, 'The Digital Markets Act - Institutional Design and Suggestions for Improvement' [2021] TILEC Discussion Paper 1, 18 <https://ssrn.com/abstract=3797730> accessed 9 March 2025.

[89] M Colangelo (n 29) 430.

[90] Tao (n 34) 114.

[91] Crémer, Dinielli, Heidhues, Kimmelman, Monti, Podszun, Schnitzer and de Streel (n 52) 323.

The burden of proof of demonstrating compliance is placed on the gatekeepers[92]. The rationale behind this choice lies in the fact that they, much more than the Commission itself, are «the ones who know best about their business and true technical possibilities and limitations of their services» and are therefore «in the best position to determine how to offer their core platform services in a DMA-compliant way»[93]. As previously mentioned, the fulfilment of the reporting duty imposed on the gatekeeper thus serves to reduce the informational asymmetries that separate the gatekeeper and the enforcer; this circumstance, along with the irrelevance of economic justifications[94], helps ensure a quicker enforcement of the obligations set out in the DMA compared to antitrust law, thereby resolving one of the main weaknesses (or presumed weaknesses) of the latter regulatory framework.

A key role is played by the completeness of the information provided by the gatekeeper. Specifically, an effective report should present technical and economic data that clearly illustrate the gatekeeper's compliance with the DMA. Such information must be sufficiently detailed to allow for verification by the Commission and provided with a level of granularity that ensures both utility and comprehensibility[95]. Moreover, it is within the annual compliance report that the gatekeeper must demonstrate that «the implementation of the compliance solutions is workable»[96].

It is surprising, especially when compared with choices made in other contexts, the degree of freedom left by the Regulation to gatekeepers in drafting the reports. In addition to the (very few) guidelines found in Article 11 of the DMA, gatekeepers must adhere to the template published by the European Commission on 9 October 2023[97], which outlines «the minimum information that gatekeepers should provide in the Compliance Report» while leaving a considerable amount of flexibility to the obligated companies.

[92] However, as observed by Ribera Martínez (n 51) 11, «if a gatekeeper fights the scope of application of a provision, then the burden reverts to the EC to prove the undertaking wrong so that the burden of proposing new compliance solutions shifts back to the gatekeeper»; thus «the gatekeeper will not deliver the renewed technical implementation within the expected compliance deadline nor in the quickest possible manner».

[93] Bacchiega and Tombal (n 7) 193. See Crémer, Dinielli, Heidhues, Kimmelman, Monti, Podszun, Schnitzer and de Streel (n 52) 326, who underline that «gatekeepers know best the changes they have made and have access to data on the results».

[94] According to Emely von Platen, 'With or without efficiency defence? Analysing the role of efficiency defence in traditional ex-post enforcement, the EU Digital Markets Act & the UK Digital Markets, Competition and Consumers Act' (2024) (28) North East Law Review 22, 28: «concerns arise about potential overregulation and reduced flexibility due to the absence of an efficiency defense».

[95] Crémer, Dinielli, Heidhues, Kimmelman, Monti, Podszun, Schnitzer and de Streel (n 52) 325, who also underline that «an unsatisfactory or incomplete report should be seen as a signal that the obligation was not met, and hence should increase the probability of finding an infringement», just as «an obfuscatory report might signal non-compliance, and hence encourage the regulator to focus its attention on the gatekeeper who submitted it».

[96] Christophe Carugati, 'Compliance principles for the Digital Markets Act' (2023) 21 Policy Brief 1, 11.

[97] Commission, 'Template form for reporting pursuant to Article 11 of Regulation (EU) 2022/1925 (Digital Markets Act)' <https://digital-markets-act.ec.europa.eu/document/download/904debdf-2eb3-469a-8bbc-e62e5e356fb1_en?filename=Article%2011%20DMA%20-%20Compliance%20Report%20Template%20Form.pdf> accessed 9 March 2025.

It is precisely this flexibility, however, that has led to the emergence – particularly in the first wave of reports – of two different "types" of reports: some are very detailed, consisting of hundreds of pages of descriptions, while others are quite generic, full of vague and marketing-approved information[98]. In this regard, it is worth noting that, under Article 29 of the DMA, «the incomplete submission of non-confidential reports (based on Article 11 DMA) misses the mark of sustaining a standalone infringement whilst substantially undermining the DMA's efficacy with respect to third party»[99].

One may then wonder if the need for complete and comparable (public) reports might not make it appropriate to foresee a more detailed reporting obligation, similar to what is established by the Regulation on the European Single Electronic Format (ESEF), which requires – for financial compliance purposes only – the use of the European Single Electronic Format, with the stated aim of ensuring the automated readability of the related reports to facilitate analysis by investment firms and supervisory authorities.

4 Technological compliance tools

The compliance reports reveal a wide range of advanced technological tools designed by gatekeepers to comply their core platform services with DMA obligations.

The financial and human resources required to achieve full technical compliance are particularly substantial[100]. This reality is openly acknowledged by gatekeeper companies, which, in their compliance reports, explicitly highlight the significant multidisciplinary (legal expertise, engineering proficiency, and executive oversight) effort associated with ensuring adherence to the DMA obligations for their core platform services. For instance, *Meta* discloses allocating 11,000 personnel to DMA-related tasks and dedicating over 590,000 hours, illustrating the substantial human capital devoted to compliance[101]. Similarly, *BHI* underlines in its report that «hundreds of employees, from front-line account teams to senior executives, have been involved over the past two years in assessing BHI's compliance position, building tools to ensure that BHI operates in

[98] Ribera Martínez (n 10).

[99] Ribera Martínez (n 51) 13-19, who underlines that «there is no credible threat that the EC may set forth so as to disincentivise the motion as deriving from the letter of the law», since «the EC cannot trigger individual action to sanction the gatekeeper for an infringement of the terms of Article 11 DMA».

[100] Andriychuk (n 30) 127, identifies a potentially punitive dimension of the DMA, asserting that its obligations are intended to slow down gatekeepers, thus making room for new entrants.

[101] Meta, *Meta's Compliance Report* (2024) 2 <https://scontent-ord5-3.xx.fbcdn.net/v/t39.8562-6/431009250_1846639239090452_3219463139934460359_n.pdf?_nc_cat=107&ccb=1-7&_nc_sid=b8d81d&_nc_ohc=5BSmm3MqV1wQ7kNvwHu-Hwx&_nc_oc=AdkUMz7pqTcVjSf4Z-Xb7c2AyVAc0WyAefO95EWCt1X-bJlBAXjZ3Byoyf5iNGpGOPxK9UIV9t7xffpBrXDvsqii&_nc_zt=14&_nc_ht=scontent-ord5-3.xx&_nc_gid=tva-JsdTZKwO6jxiPjL5-Q&oh=00_AfOH2NVz2FWKgDJatAQZ8moRaQvkSbQOLQVbAibLayR4Sg&oe=68682F13> accessed 20 June 2025.

compliance with the DMA's requirements, and in communicating these changes to our partners»[102].

Certainly, in many cases, gatekeepers had already adopted, well before the application of the DMA, a conduct compliant with the rules set by the European legislator. However, in many other cases, the gatekeepers had to face – depending on the specific DMA obligation – the need to «building technical solutions, amending existing mechanisms, and reviewing and revising existing policies»[103]. In this regard, it is worth noting that the main innovations were seen primarily in two areas: data portability[104] and service interoperability[105].

As for the data portability mechanisms to ensure users can freely transfer their data between services, gatekeepers have begun to offer streamlined solutions, ranging from user-friendly application programming interfaces (APIs) to secure data export portals. Such measures aim to reduce switching costs and encourage competition by allowing users to choose alternative platforms without losing valuable data, thus facilitating the simultaneous use of multiple competing platforms (the so-called multi-homing). Indeed, the greatest risk stems from platforms that hold bottleneck power—«a situation where consumers primarily single-home and rely upon a single service provider (a "bottleneck"), which makes obtaining access to those consumers for the relevant activity by other service providers prohibitively costly»[106]. It is precisely in this case that the platform becomes the sole point of access for these users, acquiring the capacity (and incentive) to establish "the rules of the game" even possibly "manipulating" users' preferences, who have no other option but to comply[107]. In other words, platforms «act as regulators of the interactions they host»[108]: they unilaterally set the contractual rules, which users voluntarily accept by agreeing to the terms and conditions of service[109].

[102] BHI, *BHI's Compliance Report* (2024) 4 <https://build-health-international.shorthandstories.com/2024-bhi-annual-report/index.html> accessed 20 June 2025.

[103] Amazon, *Amazon's Compliance Report* (2024) <https://s2.q4cdn.com/299287126/files/doc_financials/2025/ar/Amazon-2024-Annual-Report.pdf> accessed 5 June 2025.

[104] Within the framework of the DMA, the right to data portability becomes a fundamental pillar for enabling competition among digital enterprises (and not merely, as in the GDPR, an individual right). See Federico Ruggeri, *Poteri privati e mercati digitali. Modalità di esercizio e strumenti di controllo* (RomaTre Press 2023) 183.

[105] Bertin Martens, 'An Economic Policy Perspective on Online Platforms' Institute for Prospective Technological Studies Digital Economy Working Paper 44 (European Commission 2016): «the value of data is often limited by regulatory, commercial and practical barriers to interoperability».

[106] Stigler Committee on Digital Platforms, 'Final Report' [2019] <https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler- center.pdf> accessed 9 March 2025.

[107] Ryan Calo, 'Digital Market Manipulation' (2014) 82 The George Washington Law Review 995, 1000, redefines the concept of "market manipulation" to account for companies' ability, in the context of digital marketplaces, to exploit consumers' cognitive limitations and "target" them, with the aim of persuading them through the complete personalisation of every aspect of their experience.

[108] Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, *Competition policy for the digital era. A report* (Publications Office of the European Union 2019) 71.

[109] Jack M Balkin, 'Free speech is a triangle' (2018) 118(7) Columbia Law Review 2011.

For real interoperability and the possibility of migration between competing platforms to be achieved, establishing complex mechanisms for downloading and transferring personal data can be not sufficient. It is essential that gatekeepers provide *effective* data portability for both business users and end users[110]. Therefore, it is necessary that the service is, on the one hand, user-friendly, so that it can be easily utilised – in a self-service perspective, without the need for external support – by users with limited knowledge in the field of information technology[111]; and, on the other hand, efficient and prompt, so as to avoid "technical disincentives" (related to excessive timing of the data download and transfer function) that would prevent migration to alternative platforms.

On the first aspect, very often the mechanisms provided by the gatekeepers are specifically described in compliance reports through mobile screenshots. This circumstance highlights the usability of compliance reports as communication tools to facilitate the public's understanding of the technological solutions adopted by gatekeepers[112]. On the second point, compliance reports show how gatekeepers have, on various occasions, technically improved their data download and transfer services even beyond what is strictly required under the DMA, upon European Commission's nudge[113].

In other circumstances, compliance reports describe the future developments of the services offered by gatekeepers, which in the area of data download and transfer are clearly moving towards a better (and faster) functionality of the provided services. In this regard, it is certainly worth mentioning the example of *ByteDance*, which, even before being designated as a gatekeeper, had already equipped its core platform service *TikTok* with «various data portability solutions» functionalities (such as the "Download Your Data - DYD"), which provide users with the ability to port their data, including their videos. In addition, *ByteDance* has enabled *TikTok* users «to (a) download their own videos and (b) instantly share them on multiple other platforms from the TikTok app»[114]. Even for these services, the impact of the obligations set out in Article 6(9) of the DMA has resulted in

[110] Petit (n 73) 536.

[111] On the other hand, a different approach would exclude precisely the most vulnerable users from the protection afforded – albeit indirectly – by the DMA, as these individuals do not have sufficient familiarity with IT systems and are therefore at greater risk of being discouraged (if not practically barred) from migrating from one service to another.

[112] See Amazon (n 103) 10, where the technical solutions adopted by *Amazon* are described as «customer- and developer-friendly».

[113] Meta's Compliance Report (2024) states that *Meta* – after its dialogue with the European Commission – has further improved its services. Although the company had already made data download and transfer mechanisms available to its users (*ie*, the "Download Your Information – DYI" and the "Transfer Your Information Tool – TYI"), and although through these services *Meta* was already compliant with the obligations under Article 6(9) of the DMA, «in response to the Commission's feedback, *Meta* has increased the recurrence of TYI transfers for monthly to daily and increased the duration from 3 months to 1 year».

[114] ByteDance's Compliance Report (2024) par 18.2. The most recent enhancements to *TikTok*'s data portability offering, in line with Article 6(9) of the DMA, «consist of three main parts: *i*) developing a Data Portability API (...); *ii*) improving data access speeds (...); and *iii*) offering a more granular selection of the data to be ported (...)», which enables users to make a more granular selection of data types for portability (users can choose either the complete archive or select specific categories of data such as posts and user profiles).

some technical improvements to the services planned for the near future: as declared in the compliance report, *TikTok*'s DYD will be further enhanced and its data storage and serving system upgraded to shorten the time between the portability request and the porting from 1-2 days to an estimated seconds or minutes.

Complementary to this aspect are the interoperability solutions, which remain a cornerstone of the DMA's vision for an open digital ecosystem, as they can lower entry barriers. Gatekeepers are required to facilitate interactions with rival services, whether through integrated messaging platforms or standardised protocols that allow smaller market participants to connect with the gatekeeper's user base. Achieving genuine interoperability can be technically complex, often involving protocol adaptation or the creation of bridging solutions, but it allows for «rebalancing the allocation of resources between gatekeepers and their competitors»[115] to ensure equal opportunities. Naturally, the implementation of such solutions requires significant technical efforts from gatekeepers to ensure, on the one hand, the efficiency and robustness of the systems (so as not to worsen the user experience) and, on the other hand, the protection of the data and information shared via these integrated services.

Another particularly impactful aspect of the DMA, with significant consequences for the operations of gatekeepers, concerns the functioning of the automated ranking mechanisms operated by digital platforms. The adoption of advanced and increasingly sophisticated algorithmic tools offers both opportunities and risks[116]. While these technologies enhance process efficiency, they also introduce opacity into decision-making mechanisms[117], potentially leading to covert distortions in competition among business users relying on a gatekeeper's core platform services. Given that algorithmic transparency and non-discrimination are crucial for mitigating covert manipulation and ensuring fair market conditions, it is essential to continuously evaluate both the foundational structures and the outputs of the algorithmic processes in place[118].

Gatekeepers frequently deploy algorithms to rank search results, recommend products, or personalise user interfaces. In pursuit of non-self-preferencing, some gatekeepers have implemented transparent ranking parameters. Although the exact details of these algorithms are often proprietary, compliance reports detail the efforts made to remove undue bias and ensure that third-party listings have equitable visibility. In this context, *Amazon* states in its 2024 compliance report that its «ranking processes operate in an unbiased manner, using objective inputs and weighing them neutrally to facilitate the

[115] Maggiolino (n 32) 271.

[116] See Filippo Donati, 'Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale' in Alessandro Pajno, Filippo Donati and Antonio Perrucci (eds), *Intelligenza artificiale e diritto: una rivoluzione? Diritti fondamentali, dati personali e regolazione* (Il Mulino 2022) 112.

[117] Frank Pasquale, *The black box society. The Secret Algorithms That Control Money an Information* (Harward University Press 2015).

[118] Mariateresa Maggiolino, *I big data e il diritto antitrust* (Egea 2018) 37-43.

best possible customer choice irrespective of whether a product is offered by Amazon Retail or Sellers», in order to be compliant with Article 6(5). Additionally, to meet the requirements set forth in Articles 5(9), 5(10), and 6(8), *Amazon* reports having added «more granularity» to pricing reports to provide detailed data on the fees paid by advertisers and received by publishers for ads displayed on third-party websites and apps. The company also highlights updates to its advertising services, including the introduction of a new clean room, allowing advertisers to independently verify the performance and impact of their campaigns. Moreover, in its 2025 compliance report, *Amazon* states that, following the adoption of specific compliance measures related to its automated systems supporting retail decisions (including any automated algorithm, model, or tool), «all automated systems in connection with the decisions that could be viewed as "in competition with business users" do not ingest non-public business user data»[119].

Finally, it is not excluded that gatekeepers may use advanced machine-learning tools to monitor and report compliance continuously. These systems could track metrics such as how often third-party applications are recommended compared to the gatekeeper's own services or whether user data handling procedures align with DMA stipulations[120].

In contrast, compliance with some obligations, though still significant, has required modest technical efforts, as they refer to gatekeeper companies as providers of multiple (and interconnected) core platform services. For example, consider the compliance with the obligation set out in Article 5(8) of the DMA (according to which «the gatekeeper shall not require business users or end users to subscribe to, or register with, any further core platform services listed in the designation decision pursuant to Article 3(9) or which meet the thresholds in Article 3(2), point (b), as a condition for being able to use, access, sign up for or registering with any of that gatekeeper's core platform services listed pursuant to that Article»), where, in some cases, it proved sufficient to remove the login screen that previously required access to a different service offered by the gatekeeper[121].

The same applies to the obligation under Article 5(2) of the DMA[122]. In this case, it was sufficient for gatekeepers to include in the initial screen of its core platform services a

[119] Amazon, *Amazon's Compliance Report* (2025) <https://www.aboutamazon.eu/news/policy/amazon-and-the-digital-markets-act> accessed 5 June 2025 par 136.

[120] For instance, Amazon has declared—albeit somewhat vaguely—that it has implemented «guidelines as forward-looking compliance mechanisms designed to prevent any new agreements from containing clauses inconsistent with Article 5(3) […] Articles 5(4) e 5(6)». In addition, Amazon states that it has implemented «a range of mechanisms designed to maintain continued compliance with the requirements of Article 6(2) of the DMA, both in relation to automated and manual decision-making. Such mechanisms include review processes to audit proposed system changes, refresher training courses for employees, and updating the controls, monitoring, and auditing mechanisms that apply to relevant data access paths on an ongoing basis».

[121] See Meta, *Meta's Compliance Report* (2025) <https://ppc.land/content/files/2025/03/481770322_1578920512785307_385504078597978166_n.pdf> accessed 5 June 2025 par 71.

[122] According to Article 5(2) of DMA, «the gatekeeper shall not do any of the following: (a) process, for the purpose of providing online advertising services, personal data of end users using services of third parties that make use of core

section offering users the choice to either use the services jointly (allowing the gatekeeper to combine the data) or use them separately[123]: *Meta*, *Alphabet* and *Amazon*, for example, acted in this direction, as stated in their compliance reports[124].

5 Compliance functions in gatekeepers' corporate governance

Beyond the field of technical innovation, the DMA underscores the importance of robust organisational structures for ensuring sustained compliance.

Pursuant to Article 28, gatekeepers are required to establish a dedicated compliance function, independent from their operational functions and equipped with sufficient authority, stature, and resources. The DMA compliance function must also have direct access to the gatekeeper's management body to actively advise on and oversee the implementation of strategies and policies for adopting, managing, and monitoring compliance with the DMA.

The European legislator, therefore, places companies designated as gatekeepers on par with other supervised entities (particularly in the banking sector), in line with the current trend of extending the scope of oversight by granting explicit powers in this regard to the board of directors, expanding those of the supervisory body, and creating a proliferation of functions, bodies, and committees.

These functions are situated in a high-level management sphere and remain near the corporate bodies, with whom the responsible individuals interact continuously[125]. The function envisaged under Article 28 of the DMA is thus integrated into the polycentric system of controls adopted by gatekeepers, which is itself delicate and heterogeneous[126].

The precise configuration of these functions is, however, not easily determined. It is worth noting, in fact, that the concept of compliance risk and the provision for the corresponding function do not appear in primary legal sources and remain rather

platform services of the gatekeeper; (b) combine personal data from the relevant core platform service with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services; (c) cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice versa; and (d) sign in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice (…)».

[123] However, according to Alphabet's Compliance Report (2025) 7, to comply with Article 5(2), Alphabet developed and launched controls «through measures within both the front-end of Google's services (ie, the end-user facing portions of Google's services) and Google's backend infrastructure (ie, the systems and code that underpin the provision of services to end users)».

[124] Meta (n 121) par 1, lett b); Alphabet's Compliance Report (2025) 7; Amazon (n 103).

[125] Sabino Fortunato, 'Il dirigente preposto ai documenti contabili nel sistema dei controlli societari' (2008) 4 Le Società 401, 402, has long referred to the "baroque" construction of the control system.

[126] Paolo Montalenti, *Impresa, società di capitali, mercati finanziari* (Giappichelli 2011) 143; Francesco Chiappetta, 'Il controllo interno tra compliance normativa e attività gestionale' in Umberto Tombari (ed), *Corporate governance e "sistema dei controlli" nella s.p.a.* (Giappichelli 2013) 53.

underexplored in legal literature and case law[127]. Conversely, the focus on compliance with laws and regulations – and thus the establishment of a dedicated function – has long been embedded in the regulatory framework governing banks and financial intermediaries. It has also been comprehensively embraced in the field of management, which recognises the full proceduralisation of corporate and business organisation and activities. Through organisational and functional charts, the various operational, support, and control functions – reporting to the governance bodies – are delineated, specifying their respective responsibilities, execution methods, designated personnel, and allocated resources.

The compliance function constitutes a tool in the hands of management[128] for the informed and dynamic management of regulatory compliance risk, namely the risk of incurring judicial or administrative sanctions, significant financial losses, or reputational harm because of violating mandatory rules (whether legal or regulatory) or self-regulatory measures (e.g., statutes, codes of conduct, self-regulation codes)[129]. Given that this risk cuts across every level of the organisation (being not only operational but also reputational, and therefore multidimensional[130]), it is evident that the compliance function, endowed with independence and autonomy, its own budget, and a dedicated organisational structure, is entrusted with assurance and advisory tasks. These tasks ultimately aim to promote a culture of reputational value within the organisation[131].

This typically entails the identification of compliance officers and the establishment of compliance committees. These are individuals or bodies within the corporate governance hierarchy who oversee compliance processes, resolve internal disagreements, inform and advise managers and employees regarding adherence to the DMA, and collaborate with the Commission. It is also necessary to designate a senior independent executive with distinct responsibilities for the compliance control function, placed in a suitable hierarchical and functional position, who will serve as the head of the compliance control function and, as such, report directly to the gatekeeper's management body.

[127] See Roberto Wiegmann, *Responsabilità e potere legittimo degli amministratori* (Giappichelli 1974) 303, 364; Berardino Libonati, *L'impresa e la società. Lezioni di diritto commerciale* (Giuffrè Editore 2004) 264.

[128] Umberto Tombari, 'Governo societario, compliance e indagini "interne" nella s.p.a. quotata' in Guido Rossi (ed), *La Corporate Compliance: una nuova frontiera per il diritto?* (Giuffrè Editore 2017) 263.

[129] See EBA, 'Guidelines on internal governance under Directive 2013/36/EU' [2021] par 33 («the compliance function monitors compliance with legal and regulatory requirements and internal policies, provides advice on compliance to the management body and other relevant staff and establishes polices and processes to manage compliance risks and to ensure compliance»). The concept of compliance risk and the need to establish a compliance function within banks and banking groups has been highlighted, since 2005, also by the Basel Committee on Banking Supervision (see BCBS, 'Compliance and the compliance function in the banks' [2005]).

[130] BCBS, 'Proposed Enhancements to the Basel II Framework' [2009], where it is clarified that such risk is to be understood as «the risk arising from negative perception on the part of customers, counterparties, shareholders, investors or regulators».

[131] Alessandro De Nicola, *Il diritto dei controlli societari* (Giappichelli 2023) 290.

Such governance frameworks are designed to institutionalise compliance; however, gatekeeper companies bear the burden of transforming it from a box-checking exercise into a core business function. By embedding compliance at the highest levels of corporate governance, gatekeepers aim to foster a culture where meeting regulatory standards is treated as a strategic priority rather than a peripheral cost.

In this regard – and in view of the influence that the compliance function is intended to exert on the decision-making process and the board of directors' monitoring activities – technical standards, guidelines, opinions, recommendations, and Q&As issued by legislators and supervisory authorities in regulated sectors beyond the digital domain are extremely helpful. In short, these flexible and multifaceted regulatory instruments, lacking binding effect yet not without force, perfectly align with the latest trends[132].

The role of the head of the compliance control function is significant, especially regarding the relationship with the gatekeeper's management body. It should be noted that this role typically (though not necessarily) exists *outside* the management body[133]. Nevertheless, pursuant to Article 28(2), gatekeepers must take all necessary measures to ensure that the head of this function has full access to the management body. In this regard, the precise allocation of competences and decision-making authority (from which clear implications arise in terms of liability) between the compliance officer and the management body has yet to be fully understood[134].

A constructive exchange can therefore develop between the head of the function and the board to ensuring thorough and genuine adherence to the obligations set out in the DMA. Consistent with regulatory provisions and established practice, this function is supervised by the gatekeeper's management body, with which it keeps constantly proactive dialogue[135]. At the same time, it maintains an operational role in support of the supervisory body for conducting inspections and investigations, and it requires continuous information flows with other compliance functions, as well as with risk management and internal audit. This confirms a relatively recent approach that views the organisational system as a whole, recognising the interplay between governance bodies and the

[132] See Luisa Torchia, 'I poteri di regolazione e di controllo delle autorità di vigilanza sui mercati finanziari nella nuova disciplina europea' in Giuseppe Carcano, Maria Chiara Mosca and Marco Ventoruzzo (eds), *Regole del mercato e mercato delle regole. Il diritto societario e il ruolo del legislatore* (Giuffrè Editore 2016) 355.

[133] The European legislator does not intervene on this topic, presumably in consideration of (the lack of harmonisation and) the national peculiarities characterising corporate and business law at the Union level.

[134] See Luigi A Bianchi, 'Key manager e gestione dell'impresa: appunti per una futura ricerca' (2022) 2(3) Rivista delle società 646, who also criticises the legislative void that characterises Italian corporate law *in subiecta materia*.

[135] On the pivotal role of the management body, see Maurizio Irrera and Elena Fregonara, 'I sistemi di controllo interno e l'organismo di vigilanza' in Maurizio Irrera (ed), *Diritto del governo delle società per azioni e delle società a responsabilità limitata* (Giappichelli 2020) 261. On the proliferation of oversight demands in the face of increasingly complex internal decision-making processes and corporate programs, see Gastone Cottino, 'Dal vecchio al nuovo diritto azionario: con qualche avviso ai naviganti' (2013) 1 Giurisprudenza commerciale 5, 26; Giovanni Strampelli, *Sistemi di controllo e indipendenza nelle società per azioni* (Egea Editore 2013) 2.

corporate structure and functions, as well as the need for predefined organisational and behavioural rules[136].

Obviously, the effectiveness of the information exchange between the head of the control function and the board can be enhanced when the latter is better equipped in terms of knowledge, skills, and experience. In this regard, it is worth noting that some gatekeepers have chosen to "replicate" certain provisions established in the banking sector concerning the suitability of the board of directors[137]. As an example, *BHI* stipulates that the management body must be «well-suited to fulfil the duties and responsibilities outlined in the DMA» and «devote sufficient time to managing and monitoring DMA compliance, actively participate in major decisions, and ensure adequate resources are allocated»[138]. A similar perspective emerges in *Microsoft*'s compliance report, which outlines how the introduction of new duties and responsibilities for members of the management body – particularly in light of the need to collaborate with the head of the compliance function – has influenced the board member selection process[139].

To ensure that the head of the compliance function can effectively fulfil their assigned duties without undue external influence, it is established that this individual should report exclusively to the board of directors or a dedicated committee (as in the case of *Meta*), rather than to senior executives. Likewise, to ensure independence and strengthen this position, Article 28(4) provides that the head of the function may be removed only with the prior approval of the management body. For example, *ByteDance* states that to ensure the independence of the DMA compliance function, the personnel «are not instructed by the ByteDance management body or the TikTok Ireland board regarding the exercise of their activities and tasks»[140].

Hence, the compliance function occupies a central role in supporting and guiding both management and top-level bodies. This makes it advisable to formalise procedures capable of ensuring the possibility and continuity of the function's involvement in the

[136] Michele De Mari, 'Gli assetti organizzativi societari' in Maurizio Irrera (ed), *Assetti adeguati e modelli organizzativi nella corporate governance delle società di capitali* (Zanichelli 2016) 23, 26-27.

[137] See Article 91 of Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC [2013] OJ L 176, as amended by Directive (EU) 2024/1619 of the European Parliament and of the Council of 31 May 2024 amending Directive 2013/36/EU as regards supervisory powers, sanctions, third-country branches, and environmental, social and governance risks [2024] OJ L.

[138] BHI, *BHI Compliance Report* (2024) <https://build-health-international.shorthandstories.com/2024-bhi-annual-report/index.html> accessed 5 June 2025 sec 3, 28.

[139] Microsoft, *Microsoft's Compliance Report* (2025) <https://www.microsoft.com/en-us/legal/compliance/dmacomplianceresourcesandreports> accessed 5 June 2025 par 35, 13: «Microsoft selected the members of its Management Body to ensure that they can fulfil» DMA's obligations.

[140] ByteDance's Compliance Report (2024) sec 3, par 16 <https://sf16-va.tiktokcdn.com/obj/eden-va2/uhsllrta/DMA/2025%20DMA/Bytedance%20DMA%20Compliance%20Report%20Public%20Overview_2025.pdf> accessed 20 June 2025.

operational structure's processes[141]. In this regard, many gatekeepers report significant investment in staff education to ensure that legal obligations are fully integrated into daily operations. This includes comprehensive training programs, internal legal audits, and the dissemination of up-to-date policy manuals.

Internal guidelines and training play a crucial role in concretising the otherwise broad and undefined suitability requirements imposed by the Regulation on compliance function officers. These measures ensure that officers possess the necessary professional qualifications, knowledge, experience, and skills to effectively perform their duties[142]. However, the Regulation does not provide specific criteria in this regard, nor does it grant the Commission the authority to adopt delegated acts to further define these requirements. Therefore, further clarity would indeed be advisable with respect to compliance management training programs, aimed at defining and enhancing the requisite managerial and operational skills, establishing procedures for identifying the relevant rules and practices to prevent infringements, and fostering a culture of behavioural integrity. In any event, responsibility for verifying the actual suitability of the relevant individuals – particularly the head of the function (as well as for setting more or less stringent selection requirements) – lies with the gatekeeper and would presumably be the subject of subsequent interactions with the Commission[143].

From an examination of the compliance reports, it appears that the requirement in question is observed in all cases[144], but a certain unevenness of information can be discerned especially in the early versions of 2024. For instance, while some gatekeepers such as *ByteDance* and *Alphabet* provide highly detailed and sophisticated descriptions of the function and its organisation (excluding, of course, any redacted references to personal information and business secrets), *Apple*, *BHI* and *Amazon* offer significantly fewer details[145].

---

[141] Marco Saverio Spolidoro, 'La funzione di compliance nel governo societario' in Guido Rossi (ed), *La Corporate Compliance: una nuova frontiera per il diritto?* (Giuffrè Editore 2017) 184.

[142] Article 28(3) of DMA.

[143] The dialogue between the Commission and the gatekeeper regarding compliance with the obligation under Article 28 It is emphasised in paragraph 39 of the Commission, 'DMA Annual Report 2023' (*Digital Market Act Annual Report* 2023) <https://digital-markets-act.ec.europa.eu/about-dma/dma-annual-reports_en> accessed 9 March 2025 («The Commission has been monitoring the establishment of such a compliance function by each designated gatekeeper to ensure that it meets the requirements laid down in Article 28 DMA. After discussions with and guidance from the Commission regarding these requirements, all designated gatekeepers have appointed compliance officers following principles laid down in Article 28 DMA and communicated the details to the Commission»). It is rather doubtful whether the Commission can in any way influence the selection of the individual holding such a function, given that no specific removal powers are conferred on the Commission.

[144] This is also summarily confirmed by the Commission, 'DMA Annual Report 2023' (n 143) par 39.

[145] Amazon (n 103) merely stated — within the (sole) introductory paragraph dedicated to its "approach to compliance" — that *Amazon* has «established robust internal compliance monitoring and governance reporting processes, including setting up a DMA-specific compliance function». However, in 2025, *Amazon* has produced a much more detailed compliance report on this point (including a separate attachment as indicated in the Commission's timetable): see Amazon (n 119) 88.

From an external perspective, the head of the compliance control function plays a fundamental role both in preparing compliance reports and in serving as a counterpart to the European Commission (as well as, potentially, in providing «a focal point for external engagement»[146]). Including the head of the compliance control function in all meetings with the Commission is particularly important, as they effectively represent the gateway to dialogue with the gatekeeper. Strengthening relations between the gatekeepers' compliance function and the Commission—by developing clear information-sharing procedures and engaging in regular reporting—helps to minimise potential information gaps and grants the head of the function that «soft power»[147] (stemming from complete information) which is undoubtedly essential. Maintaining ongoing, open dialogue in this manner could also allow the gatekeeper to more swiftly identify potential breaches of the DMA's provisions and intervene early in technological processes.

6 Final remarks

Compliance with the obligations laid down by the DMA for companies designated as gatekeepers has, in most cases, required the deployment of substantial human and financial resources.

The analysis carried out has first and foremost emphasised the importance of the compliance reports that gatekeepers are required to prepare and submit to the European Commission under Article 11. The experience gained from two years of reports (most gatekeepers have already submitted the second annual report, updated to 6 March 2025) has demonstrated that these documents not only enable gatekeepers to perform an appropriate self-assessment, but also make it easier for the Commission to conduct its monitoring activities as the sole enforcer of the DMA, reduce information asymmetries, and enable the involvement of public stakeholders, thus also serving as an important mechanism for voicing concerns.

A key dimension highlighted by the compliance reports is the dynamic interplay between gatekeepers and the European Commission, supported by a broader circle of stakeholders that includes competitors, consumer associations, and the academic community. Through processes such as workshops, feedback sessions, and iterative consultations, the European Commission has assumed a dual role: regulator and ally in navigating complex implementation hurdles. The DMA's emphasis on transparency – embodied by the "comply and explain" mechanism – allows for a multi-layered dialogue that not only strengthens enforcement but also fosters greater trust and legitimacy among market participants. Whether this dialogue – especially with the broader public of stakeholders – can consistently deliver the DMA's ambitious goals will depend (also) on

[146] de Streel, Feasey and Monti (n 62) 34-35, who, however, point out that, in most cases, compliance officers «do not appear to be very visible outside of the gatekeeper organisations».
[147] Crémer, Dinielli, Heidhues, Kimmelman, Monti, Podszun, Schnitzer and de Streel (n 52) 327.

gatekeepers' willingness to cooperate in good faith, since the DMA does not allow the European Commission to impose a specific sanction for the incomplete drafting of the non-confidential version of the report.

The study has demonstrated that, with a view to ensuring full compliance with the DMA obligations, gatekeepers have undertaken an extensive revision of their business models, driven by changes in some of their core platform services, as well as a fundamental restructuring of their corporate governance frameworks.

Gatekeepers have introduced or strengthened a wide range of tools – from data portability and interoperability solutions to algorithmic transparency protocols – that align with the DMA's goal of ensuring fairness and contestability in digital markets. The public and private versions of their compliance reports underscore both the scale of the endeavour and the resource-intensive nature of the compliance process, particularly in relation to the ongoing obligation to self-assess and explain.

From a governance perspective, the mandatory establishment of an independent compliance function with direct access to the highest corporate bodies marks an important step toward institutionalising compliance at the core of gatekeepers' strategic decision-making. Inspired in part by practices in regulated sectors like banking and finance, this structure seeks to ensure that compliance is not merely a formal obligation, but a process embedded in the corporate governance of each entity. Establishing this function, however, is neither straightforward nor free from challenges. The same flexibility that allows gatekeepers to tailor internal governance to diverse business models leaves room for disparity in how compliance requirements are interpreted and fulfilled. Over time, practice may reveal whether stronger or more detailed rules – perhaps issued through soft law – are needed to reduce the risk of under-compliance and to promote a consistent approach.

