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.