Ultimately, the DMA signals a turning point in European Union's approach to governing digital markets. It builds upon, but also transcends, traditional antitrust principles (and tools) by imposing a tailor-made proactive framework for the most influential digital actors. The test of time and digital markets evolution will tell us whether the significant transformations in how gatekeepers structure their services and their internal corporate governance will be sufficient to achieving the ambitious goals set-up by the European legislator in terms of competition, equity, innovation, and consumer choice across the digital landscape.

*Alessandro Piovano**
*Carlo Federico Vescovo**
*Cristina Poncibò**

SPECIAL SECTION

AUTOMATING DSA ENFORCEMENT

A Socio-Technical framework for transparency compliance

Abstract

The European Union's Digital Services Act (DSA) is a landmark law aiming to make online platforms more transparent, accountable, and safe for users. But effective enforcement of the DSA poses significant challenges due to the scale of digital platforms and the complexity of their operations. This article presents a socio-technical legal framework designed to automate aspects of DSA enforcement, focusing on transparency obligations as a measurable and accessible starting point. The proposed framework combines legal analysis with computing techniques, such as web data extraction, natural language processing, and logic-based rule modelling, to continuously monitor platform compliance and designed to provide technological support to authorities and privates engaged in inspection and monitoring activities. By formalising DSA requirements into computable rules and developing tools to detect and report non-compliance, the approach seeks to bridge the gap between regulatory objectives and practical oversight capabilities. Case studies on selected DSA provisions (including obligations for contact points, terms of service clarity, transparency reports, notice-and-action systems, and advertising and recommender transparency) illustrate how the framework operates across different compliance areas. The article emphasises clarity and cross-disciplinary accessibility, aiming to foster dialogue between legal, policy, business, and technical stakeholders, and suggesting how regulatory automation tools can support authorities and platforms in upholding the DSA, and potentially other digital regulations, by providing scalable, objective, and transparent enforcement mechanisms.[1]

JEL CLASSIFICATION: K24, K23, C88, L86

SUMMARY

* PhD Student, Department of Law, University of Turin, Email: a.piovano@unito.it
* Research Assistant, Department of Law, University of Turin, Email: carlofederico.vescovo@unito.it
* Full Professor of Comparative Private Law, Department of Law, University of Turin, Email: cristina.poncibo@unito.it
[1] This work was developed as part of the PARASOL project at the Department of Law, University of Turin. For further information, contact the Authors.

DOI 10.13135/2785-7867/12271

1 Introduction

The Digital Services Act (DSA) represents a milestone in European digital regulation, introducing comprehensive rules to ensure that online platforms operate in a transparent, secure, and rights-respecting manner.[2] As part of a broader legislative package alongside the Digital Markets Act, the DSA's overarching goal is to create a safer and more accountable online environment while fostering innovation and competition in the EU digital market.[3]

The DSA emerged in response to some urgent issues identified over the past decade and a half, including the fragmentation of national regulations, extreme information asymmetries between users and platforms, challenges around meaningful digital consent, and the outsized influence of large technology companies on markets and society.[4]

Prior to the DSA, platforms operating across EU countries faced a patchwork of different rules, making compliance cumbersome and impairing smaller businesses.

The DSA, being an EU Regulation, directly harmonises these rules across Member States, aiming to reduce compliance burdens and provide uniform protections for consumers and businesses alike.[5] At its core, the DSA seeks to balance fundamental rights with technological innovation, indeed, EU legislators crafted the law to safeguard users' rights (such as freedom of expression and data protection) without unduly stifling the growth of digital services;[6] they also tackled pressing safety concerns, as the spread of illegal or harmful online content (like hate speech, disinformation, and counterfeit goods) had been exacerbated by social media and e-commerce growth.[7]

[2] Pietro Ghirlanda, 'How platform cooperatives can redress abuses of authority within digital markets' (2024) 3(3) Journal of Law, Market and Innovation 214.

[3] Andrej Savin, 'The EU Digital Services Act: Towards a More Responsible Internet' (2021) 04 CBS Law Research Paper 1; Andrea Turillazzi and others, 'The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications' (2023) 15(1) Law, Innovation and Technology 83.

[4] Marsel Imamov and Natalia Semenikhina, 'The impact of the digital revolution on the global economy' (2021) 5(S4) Linguistics and Culture Review 968; Fischer-Lescano A and Teubner G, 'Regime-collisions: the vain search for legal unity in the fragmentation of global law' (2003) 25 Michigan Journal of International Law 999.

[5] Urbano Reviglio and Matteo Fabbri, 'The Regulation of Recommender Systems Under the DSA: A Transition from Default to Multiple and Dynamic Controls?' (*DSA Observatory*, 22 November 2024) <https://dsa-observatory.eu/2024/11/22/the-regulation-of-recommender-systems-under-the-dsa-a-transition-from-default-to-multiple-and-dynamic-controls/> accessed 20 June 2025.

[6] Savin (n 2).

[7] Nataliia Filatova-Bilous, Tetiana Tsuvina and Bohdan Karnaukh, 'Digital Platforms' Practices on Content Moderation: Substantive and Procedural Issues Proposed by DSA' in Conference on Integrated Computer Technologies in Mechanical Engineering – Synergetic Engineering (Springer Nature 2023).

To address this, the DSA imposes transparency obligations and "notice-and-action" mechanisms so that illegal content can be reported and removed quickly, with appropriate checks to protect lawful speech. Notably, the DSA positions the EU as a global leader in platform governance establishing standards for accountability and user empowerment that could influence internet regulation worldwide and the related economics trends[8]. The Regulation's implementation is thus entwined with Europe's "Digital Sovereignty"[9] ambitions to assert control over online harms and market fairness, and to export a values-based approach to digital governance.[10]

While the DSA's passage was a significant legislative achievement, enforcing its provisions effectively is an equally critical challenge yet to be resolved. Indeed, the law distinguishes obligations by platform size, subjecting Very Large Online Platforms (VLOPs, those with over 45 million EU users) to stricter requirements than smaller services, in line with proportionality principles,[11] acknowledging that the biggest platforms have the greatest impact and resources, and thus can bear more intensive compliance measures, whereas smaller businesses should not face undue burdens. Yet across all sizes, turning the DSA's legal mandates into practical reality will require new tools and strategies. Recognising this, our work proposes a technology-assisted enforcement framework, conceived as an auxiliary tool to facilitate the supervisory and verification functions of the competent authorities with respect to the provisions under examination, without in any way substituting their institutional prerogatives or discretionary decision-making powers.[12]

We build on the idea that "code can complement law"[13] by embedding regulatory checks and processes into digital systems; in other words, effective oversight of platforms may require automated or semi-automated systems working jointly with human regulators. This approach views the DSA not merely as a legal document, but as a system of rules that can be formally modelled and continuously monitored with the help of a software, designed as proposed in this article. By embracing innovations in data analysis and artificial intelligence for governance purposes, regulators can better keep pace with the fast-moving tactics of the online industry.

This article outlines a legal-informatics design for automated enforcement of key DSA transparency obligations, aiming to show the potential of the combination of legal research and computing techniques, which can make DSA compliance verification more systematic and scalable.

[8] Reviglio (n 4).
[9] Luciano Floridi, 'The fight for digital sovereignty: what it is, and why it matters, especially for the EU' (2020) 33 Philosophy & Technology 369.
[10] Turillazzi (n 2).
[11] Reviglio (n 4).
[12] Frank Pasquale, 'A rule of persons, not machines: the limits of legal automation' (2019) 87 (1) George Washington Law Review 1.
[13] Samer Hassan, Primavera De Filippi, 'The expansion of algorithmic governance: from code is law to law is code' (2017) 17 Field Actions Science Reports 88–90.

Following this introduction, Section 2 discusses the enforcement structure and the challenges that motivated an automated approach, highlighting issues such as algorithmic opacity and resource asymmetries. Section 3 presents our design, explaining why we focus on transparency-related duties and describing the technical components (from web data gathering to natural language processing and logical rule modelling) that make up the enforcement toolkit. In Section 4, we apply the framework on selected DSA provisions as case studies, illustrating how the framework has the potential to be the starting point to verify compliance with specific legal requirements (like providing proper contact points, publishing clear terms of service and transparency reports, handling user notices, and ensuring advertising and recommender system transparency). Section 5 concludes by reflecting on the benefits and limitations of this approach and its broader implications for digital governance. Throughout this work, we emphasise clarity and accessibility, aiming to inform a wide audience, including legal scholars, policymakers, technologists, and industry practitioners about how automated tools can support the DSA's successful implementation.

2 DSA enforcement structure and challenges

The Digital Services Act (DSA), formally Regulation (EU) 2022/2065, establishes a legal framework for the oversight and enforcement of digital services within the European Union.[14] This framework is characterised by a multilayered governance structure, allocating responsibilities between national authorities and EU institutions, with the objective of ensuring effective and coherent supervision of online intermediaries.[15]

At the national level, each Member State is required to designate a Digital Services Coordinator (DSC),[16] who acts as the competent authority responsible for monitoring compliance by service providers established within its territory. The DSCs are entrusted with investigatory powers, the ability to impose administrative sanctions, and the obligation to cooperate with other national coordinators and EU bodies to facilitate cross-border enforcement.[17]

At the supranational level, the European Commission retains exclusive supervisory and enforcement competences over Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), as defined by the Regulation. These entities, identified based on a minimum threshold of 45 million average monthly active users in the EU, are

[14] cf Recital 4 DSA.
[15] Jens-Peter Schneider, Kester Siegrist and Simon Oles, Collaborative Governance of the EU Digital Single Market established by the Digital Services Act (2023) 9 University of Luxembourg Law Research Paper 1.
[16] Un sito ufficiale dell'Unione europea <https://digital-strategy.ec.europa.eu/it/policies/dsa-dscs> accessed 20 June 2025.
[17] Petros Terzis, Michael Veale and Noelle Gaumann, 'Law and the emerging political economy of algorithmic audits' in Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency ((FACCT '24), June 03–06, 2024, Rio de Janeiro, Brazil) 1255.

subject to enhanced obligations due to their systemic relevance for the information environment, the digital economy, and the protection of fundamental rights.[18]

To ensure effective compliance with such obligations, the Commission is vested with a wide array of investigative and coercive powers. It may initiate formal proceedings against providers suspected of breaching the Regulation, upon notification to national coordinators and the European Board.[19]

Upon initiation of such proceedings, the Commission assumes a leading role and may temporarily suspend the supervisory competences of national authorities; indeed, the Commission may also request cooperation from Member State authorities in accessing documents, information, and premises located in their jurisdiction, insofar as they are relevant to the investigation.[20]

To collect evidence, the Commission may issue simple requests or binding decisions requiring the disclosure of information, these may be addressed to platforms and to third parties reasonably presumed to possess relevant data.[21]

Any such request must specify the legal ground and the purpose of the inquiry, the type of data required, the deadline for submission, and the consequences for failure to comply, which include financial penalties and daily fines, indeed, addressees are under a legal obligation to provide complete and accurate responses, and remain fully liable in case of omissions, delays or inaccuracies.[22]

The Commission may also demand access to platform databases and algorithms, as well as detailed technical explanations of their functioning. This kind of investigative actions may include the appointment of independent auditors and external experts, potentially in coordination with national authorities, who support the Commission in verifying compliance and ensuring impartial assessments.[23] Moreover, the Commission may require the preservation of technical documentation deemed necessary to assess regulatory implementation.

Where a breach of substantive or procedural obligations is established, the Commission may adopt a formal decision of non-compliance and order the provider to implement corrective measures within a specified period.[24] If the provider fails to comply, the Commission is empowered to impose financial penalties of up to 6% of the provider's total worldwide annual turnover, additional fines of up to 1% may be levied in instances of obstruction, misleading information, or non-cooperation during investigations.[25] This dual-

[18] cf Article 33 DSA.
[19] cf Article 66 DSA.
[20] Ilaria Buri and Joris van Hoboken, The DSA supervision and enforcement architecture (DSA Observatory 2022) 24.
[21] cf Article 67 DSA.
[22] Folkert Wilman, 'The Digital Services Act (DSA) – An Overview' [2022] SSNR https://ssrn.com/abstract=4304586 or http://dx.doi.org/10.2139/ssrn.4304586 accessed 26 June 2025.
[23] cf Article 72 DSA.
[24] cf Article 73 DSA.
[25] cf Article 74 DSA.

tier sanctioning regime reinforces the Commission's executive function and constitutes one of the most stringent enforcement mechanisms under EU digital regulation.[26]

To ensure institutional coordination, the DSA also establishes the European Board for Digital Services,[27] composed of the national DSCs and chaired by the Commission. The Board's tasks are various and include, especially, promoting the consistent application of the Regulation, exchanging best practices and tools, and issuing non-binding opinions on emerging regulatory challenges.[28]

Finally, the Regulation introduces a series of procedural safeguards aimed at reinforcing operational enforcement capacity. VLOPs and VLOSEs are required to grant access to data essential for compliance monitoring,[29] to undergo independent audits (cf Article 42 DSA), and to cooperate proactively with authorities to facilitate regular, transparent, and proportionate oversight.

This complex architecture reflects the DSA's ambition to address the challenges of the digital environment by combining decentralised supervision with centralised enforcement. However, as the subsequent analysis will demonstrate, the actual effectiveness of this framework depends heavily on the availability of adequate resources, specialised technical expertise, and innovative tools capable of responding to the dynamics of a rapidly evolving digital ecosystem.

In addition to public enforcement, the DSA assigns an active role to platforms themselves, which are required to implement mechanisms for content moderation and self-regulation these obligations constitute a form of private enforcement, whereby service providers must develop and manage tools for receiving notices of illegal content, act promptly, report the decisions taken, and ensure algorithmic transparency. This kind of co-responsibility implies that technological enforcement solutions must interact not only with public authorities but also with the internal systems operated by platforms.[30]

From the moment it was approved, a clear tension emerged between the DSA's regulatory goals and the practical realities of enforcement, indeed, several factors make traditional enforcement methods (eg, manual audits or complaint-driven investigations) often inadequate in the digital context[31]. First, modern platforms rely heavily on complex machine learning algorithms and deep neural networks to manage vast volumes of user content, giving rise to what scholars call "algorithmic opacity".[32] Furthermore, the

[26] Buri and Van Hoboken (n 19).

[27] Official site of European Board for Digital Services <https://digital-strategy.ec.europa.eu/en/policies/dsa-board> accessed 26 June 2025.

[28] cf Article 61 DSA.

[29] cf Article 40 DSA.

[30] Miguel Del Moral Sanchez, 'The devil is in the procedure: private enforcement in the DMA and the DSA' (2024) 9 University of Bologna Law Review 7.

[31] Afzal Jamil, "Digital Law Enforcement Challenges and Improvement" in *Implementation of Digital Law as a Legal Tool in the Current Digital Era* (Singapore: Springer Nature 2024) 47, 48.

[32] Motahhare Eslami, Kristen Vaccaro, Min Kyung Lee, Amit Elazari Bar On, Eric Gilbert, Karrie Karahalios, "User attitudes towards algorithmic opacity and transparency in online reviewing platforms" in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (New York, ACM 2019) 1, 14.

decision-making processes are often so complex, or kept proprietary, in a way that outsiders (including regulators) cannot easily understand or scrutinise them and in some cases, platforms intentionally design systems to be opaque or resistant to scrutiny. For example, through techniques of algorithmic laundering, a company might obfuscate how its content moderation AI works by continuously altering training data or model parameters, thereby thwarting external audits.[33]

The result is a large "grey area" where detecting violations of the DSA becomes exceedingly difficult without specialised tools. Another challenge is the global and distributed nature of online services: major platforms operate data centres and content delivery networks across multiple jurisdictions, which can facilitate regulatory arbitrage by letting companies locate certain business functions in countries with more lenient rules, impeding the enforcement of the DSA. This jurisdictional fragmentation allows companies to partially evade oversight, as noted by observers of EU digital regulation.[34] Additionally, the sheer disparity in resources between large tech companies and regulatory agencies raises concerns as Big Tech firms may employ hundreds of engineers and lawyers focused on content policies, whereas national regulators might have only a handful of technical experts at their disposal. This asymmetry means platforms can often adapt or reinterpret rules faster than authorities can monitor or respond. As a European Commission report pointed out, even well-intentioned regulations can fall short if enforcement bodies lack the technical tools and staff to keep up.[35]

The DSA's success hinges on addressing enforcement gaps created by modern technology, indeed, primary challenges include the opacity of algorithms and decision-making on platforms, which frustrates accountability, platforms' ability to exploit cross-border differences and technicalities to dodge compliance, and the limited capacity of regulators to perform large-scale, real-time supervision of platform activities. Recognising these challenges suggests that traditional enforcement must be augmented with automated, tech-assisted solutions.[36] If regulators can leverage advanced tools to inspect platforms continuously and objectively, they stand a better chance of ensuring that the DSA's provisions (for example, requirements about content moderation transparency or data access for researchers) are met in practice. These issues underscore why we view enforcement as the "Achilles' heel" of the DSA's otherwise robust legal framework, leading us to develop a methodology that directly tackles the enforcement challenge by combining legal criteria with computational monitoring.

[33] Meghan J Ryan, 'Secret algorithms, IP rights, and the public interest' (2020)21(1) Nevada Law Journal 61, 90.
[34] Caroline Cauffman, Catalina Goanta, 'A new order: The Digital Services Act and consumer protection' (2021) 12(4) European Journal of Risk Regulation 758, 774.
[35] Jamil (n 30).
[36] Suzanne Vergnolle, 'Enforcement of the DSA and the DMA – What did we learn from the GDPR?' in Heiko Richter, Marlene Straub, and Erik Tuchtfeld (eds), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package* (Munich 2021) 103.

Building upon these challenges, it becomes evident that the architecture of the DSA, while ambitious, leaves open critical enforcement vulnerabilities that require innovative regulatory thinking.[37] Indeed, the reliance on procedural guarantees and transparency obligations may create a lack of compliance, where platforms formally adhere to reporting duties without substantially altering harmful practices, thus enabling platforms to meet the letter of the law while circumventing its spirit.[38]

In this regard, mere disclosure obligations such as the requirement to publish transparency reports or content moderation policies are insufficient if regulators lack the technical capacity to audit, verify, and interpret such disclosures effectively. Without tech-tools capable of parsing vast datasets, identifying inconsistencies, and cross-referencing publicly disclosed information against actual platform behaviours, the DSA's transparency measures risk becoming performative rather than transformative. Moreover, the asymmetry of information between regulators and platforms is compounded by the dynamic and evolving nature of algorithmic decision-making, unlike static compliance parameters in traditional industries, the digital ecosystem is characterised by constant iteration. Machine learning models undergo continuous retraining, and new recommendation strategies are deployed frequently, often without prior notice or public scrutiny; this algorithmic drift undermines the stability of compliance assessments, rendering periodic human audits obsolete almost immediately after completion.[39]

To further complicate enforcement, the DSA's regulatory framework faces the inherent challenge of legal ambiguity in defining key concepts. Terms such as "systemic risks", "appropriate content moderation", and "effective transparency" are open to interpretive variance, both in judicial application and in technical implementation. While this flexibility allows the DSA to remain adaptive to future technological developments, it also creates space for platforms to strategically interpret these obligations in ways that minimise compliance costs without necessarily advancing the Regulation's fundamental objectives.[40] This ambiguity has a direct impact on the enforceability of substantive rights under the DSA, indeed, without a precise normative framework that translates high-level legal concepts into measurable, operational criteria, the effectiveness of any enforcement, manual or automated, can be compromised. Additionally, the DSA does not fully account for the phenomenon of "compliance theatre" wherein platforms present curated datasets and controlled access to regulators and researchers, effectively shaping the narrative around their compliance efforts.[41]

[37] Ghirlanda (n 1).
[38] Florence G'sell, 'The digital services act (DSA): a general assessment' in Antje von Ungern-Sternberg (ed), *Content Regulation in the European Union – The Digital Services Act, TRIER STUDIES ON DIGITAL LAW*, Vol 1 (IRDT 2023).
[39] Christoph Busch, 'From algorithmic transparency to algorithmic choice: European perspectives on recommender systems and platform regulation' in S Genovesi, K Kaesling and S Robbins (eds), *Recommender Systems: Legal and Ethical Issues, The International Library of Ethics, Law and Technology*, Vol 40 (Springer 2023).
[40] U Kohl, 'Toxic recommender algorithms: immunities, liabilities and the regulated self-regulation of the Digital Services Act and the Online Safety Act' (2024) 16(2) Journal of Media Law 301.
[41] G'sell (n 37).

Considering these obstacles, enforcement bodies face a triple challenge: (i) legal ambiguity that complicates the translation of regulatory objectives into enforcement actions; (ii) informational asymmetries that impede the discovery of non-compliance; and (iii) resource constraints that limit their ability to keep pace with fast-moving technological changes.[42]

The solution, therefore, cannot rely solely on traditional supervisory practices or the goodwill of regulated entities, instead, it necessitates the integration of automated, technology-assisted enforcement mechanisms capable of continuous, objective, and scalable monitoring, indeed by embedding regulatory logic directly into computational systems, enforcement agencies can proactively detect patterns of non-compliance, assess the authenticity of transparency disclosures, and identify latent systemic risks without depending exclusively on platform cooperation.[43]

This approach anticipates the subsequent sections of our work, where we outline a design framework that formalises DSA obligations into machine-readable rules and employs advanced data extraction and natural language processing techniques to verify compliance autonomously. Specifically, by focusing initially on the DSA's transparency obligations, arguably the most objectively verifiable and publicly accessible set of rules, we establish a foundation for a broader framework capable of extending into more complex compliance areas, including content moderation practices, advertising transparency, and systemic risk mitigation. While the DSA represents a significant regulatory advancement, its enforcement success hinges on the development of technological infrastructures that complement legal mandates with real-time, automated oversight. Only through this synergy between law and technology can the European Union hope to close the enforcement gap and ensure that the DSA achieves its intended effect of creating a safer, more transparent, and accountable digital environment.

3 A design for automated DSA enforcement

3.1 The starting point: transparency obligations

As a starting point in automating the enforcement of the DSA, we decided to delimit the area of concern by focusing first on transparency obligations, the duties of platforms to disclose certain information about their operations to regulators and the public. We identified transparency-related requirements as an ideal starting point for automation design because they are among the most concrete and observable rules in the DSA. Unlike some obligations that might require subjective judgments or internal data (eg, assessing whether content moderation decisions were "appropriate"), transparency measures often

[42] ibid.
[43] Robert Mor and Johannes Dimyadi, 'The promise of automated compliance checking' (2021) 5 Developments in the Built Environment 1.

manifest as information that platforms must publish openly. This means compliance (or non-compliance) with these rules can be checked from an external perspective, including by users or automated systems, without special access to a company's internal databases, in other words, transparency provisions create data that is intentionally public-facing, which we can leverage for independent verification and to carry out preliminary tests aimed at assessing the effectiveness of the applied technological solutions. Transparency in the DSA is not just an abstract principle, but it is implemented through specific mandates, notably, platforms are required to publicly disclose key information about how they moderate content, how their recommender algorithms work, and how online advertising on their service is targeted and presented.[44]

For example, if a social media platform removes a user's post, the DSA obliges the platform to provide an explanation to the user, including the reason and the basis in their terms of service.[45] Likewise, large platforms must maintain advertising archives where details of ads (such as who paid for them and what targeting criteria were used) are available for scrutiny by anyone.[46] These transparency reports and databases are valuable because they offer observable indicators of compliance. By examining them, one can infer whether a platform is following the rules, for example by assessing whether the required information is provided in a clear manner and whether the content moderation reports are updated as mandated.

Focusing our design methodology on transparency obligations offered several advantages. First, as noted, verifying transparency does not require privileged access to a platform's back-end systems or personal user data, preserving user privacy. This increases the feasibility of independent oversight.[47] Second, transparency criteria are often binary or clearly defined whether an item (like a contact email or a summary of terms) is published or it is not; either a report contains certain statistics, or it does not, this allows us for objective checks. Third, many transparency duties apply across all platforms (with additional intensity for VLOPs but still relevant to smaller ones), meaning an automation approach here can scale to various contexts.[48] Finally, transparency requirements typically involve periodic disclosures (eg, monthly content moderation reports, continuously updated ad repositories), this creates a need for continuous monitoring, which is well-suited to automation. An automated system can be scheduled to regularly crawl and analyse the latest disclosures from platforms, catching compliance lapses (such as a report not being updated on time) much faster than occasional human audits could.

[44] Wilman (n 21).
[45] cf Article 14 DSA.
[46] Magdalena Knapp, Anna Piszcz, "Moving towards more transparent online platforms under the Digital Services Act" in Dušan V Popović and Rainer Kulms (eds), *Repositioning Platforms in Digital Market Law* (2024) 105, 123.
[47] Cauffman, Goanta (n 33).
[48] Amanda Reid, Evan Ringel, 'Digital intermediaries and transparency reports as strategic communications' (2025) 41(1) The Information Society 1, 18.

In our design, we thus narrowed the scope initially to a set of DSA provisions that revolve around transparency and accessibility of information; by doing so, we established a solid foundation of public data and clear-cut criteria on which to build automated enforcement tools. This choice is not meant to diminish the importance of other DSA facets (like risk assessments or crisis response duties), but rather to phase the development and proving the concept on transparency can pave the way to extending automated checks to more complex obligations in the future.[49] The next subsection details how we identified the specific articles to target and how those choices guided the technical implementation.

3.2 Scope and article selection

Within the DSA's many provisions, we selected a subset of articles that are both central to the Act's transparency goals and amenable to automated monitoring; this selection was guided by a dual logic: prioritising rules that have high regulatory importance and those that can be translated into clear computational checks. On the one hand, transparency is a cornerstone of the DSA's approach to balancing innovation with fundamental rights protection,[50] so it made sense to focus on articles enforcing transparency, on the other hand, each legal obligation is worded differently, some are straightforward (eg, "provide a point of contact"), while others are more qualitative (eg, "terms of service must be clear and understandable"). The first step was to ensure we target the right entities; Article 3 of the DSA defines which online services fall under which category (eg, intermediary services, hosting services, online platforms, VLOPs).[51] Any automated enforcement tool must incorporate this scope determination and checking whether a given website or service is subject to certain obligations, for instance, an obligation might apply only to "online platforms" but not to mere conduits (like ISPs). We included this classificatory step as a prerequisite in our framework, if a platform does not meet the DSA's definitions, our system is designed to recognise that and avoid a false non-compliance flag.

Next, we identified specific transparency obligations to analyse. Article 11 and Article 12 were chosen as a combined case focusing on points of contact, the first requires platforms to designate a single point of contact for communicating with regulators, and the second requires an electronic contact point for users, which must be easy to access and not purely automated (ie, users should be able to reach a human). These provisions are fundamental because if regulators or users cannot effectively contact a platform, enforcement of other rules becomes difficult, from an automation perspective, verifying compliance with Articles 11-12 is feasible by scanning the platform's website for contact info and testing its accessibility, for achieving this goal, we broke down this verification

[49] Knapp, Piszcz (n 45).
[50] Turillazzi (n 2).
[51] cf Article 3 DSA.

into specific metrics: (a) the contact information must be clearly visible and reachable within a couple of clicks from the homepage, (b) at least one non-automated channel (eg, a human-monitored email address or phone number) must be provided,[52] and (c) any descriptions around the contact must not be misleading or overly technical (to satisfy the "easily accessible" spirit). For example, the tool is designed to check that a user can navigate to the "Contact" or "Legal" page and find an email address without encountering login walls or obscure menus. We also included text analysis to ensure the language describing the contact is straightforward (no confusing jargon that might deter users). These criteria have the potential to translate the ambiguous terms "easily accessible" and "not exclusively automated" into concrete checkpoints that an algorithm can evaluate.[53]

We also targeted Article 14, which deals with terms and conditions transparency, under this article platforms must state their content moderation policies clearly in their terms of service, notify users of any significant changes to those terms, and ensure terms are appropriate for minors if the service is likely to be accessed by them. This was included because terms of service are a primary way platforms communicate rules to users, and lack of clarity here undermines user rights.[54] We identified multiple aspects of Article 14 to examine including whether the terms are presented in plain language, whether changes to the terms are announced or highlighted (as required), whether there is a concise summary of key points (the DSA encourages summaries for accessibility), and if the platform is known to be used by minors, whether the terms account for that (eg, simpler language or special sections.[55] These can be checked by analysing the text of the terms; in fact readability metrics can signal if the language is too complex, and a comparison of different versions of the terms over time (tracked via our tool) can show if changes were disclosed.[56]

Another important metric is whether a change log or notice is provided when the terms update, which we can detect by looking for dates or "last updated" notices and comparing content snapshots. An additional crucial area is transparency reporting, covered by Article 15, under this provision, larger online intermediaries must regularly publish reports with statistics on content moderation (eg, number of removal orders from authorities, number of user complaints, outcomes, etc). We chose Article 15 to see how our method can handle quantitative data and cross-referencing, for instance, if a platform's transparency report claims it handled a certain number of illegal content notices, our system could cross-check

[52] cf Article 12's requirement.
[53] Orlando Amaral Cejas, Muhammad Ilyas Azeem, Sallam Abualhaija and Lionel C Briand, 'NLP-based automated compliance checking of data processing agreements against GDPR' (2023) 49(9) IEEE Transactions on Software Engineering 4282.
[54] Katarzyna Wiśniewska and Przemysław Pałka, 'The impact of the Digital Content Directive on online platforms' terms of service' (2023) 42 Yearbook of European Law 388.
[55] cf Article 14 DSA.
[56] Marco Lippi, Przemysław Pałka, Giuseppe Contissa, Francesca Lagioia, Hans-Wolfgang Micklitz, Giovanni Sartor, Paolo Torroni, "CLAUDETTE: an automated detector of potentially unfair clauses in online terms of service" (2019) 27(32) Artificial Intelligence and Law 117, 139; Cauffman, Goanta (n 33).

consistency by verifying that each required category (eg, notices from governments vs notices from users) is present and that the report is updated on schedule.[57] We also consider the quality and granularity of the information, checking if each report breaks down the data as the DSA requires and if there are obvious omissions. Our design framework employs text parsing and pattern matching to locate relevant sections of the report and ensure key terms and figures are included. One of our future works is to understand how to cross-validate some figures with external data (for example, if the EU Commission publishes how many orders it sent to a platform, the platform's report should not conflict with that number).

We later considered Article 16, the "notice-and-action" mechanism, which requires platforms to provide easy ways for users to notify them of illegal content, and to act on those notices promptly while informing users of the outcome.[58] This provision is about the user experience of reporting content so, to automate enforcement, we examine whether the platform's interface offers clear and accessible reporting channels.[59] The system will simulate a typical user experience to assess the availability and accessibility of reporting mechanisms, for instance, the presence of a "Report" button or a dedicated form for notifying illegal content. It further examines compliance with procedural requirements, such as whether the platform issues confirmations or follow-up communications in response to user notices, as mandated by the regulation. Some of this can be inferred by analysing the help pages or terms (which should describe the notice process). Additionally, we check if multiple channels for reporting exist (webform, email, etc), since accessibility is improved by offering alternatives. While fully testing the responsiveness (eg, measuring actual removal times) is beyond a static crawl, our methodology flags whether the necessary systems appear to be in place and documented.

Finally, we addressed Articles 26 and 27, which focus on online advertising and recommendation algorithms transparency for large platforms, article 26 mandates that users be clearly informed when content they see constitutes advertisement and be able to access details such as who paid for the ad and why it was shown to them (targeting criteria). Article 27 requires platforms to disclose the "main parameters" of their content recommendation algorithms (for instance, the criteria that determine news feed rankings) and to offer users options to modify or opt out of personalised recommendations. These obligations are at the frontier of transparency, aiming to unveil algorithmic influence that users historically had little insight into; they are also among the hardest to monitor externally.[60] We approached them by focusing on whether the platform provides the required disclosures in an intelligible way. For ads (Art 26), our scraper checks if ads on a

[57] Reid, Ringel (n 47).
[58] cf Article 16 DSA.
[59] Daniel Holznagel, 'How to apply the notice and action requirements under Art. 16(6) DSA—Which action actually?' (2024) 25(6) Computer Law Review International 172,179.
[60] Vergnolle (n 35).

platform are labelled (like with "Sponsored" tags) and if clicking those labels leads to further information (many platforms have an "Why am I seeing this ad?" feature which should contain the mandated info).[61] We also look for the existence of the platform's ad repository (for VLOPs, the DSA requires a public archive of all ads served). For recommender systems (Art 27), we search the platform's user settings and help pages for explanations about how recommendations are generated and instructions for users to change their feed settings. A challenge here is that compliance might be formal rather than effective; a platform could nominally state some generic info about its algorithm without truly empowering users. To tackle this, our methodology incorporates an "explainability" check. For instance, we scan for whether concrete parameters (like "based on posts you liked" or "chronological feed option") are mentioned as opposed to vague language.[62] We also note if the user interface allows switching off personalisation, as Article 27 effectively demands offering a non-personalised alternative.

By deliberately selecting Articles 11, 12, 14, 15, 16, 26, and 27, we created a testbed of varied transparency obligations, each bringing out different dimensions related to contact info availability, clarity of legal terms, quantitative reporting, interactive user-facing processes, and algorithmic transparency. The next step was to devise a unified method to automate the checking of all these elements. We proceeded to break down the enforcement verification into phases and components that could handle this diversity systematically.

3.3 Technical components of the framework

To implement the above enforcement checks, we developed a multi-phase design methodology integrating several technical instruments, in broad terms, the process involves: (i) gathering the relevant information from platforms (data collection), (ii) standardising and encoding the legal rules in a form a computer can work with, (iii) automatically analysing the collected data against those rules, and (iv) storing results and presenting them in a meaningful way, in the following sections, we describe each of these components and the technologies used.

3.4 Information gathering

In the absence of direct data-sharing interfaces from platforms, our system relies on web scraping to collect publicly available information.[63] Web scraping is an automated method of retrieving web pages and extracting specific content from them, for this we designed scrapers to target the sections of a platform's website likely to contain

[61] Knapp, Piszcz (n 45).
[62] Hassan, De Filippi (n 12).
[63] Moaiad Ahmad Khder, 'Web scraping or web crawling: State of the art, techniques, approaches and application' (2021) 13(3) International Journal of Advances in Soft Computing & Its Applications 1, 12.

compliance-related information, for instance, the "Terms of Service" page, the "Transparency Report" page, the footer where contact details are often listed, and any dedicated "DSA compliance" or legal resources if provided by the platform. Using a combination of HTTP requests and browser automation, our tool aims to handle both static pages and those that require running JavaScript (some transparency portals are interactive or only load data via scripts). For static pages (like a simple terms of service text), an HTTP fetch followed by parsing the HTML for relevant sections (using selectors for headings like "Contact" or keywords like "Transparency") is sufficient, otherwise for dynamic content (like an interactive transparency report dashboard), we can use a headless browser controlled via scripts (eg, Selenium) to render the page and simulate user clicks.[64] This ensures that even content which only appears after the JavaScript code has been run is analysed.[65]

The scrapers respect websites' robots.txt rules when applicable and throttle requests to avoid overloading servers, legally, when platforms offer official APIs or data feeds for certain information, we utilise those instead, since they are more stable and sanctioned by the provider (eg, some platforms might have an API for their ad library). Robustness is addressed by including into the design of the tool an error handling for common issues (like pages not found, timeouts, or content changes) and logging each step so that a human can review if something goes wrong. The output of this phase is designed to be a structured set of data ready for analysis, for example, the text of the latest terms of service, the list of contact points found, the content of a transparency report PDF, etc.

3.5 Deontic logic formalisation

A distinctive aspect of our approach is the use of deontic logic to model legal rules. Deontic logic is a method for representing normative concepts like obligations (things that must be done) and prohibitions (things that must not be done) in a formal, logical structure.[66]

We created what we call "deontic tables" for each DSA article in our scope. These tables break down an article into individual requirements and link each requirement to measurable criteria and verification methods. For example, for Article 11 and 12's user contact obligation, one the deontic table would be:

Obligation: Provide an easily accessible contact method for users; Computational Metric: Contact page reachable in ≤2 clicks; Verification: crawl site navigation and count clicks (see Section 4.1 for this case). By doing this for each identified obligation or

[64] ibid.
[65] Daniel Glez-Peña, Analia Lourenço, Hugo López-Fernández, Miguel Reboiro-Jato and Florentino Fdez-Riverola, 'Web scraping technologies in an API world' (2014) 15(5) Briefings in Bioinformatics 788.
[66] Roel Wieringa, John-Jules Meyer, Hans Weigand, 'Specifying dynamic and deontic integrity constraints' (1989) 4(2) Data & Knowledge Engineering 157, 189.

prohibition, we essentially translate the legal text into a checklist that software can easily follow.[67]

Table 1. Deontic Table Art 11-12

Deontic Norm	Description	Computational Metric	Automated Verification
OB: Easily Accessible Information	The contact point must be clearly identifiable and reachable with minimal steps.	Explicit text with clear contact details, reachable in ≤2 clicks.	Web scraping, text analysis with NLP.
OB: Presence of at Least One Non-Automated Channel	A human contact option must be available.	Identification of an email or phone number among the listed channels.	NER for entity recognition (email, phone number).
IM: Vague or Ambiguous Language	Generic information without precise instructions must not be present.	Detection of vague phrases or generic terms.	NLP models for semantic analysis (BERT, GPT).
OB: Multilingualism	Information must be available in the official languages of the EU.	Number of supported languages compared to regulatory requirements.	Language detection to identify present languages.

The benefit of formalising rules is twofold because it reduces ambiguity in interpretation, and it creates a template that can be consistently applied across many platforms. If the rule says, “provide an email or electronic form for contact”, our formal model might specify “an email address or web form must be present on the contact page.” This removes uncertainty about what counts as compliance, it also allows our system to scan multiple platforms and apply the exact same detection pattern for an email address on each, yielding objective and repeatable comparisons, which can be rigorously explained and verified by humans. In building these tables, we referenced not only the

[67] Dagfinn Føllesdal, Risto Hilpinen, “Deontic Logic: An Introduction” in Risto Hilpinen (ed), *Deontic Logic: Introductory and Systematic Readings* (Springer Dordrecht 1970) 1.

DSA text but also any guidance around it to capture the intent, each row in a deontic table corresponds to one compliance question (eg, "Is there an email address for user contact?") and the expected answer if compliant ("Yes, at least one email found"). This logical decomposition and its embedding represent the link between law and code in our framework, ensuring that when our system flags something, we can trace it back to a specific legal requirement.

However, it is important to acknowledge that deontic logic, while valuable for formalising normative requirements, cannot fully resolve the inherent ambiguity of legal concepts. Legal interpretation often requires contextual, purposive, and teleological reasoning that exceeds the capabilities of formal logic systems; our design methodology mitigates this limitation by focusing on transparency obligations, which are relatively objective and externally verifiable. Nevertheless, extending this approach to more subjective DSA requirements would necessitate additional interpretative frameworks and more "human-in-the-loop"[68] review mechanisms.

3.6 Automated verification via NLP

Once data is collected and rules are defined, the core analysis occurs. We employ a combination of rule-based checks and Natural Language Processing (NLP) techniques to examine the content for compliance.[69] NLP is crucial because many obligations (like clarity of language or presence of certain statements) involve interpreting text, for instance, determining if terms of service are "easily understandable" is partly subjective, but NLP can assist by measuring reading complexity (eg, average sentence length, use of common vs. legal terms) and by identifying potentially problematic clauses.[70] We designed our system to recognise certain patterns, as for example, detection of contact info (using regular expressions for emails, phone numbers), classification of text as human-oriented or auto-response (using keywords like "no-reply" addresses or the presence of chatbots), of vague language (phrases like "at our sole discretion" might undermine clarity), and identification of multiple languages in a document (through language identification libraries).

For structured data such as transparency report numbers, simple comparisons are done (eg, "does the report include a figure for government removal orders?"). For unstructured text, more advanced NLP, potentially using transformer-based models, helps in semantic analysis. For example, we are developing an NLP classifier that can read a snippet of terms of service and decide if it's informing users about changes in policy or not. Another NLP

[68] Fabio Massimo Zanzotto, 'Human-in-the-loop artificial intelligence' (2019) 64 Journal of Artificial Intelligence Research 243.
[69] Vijayaragavan Pichiyan, S Muthulingam, G Sathar, Sunanda Nalajala, Ch Akhil, Manmath Nath Das, 'Web scraping using natural language processing: exploiting unstructured text for data extraction and analysis' (2023) 230 Procedia Computer Science193.
[70] Lippi and others (n 55).

task is Named Entity Recognition (NER), which we used to differentiate between different types of contact info listed (to ensure human contact is among them, the system must tell an email apart from a chatbot link). The verification module essentially cross-references the scraped data with the computational metrics from the deontic tables; each metric becomes a test (pass/fail or a score) and the module aggregates these to determine overall compliance status for each article per platform. It is important to note that the NLP models chosen in this framework, including rule-based classifiers and transformer-based models, are promising, but these models should be viewed as experimental tools rather than definitive solutions. In fact, their accuracy and robustness in complex legal language processing remain subjects for further empirical validation, particularly in handling nuanced or borderline cases of compliance.[71] Ongoing development focuses on expanding training datasets and integrating domain-specific language models to improve interpretability and reliability. Every automated decision must be systematically logged, and evidence of compliance or non-compliance recorded; this mechanism also must respond to fundamental legal requirements of accountability and transparency, as codified in Article 5(2) GDPR).[72]

Furthermore, it is important to remember that use of artificial intelligence technologies such as those just described, raises important considerations under the AI Act as well, if employed by public authorities for enforcement purposes, even under human supervision and without any degree of autonomy, such tools may nonetheless qualify as high-risk systems insofar as they are intended to assess compliance with legal obligations.[73]

Accordingly, the tool whose design is being proposed must incorporate specific technical and organisational safeguards concerning transparency, documentation, auditability, and human oversight, in line with Articles 9–15 of the Regulation. Compliance with these requirements would not only render the tool legally admissible but would also enhance its reliability and effectiveness as a mechanism for supporting administrative enforcement.

To try to give a more practical description then we highlight how, if the system identifies a breach of Article 12 DSA, it automatically stores the relevant web page content and highlights, for example, that only a chatbot was available. This practice also satisfies the guarantees of effective remedy under Article 47 of the Charter of Fundamental Rights of the European Union (CFREU), enabling supervisory authorities which use the tool to verify and contest enforcement actions based on objective evidence. Moreover, this traceability framework directly refers to auditability obligations established by the DSA, indeed, under Article 15 DSA, providers must keep detailed records of content moderation

[71] ibid.
[72] Elena Gil González and Paul De Hert, 'Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles' (2019) 19(4) ERA Forum 597.
[73] Delaram Golpayegani, Harshvardhan J Pandit and D Lewis, 'To be high-risk, or not to be—semantic specifications and implications of the AI Act's high-risk AI applications and harmonised standards' in *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (2023) 905.

and enforcement decisions, while Article 42 mandates transparency reporting obligations. By facilitating systematic evidence collection and enabling human oversight, the system also respects the safeguards against purely automated decision-making enshrined in Article 22 GDPR, applied here by analogy.

Such a system wants to ensure that regulatory supervision remain dynamic and adaptive, as platforms continually evolve and introduce novel compliance strategies, the systematic recording of evidence allows Digital Services Coordinators[74] and the European Board for Digital Services (Articles 61-63 DSA) to have socio-technical support in analysing patterns of non-compliance, identify systemic risks, and refine enforcement methodologies in line with the cooperation mechanisms outlined in Articles 57 and 58 DSA.

3.7 Data management and interface

All results and data are stored in an organised manner so they can be reviewed and analysed: we use a database management system to keep records of each platform's fetched data (such as a copy of the terms of service text, timestamped) and the outcomes of each compliance check. This historical database allows tracking changes over time for example, if a platform initially failed to provide an ad repository but added one later, we can document that evolution. Historical analysis can reveal trends, such as improvement after regulatory guidance or repeated lapses.

The tool will provide, also, a simple user interface for the enforcement system's output, the interface can be an internal dashboard for regulators where they see, for each platform, a compliance report card: which obligations are met, which are unmet, with details and evidence. There could also be a public-facing component to fulfil the DSA's ethos of transparency, perhaps an anonymised or aggregated view that shows overall industry compliance levels. In our designed prototype, we include features like filtering (to see all platforms that failed a particular requirement) and drill-down (to inspect what exactly was found on a given site). For instance, an enforcement officer could click on "Platform X – Article 11 compliance: FAIL" and see the snippet of the homepage where the contact link was supposed to be, but perhaps wasn't present. The idea is to make the tool's findings accessible and actionable to human decision-makers. By providing a clear presentation, we strive to enable regulators to efficiently focus on the most severe or persistent violations identified by the system.

The methodology combines web scraping for data acquisition[75]), deontic logic modelling for rule formalisation[76], and NLP/data analysis for automated verification. These are supported by a data management backend and an interface for results. Through these

[74] cf Article 49 DSA.
[75] Khder (n 62).
[76] Wieringa and others (n 65).

components, we translate the DSA's requirements into an automated workflow that can monitor numerous platforms continuously.

At the current stage, the proposed design is being developed as a prototype, primarily designed for experimental validation and proof-of-concept demonstrations. While the system effectively automates core compliance checks across selected DSA provisions, it remains an experimental tool requiring further refinement before large-scale deployment, future development plans include testing on a wider set of platforms and integration with official regulatory data sources.

The next section will show how this framework is applied to the specific DSA articles we selected, detailing what the system can verify for each article and what findings it can produce.

4 Case studies: automated enforcement for selected DSA obligations

4.1 Contact point obligations (Articles 11-12)

Articles 11 and 12 of the DSA ensure that communication channels exist between platforms, regulators, and users. Article 11 requires intermediaries to have a single point of contact for authorities (eg, a dedicated email for officials to send takedown orders or inquiries). Article 12 requires an easily accessible electronic contact method for users to reach the platform, and crucially, this contact method cannot rely solely on automation (so users shouldn't be forced to talk to a bot with no option of human support). Using our socio-technical framework, we are automating the verification of these requirements as follows.

For each platform in our sample, the system navigates to find any "Contact Us" or legal notice page. It checks if an official contact point for authorities is listed (some platforms have a section like "Law Enforcement Inquiries"). At minimum, Article 11 compliance might be evidenced by a statement such as "Regulatory authorities may contact us at legal@platform.com." Our scraper searches for keywords like "authority" or "DSA" on relevant pages. If none are found, it flags that Article 11 may be unmet. For user contact (Article 12), the system looks for a general contact email or form accessible to ordinary users, it evaluates accessibility by seeing how many clicks it takes from the homepage to reach that information. We defined a threshold (two clicks) as a reasonable measure of "easily accessible," based on web usability norms and the idea that users shouldn't have to dig through many pages.[77] If our crawler had to traverse an overly complicated path, that's recorded as a potential violation.

To address the "not exclusively automated" clause, our NLP component analyses the text around the contact method. If the only contact offered is a chatbot or a list of FAQs

[77] Section 3.2 discussed this metric.

(frequently asked questions) without any direct human email or phone, we mark this as non-compliant. We trained a simple classifier to differentiate between contact info that likely reaches a human (eg, presence of an email address or a physical office address) and purely automated channels (eg, a link that says "Chat with our virtual assistant"). The presence of an email address or a support ticket form that promises human follow-up satisfies the requirement.

Additionally, we check if the contact page content is provided in multiple languages (since DSA encourages platforms operating in the EU to cater to different official languages for user-facing information). Through language detection on the contact page, the tool can note if, for example, a platform only provides contact info in English despite operating in several EU Member States.

4.2 Terms of service (Article 14)

Article 14 obliges platforms to be transparent and fair in their terms of conditions (ToC), especially regarding content moderation rules. It also requires notifying users of significant changes and includes special considerations if a service is widely used by minors. Our automated approach treats the platform's Terms of Service document as the primary data source to assess compliance with respect to Article 14.

Firstly, the scraper retrieves the latest Terms of Conditions or User Agreement page, indeed, our system is designed to scan it for certain content moderation policy disclosures that Article 14 expects. For instance, the DSA requires that terms clearly explain any rules about permissible content or user behaviour (so users know what could lead to removal or suspension). Using keyword searches, we identify if the terms mention things like "we may remove content that … (violates X)" or a section on "Content guidelines" exists, if such sections are missing or very unclear, that's a red flag.

Next, we evaluate the clarity and accessibility of the terms, and the system calculates the Flesch-Kincaid reading ease score.[78] While legal terms are often complex, an extremely difficult score might indicate the text is not "clear and unambiguous" as the DSA intends, after computing scores for a statistically significant sample of ToCs, a warning and a critical threshold will be provided in our deontic tables to guarantee grounded and reproducible results.

We also look for formatting that aids understanding, such as headings, summaries or bullet points. Some forward-thinking platforms include a summary or FAQ alongside their full legal terms. If our tool finds a summary (for example, a TL;DR section), it notes that as a positive compliance feature aligned with accessibility best practices. Conversely, if the entire ToS is a single dense block of text, we highlight that as problematic from an accessibility standpoint.

[78] J Peter Kincaid, Robert P Fishburne Jr, Richard L Rogers, Brad S Chissom, 'Derivation of new readability formulas (automated readability index, fog count and flesch reading ease formula) for navy enlisted personnel' (Millington 1975).

To check compliance with notification of changes, our design leverages a version history, indeed, we store the fetched terms of service text with a timestamp. When run periodically, the system can compare the new version to the old, if changes are detected and Article 14 requires that users be informed of "any significant change," we look on the platform's site for evidence of such notice (often platforms will post a blog update or a banner announcing updated terms). If our periodic check finds that terms have changed but no announcement was found, that could indicate non-compliance. In testing, we found one instance where a platform updated its terms (the text differed) but the only way a user could know was by checking a small date stamp on the terms page-arguably not a sufficient notice, this would be flagged for regulators to examine.

We also incorporate the minor protection aspect: if a platform is known to be popular with minors (for example, a gaming or social media app), Article 14 expects the terms to be appropriate for that audience. Our tool doesn't have an age-popularity database built in, but we used an external list of youth-oriented services to trigger this check. For those services, we ensure the terms include any special provisions for under-18 users.[79]

Overall, the automated analysis of ToS produces a multi-faceted result: a measure of readability, a checklist of required disclosures (found or not), an indicator of whether changes are being tracked and communicated, and notes on any unusual or potentially unfair clauses (our NLP flags extremely one-sided clauses like "we can remove content for any or no reason" as something that might undermine transparency). While the system cannot judge fairness in a legal sense, it points out elements that human regulators or courts might scrutinise under the DSA's provisions against unfair terms. For this reason, another future work consists in defining a total compliance score for Terms of Service obtained by computing sub-scores for each compliance check defined in this subsection, following the example set by the Flesch-Kincaid reading ease score, and aggregating them by calculating the weighted sum using appropriate coefficients, which will be established after an in-depth evaluation of a statistically significant sample of ToS documents.

4.3 Transparency reporting (Article 15)

For Article 15, the input data is the platform's transparency reports. Many large platforms publish periodic reports (quarterly or biannually) detailing metrics such as how many pieces of content were removed, how many user notices were received, average response times, etc, as required by the DSA. Our automated tool is configured to fetch these reports (often PDFs or web pages).

We parse the content of each report and verify that it contains certain core statistics mandated by the DSA: for example, number of orders from public authorities to remove content, number of content removal actions taken by the platform on its own initiative,

[79] for example, parental consent clauses or simplified language sections.

breakdown of the reasons for removals, number of complaints received and processed, and outcomes of those complaints. We have templates of expected sections, and the system searches the text for corresponding keywords (like "government requests: X" or "content removed: Y"). If any key metric is missing, that's a compliance issue.[80]

Additionally, we designed a way to examine the granularity and format. Article 15 expects that the information be provided in a way that allows understanding and analysis. If a report is extremely high-level or aggregates things too broadly, it might not fulfil the obligation. For example, if a platform simply states "We removed 50,000 posts last year" without context or category, it's not very transparent. Our method doesn't fully judge the sufficiency of detail (which can be subjective), but it does compare the report content against known standards or typical reports from peers. A platform that provides a multi-page detailed report will pass our checks easily, whereas one that posts a one-paragraph summary will likely fail some checks (like missing breakdowns per category of illegal content).

We also aim to integrate a timing check; indeed, Article 15 requires reports at least once a year. Our system notes the dates of the reports and can alert if a scheduled report is overdue or if the interval is too long. For instance, if a VLOP hasn't updated its transparency report in over a year, it's likely not compliant and the system will show it.

4.4 Notice-and-action mechanism (Article 16)

Article 16 ensures users have a channel to notify platforms of illegal content and receive a timely response, which is central to user empowerment in content moderation, for this, our method for evaluating Article 16 is somewhat interactive because we simulate the role of a user trying to report content. While we do not actually submit reports (to avoid sending false reports to platforms), we go through the motions up to the point of submission.

The system checks if each piece of user-generated content (eg, a post or video) on the platform has an obvious "Report" function, we are training it on known patterns (a flag icon, a "Report" button in dropdown menus, etc.) and if none is found on a representative sample of content, that's a direct violation (users have no way to report).

If a reporting interface exists, our tool accesses it (for example, clicking "Report" opens a form or modal); we then analyse the options provided within the form, including whether it allows the user to specify the type of illegal content (such as hate speech, piracy, etc) in accordance with the expectations set by the DSA. We also examine whether the process is accompanied by explanatory information, such as statements like "We will review and respond within 24 hours" or the presence of a confirmation message.

[80] Reid, Ringel (n 47).

Our system also is designed to look for terms of service or help centre descriptions of the notice-and-action procedure, indeed, Article 16 requires platforms to acknowledge receipt of notices and inform users of decisions. We search the site for statements like "you will receive an email confirmation" or "we will inform you of action taken." If the platform publicly describes such a process, we take that as a sign of compliance (and if the description is absent, it might indicate the process isn't well established).

We also consider usability factors like if there is a reporting mechanism hidden behind too many clicks or one that requires unwarranted information from the user could be non-compliant because it's not "easily accessible." Our designed tool aims to time how long it takes to reach the final stage of the report form, if it's overly convoluted or, say, only available to logged-in users when it should be open, it notes that.

Since full testing would involve submitting actual notices and awaiting platform responses (which is beyond our automated script's ethical scope), we flag elements that suggest whether the follow-through happens, for instance, if the platform's form asks for the user's email, that implies they will send a confirmation (positive sign), if it doesn't that discrepancy is flagged.

Through these steps, the tool can output an assessment like: "Platform X provides a reporting form reachable through two clicks on each post. The form covers the required categories of illegal content and promises a confirmation email (as evidenced in help pages). Platform Y, however, only allows reporting via a generic contact email found in the help section, which is less accessible and provides no info on response times potentially not fulfilling Article 16 requirements." This kind of comparative, automated review helps regulators quickly see which platforms might be making it hard for users to report issues, thereby undermining the DSA's notice-and-action system.

4.5 Advertising and recommender transparency (Articles 26-27)

For VLOPs and other large services, advertising and recommendation disclosures are novel obligations that our methodology tackles by a mix of content scraping and interface inspection.

To check ad transparency (Article 26), our system does two main things: it looks at the interface where ads appear to ensure they are labelled, and it searches for the platform's ads repository. For labelling, the scraper might load a user feed and identify sponsored content elements (most platforms embed a label like "Sponsored" or "Ad" in the HTML), if our parser finds posts that seem to be ads (by structure) but without a clear label in the text, that's a failure to meet the basic transparency of labelling ads; then, for each detected ad, we try to find the "Why am I seeing this ad?" feature (common on Facebook, Twitter, etc).[81] That usually brings up a pop-up or page with details on targeting, we

[81] Tami Kim, Kate Barasz and Leslie K John, 'Why am I seeing this ad? The effect of ad transparency on ad effectiveness' (2019) 45(5) Journal of Consumer Research 906.

capture that content and check if it includes the required information: advertiser identity and targeting criteria; if a platform does not provide that detail or such a feature is missing, it likely violates Article 26's second part. Additionally, the DSA's requirement of an ad repository means there should be a publicly accessible archive of ads, our tool attempts to find this by looking for links titled "Ad Library" or scanning the sitemap/robots file for references to an ads archive, if found, it can scrape it to see if it's functional (though analysing its completeness is complex, we at least verify it exists and is reachable), indeed, a missing ad repository for a platform that should have one is a significant compliance gap.

For recommender systems transparency (Article 27), the checks are somewhat qualitative; we search for a user-accessible explanation of the main parameters. Platforms often implement this via a "Personalisation settings" page or an info box that explains, for example, "Your feed is sorted by relevance, which takes into account your likes and follows." We gather such text and evaluate clarity (is it in plain language?) and completeness (does it mention key factors like user behaviour, popularity, etc?). We also verify the presence of a toggle or option for users to adjust recommender settings. The DSA effectively gives users the right to influence how content is recommended, which many interpret as offering at least a chronologically sorted feed or some non-personalised alternative. Our proposed automated test looks in the settings menu for any option related to feed order or recommendations: if not found, we suspect non-compliance.

One challenge with Article 27 is that simply stating "our algorithm suggests content based on your interests" might be technically compliant but not very useful. We leverage some criteria from emerging best practices on algorithmic transparency to gauge depth. For example, we consider it a better compliance if the platform enumerates specific input signals (like "we use your watch history and your location") rather than vague statements. Finally, the system notes if user controls are effective. We can test a simple scenario: if a user opts out of personalised recommendations (if that option exists), does the feed change order or content? This is tricky to do automatically, but we can at least confirm if such an option triggers any visible change in the HTML or if the platform acknowledges the choice ("You are now seeing posts in chronological order"). A completely static response might indicate the option is decorative rather than functional.

In applying our automation to Articles 26–27 on a sample platform, we might get results like: "Platform X clearly labels ads and provides an accessible ad library link (compliant with Art 26). It also gives users the choice between a personalised and chronological feed and explains in its help centre that recommendations are based on user activity (mostly compliant with Art 27, though explanation could be more detailed). Platform Y, however, does not visibly label ads: our scraper could not find any 'Sponsored' tags on ads, and we could not locate any public ad archive. Its feed is algorithmic with no user toggle, and no explanation of how content is chosen was found, this suggests Platform Y falls short on both ad and recommender transparency requirements." Such findings underscore the

areas where automated tools can immediately highlight likely non-compliance, prompting enforcement action or further inquiry.

5 Conclusion

This study has presented a socio-technical framework that combines legal analysis with technical innovation to help automate the enforcement of the DSA's transparency obligations. In doing so, it provides a view of how technology can complement traditional regulatory oversight.[82]

Our proposed framework, centred on web scraping, natural language processing, and logical formalisation of rules, wants to offer to Authorities a scalable tool to monitor whether digital platforms are meeting their DSA duties in real time. By systematically checking for contact points, scanning terms of service for clarity, validating transparency reports, simulating user notice processes, and inspecting interfaces for ad and algorithm disclosures, the approach translates high-level legal requirements into actionable audit tasks that a computer can perform across many services at once.

The advantages of such an automated enforcement tool are evident in a landscape where manual supervision is increasingly impractical. Platforms generate enormous amounts of data, and their practices evolve rapidly, a human-only enforcement regime would struggle to keep up.[83]

Automation improves speed and consistency so it can quickly identify issues when a platform deviates from compliance, and it applies the same standards uniformly, reducing the risk of oversight being uneven or biased, therefore enhancing the effectiveness and credibility of enforcement. Moreover, by providing a continuous check, it encourages platforms to maintain compliance proactively (knowing that lapses will be caught sooner than later), thereby furthering the DSA's goals of accountability and user protection.

However, it is important to acknowledge the limitations and challenges that remain, firstly, the system's assessments are only as good as the rules and patterns it's given; complex legal interpretations or context-specific judgments are still difficult to encode. There's a risk of false positives (flagging non-issues) or false negatives (missing subtle forms of non-compliance) if the logic isn't carefully calibrated. For example, an overly strict parser might mark legal language as "unclear" when it's acceptable or miss a cleverly hidden contact link. We are addressing this by proposing the incorporation of human reviewers in the loop as our results are meant to aid, not replace, human regulators.[84] The framework provides leads and evidence, but enforcement decisions will often require a human confirming that a violation is real and significant. This hybrid model

[82] Hassan, De Filippi (n 12).
[83] Afzal (n 30).
[84] Sriraam Natarajan, Saurabh Mathur, Sahil Sidheekh, Wolfgang Stammer and Kristian Kersting, 'Human-in-the-loop or AI-in-the-loop? Automate or collaborate?' in *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol 39, no 27 (2025) 28594.

is likely to persist; full automation without oversight could lead to disputes, especially if a platform argues the tool misinterpreted something (which is why our design logs evidence for transparency).

Secondly, technical improvements are needed to keep the enforcement tool robust, indeed, platforms may change their site structure or even attempt to game automated checkers (in a scenario where they know regulators use them). Ongoing development of more sophisticated NLP models that understand context and nuance (eg, distinguishing a genuine attempt at clarity from legalese) will help: advances in AI, such as domain-specific language models (like a "LegalBERT" trained on policy documents), could enhance the tool's ability to interpret terms of service and other text with greater fidelity to legal meaning. We foresee integrating such models to better evaluate qualitative aspects, like fairness of terms or adequacy of algorithmic explanations, which are areas current simple checks only approximate. Future works will explore in-depth each component employed in the framework analysed in this paper by implementing and evaluating experiments aimed at providing numerical and replicable results.

Another consideration is ensuring the enforcement tool itself is transparent and accountable, just as we demand platforms to be transparent, any regulatory algorithm should be explainable. We have built in explainability by using deontic logic tables that clearly map to legal provisions and by recording how conclusions are reached. As this project advances and is implemented, we would aim to further open the tool's methodology, perhaps even publishing an open dashboard showing overall compliance statistics across platforms (without revealing confidential details). This could empower civil society and researchers to participate in oversight, aligning with the DSA's aim to foster a public-private enforcement.

Our paper concludes that automated enforcement can enhance the effectiveness of the DSA, assuming that automated tools are carefully designed and implemented by private business and public authorities. Regulators would need training to use such tools and processes to respond swiftly to the findings (eg, sending notices to platforms when an issue is flagged or coordinating between EU countries if widespread non-compliance is detected). The tool could also benefit from input by platforms themselves; for instance, if platforms share data or APIs for compliance info, the tool can plug in to get more reliable data than scraping. Encouraging a cooperative approach where platforms are aware of the automated checks and perhaps even pre-emptively use similar tools internally to audit their compliance could create a constructive compliance culture.

More generally, the approach we have developed can serve as a framework for regulatory automation in other domains, the concept of translating legal obligations into machine-readable rules and verifying them through data analysis could apply to data protection (imagine a tool scanning a website for GDPR compliance indicators), consumer

protection (automatically detecting unfair clauses in terms[85]), or financial services compliance, among others. As digital regulation expands, regulators will increasingly need tech-assisted methods to uphold the law effectively. Our work contributes to that emerging field of RegTech (regulatory technology) by showing a practical example in the realm of platform governance.

In conclusion, the enforcement of the DSA stands to benefit greatly from the integration of automated, intelligent systems. Such systems can ensure that transparency, accountability, and user rights, the very values the DSA champions, are not lost in the immense scale of the online ecosystem. By operationalising legal requirements through code, we take a step toward a future where regulation is written in law but also embedded in the digital infrastructure of platforms. This cross-disciplinary effort, uniting law and technology, aims to uphold democratic values in online spaces in a consistent and timely manner. While challenges remain and continual refinement is needed, the design outlined in this article offers a perspective for enhancing DSA enforcement and, ultimately, for fostering a safer and more transparent digital world.

[85] Lippi and others (n 55).

Stefanie Boss[*]
Balázs Bodó[*]

SPECIAL SECTION

DECENTRALISED LAW ENFORCEMENT: A CASE STUDY OF ETHEREUM'S PROOF OF STAKE MECHANISM FOR MODERATION PRACTICES

Abstract
This paper examines the evolving role of the Ethereum blockchain's consensus layer as a potential tool for decentralised law enforcement, with a focus on its Proof-of-Stake (PoS) mechanism and its implications for moderation practices. While it was traditionally designed for credible neutrality, Ethereum's consensus layer is now facing increasing pressure to assist in regulatory enforcement, particularly concerning the U.S. OFAC sanction list. This shift raises fundamental questions about whether a decentralised platform can effectively meet regulatory requirements without compromising its core principles of transparency, security, decentralisation and censorship resistance.
This paper dives into the roles and incentives of actors in the consensus mechanism, with a main focus on builders, relays and validators. It also looks into the complexities introduced by Maximal Extractable Value (MEV) and the Proposer-Builder Separation (PBS). The paper critically assesses Ethereum's potential to function as a regulatory enforcement tool by discussing its inherent limitations, the current stance on adhering to OFAC sanction lists, and other relevant decision-making factors. It also considers the risks associated with leveraging this decentralised platform for regulatory purposes, including the potential for unintended consequences such as privacy and security concerns, and the erosion of core values.
Ultimately, this paper aims to provide insights into whether Ethereum can effectively be leveraged as a regulatory enforcement technology while maintaining its fundamental attributes. We find that Ethereum can leverage compliance to a certain degree, particularly through mechanisms that incentivise validators to exclude sanctioned transactions, and with simple regulation to adhere to. However, the platform's decentralised nature and commitment to censorship resistance means that complete alignment with traditional regulatory frameworks is unlikely. This highlights the fundamental trade-offs that are inherent to attempting to impose centralised control on a decentralised system.

JEL CLASSIFICATION: K42

[*] PhD Candidate at the Institute for Information Law, Institute for Informatics and the Data Science Centre at the University of Amsterdam.
[*] Full Professor at the Institute for Information Law, University of Amsterdam.

DOI 10.13135/2785-7867/12272

SUMMARY

1 Introduction

"Gatekeepers wield silent power, embedded within the very architecture of systems. They determine who gets included and who is excluded, often without those affected even realizing the criteria. Control is not always visible, but it shapes access and opportunity at every step."

– Adapted from Langdon Winner, The Whale and the Reactor: A Search for Limits in an Age of High Technology

This observation encapsulates the essence of gatekeeping. The term *gatekeeper* can be understood as a 'person or organisation that controls whether people can have or use a particular service'.[1] The consensus layer of the Ethereum blockchain fits the description of a gatekeeper, due to its moderating role. Actors in the consensus mechanism decide upon the ordering, inclusion and exclusion of transactions in the Ethereum ecosystem, thus having decisive power over whether certain transactions – or all transactions from a certain user – will enter the ecosystem.

From a regulatory perspective, gatekeepers are non-state actors who can alter the behaviour of others in circumstances where the state has limited capacity to do so.[2] These properties make gatekeepers excellent potential candidates for taking part in the law enforcement domain. Therefore, there has seemingly been an increased interest among administrative authorities to involve private parties – the gatekeepers – in law enforcement activities that are traditionally a task of public regulators, particularly when it comes to content moderation.[3] In some contexts, such as content moderation on large social media platforms and internet service providers, this shift has now reached a point where it no longer merely involves assisting with compliance; instead, it requires these gatekeepers to take a proactive role in balancing the conflicting rights and freedoms of their users, and it may even risk holding them accountable for their users' actions.[4] This extent may also be characterised as responsibilisation, which indicates that these private

[1] 'Gatekeeper' (*Cambridge Dictionary*) <https://dictionary.cambridge.org/dictionary/english/gatekeeper>.
[2] Emily B Laidlaw, 'A Framework for Identifying Internet Information Gatekeepers' (2010) 24 International Review of Law, Computers & Technology 263.
[3] Orla Lynskey, 'Regulating 'Platform Power'' (2017) 1 LSE Law, Society and Economy Working Papers 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2921021> accessed 20 June 2025.
[4] Stanisław Tosza, 'Internet Service Providers as Law Enforcers and Adjudicators. A Public Role of Private Actors' (2021) 43 Computer law & security review 1.

parties - the gatekeepers - can now be held responsible for a task that would previously have been the duty of another actor – the state - and sometimes even imposes liability on them.[5] This emerging trend of including technical infrastructures in compliance strategies aligns with broader EU strategies aimed at enhancing digital compliance and enforcement, particularly under frameworks like the Digital Services Act (DSA). However, this form of decentring of regulation may raise concerns, since these gatekeepers that now execute public law functions normally do not serve the public interest, and may not adhere to the relevant public values, such as openness, fairness, participation, consistency, rationality and impartiality of decision-making.[6]

This regulatory debate also strikes the Ethereum blockchain due to recent developments in the context of its consensus mechanism. Lately, there appears to be a tendency among its actors to voluntarily assist regulators in the enforcement of sanction lists by excluding transactions from sanctioned addresses. The Ethereum consensus layer was initially designed to be credibly neutral, meaning that it would be a system designed to validate and order transactions based on objective rules, whilst treating all users and data equally. However, recent developments have shown how the system may be shifting away from neutrality towards a more ambiguous gatekeeping system. First, a recent update to the Ethereum network introduced a new consensus mechanism and strengthened economic incentives for participants in its consensus layer.[7] Second, when the United States' Office of Foreign Asset Control added Ethereum addresses to its sanction list and included Tornado Cash in a more particular fashion, the debate around Ethereum's regulatory capabilities and responsibilities started to gain attention.[8] This shift has raised a fundamental question: Can Ethereum, despite its inherent decentralisation, be effectively leveraged as a regulatory enforcement technology?

Ethereum's inherent design relies on autonomy and decentralisation. Blockchain technology underpins these features, relying on a network of interconnected nodes that

[5] Aleksandra Kuczerawy, 'Private Enforcement of Public Policy: Freedom of Expression in the Era of Online Gatekeeping' (PhD thesis, KU Leuven 2018).

[6] Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World' (2001) 54 Current legal problems 103; Jody Freeman, 'Private Parties, Public Functions and the New Administrative Law' in Steven Cann (ed), *Administrative Law* (Routledge 2018); Kuczerawy (n 5); Tosza (n 4).

[7] Burak Öz and others 'Time Moves Faster When There Is Nothing You Anticipate: The Role of Time in Mev Rewards,' *Proceedings of the 2023 Workshop on Decentralized Finance and Security* (ACM 2023) <https://doi.org/10.1145/3605768.3623563> accessed 20 June 2025.

[8] Zhipeng Wang, Xihan Xiong and William J Knottenbelt, 'Blockchain Transaction Censorship:(In) Secure and (In) Efficient?' *The International Conference on Mathematical Research for Blockchain Economy* (Springer Nature Switzerland 2023) <https://doi.org/10.1007/978-3-031-48731-6_5> accessed 20 June 2025; U.S. Department of the Treasury, 'U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash' *U.S. Department of the Treasury News* (Washington, 8 August 2022) <https://home.treasury.gov/news/press-releases/jy0916#:~:text=WASHINGTON%20%E2%80%93%20Today%2C%20the%20U.S.%20Department,since%20its%20creation%20in%202019.> accessed 20 June 2025; Anders Brownworth and others, 'Regulating Decentralized Systems: Evidence from Sanctions on Tornado Cash' (Federal Reserve Bank of New York 2024) <https://doi.org/10.59576/sr.1112> accessed 20 June 2025.

maintain a shared, immutable ledger of transactions.[9] This structure theoretically eliminates the need for centralised authorities, fostering trust and transparency.[10] However, the very nature of a blockchain—its capacity to record and validate transactions—also raises the possibility of utilizing it to enforce regulatory mandates. While the current dynamics within Ethereum's consensus mechanism present opportunities for the system to take part in regulatory compliance, the prospect of it acting as an enforcement technology is complex, demanding a nuanced understanding of its mechanism design, the motivations of its participants, and the potential implications for its core principles. This paper explores these opportunities and challenges through a critical assessment of Ethereum's ability to be leveraged for regulatory enforcement while preserving its fundamental attributes, such as decentralisation. To achieve that, this paper will take the following approach. First, we will provide some background on the concept of the Ethereum consensus mechanism and its properties. Thereafter, we will discuss Ethereum's potential to function as a tool for regulatory enforcement by discussing its (limiting) properties, the current stance of its regulatory capability through the discussion of its adherence to the OFAC sanction list, other relevant decision-making factors, the sanction effectiveness, and the risks that come with this approach. To understand the real-world implications, we mostly rely on empirical and experimental literature for these sections. Lastly, we will conclude with recommendations and insights into Ethereum's ability to be effectively leveraged as a regulatory enforcement technology.

2 Ethereum's consensus mechanism

2.1 Blockchain technology and Ethereum

Blockchain technology refers to data structures that are used to record transactions in a peer-to-peer network, and are oftentimes built on principles such as decentralisation, immutability, distribution, privacy, security, scalability, reliability and transparency.[11] Blockchains can be categorised as either permissionless or permissioned. Permissionless blockchains, such as Bitcoin and Ethereum, are open to anyone and rely on deterministic consensus rules, rather than on trusted intermediaries to validate transactions. These consensus rules also determine the procedure to add transactions to the blockchain.[12] In

[9] Lorenzo Ghiro and others, 'A Blockchain Definition to Clarify Its Role for the Internet of Things' *2021 19th Mediterranean Communication and Computer Networking Conference (MedComNet)* (IEEE 2021) <https://doi.org/10.1109/medcomnet52149.2021.9501280> accessed 20 June 2025; Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' [2008] SSNR <http://dx.doi.org/10.2139/ssrn.3440802> accessed 20 June 2025.
[10] Ghiro and others (n 9).
[11] ibid, Nakamoto (n 9).
[12] Ghiro and others (n 9).

contrast, permissionless blockchains require specific authorisation for access or participation.[13]

The Ethereum blockchain operates as a permissionless, decentralised blockchain that supports both transaction processing and the deployment of smart contracts – self-executing code that facilitates decentralised applications.[14] The Ethereum network consists of interconnected nodes (computers or servers) that keep a copy of the blockchain and perform various functions, including validating transactions, executing transactions and supporting the consensus mechanism.[15] The aim is to find a consensus on the inclusion and order of transactions that have been requested to be added to the blockchain by its network's users.[16]

On 15 September 2022, Ethereum transitioned from the computationally heavy Proof-of-Work (PoW) consensus mechanism to the more open and energy-efficient Proof-of-Stake (PoS) consensus mechanism.[17] This upgrade is commonly referred to as "*The Merge*". The PoS system relies on verifiable stake, which means that participants must prove that they own a specific stake in Ethereum's native currency to become validators, which currently stands at 32 ETH (approx. 80,000 USD).[18] Validators are responsible for proposing and confirming blocks of transactions. Each validator is randomly assigned a proposing task every once in a while, with a likelihood that equals the proportion of tokens that have been put in stake.[19]

When zooming in on the PoS mechanism, it is structured around slots and epochs. A slot lasts 12 seconds, while an epoch consists of 32 slots (a total of 6.4 minutes). During each slot, a proposer is randomly selected to propose a block, while the other validators vote on which block is best. At the end of an epoch, at least two-thirds of the validators must support the epoch for the blocks therein to be justified. If the two-thirds majority persists in the next epoch, the blocks in the epoch become immutable.[20] Once the blocks are immutable, they cannot be altered, unless an attacker gains control over more than two-

[13] ibid.
[14] Anton Wahrstätter and others, 'Blockchain Censorship' *Proceedings of the ACM Web Conference 2024* (ACM 2024) <https://doi.org/10.1145/3589334.3645431> accessed 20 June 2025.
[15] Davide Mancino and others 'Exploiting Ethereum after" The Merge": The Interplay between PoS and MEV Strategies' *Proceedings of the Italian Conference on Cyber Security (ITASEC 2023)* (CEUR-WS 2023) <https://ceur-ws.org/Vol-3488/> accessed 20 June 2025; Benjamin Kraner and others, 'Agent-Based Modelling of Ethereum Consensus' *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (IEEE 2023) <https://doi.org/10.1109/icbc56567.2023.10174948> accessed 20 June 2025.
[16] Stefanie Boss and Balázs Bodó, 'Censorship-Resistance and Compliance Behavior in the Ethereum Consensus Mechanism' *2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (IEEE 2025) (forthcoming).
[17] Mancino and others (n 15); Anton Wahrstätter and others, 'Time to Bribe: Measuring Block Construction Market' [2023] arXiv preprint arXiv:2305.16468 <https://arxiv.org/abs/2305.16468> accessed 20 June 2025; 'The Merge' (*Ethereum.org*, 13 June 2024) <https://ethereum.org/en/roadmap/merge/> accessed 28 June 2024; Kraner and others (n 15).
[18] Ethereum (n 17); Kraner and others (n 15).
[19] Ethereum (n 17); Mancino and others (n 15).
[20] 'Gasper' (*Ethereum*, 15 August 2023) <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/gasper/> accessed 20 June 2025.

thirds of the validators – a scenario known as a 67% attack.[21] This makes the PoS inherently more secure than the PoW system, where an attacker would only need 51% control to alter blocks.[22]

2.2 Stake as an incentive

The PoS system operates on the principle that users with the largest stake have the largest interest in maintaining a properly functioning and secure network. This is because they would lose the most if the value or the reputation of the network's native currency were to diminish.[23] The stake also serves as collateral for incentivising responsible behaviour and for disincentivising malicious actions through a process called *slashing*. Slashing refers to the situation where collateral can be lost as a penalty for misconduct, such as excessive downtime (failing to sign transactions) or double signing (signing multiple conflicting blocks).[24] These penalties can result in the partial or total loss of staked collateral, ensuring that validators adhere to their responsibilities and protect the network's integrity.[25] Despite its benefits, critics argue that this system may lead to wealth centralisation. Wealthier participants can stake their assets, earn rewards, and compound their wealth over time, potentially creating a centralising force.[26] Additionally, there are concerns that a small number of token holders may validate a disproportionately large share of blocks, further concentrating power within the network.[27]

The introduction of *liquid staking* and *staking pools* added another layer of complexity to the consensus mechanism. Liquid staking is a mechanism that allows participants to receive tokenised representations of their staked assets, which enables them to retain access to their funds while still earning staking rewards.[28] These challenges the assumption that high stakes inherently incentivise network care, as users can spend or trade their liquid tokens strategically. However, liquid staking also increases accessibility

[21] Ulysse Pavloff, Yackolley Amoussou-Guenou and Sara Tucci-Piergiovanni, 'Ethereum Proof-of-Stake under Scrutiny' *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing* (ACM 2023) <https://doi.org/10.1145/3555776.3577655> accessed 20 June 2025; Lucas Nuzzi, Kyle Waters and Matias Andrade, 'Breaking BFT: Quantifying the Cost to Attack Bitcoin and Ethereum' [2024] SSNR <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4727999> accessed 20 June 2025.
[22] Pavloff, Amoussou-Guenou and Tucci-Piergiovanni (n 21); Nuzzi, Waters and Andrade (n 21).
[23] Mancino and others (n 15); Ethereum (n 19).
[24] Alpesh Bhudia and others, 'Extortion of a Staking Pool in a Proof-of-Stake Consensus Mechanism,' *2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS)* (IEEE 2022) <https://doi.org/10.1109/coins54846.2022.9854946> accessed 20 June 2025; Krzysztof Gogol and others, 'Empirical and Theoretical Analysis of Liquid Staking Protocols' [2024] arXiv preprint arXiv:2401.16353 <https://arxiv.org/abs/2401.16353> accessed 20 June 2025.
[25] Bhudia and others (n 24); Gogol and others (n 24).
[26] Mancino and others (n 15); Ethereum (n 19).
[27] Mancino and others (n 15); Ethereum (n 19).
[28] Dominic Grandjean, Lioba Heimbach and Roger Wattenhofer, 'Ethereum Proof-of-Stake Consensus Layer: Participation and Decentralization' *International Conference on Financial Cryptography and Data Security* (Springer Nature Switzerland 2024) <https://link.springer.com/chapter/10.1007/978-3-031-69231-4_17> accessed 20 June 2025.

by removing the need for participants to fully lock up their collateral.[29] *Staking pools*, such as Lido and Rocket Pool, further democratise staking by allowing users to combine their resources and collectively meet the 32 ETH requirement for running a validator node.[30] Participants in these pools share both the rewards and the responsibilities of staking. This reduces the barriers to entry for smaller stakeholders and simplifies the staking process, because it allows participants to delegate tasks to pool operators.[31] While this pooled model improves accessibility, it raises concerns about decentralisation and security. A staking pool centralises control over multiple validators, making it an easier target for malicious actors compared to individually operated nodes.[32] Despite the challenges of both liquid staking and staking pools, they have still benefited the consensus mechanism by significantly broadening the inclusivity of the system, and by providing opportunities for smaller investors to contribute to the PoS system.[33]

2.3 Proposer builder separation and maximal extractable value

The complexity of transaction ordering in Ethereum's consensus layer is primarily influenced by two key concepts: maximal extractable value (MEV) and proposer builder separation (PBS).

MEV refers to the value that users can extract within a blockchain network beyond standard protocol incentives. This phenomenon manifests itself on many of Ethereum's layers, but in the context of the consensus mechanism, MEV opportunities arise when certain actors take advantage by strategically including or excluding transactions, or by ordering a block in a certain way.[34] A key concept in consensus layer MEV is *gas*, which is the maximum price that a user is willing to pay to have their transaction included in the blockchain. Gas is calculated as the computational cost of executing a transaction on the network.[35] Each user can determine their own maximum and express this in the form of a bid. Within this specific MEV realm, there are a few common MEV strategies[36]:

[29] Apostolos Tzinas and Dionysis Zindros, 'The Principal-Agent Problem in Liquid Staking' *International Conference on Financial Cryptography and Data Security* (Springer Nature Switzerland 2023) <https://doi.org/10.1007/978-3-031-48806-1_29> accessed 20 June 2025; Gogol and others (n 24); Krzysztof Gogol and others, 'SoK: Liquid Staking Tokens (LSTs) and Emerging Trends in Restaking' [2024] arXiv preprint arXiv:2404.00644 <https://arxiv.org/abs/2404.00644> accessed 20 June 2025.
[30] Bhudia and others (n 24).
[31] ibid.
[32] ibid.
[33] ibid.
[34] Wang, Xiong and Knottenbelt (n 8); Mancino and others (n 15); Wahrstätter and others (n 14); Öz and others (n 7); Simona Ramos and Joshua Ellul, 'The MEV Saga: Can Regulation Illuminate the Dark Forest?' *International Conference on Advanced Information Systems Engineering* (Springer International Publishing 2023) <https://doi.org/10.1007/978-3-031-34985-0_19> accessed 20 June 2025.
[35] Wahrstätter and others (n 14).
[36] Ramos and Ellul (n 34).

- *Front-running*: an MEV-seeking party pays a gas price that is higher than a targeted other transaction, so that the MEV-seeker's transaction can be included in the blockchain before the targeted transaction.[37]
- *Back-running:* an MEV-seeking party places its transaction directly after a targeted transaction.[38]
- *Sandwich attacks:* an MEV-seeking party places its transaction both before and after a targeted transaction.[39]

While these MEV strategies seem lucrative at first glance, they have caused several issues. A main issue is the competitive advantage that it gives to larger validator pools and validators with successful MEV strategies, because it makes staking less accessible for smaller or individual validators.[40] Other issues included gas fee inflation, network congestion, excessive block space usage, compromised consensus security, unfairness, and problematic competition between MEV-seekers.[41] Studies have also shown significant MEV increases during times of crisis, such as the FTX collapse, with spikes between 400 and 1000%.[42] MEV on the consensus layer may also lead to undesired censorship of transactions and market manipulation practices.[43]

To address these issues, Ethereum introduced the proposer-builder separation (PBS). PBS separates the block building and the block proposal tasks, which were previously performed by validators alone.[44] This division enables competitive block construction while ensuring that block proposal and validation remain neutral, as block proposers cannot view the transaction content before signing the blocks.[45] To allow the parties to trust each other while also benefiting economically, algorithms called 'MEV-Boost relays' have been introduced as intermediaries between builders and proposers.[46] This is part of the *MEV-Boost* architecture, an opt-in mechanism that block proposers voluntarily use to access profitable blocks by proficient entities, and is adopted approximately 90% of the time[47].

When zooming out, there are a few key actors in the Ethereum consensus layer under PBS: users, searchers, builders, relays, and validators. They all have different roles and

[37] Wahrstätter and others (n 14).
[38] ibid.
[39] ibid.
[40] Yan Ji and James Grimmelmann, 'Regulatory Implications of MEV Mitigations' *International Conference on Financial Cryptography and Data Security* (Springer Nature Switzerland 2024) <http://link.springer.com/chapter/10.1007/978-3-031-69231-4_21> accessed 20 June 2025.
[41] Wahrstätter and others (n 14); Sebastian Wunderlich, 'Current State of MEV in the Ethereum Ecosystem' *Konferenzband zum Scientific Track der Blockchain Autumn School 2023* (Hochschule Mittweida 2023); Ji and Grimmelmann (n 40).
[42] Wahrstätter and others (n 14).
[43] Ramos and Ellul (n 34).
[44] Öz and others (n 7).
[45] Ji and Grimmelmann (n 40).
[46] Mancino and others (n 15); Wang, Xiong and Knottenbelt (n 8); Öz and others (n 7); Ramos and Ellul (n 34).
[47] Wahrstätter and others (n 14).

have different opportunities to deviate from remaining neutral for varying reasons, including economic or legal reasons. *Users* request transactions and specify a maximum gas fee that they are willing to pay. By bidding higher gas fees, users can potentially push through transactions that might otherwise be deprioritised or sanctioned.[48] Transaction requests flow either through a public mempool, which is a repository of pending transactions, or through a private order flow directly to block builders. *Searchers* monitor the mempool, identify MEV opportunities, restructure transactions, and submit bundles of transactions to builders through private order flow.[49] They have discretion over which transactions to include in their bundles, giving them some influence over the inclusion of sanctioned or less profitable transactions.[50] *Builders* aggregate transactions from the mempool and from private order flow sources to construct the most profitable blocks.[51] They can optimise transaction ordering by using algorithms and market-driven strategies.[52] Builders can employ inclusion or exclusion lists based on various factors, including economic incentives or compliance. This gives them medium to high influence over which transactions are included or excluded from blocks.[53] After constructing the blocks, they submit the blocks to *relays*, who act as intermediaries between builders and proposers. Relays verify the validity of the blocks that they received from builders.[54] Importantly, they can decide to enforce policies that filter out illicit transactions through their algorithm, such as those associated with sanctioned addresses.[55] This gives relays medium to high influence over transaction inclusion. Afterwards, relays send the most profitable block to the proposing validator in a blind manner, which means that the transaction contents are not revealed.[56] The proposing validator selects the most profitable block received from the relays that it is signed up to, signs it and sends it back to the relay, who verifies the signature and sends the full block to the proposer.[57] Because the blocks are blind, proposers have minimal direct autonomy over the transaction inclusion.[58] However, proposers can choose which relays they work with, thereby indirectly influencing transaction inclusion by favouring relays that filter or prioritize certain transactions.[59] When the proposer has received the full block from the relay, it propagates the block to the attesting validators in the peer-to-peer network.[60] The validators will then attest to the blocks they receive, which includes confirming the

[48] Wang, Xiong and Knottenbelt (n 8); Wahrstätter and others (n 14); Boss and Bodó (n 16).
[49] ibid.
[50] ibid.
[51] ibid.
[52] Wang, Xiong and Knottenbelt (n 8).
[53] ibid, Wahrstätter and others (n 14); Boss and Bodó (n 16).
[54] Wang, Xiong and Knottenbelt (n 8); Wahrstätter and others (n 18); Boss and Bodó (n 16).
[55] ibid.
[56] ibid.
[57] ibid.
[58] ibid.
[59] Brownworth and others (n 8).
[60] Wang, Xiong and Knottenbelt (n 8); Wahrstätter and others (n 14); Boss and Bodó (n 16).

validity and the accuracy of the data contained within a block.[61] This occurs every epoch. These validators have limited direct influence on transaction inclusion because they primarily validate blocks that are already constructed and proposed. While refusing to attest to certain blocks could theoretically allow validators to censor illicit blocks, this comes with risks of penalties like slashing.[62] Once in a while, validators may have to participate in the sync committee, for which they must create signatures to attest to the chain's head. Sync committee participation lasts 27 hours.[63] Validators receive rewards for their tasks, including consensus layer rewards (for block proposal, attestation, and sync committee participation)[64] and execution layer rewards[65] (priority fees and direct user payments).[66] They can also receive a whistleblower reward if they provide evidence of dishonest validators.[67] After a block is backed by two-thirds of the attestors, it will be added to the blockchain. All in all, the system looks as follows (figure 1).[68]

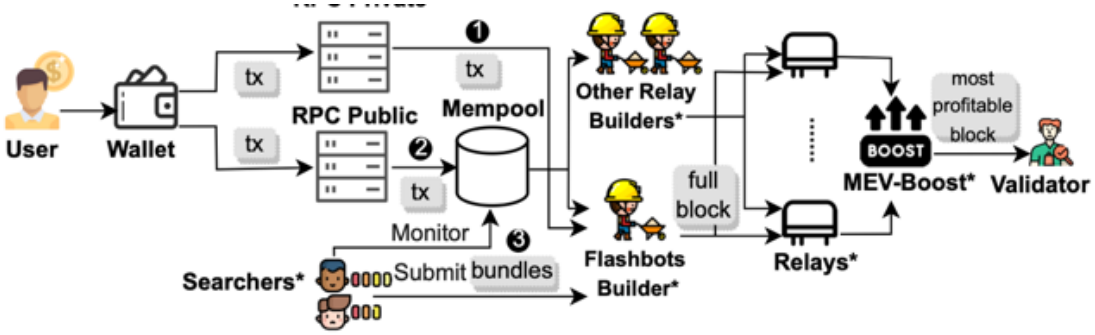


Figure 1: PBS workflow[69]

The introduction of PBS enhances efficiency by delegating block construction to specialised builders who optimise transaction selection.[70] Validators are only required to select the highest-paying block, reducing computational costs and improving network efficiency. [71] Despite its benefits, PBS also introduces new centralisation risks. The current landscape is dominated by a few relays, resulting in a degree of centralisation, with an oligarchic character.[72] Empirical studies suggest that, rather than decentralising

[61] ibid.
[62] ibid.
[63] ibid.
[64] Currently, a validator receives approximately 0.04 ETH for a successful proposal and 0.00001 ETH for a successful attestation.
[65] This is approximately 0.1 ETH per block that they propose.
[66] Grandjean, Heimbach and Wattenhofer (n 28).
[67] ibid.
[68] Wang, Xiong and Knottenbelt (n 8).
[69] ibid.
[70] ibid.
[71] ibid.
[72] Boss and Bodó (n 16); Fei Wu and others, 'From Competition to Centralization: The Oligopoly in Ethereum Block Building Auctions' [2024] arXiv preprint arXiv:2412.18074 <https://arxiv.org/abs/2412.18074> accessed 20 June 2025.

transaction inclusion, PBS has now introduced risks surrounding power concentration with a small set of block builders and relays.[73] Essentially, the issues found with dominant validators pre-PBS, such as entry barriers due to the competitive advantages, seem to have shifted towards builders and relays under PBS.[74] Additionally, entities like private RPCs, MEV searchers, builders, and relays may censor transactions based on economic incentives or regulatory compliance.[75] The upcoming section dives deeper into the censorship dilemma.

2.4 Ethereum's values: content agnosticism, credible neutrality and censorship resistance

Converse to most gatekeeping systems, such as on social media platforms where proactive moderation practices are often practiced,[76] the Ethereum consensus mechanism is designed to be content agnostic and censorship resistant. This essentially comes down to a system where filtering of any kind is not prescribed or encouraged. Actors shall, in principle, accept and include all transactions that comply with the technical standards of the network, and that are consistent with the transaction history.[77] Traditional, neutral, rules for transaction inclusion can therefore be found in network rules, and the availability of sufficient funds to complete the transaction.[78] This design promotes open participation, and provides a degree of protection against state-level enforcement.

While this standard practice does not directly open doors for Ethereum Consensus as an enforcement technology, recent developments are indicating a shift towards more complex and elaborate moderation practices. There are indications of consensus layer actors engaging in more elaborate moderation practices, where both economic incentives and regulatory incentives are playing an increasingly important role.[79] The Merge has altered the reward structure, and may have led to an intensified profit-driven nature of consensus layer participants' actions.[80] Nonetheless, the biggest shift has come from the sanctions on Ethereum addresses issued by the U.S. Office of Foreign Assets Control (OFAC), particularly the Tornado Cash sanctions in August 2022.[81] Addresses on this sanction list are considered illegal to interact with. While the sanctions have eventually

[73] Lioba Heimbach and others, 'Ethereum's Proposer-Builder Separation: Promises and Realities' *Proceedings of the 2023 ACM on Internet Measurement Conference* (ACM 2023) <https://doi.org/10.1145/3618257.3624824> accessed 20 June 2025; Sen Yang, Kartik Nayak and Fan Zhang, 'Decentralization of Ethereum's Builder Market' *2025 IEEE Symposium on Security and Privacy (SP)* (IEEE 2025) <https://www.computer.org/csdl/proceedings-article/sp/2025/223600b456/26hiUkhZyfK> accessed 20 June 2025.
[74] Wahrstätter and others (n 14); Heimbach and others (n 73).
[75] Wang, Xiong and Knottenbelt (n 8).
[76] Tosza (n 4).
[77] Michael Nofer and others, 'Blockchain' (2017) 59 Business & Information Systems Engineering 183.
[78] ibid, Boss and Bodó (n 16).
[79] Boss and Bodó (n 16).
[80] Öz and others (n 7).
[81] Wang, Xiong and Knottenbelt (n 8); Brownworth and others (n 8); U.S. Department of the Treasury (n 8).

been overturned in November 2024,[82] they have raised important questions about the extent to which legal compliance and accountability (should) influence consensus-level decisions and around the balance between these factors and other considerations.[83]

This discussion has opened the door to questions around Ethereum's ability to enforce regulation, and in what way the consensus layer could play a role in and be responsible for regulatory enforcement. This discussion centres around two key perspectives. One perspective is that it is required to be compliant with regulation, or to at least try to enforce the law, while the other perspective uses the shield of credible neutrality to argue that they shall not engage in censorship behaviour that follows from regulatory pressure. Those against censorship tend to compare the situation to internet governance and net neutrality. In both systems, the base layer participant solely engages in the recording of data. Some other actors argue that record-keeping on the blockchain is no different than financial messages being transmitted through – for instance – internet service providers, routers, network switches, email and chat programs, and that they should be granted the same neutrality exceptions.[84] Therefore, there runs a sentiment that validators should not have to monitor or censor transactions according to the law.[85]

3 Ethereum's efficacy in compliance and enforcement

To be able to assess whether and to what extent the Ethereum consensus mechanism would be able to deal with regulatory enforcement in the context of European regulation, it is important to dive into empirical evidence regarding its current state of compliance practices. We will first establish a few prerequisites for the evaluation framework. Then, we will discuss evidence for compliance with the OFAC sanction lists. In the later sections, we will discuss economic, reputational and jurisdictional factors and risks that may influence the decision-making process of the consensus layer participants, which could potentially be considered when evaluating potential improvements of the system design or incentivisation in the context of regulatory compliance. Thereafter, we will discuss the sanction effectiveness, and the risks associated with Ethereum as a regulatory enforcement tool.

3.1 Prerequisites and system limitations

It is first relevant to make a distinction between direct and indirect censorship. Direct censorship refers to the explicit exclusion of specific transactions by validators to, for

[82] Nate Raymond, 'Court Overturns US Sanctions against Cryptocurrency Mixer Tornado Cash' (*Reuters*, 27 November 2024) <https://www.reuters.com/legal/court-overturns-us-sanctions-against-cryptocurrency-mixer-tornado-cash-2024-11-27/> accessed 20 June 2025.
[83] Wang, Xiong and Knottenbelt (n 8).
[84] Rodrigo Seira, Amyaixizhang and Dan Robinson, 'Base Layer Neutrality' (*Paradigm*, 8 September 2022) <https://www.paradigm.xyz/2022/09/base-layer-neutrality> accessed 20 June 2025.
[85] ibid.

instance, comply with regulations such as OFAC sanctions.[86] For instance, a validator might refuse to broadcast a received transaction, sign an attestation, or include a transaction in a block. Indirect censorship involves a 'coincidence' kind of censorship, as it results from economic optimisation strategies, such as MEV exploitation, where transaction selection is biased for profit, rather than for explicit rules.[87] Indirect censorship may also occur due to transaction delays that originate from external entities like relays or RPC providers.[88]

There are also some limitations to consider. Ethereum's consensus mechanism design plays a pivotal role in shaping how different actors approach transaction censorship, but comes with its own instructions and limitations in the context of compliance. The system's architecture creates a nuanced landscape where participants' abilities to influence transaction inclusion vary significantly based on their roles.[89] At the forefront of this dynamic are builders and relays, because their direct access to transaction details empowers them to make informed decisions about which transactions they include or exclude from blocks. This position allows for more deliberate choices, potentially balancing profit motives against regulatory compliance.[90] In contrast, proposers and validators operate in a more constrained environment. Proposers interact with opaque blocks, unable to scrutinise individual transactions before proposing or validating. This more or less 'blind' approach inherently limits their capacity for targeted transaction censorship, shifting the balance of power in the censorship ecosystem to block builders and relays.[91] Attesting validators face constraints as well, as they are most at risk of facing negative consequences for censorship behaviour with the slashing risks.

It is further important to notice that Ethereum's consensus mechanism is fundamentally designed to make binary decisions about transaction inclusion or exclusion, based on predefined rules. The design, as outlined in section 2, may struggle to deal with nuanced regulatory requirements. This limitation is particularly evident when considering the time constraints of Ethereum's 12-second slot time, due to which most actors use algorithms to execute their tasks. They pre-program their desired decision-making path, which necessitates that all regulatory compliance is algorithmically programmable. While such algorithms can effectively implement straightforward rules, such as blocking transactions from specific blacklisted addresses, it likely lacks the sophistication to handle complex compliance scenarios that often require contextual interpretation. This limitation is particularly problematic when dealing with European digital regulations, which frequently demand nuanced understanding and application. The evaluation of such regulatory criteria

[86] Heimbach and others (n 73); Wahrstätter and others (n 14).
[87] Wu and others (n 72); Zihao Li and others, 'Demystifying Defi Mev Activities in Flashbots Bundle' *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (ACM 2023) <https://doi.org/10.1145/3576915.3616590> accessed 20 June 2025.
[88] Wu and others (n 72); Li and others (n 87).
[89] Boss and Bodó (n 16).
[90] ibid.
[91] ibid, Yang, Nayak and Zhang (n 73).

requires human interpretation, especially when navigating evolving regulations or grey areas in compliance. However, the 12-second timeframe for block creation makes human intervention impossible, and programming such complex decision-making into an algorithm that must also optimise for economic factors is highly challenging. Another complicating factor is the diverse and sometimes conflicting nature of international regulations. As it is often impossible to determine the country of origin for a transaction, any implemented regulation must be universally applicable or at least not directly conflict with rules from other jurisdictions. Given these constraints, it's crucial to recognise that Ethereum's consensus mechanism would only be effective for regulatory enforcement if the rules in question are binary, universal or simple enough to be programmed into an algorithm. In the following sections, we will therefore evaluate the enforcement capabilities based on the premise that the regulation in question is a programmable, straightforward rule, such as the OFAC sanctions list.

3.2 Direct censorship: OFAC sanction list enforcement

Due to the increased attention for regulatory compliance-related censorship in Ethereum, several empirical studies have investigated the extent to which regulatory compliance is followed in this realm. These studies show that compliance-based censorship in Ethereum is not incidental, but is systemically enforced by major relays and builders, with behaviour varying among different consensus layer participants. Interestingly, compliance appears to be an important factor in the inclusion or exclusion of sanctioned transactions: the fees offered for blocks that include sanctioned addresses are lower than those that exclude them, indicating that non-compliance may be a conscious, philosophical choice, rather than a monetarily driven choice.[92]

Some large relays, including Flashbots, Eden and bloXroute Regulated, explicitly state that they exclude sanctioned transactions.[93] These relays indeed demonstrate the lowest inclusion percentages of sanctioned addresses, albeit not being 0%, regardless of how many blocks they are involved in.[94] This compliance suggests these actors are likely trying to mitigate legal repercussions, potentially in jurisdictions with a strong regulatory enforcement culture, indicating that legal considerations play a significant role for some participants.[95] A similar suspicion holds for block builders, as a study reveals that regulatory pressure may potentially alter the structure of the block-building market and, to some extent, intensify transaction censorship tendencies.[96]

When zooming in on the transactions themselves, studies show that transactions from Tornado Cash addresses were included significantly less often in blocks after their

[92] Brownworth and others (n 8).
[93] Wang, Xiong and Knottenbelt (n 8); Brownworth and others (n 8).
[94] Boss and Bodó (n 16); Heimbach and others (n 73).
[95] Boss and Bodó (n 16).
[96] Brownworth and others (n 8).

sanctioning, and that the inclusion is largely dependent on a single larger block builder.[97] Further, it was found that all OFAC-sanctioned addresses are significantly less likely to be included in PBS-produced blocks, with a 50 percent lower likelihood compared to non-PBS-produced blocks.[98]

The consequences of censorship are evident, with Tornado Cash transaction volume plummeting by 84% within two months of the sanctions that were announced in August 2022.[99] Additionally, studies have identified that censorship not only relates to exclusion but may also manifest as delayed inclusion when not every builder, proposer, or validator is censoring, making transaction inclusion a matter of time and luck rather than a full ban.[100]

3.3 Indirect censorship: economic factors

Some consensus layer participants may be driven to make decisions based on factors other than compliance. A key alternative factor lies in economic thinking. Literature highlights a complex relationship between economic incentives, censorship behaviour, and network stability within Ethereum's consensus mechanism. Simulation findings suggest that when staking incentives are insufficient, validators may resort to censorship strategies to safeguard their economic interests.[101] In contrast, well-structured staking reward mechanisms can strengthen censorship resistance.[102] Similarly, game-theoretic analyses of transaction fees reveal that sufficiently high fees incentivise builders to accept all transactions rather than engage in censorship, indicating that effective market pricing mechanisms can influence whether builders would be incentivised to engage in censorship for compliance purposes. [103] Empirical evidence confirms this by showing that block builders consistently prioritise MEV-profitable transactions, sidelining lower-value transactions that fail to meet profitability thresholds.[104] This creates an environment where financial incentives dominate decision-making. A similar dynamic exists with relays, which often prioritise revenue-maximising transactions over ensuring fairness and accessibility, deepening economic censorship in Ethereum's block-building process.[105]

[97] ibid.
[98] Heimbach and others (n 73); Wahrstätter and others (n 14).
[99] Wahrstätter and others (n 14).
[100] ibid.
[101] Letterio Galletta and others, 'Resilience of Hybrid Casper under Varying Values of Parameters' (2023) 2 Distributed Ledger Technologies: Research and Practice 1.
[102] ibid.
[103] Elijah Fox, Mallesh Pai and Max Resnick, 'Censorship Resistance in On-Chain Auctions' *5th Conference on Advances in Financial Technologies* (AFT 2023) (Leibniz-Zentrum für Informatik 2023) <https://doi.org/10.4230/LIPIcs.AFT.2023.19> accessed 20 June 2025; Agostino Capponi, Ruizhe Jia and Sveinn Olafsson, 'Proposer-Builder Separation, Payment for Order Flows, and Centralization in Blockchain' [2024] SSNR <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4723674> accessed 20 June 2025.
[104] Bruno Mazorra, Michael Reynolds and Vanesa Daza, 'Price of Mev: Towards a Game Theoretical Approach to Mev' *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security* (ACM 2022) <https://doi.org/10.1145/3560832.3563433> accessed 20 June 2025; Wunderlich (n 41); Ramos and Ellul (n 34).
[105] Ramos and Ellul (n 34).

The temporal dynamics of transaction censorship in Ethereum's consensus mechanism add another layer of complexity. The temporal patterns are closely tied to economic incentives, particularly those related to MEV. Studies show fluctuations in validators' block proposal frequency and their treatment of censored transactions over time, with censorship rates showing periodic surges.[106] These fluctuations appear to be driven by a complex interplay of factors, including validator market concentration, MEV-based economic incentives, and governance structures.[107] Time series analyses further demonstrate how MEV extraction patterns ebb and flow with market cycles, manifesting in changing block-building profits and evolving MEV strategies, such as sandwich attacks and liquidations.[108] Moreover, during periods of high MEV rewards, Proof-of-Stake validators have been observed strategically adjusting their block proposal timing to optimise earnings, leading to noticeable shifts in block production patterns.[109] Collectively, these findings paint a picture of a dynamic censorship landscape in Ethereum, where economic incentives, particularly those driven by MEV, play a crucial role in shaping transaction inclusion patterns over time. This suggests that optimizing transaction fee structures and staking reward mechanisms could be key to influencing censorship and compliance incentives.

3.4 Jurisdictional concerns

Ethereum's censorship landscape is closely intertwined with regulatory complexity. A recent study found that a significant portion of Ethereum's nodes, including 34% of consensus nodes and 44% of execution nodes, are located in the United States.[110] This geographic concentration raises the question whether the United States and its regulations may significantly influence the behaviour of consensus layer participants surrounding regulatory compliance, and whether they may mostly adhere to the United States' regulations, rather than to European regulations. A complicating factor in this question is the concept of "regulatory complication," which stems from blockchain's inherent design. The pseudonymous or anonymous nature of many actors on the network makes it difficult—and costly—for regulators to identify and trace those behind questionable or illegal transactions. This lack of accountability can incentivise certain actors to engage in illicit activities, particularly when there are financial rewards, such as higher transaction fees, to be gained. These actors may perceive themselves as autonomous from legal frameworks, further complicating enforcement efforts. This sense of autonomy is reinforced by blockchain's reliance on code, which allows the system to function

[106] Pavloff, Amoussou-Guenou and Tucci-Piergiovanni (n 21).
[107] ibid.
[108] Heimbach and others (n 73).
[109] Öz and others (n 7).
[110] Simon Brown, 'Measuring the Concentration of Control in Contemporary Ethereum' [2023] arXiv preprint arXiv:2312.14562 <https://arxiv.org/abs/2312.14562> accessed 20 June 2025.

independently of legal oversight—at least in theory. As a result, validators may not always prioritise compliance with legal rules when processing transactions.

3.5 Reputation

Reputation may also play a role in the decision-making process of consensus layer participants. If an actor takes part in compliance, this may in some contexts benefit their reputation – in jurisdictions that are highly regulated or at risk of regulation – or damage your reputation if you are not established in a region where regulation does not form a major risk. Further, if the majority of the network stands for neutrality, a voluntary compliant validator may risk being perceived as weak or not in accordance with the network's values. Another aspect of reputation comes in when a validator engages in self-serving behaviour.[111] If a validator obstructs the stability of the consensus system by waiting long periods to validate a block or transactions to extract value from that action, it might encounter reputation damage.[112]

3.6 Sanction effectiveness

The decentralised architecture of Ethereum poses unique challenges to the enforcement of sanctions. While sanctions aim to restrict illegal transactions, their effectiveness in such systems is inherently limited due to the network's design, which allows transactions to bypass certain layers of enforcement. The complexity arises from the decentralised nature of Ethereum's consensus system, combined with a system design that obscures the true nature of transactions for certain actors in the consensus layer.[113] Another complexity arises if a larger entity in the system decides to let sanctioned addresses through, as it permits the transaction to be added to the blockchain, with an inclusion delay as the largest consequence.[114]

While sanctions can delay the inclusion of blacklisted transactions, studies show that these transactions often find pathways to eventual inclusion in blocks. This highlights the limitations of partial enforcement, where only some actors or layers implement sanctions. Empirical observations suggest that blacklisted transactions tend to occur more frequently after their sanction date, potentially indicating attempts to move funds before sanctions are fully implemented or adopted by all actors.[115] Further, transaction volumes associated with sanctioned addresses often drop before sanctions are announced, but remain at non-zero levels after enforcement begins. This suggests that sanctions may have a limited

[111] Öz and others (n 7).
[112] ibid.
[113] Zeinab Alipanahloo, Abdelhakim Senhaji Hafid and Kaiwen Zhang, 'Maximal Extractable Value Mitigation Approaches in Ethereum and Layer-2 Chains: A Comprehensive Survey' (2024) 1 IEEE <https://espace2.etsmtl.ca/id/eprint/30326/1/Zhang-K-2024-30326.pdf> accessed 20 June 2025.
[114] Heimbach and others (n 73).
[115] Boss and Bodó (n 16).

impact on restricting the address activity in its entirety.[116] When a transaction is eventually delayed, studies show that these censored transactions experience an average delay of 20.6 seconds compared to uncensored ones, following a normal distribution pattern. [117] The average confirmation time for censored transactions (e.g., Tornado Cash-related transactions) increased from 15.8 ± 22.8 seconds in August 2022 to 29.3 ± 23.9 seconds in November 2022. Non-censored transactions maintained significantly lower confirmation times (8.7 ± 8.3 seconds).[118] Such extended delay increases failure rates and raises the likelihood of censored transactions being dropped entirely. [119]

These findings underscore the limitations of partial enforcement in decentralised systems, where sanctioning often results in delays or a 'waiting game', rather than an absolute ban. While sanctions can delay the inclusion of blacklisted transactions, these transactions often find pathways to eventual inclusion in blocks, highlighting the limitations of partial enforcement where only some actors or layers implement sanctions. Effective regulation may require a coordinated, system-wide approach involving all actors to ensure consistent enforcement.[120]

3.7 Risks

While transaction censorship for regulatory purposes could potentially provide more legal certainty in the Ethereum blockchain, it also introduces significant risks. Studies have shown that time differences in transaction acceptance may lead to de-anonymisation, compromising network privacy.[121] Furthermore, censorship behaviours have cascading effects on Ethereum's security and decentralisation. Selective transaction exclusion results in mempool congestion, reduced throughput, and increased vulnerability to attacks.[122] Adversaries may introduce complex "tainted transactions" that force miners or block builders to perform additional computations, degrading network performance.[123] Most critically, if more than 50% of validators engage in censorship, Ethereum's censorship resistance is severely compromised, threatening decentralisation by concentrating decision-making power among a few entities.[124] Decentralisation plays a crucial role in mitigating these adverse effects; higher decentralisation reduces validator manipulation risks, distributes decision-making power more evenly, and makes the network more

[116] ibid.
[117] Wahrstätter and others (n 14).
[118] ibid.
[119] Ji and Grimmelmann (n 40).
[120] Boss and Bodó (n 16).
[121] Shan Wang and others, 'Deanonymizing Ethereum Users behind Third-Party RPC Services' *IEEE INFOCOM 2024 - IEEE Conference on Computer Communications* (IEEE 2024) <https://doi.org/10.1109/infocom52122.2024.10621236> accessed 20 June 2025.
[122] Heimbach and others (n 73); Grandjean, Heimbach and Wattenhofer (n 28); Wahrstätter and others (n 14).
[123] Wang, Xiong and Knottenbelt (n 8).
[124] Wahrstätter and others (n 14).

resilient to single-point failures.[125] These risks highlight the delicate balance between regulatory compliance and preserving the core principles of blockchain technology. They also suggest that if Ethereum fully embraces legal compliance, its decentralisation mechanisms must be carefully considered, potentially requiring design upgrades to mitigate the risks of centralisation.

3.8 Can Ethereum's consensus layer assist in regulatory enforcement?

This section has explored the current state of regulatory compliance within the Ethereum consensus mechanism, particularly focusing on the enforcement of OFAC sanctions. Several empirical papers demonstrate that direct censorship, while present, is not absolute, with sanctioned transactions often experiencing delays rather than outright exclusion. This partial enforcement stems from the decentralised architecture of Ethereum, where different actors have varying degrees of control over transaction inclusion. The system's architecture creates a nuanced landscape where participants' abilities to influence transaction inclusion vary significantly based on their roles. At the forefront of this dynamic are builders and relays, because their direct access to transaction details empowers them to make relatively informed decisions about which transactions to include or exclude from blocks. This position allows for more deliberate choices, potentially balancing profit motives against regulatory compliance. In contrast, proposers and validators operate in a much more constrained environment, with proposers even interacting with opaque blocks and unable to scrutinise individual transactions. This limits their capacity for targeted transaction censorship, shifting the balance of power in the censorship ecosystem to block builders and relays.

Design features, economic incentives, jurisdictional concerns, and reputational factors further complicate the landscape, as they are simultaneously influencing the decision-making processes of consensus layer participants. Ethereum's consensus mechanism is designed to make relatively quick decisions about transaction inclusion or exclusion, based on predefined rules. The design may struggle to deal with nuanced regulatory requirements, especially with the time constraints of Ethereum's 12-second slot time, due to which most actors use algorithms to execute their tasks. Such algorithms can effectively implement straightforward rules, such as blocking transactions from specific blacklisted addresses, but they likely lack the sophistication to handle complex compliance scenarios that often require contextual interpretation. Additionally, the diverse and sometimes conflicting nature of international regulations poses a challenge, especially if several regulations may conflict with each other.

Economic factors also play a significant role, as there exists a complex relationship between economic incentives, censorship behaviour, and network stability within

[125] Christoph Mueller-Bloch and others, 'Understanding Decentralization of Decision-Making Power in Proof-of-Stake Blockchains: An Agent-Based Simulation Approach' (2022) 33 European journal of information systems 267.

Ethereum's consensus mechanism. Several studies suggest that when staking incentives are insufficient, validators may resort to censorship strategies to safeguard their economic interests, while well-structured staking reward mechanisms can strengthen censorship resistance. Relays often prioritise revenue-maximising transactions over those designed to ensure fairness and accessibility, deepening economic censorship in Ethereum's block-building process. Jurisdictional concerns also influence Ethereum's censorship landscape. A significant portion of Ethereum's nodes is located in the United States, which raises the question whether the United States and its regulations may significantly influence the behaviour of consensus layer participants surrounding regulatory compliance. This is further complicated by the difficulty in identifying and tracing actors that allow questionable or illegal transactions in the system, due to the pseudonymous or anonymous nature. This can incentivise certain actors to engage in illicit activities, particularly when there are financial rewards, such as higher transaction fees, to be gained. Reputation may also play a role in the decision-making process of consensus layer participants, as validators may risk reputational damage if a validator engages in self-serving behaviour or obstructs the consensus system.

As to the actual censorship of sanctioned addresses, it was found that all OFAC-sanctioned addresses are significantly less likely to be included in PBS-produced blocks, with a 50 percent lower likelihood compared to non-PBS-produced blocks. Censorship may also manifest as delayed inclusion, occurring when not every builder, proposer, or validator is censoring, making transaction inclusion a matter of time and luck rather than a full ban. Such extended delay increases failure rates and raises the likelihood of censored transactions being dropped entirely.

Ultimately, the effectiveness of sanctions is mostly limited by the network's design, leading to a "waiting game" where blacklisted transactions often find eventual pathways to inclusion. The inclusion is sometimes even largely dependent on a single larger block builder or relay that refuses to exclude a sanctioned transaction. The findings further underscore the challenges of achieving consistent regulatory enforcement in decentralised systems and highlight the need for a coordinated, system-wide approach to ensure effective compliance, while acknowledging the inherent risks to privacy, security, and decentralisation. Therefore, careful consideration of these risks is essential when evaluating the potential for Ethereum to serve as a regulatory enforcement technology within the European regulatory framework.

3.9 Key implications and recommendations

Addressing the challenge of promoting EU-based compliance without compromising Ethereum's core values requires a nuanced and multi-faceted approach. First, it is essential to acknowledge the inherent limitations of consensus layer participants, particularly in terms of their decision-making speed and system design features. The 12-

second time slot limitation is crucial to this consideration, as it creates a reality where decisions are typically executed algorithmically. Such algorithms cannot be overly complicated, as they must be able to reach a decision within 12 seconds. This makes it unrealistic to expect them to interpret or implement complex or ambiguous regulatory requirements in real time. Therefore, it is important that regulatory requirements for consensus layer participants are sufficiently simple to program into an algorithm – or ideally, binary.

To promote compliance with European regulations, which extend beyond their current efforts that are mainly based on the OFAC sanction list, it is essential to cooperate, rather than adopting a merely restrictive approach. Developing a simple overview of requirements from EU-based sanction lists and regulations that are feasible to comply with could encourage them to cooperate. Policymakers could also consider developing such an overview in a machine-readable format, making it easy and feasible for consensus layer participants to implement it in their operational processes.

Another important avenue is incentive alignment. Because consensus layer participants are strongly motivated by economic incentives, it could be a powerful tool for aligning regulatory compliance with these incentives. Developers could explore system-level upgrades to incentivise compliance, such as through renewed reward or penalty structures. Policymakers, on the other hand, could investigate whether a provision of additional rewards for compliance would be feasible or desirable. However, caution should be taken in this approach: overly centralised or unilateral incentive schemes could undermine Ethereum's decentralised nature. Any such optimisation should therefore be carefully evaluated, ideally through technical research and community consultation.

A final recommendation is governance-related. The decentralised nature of Ethereum makes it difficult to adopt a necessary unilateral compliance approach. To tackle this issue, consensus layer participants could experiment more intensively with decentralised governance mechanisms - such as community voting, working groups, and forum discussions - to collectively decide on compliance strategies. These options could enable consensus participants to express their compliance preferences, engage in discussions about trade-offs, and establish new norms or rules that balance regulatory requirements with Ethereum's core values.

4 Conclusions

This paper has navigated the complex terrain of Ethereum's evolving role as a potential regulatory enforcement technology. While the initial promise of a credibly neutral, decentralised system held appeal, the realities of economic incentives, regulatory pressures, and the intricacies of its consensus mechanism reveal a far more nuanced picture. Ethereum's journey toward Proof-of-Stake and the rise of mechanisms like MEV-Boost, intended to optimise network efficiency, but has inadvertently opened the door to

regulatory influence, blurring the lines between a neutral infrastructure and a potential tool for censorship and control.

However, simply classifying this shift as a betrayal of the system's ideals is an oversimplification. The Ethereum community finds itself on a tightrope of decentralisation, where it must balance the demands of regulatory compliance with the imperative to preserve the network's core principles of openness, transparency, and censorship resistance. The willingness of validators to consider OFAC sanctions, for example, highlights a pragmatic approach to ensuring the network's long-term viability in the face of legal and political pressures. This is not necessarily a sign of giving up on the original principles, but potentially a strategic adaptation to a complex and evolving regulatory landscape.

The critical challenge lies in ensuring that any form of regulatory enforcement within Ethereum remains transparent, accountable, and subject to community oversight. The risk is that unchecked regulatory capture, driven by economic incentives or external pressures, could transform Ethereum into a permissioned system in disguise, eroding the very foundations upon which it was built. The ongoing discussions around proposer-builder separation and maximal extractable value (MEV) are crucial in this regard. They represent attempts to mitigate the potential for malicious actors to exploit the network for their gain, but also to address concerns about fairness, censorship, and market manipulation.

Ultimately, the question of whether Ethereum can be effectively leveraged as a regulatory enforcement technology remains open. Its success hinges on the ability of its community to develop and implement governance mechanisms that safeguard its decentralised nature while addressing legitimate regulatory concerns. This requires a commitment to ongoing dialogue, experimentation, and a willingness to adapt to the ever-changing dynamics of the digital landscape. The future of Ethereum, and perhaps the broader blockchain ecosystem, may depend on it.

The transparent nature of blockchain technology could also offer regulators a unique tool to monitor and enforce compliance without undermining the decentralised ethos of these systems. Though, regulators that consider the Ethereum consensus mechanism as a gateway to the enforcement of their regulations must think of a few things first. If they consider adopting this strategy, they must emphasise the clarity and simplicity of the rules. We see that while Ethereum may not be suitable for enforcing complex or nuanced regulations that require human interpretation, it could potentially be used for enforcing straightforward, algorithmically programmable rules, such as the enforcement of sanctions lists. However, regulators must be aware of and deal carefully with the potential for unintended consequences, such as the chilling effect on legitimate transactions, privacy violations stemming from increased surveillance, and the increased vulnerability to targeted attacks if compliance mechanisms create new attack vectors. Another consideration is the proper incentivisation of the actors that operate the consensus mechanism. To incentivise these actors to follow regulatory guidelines, there must be

incentives that align with their usual approach, such as economic incentives or rewards for adherence. This could enhance the effectiveness of sanctions and other regulatory measures while maintaining the competitive dynamics that drive innovation within the Ethereum ecosystem. By leveraging mechanisms like MEV strategically, regulators could encourage compliant behaviour. This dual focus on compliance incentives and decentralised innovation could help bridge the gap between blockchain governance and the EU's regulatory objectives.

Future research should focus on exploring innovative approaches to decentralised compliance that address existing challenges and leverage the unique capabilities of blockchain technology. This includes exploring the development of more sophisticated incentive mechanisms that align the interests of validators with regulatory objectives, the implementation of privacy-preserving technologies that protect user autonomy, and the establishment of clear legal and ethical frameworks for the use of blockchain technology in regulatory enforcement.

The consensus layer, a ‘fractured gatekeeper’ with fractured incentives across its participants, presents both a risk and an opportunity: a risk of overreach and a loss of core principles, but also an opportunity to create a more accountable and transparent digital world. Ultimately, navigating this fractured landscape demands a commitment to preserving decentralisation while pragmatically addressing legitimate regulatory concerns. The key lies in finding this equilibrium.

*Valeria Comegna**

SPECIAL SECTION

THE PERSISTENCE OF THE OPPOSITES: AI AND BLOCKCHAIN FOR TRANSPARENT AND SECURE CROSS-REGULATORY COMPLIANCE AND ENFORCEMENT COOPERATION
TEST BEDS IN THE EU DIGITAL ACQUIS

Abstract

Artificial intelligence (AI) and blockchain technologies occupy a prominent position on both global and European regulatory agendas, functioning as both passive objects of regulation and active instruments of regulatory governance. Their shared capacity to automate and accelerate processes traditionally performed by humans renders them apt for embedding compliance and enforcement functionalities into socio-technical systems. This potential has been formally acknowledged — and in certain instances mandated — by the European legislators. The Data Act requires the deployment of interoperable smart contracts for the execution of data-sharing agreements generated by Internet of Things (IoT) devices;[1] the DLT Pilot Regime provides legal recognition for distributed ledger infrastructures in the trading and settlement of crypto-assets; and the AI Act establishes obligations around traceability, verifiability, and explainability, thereby suggesting the central role of eXplainable AI (XAI) in fostering transparency, democratic oversight, and system security. This article investigates how the ostensibly opposing properties of AI and blockchain — centralisation versus decentralisation, probabilistic versus deterministic logic, opacity versus transparency — may be harnessed to develop regulatory infrastructures that are transparent, secure, and compliant 'by design'. Building on computer science literature and extending the RegTech and SupTech paradigms beyond the financial domain, the study investigates the prospective integration of AI's adaptive and predictive capabilities with blockchain's immutability, auditability, and privacy-preserving architecture — augmented by smart contract automation — while critically addressing its potential limitations and points of failure. It argues that such convergence can support cooperative, cross-sectoral, and cross-border mechanisms for legal compliance and regulatory enforcement within the EU Digital Acquis. Two exploratory test-bed hypotheses are advanced. First, it proposes that blockchain-enhanced XAI may assist in fulfilling and

* Valeria Comegna pursued her Ph.D. in Law & Business at LUISS Guido Carli and is now collaborating with the Chair of Law and Economics at Roma Tre University, Department of Business Economics.

[1] Regulation (EU) 2023/2854 of the European Parliament and Council on harmonized rules on fair access to and use of data [2023] OJ L 2023/2854, recital 104-106; art 11 (1) "*Essential requirements regarding smart contracts for executing data sharing agreements*"; art 33 (1) "*Essential requirements regarding interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces*"; art 36 "*Essential requirements regarding smart contracts for executing data sharing agreements*".

DOI 10.13135/2785-7867/12273

enabling oversight of the transparency requirements applicable to high-risk AI systems under the AI Act. Second, the paper considers how federated learning — integrated with blockchain infrastructure — can enable privacy- and security-enhancing data sharing in accordance with the normative and technical provisions of the Data Act and the Data Governance Act. While recognising the persisting technical, legal, ethical and environmental challenges to full-scale integration, the article concludes that the AI–blockchain nexus holds considerable promise for the development of robust, transparent, and cooperative regulatory enforcement architectures across the EU evolving digital legal landscape.

JEL CLASSIFICATION: K2, K29, K300, K4

SUMMARY

1 Introduction

The expression ‘persistence of the opposites’ describes a state where two opposites permanently co-exist. It says nothing about the merits of their relationship, whether of tension or unison. Independently of the circumstances, opposites are categories that mutually affirm their existence. As Heraclitus teaches us, opposites are not mutually exclusive and act in harmony.[2]

Stark opposing polarisations connote discourses and narratives of intellectual debates cutting across human, social and natural sciences. The dichotomy regulation-innovation which conceives of the two as opposing forces exemplifies this discursive trend. Proving how mystifying this approach is goes beyond the purview of this article, that focuses on how two technologies characterised by opposite but mutually integrating features may operationalise efficient tools for compliance and enforcement of the EU Digital Aquis.

To this end, it departs from the regulatory technology (RegTech) and supervisory technology (SupTech) paradigms[3] that originated and consolidated in the banking and financial sector to transpose them in the domain of digital regulation. Artificial Intelligence (AI) and blockchain technologies occupy a central position in both global and EU regulatory agendas — as passive objects and active agents of regulation. As objects of regulation, they have been targets of legal rules and standards. As agents of regulation, technology through their human developers have thus far shaped self-regulating and self-

[2] Heraclitus, *Fragments* (Brooks Haxton tr, New York: Penguin Classics 2003) xviii, 31, 37.
[3] Douglas W Arner, Janos Barberis and Ross P Buckley, ‘A FinTech and RegTech Overview: Where We Have Come from and Where We Are Going’ in Douglas W Arner, Janos Barberis and Ross P Buckley (eds), *The RegTech Book* (Chichester, Wiley 2019).

standing — autopoietic — normative systems,[4] or participated in regulation[5] and innovation loops with public regulators.

Beyond shaping best practices, benchmarks, standards and rules on the global level, technologists work on embedding compliance and enforcement mechanisms in technological solutions.[6] By nature and purpose, technology is a human invention designed to serve human needs and, guided by ethics, to advance social and human well-being. Both AI and blockchain technologies possess the ability to accelerate and automate tasks that would traditionally require human effort. This is why they are particularly prone to turning into means for regulatory compliance and enforcement, provided certain conditions, that will be dealt with in the following, are met. This article proposes the integration of AI and blockchain technologies to support the development of systems that are 'legal-by-design' — that is, systems that are inherently transparent, explainable, and secure. It further suggests that such integration may facilitate adherence to EU regulatory frameworks, including the AI Act,[7] the Data Act,[8] and the Data Governance Act,[9] by embedding compliance and enforcement mechanisms within the technological architecture itself.

Section 2 frames the discourse on AI and blockchain, drawing definitions from the computer and legal scientific discourses. Section 3 describes their opposing while complementary features, and the pains and gains of their integration. The main advanced argument is that, with energy, computational, and security concerns in mind, integrating scalable, transparent, secure, and interoperable AI and blockchain systems may foster cooperative regulatory compliance and enforcement mechanisms across governance layers (regulators, supervisory authorities, market operators, and eventually consumers and citizens). The article further discusses how the integration of AI and blockchain may facilitate adherence to EU regulatory frameworks, such as the AI Act, the Data Act, and the Data Governance Act, by embedding compliance and enforcement within technological solutions.

The study explores two experimental hypotheses designed as testbeds for evaluating

[4] *ex multis* Gunther Teubner, 'Global Private Regimes: Neo-Spontaneous Law and Dual Constitution of Autonomous Sectors?' in Karl-Heinz Ladeur (ed), *Public Governance in the Age of Globalization* (Ashgate 2004) 71 <https://www.jura.uni-frankfurt.de/42852650/global_private_regimes.pdf> accessed 15 January 2025; Gunther Teubner, *Law as an Autopoietic System* (Oxford/Cambridge Blackwell Publishers 1993) 13.

[5] Fabio Bassan, *Digital Platforms and Global Law* (Edward Elgar Publishing 2021) 168; Fabio Bassan, 'Digital Platforms and Blockchains: The Age of Participatory Regulation' (2022) 34 (7) European Business Law Review 1103 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4244139> accessed 16 January 2025.

[6] *ex multis* Mireille Hildebrandt, 'Legal and Technological Normativity: more (and less) than twin sisters' (2008) 12(3) Techné: Research in Philosophy and Technology 169 <https://scholar.lib.vt.edu/ejournals/SPT/v12n3/pdf/hildebrandt.pdf> accessed 16 January 2025.

[7] Regulation (EU) 2024/1689 of the European Parliament and Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L2024/1689.

[8] Regulation (EU) 2023/2854 of the European Parliament and Council on harmonized rules on fair access to and use of data [2023] OJ L 2023/2854.

[9] Regulation (EU) 2022/868 of the European Parliament and Council on European data governance and amending Regulation (EU) 2018/1724 [2022] OJ L 152.

AI-blockchain integration under European digital regulatory frameworks. First, it advances that blockchain technology combined with explainable AI (XAI) can enhance compliance with and enforcement of the AI Act transparency requirements. Blockchain systems can create immutable audit trails to help XAI methods ensure algorithmic decisions remain interpretable and accountable. Second, the article investigates federated learning as a technical solution for privacy-preserving data sharing within the framework of the Data Act and Data Governance Act. This approach enables collaborative model training across organisations while keeping sensitive data local and addressing both security and privacy concerns. The research hypotheses suggest that these technological implementations offer promising pathways for regulators and market operators to meet the evolving requirements of the EU Digital Aquis while maintaining operational efficiency. Overall, this research contributes to the growing discourse on the alliance of law and technology to deliver technical solutions for regulatory compliance and enforcement.

2 AI and blockchain: definitions across the computer and legal sciences

Definitions limit, circumscribe, and set semantic and axiological boundaries of concepts, ensuring clarity and certainty across scientific disciplines. Beyond its descriptive role, language forms the constitutive building blocks of socio-legal and socio-technical architectures and has a performative nature. It influences the thoughts and attitudes of those who speak, listen, describe, prescribe, express, promise, bet, and create.[10] Words thus serve normative, performative, and creative functions, shaping both analogue and virtual realities and the meanings attached to concepts, artifacts and institutions. Humans craft technologies and other products of human ingenuity to perform actions, embedding human values and legal rights serving human needs into their structure. Legislators, scientists and technologists have long collaborated to align artificial intelligence (AI) and blockchain technologies with legal and ethical principles,[11] ensuring compatibility between natural language, machine-readable code and programming syntax.[12] The following sections outline performative definitions drawn from the computer and legal sciences to contextualise the discussion on how AI and blockchain may facilitate compliance with and enforcement of the EU Digital Acquis.

2.1 AI in computer science

As domain-specific experts, computer scientists provide detailed definitions of artificial intelligence (AI), its systems, and underlying models. There is broad consensus among

[10] John Rogers Searle, *Speech acts: an essay in the philosophy of language* (Cambridge University Press 1969) 3.
[11] *ex multis* Luciano Floridi, Josh Cowls, 'A Unified Framework of Five Principles for AI in Society' (2019) 1(1) Harvard Data Science Review 2, 10 <https://hdsr.mitpress.mit.edu/pub/l0jsh9d1/release/8> accessed 2 February 2025.
[12] *ex multis* Thibault Schrepel, 'Law + Technology' [2022] Stanford University CodeX Research Paper Series 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4115666> accessed 11 February 2025.

contemporary scholars that AI constitutes a sub-discipline of computer science, often characterised as a "*universal field [..] relevant to any intellectual task*".[13] More neutrally, AI may be understood as both an evolving academic discipline and an industrial practice, subject to scientific observation and ongoing experimentation. The origins of the field are commonly traced to John McCarthy's seminal definition: "*the science and engineering of making intelligent machines*", specifically, machines that behave "*in ways that would be called intelligent if a human were so behaving*".[14] Although many computer scientists regard AI as equivalent to — or even exceeding — human intelligence, this study does not engage with that debate. In the absence of rigorous empirical evidence, it adopts a position of neutrality.

Early research in artificial intelligence was primarily concerned with programming machines to perform specific intelligent tasks — what is now classified as Narrow AI, in contrast to Artificial General Intelligence (AGI), which is designed to operate across multiple domains, as exemplified by large language models. More recent approaches have shifted towards enhancing learning capabilities that more closely resemble human cognitive processes. This paradigm shift, often termed Software 2.0, denotes a transition from rule-based programming to data-driven learning, whereby system behaviour is shaped by training data rather than explicitly coded instructions.[15]

The most widespread type of AI in the industry is Machine Learning (ML) which blends knowledge from computer science, statistics, psychology, neuroscience, economics and control theory to enhance the abilities of computational agents in perception, reasoning and decision-making.[16]

ML can be categorised into three primary methodologies:

(i) Supervised learning, which involves training models on datasets where the input variables (features) pair with known output labels. The algorithm learns to map inputs to the correct outputs and minimise prediction errors through repeated adjustments. This method is commonly employed in tasks such as spam detection, image classification, and credit scoring, wherein historical data with known outcomes informs the model's predictive capacity.

(ii) Unsupervised learning, which centres on the identification of hidden patterns or intrinsic structures within unlabelled data. Rather than predicting a target output, the algorithm analyses input data to group similar observations (clustering) or to reduce dimensionality for enhanced interpretability, as in the case of principal component

[13] Stuart Russell, Peter Norvig, *Artificial Intelligence* (Global Edition 4th edn, Pearson Education 2021) 7.
[14] John McCarthy and others, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955' (2006) 27(4) AI Magazine 12 <https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/1904> accessed 14 February 2025.
[15] Andrej Karpathy, 'Software 2.0' (*Medium*, 11 Nov 2017) <https://karpathy.medium.com/software-2-0-a64152b37c35> accessed 14 February 2025.
[16] Ian Goodfellow, Yoshua Bengio and Aaron Courville, *Deep Learning* (MIT Press 2016) 1.

analysis. This approach is frequently applied in customer segmentation, anomaly detection, and exploratory data analysis.

(iii) Reinforcement learning, wherein an AI agent learns to make decisions through interaction with an environment, adopting a trial-and-error approach guided by feedback in the form of rewards and penalties. Over time, the agent develops a policy — a strategy for selecting actions — that maximises cumulative reward, rendering reinforcement learning particularly well suited to applications such as robotics, game-playing (eg, AlphaGo), and real-time bidding in online advertising.

Among the various approaches, Deep Learning (DL) has emerged as the dominant machine learning paradigm. Multi-layered neural networks process hierarchical representations, emulating biological neural structures and exhibiting superior generalisation across diverse data domains. Within this context, AI is increasingly conceived as an ecosystem that aspires to replicate the functioning of the human brain.

In parallel, Human-Centred AI (HCAI) places emphasis on the design of AI systems that augment human capabilities while responding to societal needs, such as surgical assistance and eldercare robotics.[17] In this model, AI assumes a supporting role in the pursuit of human well-being. It is within this anthropocentric trajectory of AI development that the deployment of AI for legal and regulatory compliance and enforcement can be situated.

2.2 AI in EU law and beyond

The European Union has adopted a harmonised definition of artificial intelligence in the recently enacted AI Act, drawing upon the OECD Recommendation on AI.[18] According to Article 3(1):

"'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

This far-reaching and open-ended definition is coherent with the horizontal and cross-sectoral approach adopted by European digital legislators, reflecting their intent to accompany, promote and delineate a 'perimeter' around the scope of innovation without unduly constraining it. The use of terminology such as "varying levels of autonomy", "may exhibit adaptiveness", and "implicit objectives" offers a degree of interpretative flexibility to both regulators and AI developers. Given that AI development is, by its nature, a continuous science-driven process, regulation must likewise evolve, with legal scholars playing a key role in accompanying this progression.

[17] Ben Shneiderman, *Human-Centered AI* (online edn, Oxford Academic 2022) 1.
[18] Organisation for Economic Co-operation and Development ('OECD') 'Recommendation of the Council on Artificial Intelligence' (2019) <https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449> accessed 20 June 2025.

Consistent with the European Union's tradition of participatory governance,[19] the AI Act introduces a range of forward-looking, or future-proofing,[20] regulatory instruments designed to be subject to ongoing review and adaptation. These include regulatory sandboxes, codes of conduct, and codes of practice, jointly developed by experts from academia, standardisation bodies, industry, the public sector, and civil society. The regulatory focus is directed towards anthropocentric, trustworthy,[21] and ethically aware AI development, deployment and use, while preventing risks that could result in the infringement of fundamental rights or pose significant threats to key societal values, such as the rule of Law, democracy and environmental protection.

The European Union's anthropocentric vision of artificial intelligence has drawn inspiration from transnational, science-based, and principle-setting initiatives such as the Asilomar AI Principles and the IEEE General Principles of Ethically Aligned AI. These frameworks continue to shape the global discourse on AI governance, as exemplified by developments such as the G7 Hiroshima Process, the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.[22] Within socio-legal systems, AI is accordingly conceptualised as a tool serving human, social, and collective welfare. From a socio-technical perspective, however, it is increasingly recognised as an instrument of power and domination, employed by states and corporations that control the material and immaterial infrastructures necessary to develop, train, and maintain AI systems. These perspectives underscore that, notwithstanding the performative force of legal language, empirical realities and geopolitical dynamics possess a significant capacity to influence the trajectory of technological advancement.

Turning back to the legal comparison, the United States as well define artificial intelligence in a statutory framework, namely under 15 U.S. Code § 9401 (Commerce and Trade), as follows:

"A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action.".

[19] Since the Lisbon Strategy through the Better Law-Making approaches, the EU has pioneered a participatory method of regulation. For a brief overview, see Bassan (n 5).

[20] Sophia Hina Fernandes da Silva Ranchordas, 'Experimental Regulations and Regulatory Sandboxes: Law without Order?' [2021] University of Groningen Faculty of Law Research Paper No 10/2021 1, 35 <https://ssrn.com/abstract=3934075> accessed 5 February 2025.

[21] European Commission (EC) High Level Expert Group on Artificial Intelligence (HLEGAI), 'Ethics guidelines for trustworthy AI' (Guidelines 2019).

[22] For a general overview of AI governance proposals: Jonas Tallberg and others, 'The Global Governance of Artificial Intelligence: Next Steps for Empirical and Normative Research' (2023) 25(3) International Studies Review 1, 18 <https://academic.oup.com/isr/article/25/3/viad040/7259354?login=true> accessed 10 February 2025.

Although the definitions of artificial intelligence articulated by the European Union and the United States exhibit significant areas of overlap, it remains uncertain whether the contemporary political reorientation towards self-regulation — initiated under the Trump administration[23] — will uphold the human-in-the-loop paradigm as a foundational element of a transatlantic AI governance model grounded in democratic principles and the rule of law. By contrast, China's regulatory approach to AI similarly invokes globally shared values such as ethics, data protection, safety, security, and human supervision.[24] However, it does so through the lens of socialist principles, national cohesion, and concerns over social stability, operationalised through a granular command-and-control framework tailored to specific application domains.[25] Collectively, these diverse regulatory trajectories illustrate the concurrent forces of convergence and divergence shaping global socio-technical approaches to AI. Whereas the EU prioritises risk-based assessment and the protection of fundamental rights, the United States adopts a market-oriented regulatory philosophy, while China regulates AI in accordance with traditional statist imperatives.

2.3 Blockchain in computer science

Blockchain technology refers to a decentralised and distributed ledger system through which users can store and transfer tokenised[26] value — including data — across a network comprising multiple nodes. This architecture caters for data integrity, transparency, and security by means of cryptographic keys. From a computer science standpoint, blockchain is underpinned by four fundamental elements: decentralisation, cryptography, consensus and the possibility to program smart contracts within the system.

Decentralisation distributes data across a peer-to-peer network, while eliminating the need for a central authority and enhancing systemic resilience by avoiding a single point of failure.[27] Cryptographic hashing ensures that each block in the chain contains the unique hash of the preceding block, granting the system tamper resistance and enhancing

[23] This shift commenced by repeal of Executive order n 14110. Ex Ord No 14110, Oct. 30, 2023, 88 F.R. 75191, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

[24] Hunter Dorwart and others, 'Preparing for compliance: Key differences between EU, Chinese AI regulations' (*IAPP*, 5 February 2025) <https://iapp.org/news/a/preparing-for-compliance-key-differences-between-eu-chinese-ai-regulation> accessed 15 February 2025.

[25] These measures distinguish AI through three interrelated but distinct categories: 1) Algorithm Recommendation Technologies: AI systems that generate, rank, or filter content based on user preferences, often employed in social media, search engines, and e-commerce platforms (Cyberspace Administration of China 2022); 2) Deep Synthesis Technologies: AI-driven generative models used for creating or modifying media, including deep fakes, synthetic speech, and virtual reality content (Chinese State Council 2022); Generative AI: Broadly encompassing AI technologies that generate new content across multiple modalities, including text, images, and audio (Ministry of Industry and Information Technology 2023). China's regulatory approach focuses on functionality rather than a single overarching definition, ensuring broad oversight while addressing AI-related risks and opportunities.

[26] The process of converting an asset or rights to an asset into a digital token, facilitating easier transfer and ownership tracking.

[27] Nakamoto Satoshi, 'Bitcoin: a peer-to-peer electronic cash system' (*Satoshi Nakamoto Institute*, 31 October 2008) <https://nakamotoinstitute.org/library/bitcoin/> accessed 16 February 2025.

both data security and privacy. While transactions remain visible on the blockchain, the identities of the transacting parties are either anonymous or pseudonymous.

Consensus mechanisms regulate the validation of transactions, determining the conditions under which new blocks are added to the chain. These mechanisms may vary depending on the type of blockchain and transaction model employed. Finally, blockchain can support self-executing agreements encoded directly onto the blockchain known as smart contracts — first popularised by Ethereum in 2015.[28]

Recent technological developments have facilitated the translation of natural language contracts into machine-readable formats and executable smart contract code. This, however, necessitates collaboration with legal and other experts to ensure interpretative fidelity.[29] Under such conditions, parties may negotiate and conclude legally binding agreements off-chain, monitor their performance in real time, and trigger automated execution on-chain when the requisite legal or factual conditions are met.

Blockchain technology has been applied across a wide range of sectors, with some of the most prominent use cases emerging in the financial domain. Here, decentralised finance (DeFi) protocols leverage blockchain infrastructures to enable activities such as lending, borrowing, and asset management without reliance on traditional financial intermediaries. Within the supply chain sector, blockchain allows for the traceability and authentication of goods across their entire life cycle. In the energy domain, blockchain supports peer-to-peer (P2P) trading models, enabling decentralised energy exchanges between producers and consumers. Additionally, various states and public authorities have implemented, or are actively exploring, the use of blockchain in public administration. Such applications include the issuance of digital identities, the notarisation of public records — such as land titles and intellectual property rights — and the development of secure, auditable voting systems aimed at increasing electoral transparency and mitigating the risk of fraud.

[28] Vitalik Buterin, 'A Next-Generation Smart Contract and Decentralized Application Platform' (White Paper 2013) <https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf> accessed 16 February 2025. Yet, the notion was coined in 1994 by Nick Szabo, an American computer scientist and legal scholar known as the precursor of the Bitcoin architecture, as follows: "a computerized transaction protocol that executes the terms of a contract. The general objectives [..] are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimise exceptions both malicious and accidental, and minimise the need for trusted intermediaries". Nick Szabo, 'Smart contracts' (*Satoshi Nakamoto Institute*, 1994) <https://nakamotoinstitute.org/library/smart-contracts/> accessed 16 February.

[29] The expression 'smart legal contract' has been defined as "*a specific application of technology as a complement, or substitute, for traditional contracts*" Banca d'Italia, Università Cattolica del Sacro Cuore, Università Roma Tre, 'Caratteristiche degli smart legal contacts' (Report 2023) 4; Fabio Bassan and Maddalena Rabitti, 'From Smart Legal Contracts to Contracts on Blockchain: An Empirical Investigation' (2023) 55 Computer Law & Security Review: The International Journal of Technology Law and Practice 1 <https://www.sciencedirect.com/science/article/pii/S0267364924001018> accessed 17 February 2025; Thibault Schrepel, 'Smart Contracts and the Digital Single Market Through the Lens of a "Law + Technology" Approach' [2021] Publications Office of the European Union <https://digital-strategy.ec.europa.eu/en/library/smart-contracts-and-digital-single-market-through-lens-law-plus-technology-approach>; Mateja Durovic and Andre Janssen, 'The Formation of Blockchain-Based Smart Contracts in the Light of Contract Law' (2019) 6 European Review of Private Law 753, 772.

More broadly, blockchain may be employed for the registration, storage, and transfer of any form of virtual information or tokenised value, offering a versatile infrastructure for a wide spectrum of administrative, economic, and societal purposes.

2.4 Blockchain in EU law and beyond

Blockchain has been defined as "*a distributed, shared, encrypted database that serves as an irreversible and incorruptible public repository of information*".[30] While the European legal literature has contributed significantly to clarifying key notions such as blockchain governance and regulation,[31] the current EU legal framework remains fragmented, piecemeal, and largely sector-specific. This condition, however, does not contradict the rationale of regulatory intervention. On the contrary, the absence of regulation may itself generate risks for markets and consumers. Regulatory authorities tend to act where a regulatory risk is perceived, be it a systemic threat to market integrity, consumer protection, or other fundamental legal interests, such as data protection or taxation.

Driven in part by international developments,[32] the European Union has sought to mitigate financial regulatory risks posed by the emergence of blockchain-based decentralised finance (DeFi) through a series of legislative initiatives. These include anti-money laundering frameworks and a suite of digital finance measures: the Markets in Crypto-Assets (MiCA) Regulation,[33] the Digital Operational Resilience Act (DORA),[34] and a pilot regime[35] designed to facilitate experimentation with decentralised finance under controlled conditions. Within the public sector, the European Blockchain Services Infrastructure (EBSI) initiative is spearheading the development of blockchain-based applications aimed at enhancing transparency and efficiency in areas such as identity

[30] Aaron Wright, Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' [2015] SSNR 1, 58 <https://ssrn.com/abstract=2580664> accessed 18 February 2025.

[31] *ex multis* Narmin Nahidi, 'Blockchain Constitutionalism: Analyzing the Impact of Political Forces on Blockchain Governance' (2025) SSRN, 1-59, <https://ssrn.com/abstract=5137305> accessed 19 February 2025; Primavera De Filippi and others 'Blockchain Technology and Polycentric Governance' (European University Institute 2024) 7, <https://cadmus.eui.eu/server/api/core/bitstreams/69ad10b2-fe42-59e2-8c7d-567dff4939dc/content> accessed 19 February 2025; Michelle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2018); Primavera De Filippi, Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018); Marcella Atzori, 'Blockchain Technology and Decentralized Governance: Is the State Still Necessary?' (2017) 6 (1) Journal of Governance and Regulation 45 <https://the-blockchain.com/docs/Blockchain%20Technology%20and%20Decentralized%20Governance%20-%20Is%20the%20State%20Still%20Necessary.pdf> accessed 20 February 2025.

[32] *ex multis* Bank for International Settlements, 'Central bank digital currencies: foundational principles and core features' (Joint Report 2020) 4; Financial Action Task Force (FATF), 'Updated Guidance for a Risk-based Approach for Virtual Assets and Virtual Assets Service Providers' (2021).

[33] Regulation (EU) 2023/1114 of the European Parliament and Council on Markets in Crypto-Assets and amending Regulations (EU) No 1093/2010 and (EU) No 648/2012 [2023] OJ L150/40.

[34] Regulation (EU) 2022/2554 of the European Parliament and Council on digital operational resilience for the financial sector (Digital Operational Resilience Act) [2022] OJ L333.

[35] Regulation (EU) 2022/858 of the European Parliament and Council on a pilot regime for market infrastructures based on distributed ledger technology [2022] OJ L151/1.

verification, cross-border transactions, and the security of governmental data. Complementing this initiative, the European Blockchain Regulatory Sandbox — launched in 2023 — offers a controlled environment for the testing of cross-border blockchain innovations under real-world conditions, while also facilitating structured engagement between regulators and innovators. Given the inherently transnational nature of blockchain technology, its legal and economic implications have drawn the attention of numerous international and transnational bodies. These actors are actively exploring its potential to facilitate electronic commerce, operationalise smart contracts, and improve transparency across global supply chains.[36] Notably, the Council of Europe has acknowledged the transformative capacity of blockchain within its broader democratic agenda. The technology is recognised as a tool for advancing accountability and transparency in democratic processes — ranging from digital identity management and informational self-determination, to supporting refugees and vulnerable populations, ensuring responsible supply chains, securing immutable land titles, enabling transparent voting systems, and enhancing the efficiency of dispute resolution mechanisms.[37]

3 AI-blockchain: converging opposites

Artificial intelligence (AI) and blockchain technologies are increasingly being considered in tandem, as their contrasting technical features may, when combined, yield significant benefits in terms of security, optimisation, and the overall efficiency of systems and processes.[38] While both are machine-based systems, their architectures and operational logics are fundamentally distinct. AI typically functions within centralised infrastructures, relying on the processing and analysis of large-scale datasets to train complex models. By contrast, blockchain is inherently decentralised, distributing both data and control across a network of nodes that collectively validate and record transactions.[39]

Although both systems operate on the basis of algorithmic logic, the nature of their algorithms diverges in substance. AI algorithms — except for certain simple linear models — are generally non-linear, non-deterministic, and non-binary, frequently producing probabilistic outputs that are difficult to predict or reproduce. In contrast, the algorithms underpinning smart contracts are deterministic and binary, operating through conditional

[36] *ex multis* Giuliano Castellano, 'UNCITRAL Colloquium: Navigating the New Era of Digital Finance 20-21 (2025) 'Digital Assets in Digital Finance Regulatory Standards and Law Reform Implications' (*UNCITRAL*, 20-21 February 2025) <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/castellano_updated.pdf> accessed 20 February 2025; Emmanuelle Ganne, 'Can blockchain revolutionize international trade?' (World Trade Organization 2018) 1.

[37] Council of Europe, 'The Impact of Blockchains for Human Rights, Democracy, and the Rule of Law' (Information Society Department, Report to the Council of Europe 2022) <https://edoc.coe.int/en/artificial-intelligence/11713-the-impact-of-blockchains-for-human-rights-democracy-and-the-rule-of-law.html> accessed 20 June 2025.

[38] Kalhed Salah and others, 'Blockchain for AI: Review and Open Research Challenges' (2019) 7 IEEE Access 10127 <https://ieeexplore.ieee.org/abstract/document/8598784> accessed 20 February 2025.

[39] Leon Witt and others, 'Blockchain and Artificial Intelligence: Synergies and Conflicts' [2024] arXiv Cornell University <arXiv:2405.13462> accessed 20 February 2025.

'if...then' structures that ensure predictability, transparency, and verifiability in execution.[40]

In terms of transparency, AI — especially when powered by sophisticated deep learning or neural networks — suffers from opacity or a notable lack of interpretability, often referred to as the "black box" problem.[41] This opacity is especially problematic when AI is deployed in sensitive decision-making contexts that may infringe upon fundamental rights and interests, given that its outputs are frequently untraceable and cannot be readily explained, even by the mathematicians and programmers themselves. Blockchain, by contrast, provides immutability, traceability, and auditability by maintaining tamper-proof and transparent records of transactions and data flows.

Another difference lies in how the two technologies address data security and privacy concerns. AI systems, particularly those trained on large datasets, are exposed to risks of personal data breaches as their functionality depends on access to vast amounts of sensitive information.[42] Blockchain, in contrast, employs cryptographic protocols that facilitate privacy by design. It enables the pseudonymous and secure recording of transactions without disclosing personal data, thereby significantly mitigating the risks of unauthorised access and data leakage.[43]

Another salient distinction between the two technologies lies in their respective security paradigms. AI systems are typically associated with external security functions, such as the detection of anomalies, threats, and fraudulent activities through the analysis of large datasets. This makes AI an increasingly essential component of risk management infrastructures across diverse sectors. Blockchain, on the other hand, embodies an internal security model rooted in its decentralised and distributed architecture. By dispersing control across multiple nodes, blockchain eliminates single points of failure and substantially reduces vulnerabilities to systemic attacks. This structural feature ensures that no single entity can unilaterally compromise or manipulate the system, thereby embedding security within the technological design itself.

The regulatory applications of these technologies further highlight their divergence. AI is progressively being employed as a compliance tool, assisting institutions in navigating complex legal and regulatory landscapes through automated monitoring, reporting, and analysis of value chain activities. Conversely, smart contracts deployed on blockchains serve as instruments of legal and regulatory enforcement. By maintaining tamper-proof,

[40] Although non-linear blockchains exist and are implemented to incorporate multiple chain structures involving parent-child chains, main-side chains and parallel chains. Olexandr Kuznetsov and others, 'On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security' (2024) 12 IEEE Access 3881, 3897 <https://iris.univpm.it/retrieve/f30e2f03-eaf3-41ac-bf05-fab78db9a86a/Kuznetsov_integration_artificial_intelligence_2024.pdf> accessed 21 February 2025.

[41] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

[42] Dalila Ressi and others, 'AI-Enhanced Blockchain Technology: A Review of Advancements and Opportunities' (2024) 225 Journal of Network and Computer Applications 1 <https://www.sciencedirect.com/science/article/abs/pii/S1084804524000353> accessed 20 February 2025.

[43] ibid.

append-only, and verifiable records, blockchains facilitate regulatory auditability and provide evidentiary support for compliance.[44] Smart contracts add a dynamic operational layer to blockchain's otherwise static infrastructure. Through automated self-execution of contractual terms upon fulfilment of predefined conditions, they enable seamless legal enforceability and operational efficiency in decentralised ecosystems. Figure 1 below systematises the opposing features of these technologies, showing how their differences may complement each other.

AI	Blockchain
Centralised system	Decentralised system
Non-deterministic, non-binary functioning (hard-to-predict outcome)	Deterministic, binary functioning (predictable outcome)
High opacity (especially in advanced ML, DL, GenAI)	Transparency (traceability, verifiability, immutability)
Risks of personal data breaches	Cryptography ensures privacy-by-design
External security (fraud detection, risk management)	Internal security (no single point of failure)
Technology for legal/regulatory compliance	Technology for legal/regulatory enforcement

Figure 1: The opposite features of AI and BC.

3.1 Gains of integration

The integration of blockchain technology with artificial intelligence (AI) holds significant potential for mutual technical enhancement. This justifies the development of a theoretical framework that supports their convergence. Both technologies are inherently designed to process and manage substantial volumes of data. Blockchain offers a secure, transparent, privacy-by-design, and tamper-resistant infrastructure for data registration, access, and exchange. When implemented through smart contracts, it enables the

[44] Georgios Zekos, 'Risk Management Developments' in Georgios I Zekos, *Economics and Law of Artificial Intelligence* (Springer Link 2021) 147.

automated execution of human-defined conditions. Conversely, AI systems facilitate the real-time analysis of complex datasets and can generate insights, predictions, and anomaly detection; they can further suggest courses of action, make decisions, and implement them autonomously.[45]

There is a compelling argument for integrating AI and blockchain within a unified architecture, given their complementary functionalities. It departs from one of the most pressing concerns surrounding advanced AI — particularly models based on deep neural networks: the opacity associated with training data and modelling methodologies.[46] This opacity reverberates on the interpretability and explainability of AI outputs. Poor quality of training datasets affects the quality of AI systems and results in inaccuracies, hallucinations, biases and algorithmic discrimination, thus rights violations.[47] In fact, these dysfunctionalities have brought litigants to court in various jurisdictions and regulatory areas such as banking and insurance credit scoring,[48] public-sector automated decision-making systems and employment law.[49]

[45] This is the case of the emerging Agentic AI, Yonadav Shavit and others, 'Practices for Governing Agentic AI Systems' OpenAI Research Paper (2023) 2, 18 <https://cdn.openai.com/papers/practices-for-governing-agentic-ai-systems.pdf> accessed 22 February 2025: "*systems that adaptably pursue complex goals using reasoning and with limited direct supervision*" "*characterized by the ability to take actions which consistently contribute towards achieving goals over an extended period of time, without their behaviour having been specified in advance*".

[46] Stanford University Institute for Human-Centered AI, 'The AI Index 2024 Annual Report' (2024) para 6 <https://hai.stanford.edu/ai-index/2024-ai-index-report> accessed 20 June 2025.

[47] Philipp Hacker, 'Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law' (2018) 55 Common Market Law Review 1143, 1186 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3164973> accessed 23 February 2025; Jeremias Adams-Prassl, Reuben Binns, Aislinn Kelly-Lyth, 'Directly Discriminatory Algorithms' (2022) 86(1) Modern Law Review 144 <https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-2230.12759> accessed 27 February 2025; Katja Langenbucher, 'Consumer Credit in the Age of AI – Beyond Anti-discrimination Law' [2023] ECGI Working Paper Series in Law, WP N 663/2022, 2, 52 <https://ssrn.com/abstract=4298261 > accessed 27 February 2025.

[48] Case C-634/21 *OQ v Land Hessen (SCHUFA Holding (Scoring))* [2023] ECLI:EU:C: 2023:940. The CJEU was called to ensure the correct interpretation and application of Art. 22 (1) of the GDPR concerning decisions made based on automated algorithmic systems. In the recently settled SCHUFA case, the German credit agency applied an automated credit scoring process that played a determining role in the lender's decision to deny credit. According to the ruling, SCHUFA itself acted as a decision-maker within the purview of the GDPR provisions on Automated Decision-Making (ADM). Under Artt 22(3), 13-15 GDPR, the addressee of an algorithmic-based decision enjoys a right to explanation, whereby a data subject has the right to '*express his or her point of view and to contest the decision' which is 'based solely on automated processing'*, and to obtain '*meaningful information about the logic involved*' in the processing of personal data; Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2017) 38(3) AI Magazine 50 <arXiv:1606.08813> accessed 28 February 2025; Margot E Kaminski, 'The Right to Explanation, Explained' (2019) 34 (1) Berkeley Technology Law Journal 196 <https://ssrn.com/abstract=3196985> accessed 29 February 2025; Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7(3) International Data Privacy Law 243 <https://academic.oup.com/idpl/article-abstract/7/4/243/4626991?login=false> accessed 1 March2025.

[49] Hofmann CH Herwig, Felix Pflücke, 'Automated Decision-Making (ADM) in EU Public Law' in Herwig C H Hofmann, and Felix Pflücke (eds), *Governance of Automated Decision-Making and EU Law* (Oxford Academic 2024); Vincenzo Pietrogiovanni, 'Deliveroo and Riders' Strikes: Discriminations in the Age of Algorithms' (2021) 7(3) International Labor Rights Case Law 203 <https://www.researchgate.net/publication/357123841_Deliveroo_and_Riders'_Strikes_Discriminations_in_the_Age_of_Algorithms> accessed 1 March 2025.

Computer scientists posited that blockchain technology could enhance transparency by logging AI data points for independent verification and auditing.[50] The same authors have further proposed that smart contracts could establish immutable parameters for AI operations creating templates that prescribe acceptable data sources and prompt structures.

Moreover, the use of oracles — computer protocols that import verified real-world data into the blockchain — enables AI responses to be cross-validated against transparent, verifiable and tamper-proof on-chain information. These decentralised oracle systems can verify AI-generated content by triangulating it with multiple authenticated sources, potentially expanding the scope of verification from mere factual accuracy to more sophisticated domains, including data for regulatory compliance. Additionally, the integration of AI and blockchain can manifest in the form of federated learning, which enables decentralised data sharing for AI collaborative development[51] (see further sub 5.2). Within such a hybrid algorithmic environment, stakeholders may gain access to AI training datasets and emergent data patterns, which they may monitor, interpret and explain. These features of accessibility and auditability could prove particularly valuable for regulatory compliance, allowing auditors and stakeholders to reconstruct and evaluate the reasoning underpinning AI outputs and decisions.[52]

Conversely, AI may optimise blockchain's efficiency, decision-making processes and scalability. AI-driven data analysis caters for the detection of vulnerabilities and anomalies through ML techniques[53] that identify suspicious patterns within blockchain transactions,[54] thus contributing to the prevention of fraud and attack.[55] These features add security in AI-assisted smart contract ecosystems and increase overall network resilience.

Furthermore, AI can enable dynamic consensus mechanisms models that adjust parameters based on network conditions. For instance, reinforcement learning (RL) algorithms can fine-tune consensus rules depending on real-time transaction loads,

[50] Jordan Brewer and others, 'Navigating the challenges of generative technologies: Proposing the integration of artificial intelligence and blockchain' (2024) 67 (5) Business Horizons 525 <https://www.sciencedirect.com/science/article/pii/S0007681324000569> accessed 1 March 2025.

[51] Dinh C Nguyen Ming Ding and others, 'Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges' (2021) 8(16) IEEE Internet of Things Journal 12806 <https://ieeexplore.ieee.org/document/9403374> accessed 1 March 2025.

[52] See Salah and others (n 38).

[53] AI-driven models, such as those proposed by some authors, that use machine learning to detect vulnerabilities with over 95% accuracy in seconds. Pouyan Momeni and others 'Machine Learning Model for Smart Contracts Security Analysis' [2019] 17th IEEE International Conference on Privacy, Security and Trust (PST) 1 <https://ieeexplore.ieee.org/document/8949045> accessed 2 March 2025.

[54] Muneeb Ul Hassan, Mubashir Husain Rehmani, Jinjun Chen, 'Anomaly Detection in Blockchain Networks: A Comprehensive Survey' (2023) 25(1) IEEE Communications Surveys & Tutorials 1 <https://arxiv.org/abs/2112.06089> accessed 2 March 2025.

[55] Bakkiam David Deebak and Fadi M. Al-Turjman, 'Privacy-Preserving in Smart Contracts Using Blockchain and Artificial Intelligence for Cyber Risk Measurements' (2021) 58 Journal of Information Security and Applications 1 <https://www.sciencedirect.com/science/article/pii/S2214212621000028> accessed 2 March 2025, AI techniques, such as XGBoost-based regression models, can analyse transaction patterns to detect fraudulent activity in smart contracts.

thereby improving system efficiency and scalability.[56] AI may also analyse network traffic to predict future demand, thus optimising blockchain performance during periods of high activity and mitigating latency while preserving security standards.[57]

Finally, AI can contribute to the formulation, testing and validation of smart contract code.[58] Large AI models can assist developers by interpreting and explaining code, detecting potential errors and suggesting or taking contract security measures. However, it must be noted that the outputs of such models remain inherently probabilistic and require human oversight.

A theoretical framework for AI-blockchain integration, besides legal and ethical principles, could be built upon principles of mutual enhancement, decentralised accountability and transparency, and data lifecycle integrity and interoperability. This framework would conceptualise blockchain as an infrastructure layer that provides certainty of data origin, auditability and smart contract-based enforcement for regulatory operations, while AI performs adaptive intelligence, pattern recognition, and operational optimisation to blockchain systems. The framework would further incorporate multi-party and multi-layered trust models, underpinned by blockchain-based validation mechanisms that integrate cryptographic proofs with explainable AI methodologies. This combination aims to establish robust confidence in data-driven decision-making processes, especially in complex or high-stakes ecosystems.

Each technology enhances the strengths of the other while compensating for its limitations. Mutual augmentation requires the development of systems that are not only intelligent and responsive but also trustworthy and verifiable. Decentralised accountability is achieved by leveraging blockchain's immutability to document the behaviour of AI systems in a transparent and auditable manner, while interoperability comes with data semantics standardisation. Training datasets, inference logs, and decision-making parameters can be recorded on-chain, making it possible to trace how outcomes are produced and to ensure that AI operations adhere to ethical guidelines and regulatory standards. This approach shifts trust from opaque algorithms to verifiable processes to spur confidence among stakeholders. The integrity of the data lifecycle can be preserved through mechanisms such as decentralised oracles, which ensure that data used across AI processes — from training through deployment — remains verifiable. The blockchain infrastructure supports the consistent and auditable use of data, while smart contracts can enforce predefined operational boundaries for AI models, limiting their behaviour to acceptable parameters. To reinforce trust in this integrated system, the framework incorporates layered trust models that combine cryptographic proofs with

[56] Ressi and others (n 42).
[57] Mujistapha Ahmed Safana, Yasmine Arafa, and Jixin Ma, 'Improving the Performance of the Proof-of-Work Consensus Protocol Using Machine Learning' in *Proceedings of the 2020 Second International Conference on Blockchain Computing and Applications* (BCCA) (IEEE 2020) 16 <https://ieeexplore.ieee.org/document/9274082> accessed 3 March 2025.
[58] Ressi and others (n 42).

explainable AI methods. These layers allow algorithmic decisions to be interpreted, validated, and trusted by both human and institutional actors. By uniting transparency, accountability, and a combination of natural and artificial intelligence, this model aims to support regulatory compliance, system robustness, and sustainable stakeholder trust in complex, data-driven ecosystems.

3.2 Pains of Integration

Besides the promising benefits, the integration of AI and blockchain technologies presents several challenges, including computational intensity, environmental sustainability,[59] data-related limitations, scalability, and replicability. It is crucial that both computer scientists and regulators address these issues to ensure the effective deployment and long-term sustainability of AI-blockchain solutions for regulatory compliance and enforcement. A primary concern is the high energy consumption demands associated with both technologies, as well as the intensively extractive industry underpinning their development, which raises serious ethical and environmental considerations. However, it is worth noting that not all blockchain networks require substantial computational power. Those relying on energy-intensive Proof of Work (PoW) consensus mechanisms are particularly problematic, but alternatives — such as proof-of-stake (PoS) and other low-energy consensus models — offer more sustainable solutions. The large-scale adoption of blockchain technologies necessitates a transition towards 'green' blockchains that employ energy-efficient consensus algorithms capable of validating transactions rapidly and with minimal environmental impact. Likewise, the lifecycle of AI systems — including their construction, training, deployment, and maintenance — demands substantial material and human resources.[60] This includes the extraction of minerals, intensive water use in data centres, human labour, and the social acceptability of AI applications, all of which contribute to ethical and sustainability challenges. The resource-intensive nature of both technologies consequently poses barriers to scalability, particularly for real-time or large-scale applications.

Beyond environmental concerns, the integration of AI and blockchain faces three core technical challenges: limitations in data availability and quality, challenges in scaling the systems efficiently, and issues related to the replicability of results.[61]

Concerning the first challenge, the principal difficulty lies in the quality and heterogeneity of data available for training AI systems within blockchain environments. Although public blockchains record vast volumes of data, this does not necessarily equate

[59] Next to energy consuming blockchains exist carbon-neutral blockchains. See, for instance, Cosimo Bassi and Naveed Ihsanullah, 'Proof of Stake Blockchain Efficiency Framework' (Algorand Foundation 2022) <https://medium.com/algorand-foundation/proof-of-stake-blockchain-efficiency-framework-d1e8b4350905> accessed on 3 March 2025.
[60] Kate Crawford, *Atlas of AI: Power, Politics and the Planetary Costs of Artificial Intelligence* (Yale University Press 2022) 1.
[61] Ressi and others (n 42).

to the availability of high-quality, well-structured datasets suitable for machine learning purposes. Data redundancy in such contexts may limit the capacity of AI systems to detect novel vulnerabilities and reduce the diversity of training datasets. The challenge becomes more acute in private or permissioned blockchain networks, where access to data is highly restricted, thereby impeding the development of robust and generalisable AI models.[62] Additionally, AI models struggle with adaptation when data inputs change such as modifications in programming languages or the emergence of new attack vectors.

With regard to scalability, AI-based vulnerability detection methods typically outperform traditional static analysis tools in terms of speed and accuracy. However, they frequently encounter difficulties in scaling effectively when confronted with new vulnerabilities arising from blockchain protocol updates.[63] The absence of standardised benchmark datasets exacerbates this problem.[64] In the absence of high-quality, consistent data, the processes of training, testing, and validating AI models against emerging or evolving threats can become inefficient and unreliable.

The issue of replicability and interoperability complicates the picture. The interaction between AI algorithms and decentralised blockchain architectures makes it difficult to ensure that results remain reliable and replicable across different systems. Without standardised methodologies, inconsistencies in detection outcomes could undermine trust and discourage adoption.

All in all, while AI and blockchain integration hold immense potential for transparency, security, automation and efficiency, these unresolved challenges spanning energy consumption, scalability, data reliability and security vulnerabilities yet hinder their widespread adoption. Addressing these limitations through sustainable infrastructures, standardised benchmarking and adaptive AI models is essential for trustworthy and sustainable AI-blockchain ecosystems.

3.3 Use cases in the industry

AI-blockchain integration is already operational in the private sector and industrial settings. In health care, AI-powered blockchain has been implemented to provide a patient-controlled electronic medical records system, where AI comes into play to generate insights into patient health, predict diseases and provide personalised therapeutic recommendation.[65] IBM has launched the Food Trust Project, a supply chain management system that combines AI and blockchain to create a platform for a transparent and immutable record of food items from farm to store on the blockchain,

[62] ibid.
[63] ibid.
[64] ibid.
[65] Rajesh Kumar and others, 'AI-Powered Blockchain Technology for Public Health: A Contemporary Review, Open Challenges, and Future Research Directions' (2022) 11(81) Healthcare 1, 32 <https://pubmed.ncbi.nlm.nih.gov/36611541> accessed 4 March 2025.

food anomalies or contamination detection and food demand prediction through AI. In the financial sector, a hedge fund has built a blockchain marketplace to share AI models that consumers use to optimise investment decisions.[66] Scientific surveys enumerate these and further use cases in education, IoT security, energy grids, labour transactions and any other applicative scenarios where data and value exchanges are at stake.[67]

4 Cooperative regulatory compliance and enforcement

The application of technological solutions to smooth regulatory compliance and oversight is a well-established concept and best practice.[68] Since the 1980's, technological solutions have been deployed to facilitate risk management by financial institutions as finance became increasingly quantitative and reliant on information technology systems. With the development of more sophisticated big data analytics and governance technologies such as AI, blockchain[69] and the cloud, regulatory technology (RegTech) and supervisory technology (SupTech) have evolved significantly and reached beyond merely operational functions. RegTech has been felicitously defined as "*the use of technologies to solve regulatory and compliance requirements more effectively and efficiently*",[70] while SupTech as "*the use of technologies to help authorities to improve their supervisory capabilities*".[71] At the outset, RegTech unfolded in the application of technology in regulatory monitoring and reporting to drive cost reduction benefits in response to the regulatory wave following the global financial crisis.[72]

The outbreak of the COVID-19 pandemic accelerated the processes of digitisation and datafication across the global economy, rendering technological tools indispensable for

[66] See, for instance, a site of a quantitative global equity market-neutral hedge fund, which is unsuitable for most investors: 'The hardest data science tournament in the world' <https://numer.ai/> accessed 4 March 2025.
[67] Kuznetsov and others (n 40).
[68] Ressi ond others (n 42).
[69] Karen Yeung, 'Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law' (2019) 82 Modern Law Review 1 <https://onlinelibrary.wiley.com/doi/10.1111/1468-2230.12399> accessed 4 March 2025.
[70] See Douglas W Arner and others (n 3).
[71] idem; Contemporary RegTech applications covers automated Know Your Customer (KYC) and Anti-Money Laundering (AML) processes, which use machine learning algorithms to detect suspicious patterns and ensure compliance with evolving regulatory standards. One such example in the financial sector is ComplyAdvantage, a platform which employs machine learning to facilitate anti-money laundering (AML) compliance by screening transactions and clients against real-time global sanctions lists and adverse media sources. Another RegTech real-world application unfolds in transaction monitoring systems powered by real-time analytics and natural language processing tools that scan regulatory texts to aid in reporting obligations further illustrate the potential of RegTech. For instance, OneTrust is a widely adopted compliance platform, assists organisations in managing obligations under the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) by automating tasks such as cookie consent management, data mapping, and subject access requests. Additionally, smart contract auditing tools on blockchain platforms enable compliance with legal and financial regulations by embedding rules into the code itself, ensuring automatic execution aligned with regulatory frameworks. These examples underline that RegTech streamline compliance processes while enhancing the predictive and preventative capacities of financial institutions.
[72] Ross Buckley and others, 'The Evolution of Fintech: A New Post-Crisis Paradigm?' (2016) 47(4) Georgetown Journal of International Law 15; Douglas W Arner, Janos Nathan Barberis and Ross P Buckley, 'FinTech and RegTech in a Nutshell, and the Future in a Sandbox' (2017) 3(4) CFA Institute Research Foundation 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3088303 > accessed 26 February 2025.

communication, commercial transactions, and the delivery of goods and services. Market operators, consumers, public bodies and citizens adapted to the new course of socio-economic transactions. Progressively, RegTech evolved into a multifunctional tool facilitating cooperation between public authorities, ie, regulators and supervisors, and private actors, including market participants and infrastructure providers. On the public side, RegTech supports supervisory authorities in the development of simulation environments and regulatory sandboxes. These tools are deployed to test compliance mechanisms, evaluate systemic risks, and enhance market oversight.[73] They serve core public interests such as regulatory efficiency, institutional transparency, and the safeguarding of financial stability. On the private side, RegTech enables firms to streamline internal compliance operations, reduce the burden of regulatory obligations, and demonstrate adherence to legal requirements. In doing so, RegTech helps align private sector operations with prevailing regulatory expectations.

Despite the mutual benefits of RegTech-driven collaboration, the objectives of public and private stakeholders remain distinct. Public bodies are primarily concerned with the protection of systemic integrity and the upholding of the rule of law, whereas private actors tend to prioritise operational efficiency and legal certainty. In parallel, supervisory technology (SupTech) equips regulators with continuous monitoring tools that enable the detection of emerging issues in real time, thereby reducing the response time required to investigate and address potential compliance breaches.

Regulatory technology (RegTech) and supervisory technology (SupTech) are predominantly associated with the financial and banking sectors, where they first emerged and have since matured. In recent years, the European Union has actively promoted their development as a central pillar of its Digital Finance Strategy.[74] This strategic framework underscores the potential of technologies such as Natural Language Processing (NLP) and machine-readable regulations to enhance regulatory compliance, reduce the complexity of reporting obligations, and foster a shift towards more automated and data-driven modes of governance.

One notable area of application is the Digital Operational Resilience Act (DORA),[75] which seeks to strengthen supervisory oversight of cyber risks within the financial sector arising from the dependence of financial institutions on third-party information and communication technology (ICT) service providers. DORA establishes a harmonised incident prevention, mitigation and response system, an ICT third-party risk management framework and a cross-border and cross-sectoral oversight mechanism coordinated among

[73] The sandbox allows cooperation between regulators and regulatees to propose and experiment technology-driven innovative products, services and business models under a regime of regulatory exemptions and help regulators assess the potential impact of proposed reforms and shape novel regulatory approaches.
[74] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU European Commission, [2020] 591 final.
[75] Regulation (EU) 2022/2554 of the European Parliament and Council on digital operational resilience for the financial sector 'Digital Operational Resilience Act' ('DORA') [2022] OJ L333.

national competent authorities, the European Supervisory Authorities, and a Joint Oversight Network.[76] Within this approach, a multi-layered and interoperable AI-blockchain-based RegTech and SupTech infrastructure may well operationalise DORA's objectives to increase the efficiency, consistency, and interoperability of the European Union's supervisory architecture, and enhance the overall compliance with the operational resilience requirements imposed upon both financial entities and ICT service providers.

4.1 Cooperative regulatory compliance and enforcement beyond the financial sector

In abstract and in practice, there is no reason to rule out the application of the RegTech and SupTech paradigms in other regulatory domains where coordination between regulatory authorities may smooth compliance and enforcement and the approximation of rules and procedures. RegTech encompasses a wide array of applications aimed at ensuring and streamlining compliance with regulatory requirements.[77] For instance, in the environmental domain, private entities employ automated reporting systems and real-time data analytics tools to monitor emissions and ensure adherence to environmental regulations, such as limits on CO_2 output or hazardous waste disposal. In the context of civil aviation, RegTech supports the supervision of intercontinental aircraft routes through digital platforms that automatically verify compliance with international air traffic regulations and safety protocols by integrating flight data with regulatory frameworks. Such technologies significantly reduce the need for manual intervention, increase the accuracy of compliance monitoring, and provide timely alerts to both regulators and regulated entities. This substantiates a model of continuous compliance, whereby real-time feedback loops ensure that regulatory breaches can be identified and addressed promptly.

Both RegTech and SupTech systems pursue a sector-neutral goal: to coordinate and harmonise compliance requirements across markets though the development of standardised reporting formats and the facilitation of data sharing among regulators, market participants and informed consumers. Notably, even public sector initiatives can be understood as part of a broader RegTech phenomenon.[78] The European Central Bank's (ECB) Digitalisation Roadmap[79] and the establishment of the SupTech Hub exemplify the institutional commitment to advancing RegTech and SupTech within the EU Digital Acquis. The strategy is based on the cross-border regulatory cooperation between supervisory authorities and the promotion of stakeholder engagement, including start-ups, academic

[76] Artt 47-49 DORA.
[77] See Douglas W Arner and others (n 3).
[78] In the public sector, for example, Estonia's e-government model began experimenting with cryptographic techniques to secure data and transactions as early as 2008, six months prior to the creation of Bitcoin. Similarly, in Italy, the Ministry of Economy and Finance (MEF) initiated trials on the use of cryptography for data and transaction security in 2015.
[79] European Central Bank, *Progress on the preparation phase of a digital euro* (Second progress report, ECB 2025).

institutions and private sector. A central feature of this model is the implementation of a 'hub-and-spoke' innovation architecture, which hosts the development of collaborative projects and a digital culture among supervisors. This framework places particular emphasis on technologies such as artificial intelligence, machine learning, and blockchain-based compliance solutions. The ECB's approach prioritises the automation and enhancement of existing mechanisms for compliance monitoring, fraud detection, and regulatory reporting. By reducing procedural inefficiencies and reinforcing systemic transparency and stability, the ECB's model provides a valuable blueprint for the broader adoption of RegTech and SupTech across the European Union. It lays the foundation for a more interconnected, responsive and adaptive regulatory ecosystem.

Some legislative instruments forming part of the European Union's Digital Acquis endorse cooperative regulatory methods. In addition to the Digital Finance Package,[80] the Artificial Intelligence Act promotes the establishment of joint cross-border AI regulatory sandbox, with the European Commission providing technical assistance.[81] It further encourages collaboration among national competent authorities, relevant regulatory bodies, and other actors within the broader AI ecosystem.[82] In parallel, more than fifty EU authorities and regulatory bodies have joined the European Blockchain Regulatory Sandbox. This initiative facilitates confidential dialogues regarding selected use cases, with the objective of balancing legal certainty with regulatory innovation. Upon conclusion of these dialogues, the European Commission is expected to publish a report outlining best practices and key insights, while maintaining the confidentiality of the discussions. However, it remains uncertain whether the coexistence of multiple AI regulatory sandboxes across the Union will be implemented in a coherent and coordinated manner.

The success of such frameworks will largely depend on the consistency of cross-border collaboration and the interoperability of national regulatory initiatives. To this end, the competent authorities should set out uniform procedures, interoperable technology and services, and harmonised data semantics.

In this vein, under the Data Governance Act, the European Union legislature has opted to establish an ad hoc body — the European Data Innovation Board[83] — tasked with

[80] Eg, the MiCAR provides for cooperation among EU regulatory entities (EBA, ESMA and the ECB) to shape technical standards (Artt 36 para 4, 38, para 38 (5); 42 (4); 45 para 7; etc) that may be operationalised with technological compliance tools powered by the integration of AI and blockchain.

[81] Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence ('AI Act') [2024] Art 57.

[82] European Commission *European Blockchain Regulatory Sandbox* (European Commission 2023).

[83] Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance [2022] Data Governance Act ('DGA') Recital 54. The European Data Innovation Board (EDIB) plays a key role in coordinating national data policies and promoting cross-sectoral data use in alignment with the European Interoperability Framework and international standards. It works alongside the EU Multi-Stakeholder Platform for ICT Standardisation and other initiatives, ensuring the adoption of common technical and legal standards for data transmission between processing environments. The Board's responsibilities include identifying standardisation priorities, distinguishing between cross-sectoral and sector-specific standards, and supporting the organisation of data spaces. It collaborates with sectoral

coordinating national data policies and promoting cross-sectoral data use in accordance with the European Interoperability Framework and relevant international standards. The Board is expected to collaborate with both sector-specific and cross-sectoral bodies, as well as expert groups, to develop common technical and legal standards for the implementation of European Data Spaces.

A further illustration of coordinated governance can be found in Article 22 of the NIS 2 Directive,[84] which mandates joint risk assessments of critical supply chains for essential and important entities. These assessments are to be carried out by the Cooperation Group, in conjunction with the European Commission and the European Union Agency for Cybersecurity (ENISA).

Each of these legislative instruments delegates responsibilities to a multiplicity of authorities, some of which predate the legislation and are embedded within the existing EU institutional framework and the national systems of Member States. Others have been newly constituted to meet specific regulatory objectives.

In an effort to bridge divergent regulatory practices, the European Data Protection Supervisor (EDPS) has recently proposed the establishment of a "Digital Clearinghouse 2.0" aimed at implementing effective cross-regulatory cooperation.[85] This initiative envisions a framework based on mutual agreements encompassing consultation procedures, information exchange, best practice dissemination, coordinated enforcement actions, joint investigations, and clearly defined consequences for non-compliance.

The constitutional foundations for such cross-regulatory collaboration are carved in primary EU law. Article 4(3) of the Treaty on European Union (TEU) enshrines the principle of sincere cooperation, while Article 197 of the Treaty on the Functioning of the European Union (TFEU) sets forth the principle of administrative cooperation. Together, these provisions establish legal obligations for EU institutions and Member State administrative bodies to provide mutual assistance in the implementation of tasks arising from the Treaties.

In its judgment in Meta Platforms, the Court of Justice of the European Union (CJEU) clarified that the effective application of the *ne bis in idem* principle under Article 50 of the Charter of Fundamental Rights of the European Union requires the existence of "clear and precise rules" to pre-empt duplicative proceedings and ensure coordinated action among national authorities.[86]

However, competent authorities remain bound by confidentiality obligations related to data protection and the protection of commercial secrets of the entities under investigation. These obligations necessitate formal or informal cooperation mechanisms

bodies, expert groups, and networks to facilitate data reuse. Additionally, the EDIB assists the European Commission in developing a data altruism consent form, working in consultation with the European Data Protection Board (EDPB).

[84] European Parliament and Council Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union ('NIS 2 Directive') [2022] OJ L 333.

[85] European Data Protection Supervisor, 'Towards a Digital Clearinghouse 2.0 Concept Note' (EDPS 2025).

[86] Case C-252/21 *Meta Platforms and Others v Bundeskartellamt* [2023] ECLI:EU:C:2023:537 paras 57–58.

that clearly define consultation parameters and protocols for information exchange. Legislative action at the EU level — either through primary legislation or implementing measures — remains essential to establish a comprehensive and coherent framework for cross-authority coordination. Likewise, national legislative and administrative interventions are required to ensure legal certainty regarding the scope, conditions, and procedures for information sharing and inter-agency collaboration.

4.2 Integrating AI and blockchain for cooperative regulatory compliance and enforcement in the EU digital acquis

An AI-blockchain technological infrastructure stands to benefit significantly from the convergence of blockchain's features — namely traceability, privacy, transparency, and auditability — with the analytical, predictive, decision-making, and autonomous capabilities of artificial intelligence when applied to large volumes of regulatory data. This synthesis represents a promising frontier for enhancing regulatory communication and fostering cooperation among regulators, regulated entities, infrastructure providers, and, both directly and indirectly, consumers and citizens.

The advantages of the integration of AI and blockchain go beyond improvements in technological efficiency. They also present an opportunity to embed legal and ethical compliance directly within the architecture of technological systems. Blockchain's intrinsic ability to ensure data integrity, transparency, and accountability, when combined with AI's capacity to enhance data analysis, risk detection, and mitigation, may facilitate the emergence of a networked ecosystem wherein regulatory compliance, transparency, and fairness are not merely objectives but structural design features.

This technological convergence has the potential to ground a legal-by-design approach, whereby systems are configured from the outset to operate in accordance with legal and ethical standards and to support multi-stakeholder cooperation. One of the most promising prospects of this integration lies in its ability to reinforce regulatory compliance and enforcement through heightened transparency and security, applied across sectors and jurisdictions.

How, then, might the interaction between these technologies enhance data transparency, accountability in algorithmic decision-making, and data integrity across sectors? The Digital Markets Act (DMA) and the Digital Services Act (DSA) impose obligations on firms operating in the digital space to ensure transparency in automated profiling, targeted advertising, and content moderation practices. In this context, AI-powered profiling systems could harness blockchain technology to guarantee that all algorithmic processes underpinning automated decision-making are securely recorded, auditable, and traceable by both market participants and regulatory authorities. Blockchain immutable ledger could provide verifiable history of AI-driven decisions, allowing regulatory bodies to track and trace how data is processed, stored and used, on

the condition that such practices comply with the requirements of the EU General Data Protection Regulation (GDPR) and intellectual property legislation. The deployment of blockchain as a transparency-enhancing infrastructure could support firms in fulfilling their obligations under Article 22 GDPR, which governs automated individual decision-making and mandates the provision of meaningful explanations regarding algorithmic outcomes.

Additionally, blockchain's ability to timestamp records could support the enforcement of regulatory frameworks that impose disclosure obligations — such as the Artificial Intelligence Act and the Markets in Financial Instruments Directive II (MiFID II)[87] — by providing an immutable audit trail of trading decisions, risk assessments, and other relevant activities. Smart contracts could automate compliance processes within firms, reduce administrative costs and increase efficiency in regulatory reporting. In addition, decentralised blockchain infrastructures are particularly well-suited to facilitating regulatory cooperation through secure and interoperable data sharing across Member States. This potential is already being explored in several test-bed environments, including initiatives aimed at information exchange between competent authorities and real-time collaboration between regulators and firms within regulatory sandboxes.

The deployment of technology for regulatory purposes offers a dual advantage: it not only ensures that emerging technologies are aligned with EU legal standards — by embedding compliance into their operational logic — but also helps to minimise regulatory uncertainty through the inherent transparency and traceability of their functionalities.

5 Test-bed hypotheses

The following sections investigate two exploratory hypotheses concerning the integration of artificial intelligence and blockchain technologies as potential compliance tools with selected instruments of the EU digital acquis. Section 5.1 considers the extent to which blockchain can be combined with Explainable Artificial Intelligence (XAI) to fulfil the transparency obligations and support regulatory enforcement mechanisms under the proposed Artificial Intelligence Act (AI Act). Section 5.2 examines the use of federated learning models incorporating both AI and blockchain to enable privacy- and security-enhancing data sharing practices, particularly within the legal frameworks established by the Data Act and the Data Governance Act.

[87] Directive 2014/65/EU of the European Parliament and Council on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MiFID II) [2014] OJ L173/349.

5.1 Blockchain + XAI for compliance with/and enforcement of the AI act transparency rules

The primary objective of the AI Act is to build trust in AI technology and ensure its safe and rights-based development and use. To achieve these goals, the Act lays down harmonised transparency rules requiring interpretability and explainability of AI outputs.[88] Transparency is therefore intended as both the capacity to grasp what lies behind the AI outputs and decisions from a technological viewpoint (interpretability) and the possibility for users to understand decisions that affect their rights and have them explained (hence, explainability, from a legal reasoning viewpoint).[89]

In highly complex systems — such as those based on deep neural networks — the notion of transparency involves the challenge of 'opening the black box', wherein the reasoning behind AI outputs remains difficult to understand or justify, even for expert developers and mathematicians. In contrast, so-called 'white box' models, including linear regressions and decision trees, produce outcomes that are fully comprehensible and interpretable by specialists and may therefore be characterised as transparent-by-design.

However, this enhanced interpretability often comes at the expense of model expressiveness and predictive accuracy.[90] As a result, industry actors frequently favour black box systems, which, despite their opacity, tend to deliver superior performance in terms of precision and adaptability across complex datasets.

The Act does not distinguish between black or white boxes and rests on the typical EU risk-based regulatory approach informed by the legal rationale of preventing harm to human and environmental health and safety and safeguarding fundamental values and rights. The AI Act's transparency rules vary in relation to risk level, user type, and the point of market entry. As for high-risk systems, Article 13(1) states that they must be designed and developed to operate in a transparent manner and allow users to interpret outputs appropriately. Developers of high-risk AI must therefore adhere to an ex-ante transparency requirement, resulting in an 'explainability-by-design' mandate for AI system providers to give concise, complete, correct, and clear instructions to deployers. Article 14(1) spells out transparency in the possibility of human oversight throughout the AI lifecycle, for example through human-machine interface or available interpretation tools and methods, placing an ex-post explainability requirement – after a decision has been made – on high-risk AI systems. Article 12 requires the registration, or logging, of operations of the high-risk AI system (in fieri requirement).

[88] Recital 27 AI Act.

[89] Balint Gyevnar, Nick Ferguson, Burkhard Schafer, 'Bridging the Transparency Gap: What Can Explainable AI Learn from the AI Act?' in K Gal, A Nowé, GJ Nalepa, R Fairstein & R Rădulescu (eds), *Proceedings of ECAI 2023, the 26th European Conference on Artificial Intelligence. Frontiers in Artificial Intelligence and Applications* Vol. 372 (IOS Press, Amsterdam 2023) 964, 971.

[90] Diogo V Carvalho, Eduardo M Pereira and Jaime S Cardoso, 'Machine Learning Interpretability: A Survey on Methods and Metrics' (2019) 8(8) Electronics 832 <https://www.mdpi.com/2079-9292/8/8/832> accessed 28 February 2025.

Both ex-ante and ex-post requirements can be met by integrating that specific type of AI model known as explainable AI (XAI)[91] with a blockchain infrastructure. XAI is an AI model that retraces the algorithmic logics of AI outputs to provide a reasonable explanation of both output and processes. The blockchain infrastructure would enable transparent and immutable storage and sharing of logs. While XAI caters to both the technical understanding of the functioning of an AI system and the explainability/interpretability of its output, blockchain allows for registration of the explanatory information extrapolated by XAI. The instrument is relevant for developers to understand the functioning of their system for debugging or improvement purposes and for regulators to check compliance. Once translated into legal justifications and human discourse, it enables the rights-holders affected by automated decision-making to access argumentations and justifications of AI-derived decisions building upon AI outputs and, if the algorithmic outcome contravenes legal principles, resort to the appropriate legal remedies. Explainability rights upon affected legal subjects would not necessarily fully oblige AI providers to give up on their legitimate business interests, eg, divulge their trade secrets. Instead, access to internal documentation could be restricted to entities bound by confidentiality obligations (such as supervisory authorities and auditors).[92] Affected individuals would retain a more limited right to receive explanations of algorithmic decisions consisting in meaningful information about the logic used in AI decision-making

[91] For a deep dive into XAI see: Plamen P Angelov and others, 'Explainable Artificial Intelligence: An Analytical Review' (2021) 11 Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 1, 13 <https://wires.onlinelibrary.wiley.com/doi/full/10.1002/widm.1424> accessed 28 February 2025. The authors describe several types of XAI. At a high level, the ontology and taxonomy of Explainable Artificial Intelligence (XAI) can be summarised as follows: 1) Transparent models (eg, decision trees, k-nearest neighbours, rule-based systems) are inherently interpretable, though transparency does not always ensure comprehensibility. 2) Opaque models (eg, neural networks, random forests, support vector machines) are typically high-performing but lack interpretability due to their complexity. 3) Model-agnostic methods are flexible techniques that can be applied to any model type, as they work by analysing the relationship between inputs and outputs of a model without relying on internal structures. 4) Model-specific methods are tailored to specific types of models and exploit internal details to enhance transparency for those architectures. 5) Explanation by simplification involves approximating a complex model with a simpler one (eg, a linear model or decision tree) to generate interpretable surrogate explanations. 6) Explanation by feature relevance assess the importance of individual features by estimating their contribution to the output, often using approaches like Shapley values. 7) Visual explanations use visual tools and techniques to help users interpret how a model arrives at its decisions, particularly useful for image or spatial data. 8) Local explanations explain model behaviour in the vicinity of a specific input and help understand decisions in a focused and contextualised manner. The Four principles of XAI issued by the US National Institute of Standards and Technology in 2020 testify to the growing importance of this topic: "*Explanation: this principle states that an AI system must supply evidence, support; or reasoning for each decision made by the system. Meaningful: this principle states that the explanation provided by the AI system must be understandable by, and meaningful to, its users. As different groups of users may have different necessities and experiences, the explanation provided by the AI system must be fine-tuned to meet the various characteristics and needs of each group. Accuracy: this principle states that the explanation provided by the AI system must reflect accurately the system's processes. Knowledge limits: this principle states that AI systems must identify cases that they were not designed to operate and, therefore, their answers may not be reliable.*"

[92] Martin Ebers, 'Regulating Explainable AI in the European Union: An Overview of the Current Legal Framework(s)' [2022] Nordic Yearbook of Law and Informatics 2020 -2021: Law in the Era of Artificial Intelligence 103 <https://lawpub.se/en/artikel/4837> accessed 28 February 2025.
It must be acknowledged that practical feasibility of such systems may face obstacles such as the need for public authorities to develop their own XAI against the background of competition between XAI system providers and the providers of AI systems, which are reviewed/ inspected for compliance assessment purposes.

that are concise, easily accessible, clear and formulated in simple language, explaining the method and criteria used for the decision and the legal justifications thereof. The information that must be disclosed by the controller should not include technical details that the data subject would not be able to understand.

The AI Act further imposes strict compliance-oriented transparency requirements, outlining a multi-layered compliance framework encompassing risk management, data governance, documentation, monitoring, and cybersecurity. AI providers should put in place risk management protocols to implement robust methodologies for risk detection and mitigation throughout the life cycle of an AI system. Risk management, documentation and monitoring obligations require providers to maintain comprehensive technical documentation and post-market monitoring mechanisms. As concerns these compliance requirements, an AI-blockchain infrastructure interconnecting AI firms with the web of EU regulatory bodies[93] may play a critical role in AI compliance by recording risk assessments, transparency reports, and regulatory documentation in an immutable and secure manner.

5.2 Federated learning for privacy- and security-enhancing data sharing (Data Act and Data Governance Act)

The EU Digital Acquis encompasses a suite of legislative initiatives rooted in the 2020 European Strategy for Data, which aspires to create a unified European data market. Central to this strategy is the establishment of Common European Data Spaces — technological and governance frameworks designed to facilitate secure, privacy-preserving, transparent, and efficient data pooling and sharing among public and private actors (B2B, B2G, G2G) across strategic sectors and Member State borders. In addition to ensuring consistency with the General Data Protection Regulation (GDPR) and other applicable EU data laws, the legal framework underpinning the Data Spaces has been further articulated in two key instruments: the Data Governance Act (DGA) and the Data Act (DA).

The DGA, which entered into force in September 2023 and is applicable from December 2024, seeks to establish a coherent and structured framework for data sharing within the Union. It supports a dual model of data exchange, accommodating both commercial transactions (ie, data shared for remuneration) and data altruism (ie, voluntary data

[93] In relation to enforcement, the AI Act adopts a multi-level governance model that encompasses both national and supranational regulatory bodies. National Competent Authorities (NCAs) are tasked with overseeing compliance in respect of high-risk AI systems, carrying out supervision and, where necessary, enforcement actions at the domestic level. At the supranational tier, the AI Office — established within the European Commission — functions as a central coordinating authority to ensure harmonised implementation and enforcement across EU member states. The AI Office is also vested with exclusive competence over general-purpose AI systems and is responsible for developing governance frameworks, technical standards, and voluntary codes of conduct within the field of AI regulation.
Despite the establishment of these structures, enforcement beyond the scope of general-purpose AI remains fragmented and complex, owing to the involvement of multiple regulatory bodies with overlapping or divergent mandates. This institutional plurality presents ongoing challenges for coherent enforcement and consistent regulatory outcomes across the Union.

donation for the public interest). The regulation introduces a new category of data intermediaries tasked with overseeing data exchanges in compliance with relevant EU legal requirements.

The DGA distinguishes between publicly and privately held data and applies differentiated legal regimes accordingly. For public sector data, the regulation applies to protected categories — including personal data, intellectual property, and commercially sensitive information — and imposes stringent safeguards through mechanisms such as anonymisation, pseudonymisation, and secure access protocols.[94] Public authorities can charge fees for reuse but may waive them for scientific research or SME/start-up innovation. For private data, the DGA introduces data intermediation services, neutral entities entrusted with facilitating fair and secure data exchanges based on user consent, security, and interoperability.[95] These services shall operate under national regulatory supervision to ensure their independence and prevent conflicts of interest.

Additionally, the DGA envisages the establishment of the so-called 'data altruism organisations', which collect and share voluntarily donated data for research and policymaking, particularly in fields like healthcare, environmental protection, and mobility. These non-profit entities must be registered with the competent national authority where they are established and comply with transparency and security obligations.[96]

From a technological viewpoint, the Regulation envisages the creation of data altruism pools for data analytics and machine learning, organisational and technical arrangements to ensure the consent of rights holders, and structured exchange of data between public authorities for public policy design. For standardisation, interoperability, and exchange of national best practices and oversight of implementation, the Regulation sets up an EU-wide body of representatives tasked with providing interoperability standards, promoting the exchange of national best practices, and overseeing consistent implementation.

The EU Data Act (DA), which came into force in January 2024 and will apply from September 2025, establishes a harmonised framework for fair access and use of IoT-generated data. It introduces — inter alia — contractual schemes for B2B, B2C, and B2G data sharing, aimed at ensuring fair and non-discriminatory conditions and empowering IoT users to access, control, and share their data.[97] The Act promotes the deployment of interoperable smart contracts as enabling technologies for the automated execution of IoT-generated data-sharing agreements.[98]

While cloud infrastructures have been identified as key enablers of these data spaces, federated learning (FL) integrated within a blockchain infrastructure may offer an

[94] Artt 5-7 DGA.
[95] Chapter III DGA.
[96] Chapter V DGA.
[97] Regulation (EU) 2023/2854 of the European Parliament and of the Council on harmonised rules on fair access to and use of data [2023] 'EU Data Act' ('DA') Artt 4-6.
[98] Art 30 DA.

alternative, privacy-preserving mechanism for secure data sharing and processing that aligns with the normative and functional demands of the EU digital legislative framework, while advancing a European-wide AI model development. FL is an advanced machine learning paradigm that enables multiple entities to collaboratively train artificial intelligence (AI) models without transferring raw data to a central server. Instead, local data remains on premises while only anonymised model updates are exchanged and aggregated. This decentralised approach directly supports the privacy, security, and data minimisation obligations mandated by the DGA and the DA for the following reasons.

As mentioned, the DGA stipulates stringent safeguards for the reuse of protected public-sector data (e.g. personal, commercially sensitive, or IP-protected data), requiring techniques such as anonymisation and pseudonymisation.[99] FL meets these requirements by design, as it obviates the need to transfer raw or identifiable data. Furthermore, in data altruism schemes, where individuals or organisations voluntarily donate data, FL provides a technological means to uphold data subject consent and minimise risk, by allowing AI model training on-site and respecting the principle of data minimisation under both the DGA and GDPR.

In addition, FL may support fair and secure B2B and B2G data sharing mandated by the DA. The latter introduces a framework to ensure equitable access and use of IoT-generated data. Users can access and share their data under non-discriminatory terms, while maintaining protections for trade secrets and intellectual property.[100] FL enables collaborative use of such data across business and government actors without disclosing the underlying datasets. This makes it particularly relevant to B2B and B2G contexts, where stakeholders need to extract value from sensitive or proprietary data sources without exposing them.

Finally, FL systems can be integrated with AI-powered smart contracts that automate and enforce conditions attached to data usage — such as limiting access to certain users, geographies, or time periods — while ensuring compliance through blockchain-based audit trails. The DA encourages the use of interoperable smart contracts to automate the enforcement of data-sharing agreements.[101] It emerges that FL is not only a privacy-enhancing technology but also an enabler for regulatory compliance with key obligations under the Data Governance Act and the Data Act, including lawful data sharing, consent and contract management, and data protection by design.

6 Conclusion

The integration of artificial intelligence and blockchain technologies presents a promising technological mix capable of enhancing regulatory compliance and enforcement

[99] Art 5 DGA.
[100] Artt 4–6, 8 DA.
[101] Art 30 DA.

across sectors and jurisdictions within the framework of the EU Digital Acquis. While AI contributes efficiency, adaptability, and predictive functionality, blockchain offers verifiability, auditability, and decentralised privacy and security. When combined, these technologies have the potential to generate innovative responses to the challenges faced by both regulators and regulatees, fostering a cooperative socio-technical ecosystem grounded in mutual enhancement, trust and accountability. Such integration may support the development of technologically enabled cross-regulatory, cross-sectoral, and cross-border enforcement mechanisms. Nonetheless, the realisation of these benefits is contingent upon addressing several limitations and normative gaps, including the current absence of legal frameworks capable of operationalising the proposed socio-technical cooperative model. Future research could focus on developing harmonised regulatory frameworks that accommodate the consolidation of substantial and procedural rules for legal-by-design EU cross-regulatory compliance and enforcement mechanisms. Cross-disciplinary collaboration between legal experts, technologists, philosophers, policymakers and other operators is essential to refine governance models that integrate sustainable technological solutions into regulatory best practices. The synthesis of AI and blockchain has the potential to redefine regulatory compliance and enforcement cooperation through a more transparent and secure digital ecosystem. However, its success will depend on the ability of stakeholders to balance innovation with legal and ethical considerations to steer technological advancements towards societal and regulatory needs.

*Cesare Galli – Mariangela Bogni**

GENERAL SECTION

ARTIFICIAL INTELLIGENCE, NEW RESEARCH DYNAMICS AND PATENTS

Abstract

The rise of AI and its increasing use in achieving inventions has raised concerns about the effectiveness of the requirements for patent protection, which were designed prior to this technological revolution. Proposals in this regard, from the abolition of patents to the adoption of an inventive machine standard, however, circumvent the key issue in assessing patentability, which is whether or not the skilled person would have achieved the invention in an obvious way by using the available toolkit, which may include AI algorithms if they are publicly available. The fear of excessive patent monopoly resulting from the use of AI is also a false problem, since greater ease in attaining inventions will lead to more problems being solved in alternative ways, new ones being posed, and strong competition among innovators. What critics of patents forget is the effect of disclosure achieved through patenting: patent databases (normally freely accessible online) are nowadays the world's largest and most up-to-date source of technical information. The importance of this disclosure is increased precisely by the advent of AI, which needs wide availability of data to operate effectively. Thus, more than ever, patents contribute decisively to scientific and technological progress and also to its democratisation. The analysis will show that the growing use of AI in research does not require changes to existing patent law or challenge the fundamental rationale for patent protection. On the contrary, AI enhances innovation potential, reinforcing the importance of the patent system—especially its role in promoting competition and knowledge disclosure.

JEL CLASSIFICATION: K110, 031, 034

SUMMARY

* Cesare Galli, Università degli Studi di Parma; Mariangela Bogni, Università degli Studi di Parma.

DOI 10.13135/2785-7867/12274

1 Introduction

The patent for invention is deemed[1] to be the most important one among intellectual property rights, as it is fundamental in ensuring protection for investors in research leading to technical progress.

The fundamental requirement for the patentability of an invention is the so-called "inventive step", which pursuant to the US legal system can be found "*if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention* pertains"[2], while in the European Union one, it is necessary that it represents an "*original*" solution to a technical problem, ie, - according to the approach (determined by comparing the invention for which protection is claimed with the so-called *closest prior art*), which is not obvious to the person having ordinary skill in the art to which the claimed invention pertains, to the state of the art: and, more precisely, according to the criterion of the *problem and solution approach* and the so-called *could-would* rule, which is not obvious, in the absence of knowledge and suggestions that would have led (and not that *could have led*, being recognisable only *ex post* facto as suggestions) the inventor to consider "*obvious to try, with a reasonable expectation of success*" the invention then patented[3].

The results arrived at by applying these two standards are substantially homogeneous and most of the most important patents (for which protection is sought worldwide) are granted by both the USPTO, the EPO and the JPO with the same or very similar claims[4].

However, it is true (or will be true at some point in the ongoing technological evolution) that the use of *prior art* investigation tools such as those of Artificial Intelligence will more easily lead to the identification of information inherent in the solution of the technical problem and probably, by virtue of the capacity of these systems to establish correlations between data, even to point out in the known art suggestions that the human being without the aid of the machine would not have grasped (and therefore that, for the human being, *could* have *led to* the *invention* - *could* -, but would not have '*led to the*

[1] William M Landes and Richard A Posner, 'An Economic Analysis of Copyright Law' (1989) 18(2) Journal of Legal Studies 325, 'For a new work to be created the expected return – typically, and we shall assume exclusively, from the sale of copies – must exceed the expected costs'; European Commission, 'Making the Most of the EU's Innovative Potential: An Intellectual Property Action Plan to Support the EU's Recovery and Resilience' COM(2020) 760 final, 25 November 2020.

[2] 35 United States Code 103; the corresponding norm in the European Patent Convention system can be found under art 56 of the European Patent Convention.

[3] Hansjörg Knesch, 'Assessing Inventive Step in Examination and Opposition Proceedings in the EPO' (1994) 3 EPI Information 95; Pèter Szabo, 'The Problem and Solution Approach in the European Patent Office' (1995) 457 International Review of Intellectual Property and Competition Law 293; Mario Franzosi, 'Non ovvio' in *Studi di diritto industriale in onore di Adriano Vanzetti* (Milano, 2004) 474; Cesare Galli, 'Per un approccio realistico al diritto dei brevetti' (2010) 136 Il Diritto Industriale 133; Cesare Galli and Mariangela Bogni, 'Il requisito di brevettabilità dell'attività inventiva' in Galli and Gambino (eds), '*Codice commentato della Proprietà Industriale e Intellettuale*' (UTET Giuridica 2011) 578.

[4] Antoine Dechezleprêtre, Yann Ménière and Myra Mohnen, 'International Patent Families: From Application Strategies to Statistical Indicators' (2017) 111 Scientometrics 793.

invention' - *would* -, it being only in this second case that the inventive activity is lacking) and that, conversely, with the use of AI will become available (or rather recognisable as such) already *ex ante*. On the other hand, it is likely that, speculatively, the offices in charge of examining patent applications will equip themselves with AI tools to carry out their evaluations, thus in turn being able to take these suggestions into account.

For the purpose of this analysis, the definition of "AI system" given by the "AI Act", will be taken into account: therefore, an AI system will be deemed to a "*machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*"[5].

It appears that there are already examples of patented inventions made autonomously by artificial intelligence (it being understood that it will always be a human being who poses the technical problem to be solved).

The question of whether artificial intelligence systems can be recognised as inventors under patent law has been tested globally through a series of applications involving the AI system DABUS (Device for the Autonomous Bootstrapping of Unified Sentience), developed by Dr Stephen Thaler. Patent applications were filed in multiple jurisdictions listing DABUS as the sole inventor, challenging existing legal definitions of inventorship.

In the United States, the United Kingdom, and the European Union, courts and patent offices uniformly rejected the applications on the grounds that inventorship under current laws requires a natural person. Notably, the U.S. Court of Appeals for the Federal Circuit, the UK Supreme Court[6], and the European Patent Office (EPO)[7] all concluded that AI systems do not meet the statutory criteria for inventors.

In Australia, an initial 2021 Federal Court ruling accepted the premise that an AI could be an inventor; however, this was subsequently overturned by the Federal Court in 2022[8], reaffirming the necessity of human inventorship.

By contrast, South Africa granted a patent in 2021 naming DABUS as the inventor—the first known instance of such recognition. However, the decision was made without substantive examination and does not represent a binding interpretation of patent law[9].

More realistically, however, one must imagine that AI assists humans in realising an extensive part of the process leading to the invention. An emblematic example is that of the team *of* a pharmaceutical company, which, wanting to make a molecule that would

[5] See Article 3 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AI Act).
[6] *Thaler v Comptroller-General of Patents, Designs and Trade Marks* [2023] UKSC 49 (20 December 2023).
[7] EPO Board of Appeal, 21 December 2021, J 0008/20, ECLI:EP:BA:2021:J000820.20211221.
[8] *Commissioner of Patents v Thaler [2022] HCATrans* 199 (High Court of Australia, 11 November 2022).
[9] More extensively on this topic, Desmond Oriakhogba'Dabus Gains Territory in South Africa and Australia: Revisiting the AI-Inventorship Question' (2021) 9 South African Journal of Intellectual Property Law 87, 108.

target exactly one protein linked to fibrosis, used artificial intelligence (the proprietary GENTRL system), which 'designed' 30,000 molecules and automatically discarded those '*bearing structural alert and reactive groups*', reducing the viable hypotheses to a much smaller number, subsequently profiled (again by the system). Of the remaining molecules, 40 were chosen '*randomly*', with a subsequent synthesis of 6, all of which were tested, with the result that 4 of them proved active '*in* biochemical assays', 2 were validated in 'cell-based assays' and one was tested on mice, demonstrating '*favourable pharmacokinetics*'. The process took a total of 46 days, demonstrating how the use of AI proves to be a tool that can make researchers' work much faster[10]. In another well-known case, artificial intelligence is said to have 'proposed' the solution of crossed bristles for optimal toothbrush functionality, following Oral B's request to produce a new generation of toothbrushes: a device based on an artificial neural network, also the subject of a patent[11] and called the 'Creativity Machine', realised, after being fed with information about the characteristics and performance of existing toothbrushes, 2,000 possible *designs*, many of them with crossed bristles[12]. In both cases, however, it was humans who posed the problem, provided the machine with the data and made the decisive selection on the assumptions provided.

More generally, it can be hypothesised that today there are devices capable of assisting humans in achieving solutions to technical problems, analysing (in an insightful manner) the prior art administered - and possibly, filtered and calibrated - or autonomously researched by the machine, for example, through *databases* such as the EPO database, highlighting the solutions relevant to the problem, and, upstream, identifying, testing and discarding solutions.

The new potential of AI has already prompted action by lawmakers[13], who however seem to sense its risks more than its opportunities. Faced with this new reality, intellectual property scholars[14] too have begun to wonder whether the use of artificial

[10] See Bogdan A Zagribelnyy and others, 'Deep Learning Machine Enables Rapid Identification of Potent DDR1 Kinase Inhibitors' (2019) 37(9) Nature Biotechnology 1038.

[11] Patents No. US 5,659,666 and No. US 7,454,388, both filed in the name of Dr Stephen Thaler, founder of Imagination Engines, Inc, dated 13 October 1994 and 8 May 2006, respectively, available at <http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=5659666.PN.&OS=PN/5659666&RS=PN/5659666> and <http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=4&f=G&l=50&co1=AND&d=PTXT&s1=stephen.INNM.&s2=thaler.INNM.&OS=IN/stephen+AND+IN/thaler&RS=IN/stephen+AND+IN/thaler> accessed 20 June 2025.

[12] See Robert Plotkin, *The Genie in the Machine: How Computer-automated Inventing is Revolutionising Law and Business* (Stanford University Press 2009) 51, who explains that this device was able to 'not only recognise existing patterns but create new ones', making use of two special neural networks that the creator of the system, Dr Thaler, called 'the Imagination Engine' and 'the Perceptron'.

[13] Among the lawmakers that dealt with AI-related issue, *ex multis* the EU, Italy and the US can be mentioned.

[14] Noam Shemtov and Garry Gabinson, 'The Inventive Step Requirement and the Rise of the AI Machines' in FM Abbott (ed), *Research Handbook on Intellectual Property and Artificial Intelligence* (Edward Elgar 2022); Marga Schellekens, 'Artificial Intelligence and the Re-Imagination of Inventive Step' (2022) 13 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 89; Olga Gurgula, 'AI-Assisted Inventions in the Field of Drug Discovery: Readjusting the Inventive Step Analysis' (2020) 2(8) International Journal of Social Science and Public Policy 7.

intelligence will not make obvious (and easily attainable) what would not be obvious to the human being who does not use such a tool, and whether this does not impose a revision of the patentability requirements for inventions, and in particular for inventive activity, in a quantitative or qualitative sense, in order to avoid an exponential increase in exclusivity and, therefore, an excessive obstacle to competition.

These critical issues run the risk of being instrumentalised by those who have already for years taken an attitude of ideological criticism of intellectual property and patents, arguing that copyright and patents are a useless evil because they do not generate more innovation, but only hinder the diffusion of new ideas[15]. Even if, as we shall see, the analysis of these radical critics appears flawed by premises that are not in line with the legal rules governing intellectual property, starting with the identification of the content of exclusive rights and the mechanisms for legal review of their validity and infringement, one cannot underestimate the risk of patents being among the victims of the debate on Artificial Intelligence and its consequences in terms of legal policy.

It is therefore necessary to answer the questions on the compatibility of the advent of artificial intelligence with the traditional protection of inventions by means of patents granting exclusive rights to their author and then assess whether there are corrections to be made to the current system or whether new forms of protection should be considered or even the abolition of this right.

In this perspective, three main issues deserve to be addressed: firstly, it is necessary to ask whether the standards of access to patent protection, based on the criteria we mentioned at the beginning, are still able to function in a context in which the dynamics of research increasingly involve the use of artificial intelligence; then it must be ascertained whether artificial intelligence applied to inventive research does not adversely affect the balance between competition and exclusivity that underlies all intellectual property law; finally, it is necessary to ask what role can be played by the alternatives to patents that are already used today to protect technological innovations, and in particular *trade secrets*, and whether and to what extent they should be encouraged in the face of the ever-increasing use of artificial intelligence in the research from which innovations arise.

Once these issues have been addressed and resolved, it will be possible to reach conclusions and indicate possible corrections to the current system that are desirable from the perspective of the free market economy.

2 The first regulatory interventions: from the European Union's AI Act to the Italian government's draft bill

In order to properly contextualise the subject of this research, it is first necessary to

[15] Michele Boldrin and David K Levine, *Against Intellectual Monopoly* (Cambridge University Press 2008).

give an account of the regulatory framework that is taking shape in Europe regarding AI as a whole and its guiding forces.

Artificial Intelligence (AI) is a broad field of computer science that encompasses technologies designed to perform tasks typically requiring human intelligence, such as reasoning, learning, problem-solving, and decision-making. AI systems are often categorised into narrow AI and general AI. Narrow AI refers to systems designed for specific tasks, such as facial recognition or legal document review, whereas general AI aims to replicate the full range of human cognitive abilities, a capability not yet achieved.
Generative AIs[16] (often referred to as GenAIs), on the other hand, is a subset of AI, referring to models specifically designed to create new content, such as text, images, or music, based on the data they have been trained on. GenAIs, like OpenAI's ChatGPT or DALL·E, have gained particular attention due to their ability to produce human-like outputs, blurring the line between machine and human creativity. Unlike narrow AI, which is task-specific, GenAIs exhibit a higher degree of autonomy in generating novel material, often exhibiting behaviors that appear to be creative, adaptive, and innovative.

As a matter of fact, the attitude towards artificial intelligence algorithms nowadays is two-faced. On one hand, generative AI algorithms, such as the above-mentioned very popular ChatGPT, are currently widely used; on the other hand, there are loud calls warning of the alleged risks they pose to humanity's future, as though these algorithms could actually surpass human intelligence. This perspective disregards the fact that these algorithms are all based on the logical-deductive model of the "Turing machine[17]," which underpins electronic computers, while "the human brain performs functions that cannot be defined according to the Turing machine model," and "the number of different semantic structures that a human brain can generate is virtually infinite, 10 to the power of 700"[18]. As a result, the brain will never be replaced by a machine, which can only assist in performing tasks more quickly and efficiently, particularly innovation, by supporting humans in various parts of the process leading to discoveries, even though the human is the one defining the problem, providing the machine with data, and structuring it so that the machine can "learn" from it and make the critical selection among the hypotheses provided.

For the sake of clarity, it must be pointed out that Artificial Intelligence systems often rely on machine learning techniques to improve their performance on tasks over time. Two fundamental paradigms within machine learning are supervised learning and unsupervised learning, which differ primarily in how the algorithm is trained and the type

[16] As stated in Recital 99 of the AI Act: "generative AI models are a typical example for a general-purpose AI model, given that they allow for flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of distinctive tasks".
[17] A Turing machine is an idealised model of a central processing unit (CPU) that controls all data manipulation done by a computer, with the canonical machine using sequential memory to store data. Typically, the sequential memory is represented as a tape of infinite length on which the machine can perform read and write operations.
[18] Bruno Ruffilli, 'Mario Rasetti: "Non costruiremo mai una macchina complessa come il cervello umano' *La Repubblica* (Roma, 5 September 2023).

of data it processes.

Supervised learning involves training an AI model on a labelled dataset, where the input data is paired with the correct output: the model learns to recognise patterns that associate inputs with the correct labels and can later apply this knowledge to classify new, unlabelled data. This method is commonly used for tasks such as classification (eg: e-mail filtering or image classification) and prediction of patterns[19].

Unsupervised learning, by contrast, involves training a model on data without labeled outputs. The algorithm seeks to identify hidden patterns, structures, or groupings in the data: common applications include clustering, dimensionality reduction, and anomaly detection.

The choice between supervised and unsupervised learning has significant implications for how AI systems operate and the transparency of their decision-making processes—factors that are increasingly relevant in legal and regulatory evaluations of AI technologies.

However, paradoxically, the most basic (and often most dangerous) applications of AI are spreading rapidly, while calls for stringent regulations are made often prematurely, in so far as they could hinder its use precisely where it is most needed, namely, to accelerate innovation and increase the competitiveness of businesses, which can become drivers of economic development.

An attempt to strike a balance between these different thrusts was made by the European Union with the so-called AI Act, ie, Regulation (EU) 2024/1689[20], which took a quite prudent approach to the problem, although not without criticism for the extreme detail and complexity of the adopted framework, which only when put to the test of their actual implementation will be able to prove their effectiveness and manageability. This Regulation opted to regulate only high-risk AI systems (specifically identified in an annex to the regulation), systems that interact with individuals, and AI models for general purposes. It provides specific provisions for these systems to safeguard fundamental rights and foresees a gradual implementation of these provisions until 2026 (which also paves the way for possible corrective interventions), leaving the development of AI in other areas free and market-driven.

In contrast, an example of the ambivalence (and substantial misunderstanding) toward AI is the recent draft law on AI (Bill No. 1146/2024) presented by the Italian government, which is currently being discussed in the Senate[21]. Even though this bill does not contain

[19] Julianna Delua, 'Supervised vs Unsupervised Learning: What's the Difference?' (*IBM*, 13 June 2023), <https://www.ibm.com/blog/supervised-vs-unsupervised-learning/> accessed 15 May 2025.

[20] Per una più analitica trattazione dell'argomento, si rinvia alla lettura di Giuseppe Cassano and Enzo M Tripodi, *Il Regolamento Europeo sull'Intelligenza Artificiale - Commento al Reg. UE n. 1689/2024* (Maggioli Editore 2024).

[21] Cesare Galli, 'Il disegno di legge del Governo sull'intelligenza artificiale: un testo inopportuno migliorabile, in problematico rapporto dialettico con il Regolamento comunitario'(*Sistema Proprietà Intellettuale*, 3 December 2024) <https://www.sistemaproprietaintellettuale.it/53-tendenze-e-sviluppi/32328-il-disegno-di-legge-del-governo-sull-intelligenza-artificiale-un-testo-inopportuno-migliorabile-in-problematico-rapporto-dialettico-con-il-regolamento-comunitario.html> accessed 3 July 2025.

rules that could significantly affect Italian patent law directly, it is still important to consider its possible indirect effects, since the provision it may entail if approved could affect the course of innovation and the development of new technologies, which is the factual premise of the entire patent system. The text aims to promote the use of AI, provided that it is done in conditions of safety and transparency. However, this promotion is reduced to vague commitments or the stating of equally vague goals (Article 5)[22], while the constraints—such as those requiring AI systems and models to be developed "*based on data and processes whose correctness, reliability, safety, quality, appropriateness, and transparency must be ensured and monitored*" (Article 3, Paragraph 2) and ensuring "*cybersecurity throughout the entire lifecycle of AI systems and models, based on a proportional, risk-based approach, and the adoption of specific security controls to ensure resilience against attempts to alter their use, behaviour, performance, or security settings*" (Article 3, Paragraph 5) – are largely discretionary in their application and general in nature, imposing broad and indiscriminate requirements (except for the reference to "proportionality," which however is not clearly defined). These provisions may serve as a deterrent to the development of AI research and applications in Italy.

Additionally, the definitions given in the Italian bill for AI systems and models differ from those set out in the Regulation and do not align with Directive (CEE) 1991/250, as they define AI systems as "automated systems" rather than as computer programmes, as they are actually understood in the Regulation. The same issue arises with AI models, which the Regulation considers as components of systems ("Although AI models are essential components of AI systems, they do not constitute AI systems in themselves") and thus regulates them only when they are intended for general purposes. In this case, the need for guarantees for "AI system providers integrating general-purpose AI models" justifies regulatory intervention, which becomes more extensive for models that present systemic risks due to their high impact potential, particularly concerning the cumulative computational power used for training (Articles 51-55 of the AI Act).

This foundational error is further compounded by the Italian government's choice to use

[22] Article 5(d) of the Italian DDL AI introduces a preference for AI systems and services that ensure the localisation and processing of strategic data within Italian territory, with disaster recovery and business continuity solutions also hosted domestically. While the objective is to enhance national digital sovereignty, bolster security measures, and ensure adherence to transparency and ethical AI standards, this provision may potentially conflict with the EU's fundamental principle of the freedom to provide services (Article 56 TFEU).
In accordance with EU law, service providers established within one Member State must be permitted to offer their services across the Union without the imposition of restrictions that are not justified. A national rule that systematically favours domestic infrastructure – such as requiring or preferring data centres within national borders – can amount to an indirect restriction on this freedom, particularly if it disadvantages providers from other Member States who may offer compliant and secure services hosted elsewhere in the EU.
While such restrictions may be deemed justifiable on grounds of public security or the protection of critical infrastructure, it is imperative that they are subject to rigorous proportionality and non-discrimination tests. It is imperative that the measure be commensurate with its stated objective, indispensable, and that it constitutes the least intrusive alternative. The Italian provision, albeit framed as a preference rather than an explicit requirement, may nevertheless be subject to scrutiny under EU law, particularly if it results in systematic exclusion or disincentivisation of non-domestic service providers.

the sectors in which AI systems are applied as the sole criterion for applying the proportionality principle outlined in Article 3 of the bill, which governs the development of AI systems and models. This approach is inadequate and contrasts with the Regulation, as it does not consider the risk levels that these systems pose, nor whether they are intended to interact with individuals, nor whether they have general-purpose objectives (and in some cases, systemic risks). This approach prevents the national legal framework from aligning interpretively with the European framework.

Furthermore, the modification proposed in Article 24 of the bill to the Copyright Law (Law No. 633/1941), which introduces the specification that the law protects "human" works of the mind, seems unnecessary, as this has always been understood. The proposal to extend this to include works "*created with the aid of AI tools, provided they are the result of the intellectual work of the author*" is also problematic; it should also be noted that Article 25 of the Bill, even when considered in light of all relevant criminal and constitutional principles, remains highly complex – particularly in determining what should be understood as a genuine work versus a modified one. The issue is not whether there is intellectual work, but rather determining what type of creativity should be considered relevant. This issue is beyond the scope of national legislators and should be addressed at the EU level, as the concept of "work" protected by copyright is an autonomous EU law concept that must be interpreted and applied uniformly[23].

Similarly, the proposed changes to Article 70-septies of the Italian Copyright Law in the bill, allowing reproduction and extraction of works or other materials through AI models, including generative models, fail to align with EU regulations, particularly the Digital Single Market Directive, which sets limits on AI generative uses that should be respected.

Once the bill is approved, a more thorough evaluation will be possible. However, it is already evident that this regulatory intervention demonstrates a lack of understanding that, in the face of complex phenomena like AI, national legal systems are competing with one another. The laws adopted could isolate a country from critical development opportunities, relegating it to a marginal position. The introduction of limits should be justifiable only for the protection of essential legal rights, based on a balanced consideration of the subject's complexities, economic, technical, and humanistic implications, and the need for caution in recognizing the market's ability to better manage these complexities for the benefit of all.

[23] As re-affirmed with special clarity by Case C-683/17 *Cofemel* ECLI:EU:C:2019:721, on which see Cesare Galli, 'La tutela "Europea" di diritto d'autore per le opere dell'Industrial design e la necessità di un approccio realistico' (2020) 1 Rivista di Diritto Industriale II 42, 51. On the impact of AI on copyright protection see Edoardo C Raffiotta, 'La tutela delle opere generate dall'intelligenza artificiale: il principio antropocentrico tra prospettive passate e future' (2024) 6 Il Diritto Industriale 527.

3 The current debate on the patent system in the face of the challenges of artificial intelligence

The debate on the future of patents in the age of Artificial Intelligence has primarily focused on the figure of the "person skilled in the art", a central concept in assessing the inventive step (or non-obviousness) of an invention. This standard is applied from the perspective of a hypothetical expert in the relevant technical field, and it is through this lens that the obviousness of an invention is evaluated.

A key issue that has emerged is whether this hypothetical expert should be assumed to use AI tools in their problem-solving activities. This includes considering both AI's ability to combine and analyse large amounts of information and the potential need to broaden the knowledge base attributed to the skilled person—particularly in relation to adjacent or neighbouring fields of technology.

This question becomes even more complex when dealing with technical problems that cut across multiple disciplines. For example, consider a mechanical issue affecting machines in two unrelated fields, such as industrial robots and medical imaging devices. Although the machines serve entirely different purposes, they may share a common problem, such as heat dissipation in high-speed rotating parts. In such a case, it may not be sufficient to limit the skilled person's knowledge to just one field. Instead, the relevant inquiry is: what prior art or technical knowledge would the skilled person realistically have considered when faced with this particular problem?

Rather than rigidly expanding the scope of the skilled person's knowledge, the more pertinent question is which technical field is relevant to the specific problem at hand, and whether the skilled person—possibly aided by AI—would have looked beyond their core discipline to find a solution.

The suggestion at issue here is made based on American *case law*, which, for the purposes of judging inventive step, also takes into account among the variables the '*sophistication of technology*' possessed by the expert in the field[24] (of course: not the person who actually made the invention, who may have inferior or superior skills and knowledge[25]). Looking forward, therefore, in sectors where the use of artificial intelligence proves to be widespread, taking this factor into account in the construction of the branch expert's knowledge and skills would be justified, since, in a realistic approach to the assessment of inventive step, one must put oneself in the position in

[24] See Peter S Menell and others, 'Patent Case Management Judicial Guide' (2009) UC Berkeley Public Law Research Paper No. 1328659 11, 47, where it is explained that 'In determining the level of ordinary skill in the art, courts look to the inventor's educational level, the nature of the field's typical problems, the skill required to grapple with the prior solutions to the field's problems, the pace of innovation in the field, the sophistication of technology and the educational level of people working in the field' and *Envtl. Designs, Ltd. v Union Oil Co.*, 713 F.2d 693, 696 (Fed. Circ. 1983. In the same vein, see also GPAC Inc., 57 F.3d 1573, 1579 (Fed. Cir. 1995).

[25] See Catherine Seville, *EU Intellectual Property Law And Policy* (Edward Elgar Pub 2016) 147; Ana Ramalho, 'Patentability Of Ai Generated Invention - Is A Reform Of The Patent System Needed?' [2018] SSNR <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3168703> accessed 3 July 2025.

which this subject examines the *prior art*, also in relation to the tools at his disposal[26].

What is not acceptable, however, is the idea of a 'double standard', depending on whether the patent applicant claims to have used artificial intelligence in the achievement of the invention. Such an approach, in fact, would contradict the need, common to all legislations, to objectivise as much as possible the judgement of inventive activity, reconstructing the conditions in which an expert in the field with all the known art would have found himself when tackling the technical problem subject of the patent. Even in its practical consequences, without wishing to consider the hypothesis that one is not telling the truth in this regard, to benefit from the 'human' standard, such a dichotomy would end up favouring those companies that are less efficient and do not invest in equipping themselves with cutting-edge research tools[27].

4 Standards for access to patent protection and artificial intelligence

It must therefore be determined whether it is possible to take the use of Artificial Intelligence into account when judging inventive step without abandoning traditional standards of evaluation. In favour of this possibility is the circumstance that these standards are based on a realistic approach to the dynamics of research, which aims to concretely identify the knowledge and tools that the expert in the field has at his or her disposal.

In this respect, it must therefore first be considered that the term 'AI' can refer to instruments that are very different from each other in terms of capability and performance (eg: traditional AI and new generation generative AI); however, the key characteristic of all AI systems is their capability to infer. This capability to infer refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data. The techniques that enable inference while building an AI system include machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to

[26] See also Ana Ramalho (n 25), ix, according to which "if the use of AI is not a normal means of experimentation in the relevant art, a patent can be granted if the invention is not obvious for a person skilled in the art without the use of AI (even if AI was used by the inventor in question). Conversely, if the use of AI is a normal means of experimentation in the relevant art, the skills of the person skilled in the art improve and AI use is taken into account - which means that a patent can be granted if the invention is not obvious for a person skilled in the art who uses the AI (even if AI was not used by the inventor in question)'. In a similar vein, but with considerations not specifically referring to AI, see also Brenda M Simons, 'The Implications of Technological Advancement for Obviousness' (2013) 19 Michigan Telecommunications and Technology Law Review 101.

[27] On this point, see Ryan Abbott, 'Everything Is Obvious' (2018) 66 UCLA Law Review 2, republished in *IP Watch* (2019) n 19 referring to American authors discussing new criteria for inventive step and non-obviousness, citing Ana Ramalho (n 25), ix-x, who even considers it advisable 'to consider adding a 'made by AI' factor as an indication of obviousness'. This is clearly contradictory to the logic of the patent system, which - as will be discussed later in the text - seeks instead to objectify the judgement on inventive activity, rather than referring to how the inventor subjectively arrived at the patented solution.

be solved. The capacity of an AI system to infer transcends basic data processing by enabling learning, reasoning or modelling[28].

Therefore, starting from this common ground, a sort of standard of the field in which the invention is located would have to be identified: a patentable invention would exist where the result achieved would not have been obvious by using standard instrumentation, even if it would have been obvious by using non-standard instrumentation.

Possession of this non-standard equipment configures a situation not very different from that which arises (and which traditional inventive step standards already allow to be successfully addressed) when the inventor has non-public knowledge that makes it obvious to him to do what is not obvious to the person skilled in the art. In fact, according to these standards, the question is not what the author of the invention whose patentability is at issue could have done - with his knowledge and skills - but what the state of the art would suggest a person with the normal capabilities for a person skilled in the art in his field would do. In other words, neither the inventor's gap in relation to these standards nor his concrete skills are relevant.

Although the inventor subjectively engaged in an inventive effort, the resulting creation does not qualify as an invention in the objective sense, as it would have been obvious to a person skilled in the art who did not face the same knowledge gap. Conversely, if the inventor possessed exceptional skills or knowledge that made the invention appear obvious to them, such attributes cannot disqualify the invention from patentability if it would not have been obvious to the hypothetical person skilled in the art, who is presumed to have only ordinary skill and knowledge.

This "*plus*" may consist of a secret invention, but also of an artificial intelligence algorithm, unless the 'instrumentation' used was not in the public domain, because any exclusive rights over it did not exist or had expired, or because, although covered by a patent still in force, the relevant technology had been made available by its owner to anyone interested in licensing it, or purchasing the device that uses it, or availing themselves of its services, not provided under exclusivity, at least in the sector in which the invention is located.

Even more crucial than the algorithm itself, for the purposes of machine learning and, consequently, the use of Artificial Intelligence in innovation, is the structuring of the data on which AI is trained to study and generate outputs. It is particularly in this context that the identification of a standard becomes both problematic and significant—especially when multiple alternatives were available and the decisions made were not self-evident. For instance, if an AI system is designed to detect fraudulent financial transactions, the choice to include certain behavioural data (such as time of transaction, device used, or spending patterns) over other available data (like biometric verification or user browsing history) reflects non-obvious human judgment. This highlights the crucial role of the

[28] See Recital 12 of the AI Act.

'human factor' in shaping the innovation, as the outcome of the machine learning process is highly dependent on such discretionary decisions.

In this regard, it is important to emphasise that the mere fact that the individual data used to train an AI system are part of the state of the art does not necessarily mean that the outputs generated by the AI—namely, the 'output data' or insights derived from processing such data—are themselves part of the state of the art. This holds true even when the input data are standardised or publicly available, such as when they consist of all published patent applications and granted patents in a particular technological field accessible through official databases, and no subjective or selective choices have been made in assembling them.

This principle applies *a fortiori* when the data supplied to the AI are non-standard. As has been recognised in trade secret law, a party may hold exclusive rights over data that, "as a whole and in the precise configuration and combination of their elements," are not generally known, even if the individual data points—considered in isolation or arranged differently—are publicly accessible. This protection extends even further when the data have been processed or reconfigured by an artificial intelligence system, particularly if the AI itself is proprietary or trained under conditions of confidentiality.

Accordingly, the additional value or insight generated by such data processing is not considered part of the state of the art and cannot be taken into account in assessing the inventive step. This is analogous to the treatment of secret prior art: just as a confidential invention that would render a subsequent invention obvious is excluded from the state of the art, so too are confidential data-derived outputs that were not publicly accessible at the relevant time. What is certain, however, is that, as seen in the cases of the development of molecules for the treatment of fibrosis or the toothbrush, the AI can provide the suggestion that leads to the invention together with numerous others, a circumstance that cannot be disregarded from the point of view of the non-evidence of the invention, at least in the face of a selection made by the inventor (upstream or downstream of the AI's intervention), which does not constitute *routine* activity.

In other words, it seems clear that the correct application of the inventive step tests, especially if they are framed (as they must be) in the context of the balance between competition and exclusivity that underpins the intellectual property law as a whole, makes it possible to address and solve the problems posed by artificial intelligence through a case-by-case verification of what can be considered *standard* and what cannot be, what is actually accessible to the public and what is not. Under this latter profile, the teaching of the EPO *case law* on the distinction between *searchable* and non-searchable disclosures[29] is therefore also applicable to the problem we are considering here, which

[29] In the case law of the EPO *Board of Appeal* this was made clear, for example, in its decision in case T1553/06 [EPO Board of Appeal, 18 November 2008], according to which 'the mere theorical possibility of having access to a means of disclosure did not make it become available to the public', since 'what is required, rather, is a practical possibility of having access': ie, the *Board of Appeal* of the EPO has precisely ruled that the mere presence, in the abstract, of a

precisely poses the problem of *concrete* and not merely *theoretical* accessibility for a *quid* to be considered disclosed.

5 Patents created with the help of artificial intelligence and competition

Among other things, this also answers the objections of those who are concerned about the possible proliferation of patents as a result of easier access to inventions.

To put the question in these terms is to think that the problems to be solved and inventions are a kind of 'closed number', whereas it is likely that the use of artificial intelligence will increase the problems solved (and lead to the formulation of new problems) and increase the solutions, more efficient or even just alternatives, with an overall improvement. Firstly, more inventions mean more progress and thus also more opportunities to create new markets and thus new competition. Secondly, it should not be forgotten that if the possibilities of inventing grow, so does the possibility of finding *alternative* solutions to each technical problem, and thus competition *between* innovators, which in any case benefits the end users[30].

Above all, critics of patent systems seem to underestimate the scope of the *disclosure* that is achieved through patenting, since it is prescribed by the TRIPs Agreement itself (art 29) that "*Members shall require that an applicant for a patent shall disclose the invention in a manner sufficiently clear and complete for the invention to be carried out by a person skilled in the art and may require the applicant to indicate the best mode for carrying out the invention known to the inventor at the filing date or, where priority is claimed, at the priority date of the* application"[31]. The patent rules are in fact inspired by the need to ensure that "*the invention, even if patented, enters as soon as possible into the pool of technical and scientific data accessible to all*"[32] and thus form the basis for further innovation: patent databases (nowadays normally freely

document among those theoretically reachable (eg, because it is present on the Internet) is not relevant for the purpose of identifying the state of the art, if the same cannot, in practice, be found by the expert in the field (again, by way of example because the title or the other elements on which a normal search is based do not contain any reference to the field of the invention or the problem it addressed), because in such a case it cannot *really* be considered to have been brought to the knowledge of an indeterminate number of persons, as is required for purposes of disclosure.

[30] On the growing importance of 'between-patent' competition, especially in cutting-edge sectors, see Tomas Philipson and Carolanne Dai, 'Between- vs. Within-Patent Competition' (2003) 26 (3) Regulation 42, 48, which analyses the pharmaceutical market in particular, concluding that 'between-patent competition, most of which occurs while a drug is under patent, affects the returns to innovators at least as much as within-patent competition, which cannot occur until a drug is off patent'.

[31] *Agreement on Trade-Related Aspects of Intellectual Property Rights*, adopted in Marrakech in 1994 at the same time as the establishment of the *World Trade Organisation*, and which contains an essential regulation of the scope of protection and of the prerequisites for the protection of distinctive signs, patents and copyrights, as well as procedural remedies against their violation. With this agreement, the bloc of economically more advanced countries, led by the United States, had made the liberalisation of trade with the (then) less developed countries conditional upon their compliance with certain standards of protection of intellectual property rights, the most important of which were (and, to a large extent, still are) owned by subjects belonging to the first bloc of countries.

[32] Piergaetano Marchetti 'Commento all'art. 1 r.d. 29 giugno 1939 (revisione della legislazione nazionale in materia di brevetti per invenzioni industriali in applicazione della delega di cui alla legge 26 maggio 1978, n. 260)' (1981) Le Nuove Leggi Civili Commentate 677.

accessible *online*) are today the largest and most up-to-date source of technical information in the world.

Today, the importance of this *disclosure* is further increased by the advent of artificial intelligence, which, being founded on the use of algorithms capable of carrying out highly advanced statistical analyses on very significant quantities of data[33], finds in the great availability of data the possibility of operating effectively, identifying classification schemes and parameters, which, to a large extent, elude human beings (in this regard, we speak of '*deep learning*'). This allows it to determine the correct answer to the problems submitted to it and to identify new ones, thus contributing decisively to scientific and technological progress and also to its democratisation, given the public accessibility of the information contained in published patent applications and granted patents.

6 Patents vs trade secrets

The absence of patent protection would instead encourage companies to resort more extensively to secrecy protection for technological innovations, whereas today they are deterred, when these innovations are patentable, by the risk of others independently obtaining them and patenting them, because this not only makes them no longer protectable as trade secrets, but can even preclude their continued use even by those who had already achieved further use, which is only permitted within the limits of the so-called *prior use defence*, which is not recognised in all legal systems and is in any case limited. It is precisely the increased ability to innovate resulting from the use of Artificial Intelligence in research that will make it riskier to resort to the secretive exploitation of one's innovations, which, instead, in the absence of patents, would be encouraged, hindering the dissemination of knowledge. This will also make it more advisable to resort to the publication[34] - which prevents valid patenting by anyone - whenever the innovation does not guarantee an economic return from its exclusive exploitation such as to justify the costs of patenting (particularly high if one wants to extend one's patents internationally, which is indispensable to truly protect oneself in an increasingly globalised

[33] The application of deep learning techniques is significantly facilitated by the text and data mining (TDM) exception introduced by the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market [2019] OJ L130/92. Under Articles 3 and 4 of the Directive, certain uses of copyrighted works for the purposes of TDM are exempt from the exclusive rights of rightholders. Article 3 provides a mandatory exception for research organisations and cultural heritage institutions, while Article 4 introduces a broader exception applicable to any user, provided that the rightholder has not expressly reserved rights in an appropriate manner. This legal framework enables developers of artificial intelligence systems to process vast volumes of textual and data-based content—including scientific publications, online databases, and digital archives—without infringing copyright, provided the statutory conditions are met. In the context of deep learning, where the effectiveness of the model often depends on the quantity and diversity of data used in training, the TDM exception plays a crucial role in ensuring lawful access to large datasets. It therefore represents an important regulatory development for the advancement of AI-driven innovation within the European Union.

[34] On *defensive publication* (or *defensive disclosure*) strategies see eg Bill Barrett, 'Defensive Use of Publications in an Intellectual Property Strategy' (2002) 20(2) Nature Biotechnology 191.

world), but one still wants to ensure the possibility of making use, albeit not alone, of that innovation, without risking others patenting it. On the other hand, the spread of Artificial Intelligence tools, especially in the scientific community, will facilitate the use of *open source* in this field too, expanding knowledge in the public domain[35].

In this perspective, one must also consider the possibility of Artificial Intelligence being used not only to build patents, but also to evaluate them - for instance by the EPO and USPTO[36] - and to attack them, proving their obviousness. In fact, it is clear that those attacking for invalidity will prevail if they provide evidence that a *priori*, by feeding a publicly available Artificial Intelligence algorithm and whose use is part of industry practice, the invention is arrived at by taking non-inventive steps, that is, steps suggested by known technique and corresponding to industry practice: it must, of course, be a practice that includes not generically the use of Artificial Intelligence, but an Artificial Intelligence that is available (both on the side of algorism, and on the side of data and the structuring of it), even if it is expensive to obtain, and not of a 'customised' Artificial Intelligence that only the inventor (or the one who challenges its validity) possesses and for which the considerations made above regarding information and tools that do not belong to the domain expert's baggage apply.

Abolishing patents would therefore create much greater distortions to the functioning of the market than those that patent critics see as attributable to the patent system[37], because it would ensure higher returns on investment for innovations that can be exploited under secrecy - as they cannot be *reverse engineered* from marketed products - while diverting them from areas where this possibility does not exist, including, typically,

[35] On open source, see Gustavo Ghidini and Valeria Falce, 'Open Source, General Public Licence e incentive all'innovazione' (2004) 13 AIDA 3; Simona Lavagnini, 'Validità e applicazione delle licenze open source' (nota a Trib Venezia, 13 December 2021) (2022) 31 AIDA 921; Massimo Di Rienzo, 'L'organizzazione dei mondi open source: profili soggettivi' (2004) 13 AIDA 12; Elisabetta Loffredo, 'Open Source e appartenenza del software' (2004) 13 AIDA 67, 86; Giovanni Guglielmetti, 'Open Source e interoperabilità con software proprietario' (2004) 13 AIDA 144, 155; see also, from a theoretical perspective, Brian Behlendorf, 'Open Source as a Business Strategy' in Chris Di Bona, Mark Stone and Sam Ockman (eds), '*Open Sources: Voices from the Open Source Revolution*' (O'Reilly Media 1999).

[36] On what the national patent offices will be able to do in relation to the advent of new technologies, see Simons (n 26) 146, where he observes that 'Determining the prior art that PHOSITAs (Persons Having Ordinary Skills In The Art: editor's note) actually consider at the time of filing and their level of skill will be more costly and time-consuming, and often outside the scope of patent examiners' expertise'. This implies that the Offices will have to equip themselves with adequate tools and probably that at least the major ones among them (EPO, USPTO, JPO and in perspective also CNIPA) will have to collaborate more with each other, at least in exchanging the results of the use of these tools in the patent analysis, it being understood that then, in the absence of a standard in any case in the determination of the *inventive step* each of them will apply its own.

[37] On the potential distorting effects of patent exclusivity see in particular Murrey N Rothbard, *Man, Economy and State with Power and Markets* (Ludwig von Mises Institute 2004) 1134, where he observes that 'Research expenditures [...] are overstimulated in the early stages before anyone has a patent and unduly restricted in the period after the patent is received' and that further distortions derive from the fact that almost all legal systems provide for patent prohibitions or exclusivity regimes that are at least partially different for certain types of innovations, so that 'The patent system thus has the further effect of artificially stimulating research expenditures in the patentable areas, while artificially restricting research in the non-patentable areas'.

pharmaceuticals and, more generally, those pertaining to an essential public good such as health[38].

The fact that the patent system encourages companies to compete in producing innovation in all sectors in which innovation is susceptible to economic exploitation does not, however, exclude - and indeed favours - recourse by innovators also to strategies not based on exclusivity, such as open innovation or Standard Essential Patents. These strategies can achieve a positive return on investment in a way that differs from the implementation of patentable innovation under exclusivity.

Even in these cases, however, it is precisely the existence, upstream of them, of the exclusivity conferred by the patent that makes it possible to resort to these alternative strategies while avoiding opportunistic behaviour of parasitic appropriation of the fruits of others' research. In the first case, it is precisely the fact that the innovator has an exclusive right that allows him to contractually regulate the waiver of it vis-à-vis certain subjects; subordinating it, for example, to the fact that they destine to open innovation the derived innovation created from the protected one. As typically happens, in matters of copyright, the contractualisation of relations relative to the Creative Commons, typically manifests "holders of copyright and related rights aim to 'deactivate' certain restrictions related to the application of copyright in the digital world (primarily on the Internet) by reserving, for the benefit of users, the exercise not of all rights, but only of some (e.g., in addition to the right of authorship, the rights to use the work for commercial purposes or to modify or develop its content)"[39].

In the second case, as the European Commission already clarified in 2023, "*Standardisation is a key contributor to industrial innovation and competitiveness. Successful standards rest on cutting-edge technologies, which require substantial investments in research and development. Under the rules of many standards development organisations (SDOs), such as the ETSI and the IEEE, companies and individuals may patent their technical contributions to a standard. Patents that protect technology essential to a standard are known as standard-essential patents (SEPs). Typically, SDOs require that any person or company wishing to have their patented technology included in a standard commit to licensing the relevant patents to others who may wish to use the standard (firms using/implementing a standard are also known as 'implementers'). These licences must be granted to implementers on fair, reasonable*

[38] On the special importance of patent protection in this field, which the pandemic has highlighted, see eg, Fausto Massimino, 'Vaccini, brevetti e Big Pharma, tra profitto, sostenibilità e diritto alla salute' (2021) 3 Il Diritto Industriale 232; Cesare Galli, 'Il diritto della proprietà intellettuale di fronte alle sfide della pandemia' (2021) 3 Il Diritto Industriale 221.

[39] E Arezzo, G Mazziotti, 'Le misure tecnologiche di protezione e le informazioni sul regime dei diritti' in Galli and Gambino (eds), *Codice commentato della Proprietà Industriale e Intellettuale* (UTET Giuridica 2011) 3358; on this topic see also S James and R Arkley, 'Intellectual Property in Mobile Applications: The Practicalities' [2012] E-Commerce Law & Policy 12; Alessandra Fabiani, 'Creative Commons: Un Nuovo Modello di Licenza per l'Utilizzazione di Opere in Internet' [2006] Il Diritto di autore 157; and Cesare Galli, 'L'Innovazione nel Web: Opportunità e Problemi Giuridici' (2015) 2 Il Diritto Industriale 105.

and non-discriminatory (FRAND) terms and conditions. If the patent holder refuses to make such a commitment, their patented technology cannot be included in the standard"[40].

Thus, in addition to competition between creators of innovation, competition between different legal techniques for the exploitation of this innovation is also encouraged through patent protection.

7 Conclusions & key policy suggestions

The examination we have conducted shows that it is possible to take into account, in the assessment of inventive activity, the spread of AI and its progress, without there being a need to insert new rules and without the advent of this new instrument calling into question the basic reasons underlying the protection of technical innovations by the granting of the exclusive right of exploitation in which the patent consists. On the contrary, it appears from this examination that precisely the increased possibilities for innovation that the use of AI applied to research allows increases the importance of maintaining the patent system, the pro-competitive function of which it accentuates, particularly in relation to the disclosure that is attached to patenting.

The alternative methods to the patent system for managing innovation, and first and foremost the protection of innovations as *trade secrets* and the associated contractual rules, do not seem to be able to achieve the same results, if not in combination with patent protection. Therefore, before an effective replacement of the patent system can be hypothesised, these methods still need to be thoroughly investigated and developed, so that the choice facing states - and supranational aggregations, such as the European Union - remains between the patent system and direct research funding, which, however, leads to results that are usually less efficient than those given by the market and is in fact basically reserved for areas where the economic incentive cannot work properly, as in the case of rare diseases and certain forms of basic research without direct practical implications and applications, as well as research that leads to results that cannot be protected.

Rather, an already current task for scholars - and, based on their reflections, for *policy makers* - is to envisage correctives to the current law, by enhancing the patent system's ability to also incentivise derivative innovation, by broadening the scope of the compulsory licence for dependency. This licence can already be granted when the invention protected by a second patent cannot be used without prejudice to the rights relating to a first patent granted on the basis of an earlier application, but only if "*the invention claimed in the second patent shall involve an important technical advance of considerable economic significance in relation to the invention claimed in the first*

[40] EU Commission, 'Proposal for a Regulation of the European Parliament and of the Council on standard essential patents and amending Regulation (EU) 2017/1001' COM(2023) 232 final.

patent" (Article 31 of the TRIPs Agreement): this requirement in fact implies largely discretionary assessments in the granting of such a licence, which reduces the effectiveness of the rule. In the same perspective, recourse to voluntary *licensing* should be encouraged, especially for small and medium-sized enterprises, to make the patent an instrument of enhancement and not only of protection, with a view to *business-driven* use of the patent system and more generally of intellectual property rights.

Realising that in the battle for progress, the real enemies of all are bureaucracy, inefficiency, and political mediation, and not patents, means starting to lay the foundations for a new happy growth, of which intellectual property has always been the fulcrum, helping to allocate scarce resources efficiently and thus to truly realise a universal destination of goods, which will only be in the interest of peoples around the world if these goods can be produced in ever-increasing quantity and quality.

Journal of Law, Market & Innovation

ISSN: 2785-7867

https://www.ojs.unito.it/index.php/JLMI
email: editors.jlmi@iuse.it

The JLMI is edited as part of the
Open Access online scientific journals of
the University of Turin
Via Verdi 8, 10124
Turin, Italy

Vol. 4 - 2/2025