Regulation of Financial Protocol DAOs: Addressing the Problems of Decentralization and AI Governance

Salvatore Luciano Furnari and Chiara Villani

Abstract This article examines the legal challenges of regulating Decentralized Autonomous Organizations (DAOs) within financial markets, particularly those offering decentralized financial (DeFi) services. After classifying DAO in Social DAO, Investment DAO and Protocol DAO, it discusses the ambiguous legal status of DAOs, their decentralized and autonomous governance structure, and the obstacles these pose to traditional regulatory frameworks. DAOs are typically governed by smart contracts and operate on blockchain, complicating regulatory enforcement due to their decentralized, non-hierarchical structure. Additionally, the integration of artificial intelligence (AI) in DAOs introduces further complexities regarding accountability and liability, as AI lacks legal personhood. The paper reports innovative regulatory approaches, including "embedded supervision", which integrates monitoring mechanisms within DAO operations, and "polycentric co-regulation", which involves collaborative regulatory input from industry stakeholders. Ultimately, it suggests that Protocol DAOs might be more suitably considered as "infrastructural assets" rather than traditional business entities, encouraging voluntary compliance and adapting standards to their unique, decentralized nature.

Keywords Financial protocol DAO · Decentralization · Artificial intelligence

S. L. Furnari (✉) · C. Villani
Università Degli Studi Di Roma "Tor Vergata", Rome, Italy
e-mail: salvatore.furnari@leplex.it

C. Villani
e-mail: chiara.villani.tv@alumni.uniroma2.eu

M. Lustenberger et al. (eds.), *Decentralized Autonomous Organizations—Governance, Technology, and Legal Perspectives*, Springer Proceedings in Business and Economics,
https://doi.org/10.1007/978-3-032-03273-7_7

1 DAOs and Their "Unclear" Legal Status[1]

According to Wikipedia "[a] *decentralized autonomous organization (DAO), sometimes called a decentralized autonomous corporation (DAC), is an organization managed in whole or in part by decentralized computer program, with voting and finances handled through a blockchain. In general terms, DAOs are member-owned communities without centralized leadership. The precise legal status of this type of business organization is unclear*" [1].

The most significant aspect of this citation is not the attempts to provide a definition but rather the final statement, which notes that "*The precise legal status of this type of business organization is unclear*" [2]. An analysis of the revision history of this Wikipedia page reveals that, while the page was created in 2014, this statement was added in 2016. This means that, from 2016, the ambiguous legal status of this phenomenon has been highlighted on the internet's most popular encyclopedia—and it remains unchanged to this day.

In order to contribute to the mission of providing a legal status for DAO, this article in paragraph 2 offers definition and classification of DAO, examines the absence of a clear legal status, emphasizing the regulatory difficulties arising from their decentralized management and blockchain-based operations. It also highlights DAO role in financial markets through "financial" protocols (decentralized exchanges, lending protocol and yield aggregator) that operate without being traditional intermediaries. In paragraph 3, the article analyzes how the decentralized and global nature of DAOs complicates regulatory oversight and enforcement. Additionally, it explores how the integration of AI within DAOs, lacking legal accountability, challenges regulatory frameworks traditionally reliant on human oversight. Paragraph 4 discusses innovative regulatory approaches tailored to the unique characteristics of DAOs, considering their decentralized structure and the role of AI components. Paragraph 5 concludes by advocating for a shift in perspective: considering (correctly) DAOs as infrastructure rather than enterprises could be a solution to find a way to regulate these entities (*rectius* "*res*"), adopting a model based on voluntary compliance.

2 Financial Markets DAOs

2.1 Breaking the Term to Get a Definition

Beginning with definitions, a useful approach to defining a DAO is to break down the acronym into its components, focusing on the concepts of "*Decentralized Organization*" (DO) and "*Autonomous*" (A) [3].

[1] While the article reflects a joint collaboration, authorship of Par. 2, 3.1 and 5 is attributed to Salvatore Luciano Furnari, Par. 1 and 3.2 to Chiara Villani and Par. 4 to both Authors.

The middle term of DAO, "*Autonomous*" comes from "*Autonomous Agent*" [4], which in the IT sector refers to "entities" whose existence depends on humans only in their creation. Indeed, once created, their operation is indifferent to the action or will of their programmers.

A common example of autonomous agents are computer viruses, which can replicate on its own, from computer to another without any form of intervention by its creator. Like viruses, the simplest autonomous agent is bound to limited purposes; once achieved, emphatically, they die (or, rather, stop working).

Creating fully autonomous agents requires highly complex artificial intelligence systems, capable of surviving any changes in their computing environment.[2] This is far from being something to be seen in a distant future. As AI complexity advanced in recent years, it has been seen a transition from machine learning, which relies on binary code and statistical processing, to deep learning, where reprocessing capabilities and response complexity both increases. This progression leads to self-learning and self-modifying processes, driving those autonomous agents toward greater autonomy. These characteristics mark the most advanced AI systems, known as "strong" [5] systems, which can operate independently of initial inputs from creators, programmers, or users [6]. These systems make autonomous decisions, often labeled "*black box*" because the processes behind these decisions are not transparent [7]. In contrast, primordial AI systems, so-called "weak" systems, are limited to problem solving on the basis of human instructions, realizing an intelligence that is simulated but not capable of autonomous thinking. The core characteristic of autonomous agents, as relevant here, is their autonomy in performing tasks without human interference.[3]

The outer terms of DAO refer to "*Decentralized Organization*", that can be defined as a non-hierarchical organization, for the lack of a "central body" that direct its operations. To compensate for the lack of hierarchical control, "actions" within these organizations are governed by *ex ante* established rules shared by participants or incentivized through reward mechanisms. With modern technology, these rules and rewards can be entrusted to computer systems (also "*smart contracts*") that impartially guide members toward shared objectives.

The concept of a decentralized organization, or the decentralization of traditional organizations, poses theoretical challenges since hierarchy and centralization are

[2] Consider, for example, an Autonomous Agent programmed to run on the Ethereum blockchain. At the extreme, to be considered completely independent, the Autonomous Agent would have to have the ability to migrate to a different blockchain should the Ethereum network "shut down" for any reason.

[3] For greater understanding, it is useful to quote an example from Buterin [4]. According to the author, an Autonomous Agent performing an entrepreneurial activity could be a data storage Web service, which is programmed not only to store information received from users, but also to employ the revenues from the sale of its storage services to acquire new space on which to store more and more data, doing so as the demand for the service offered increases. In this example, the Autonomous Agent is not a mere executor of orders to achieve a specific and defined purpose (e.g., storing a precise number of data), but adapts the goal it has been given (providing the data storage service) based on the demand and availability of its surrounding environment in order to continue to perform its function in complete autonomy and for as long as possible.

deeply embedded in human organizations [8]. Typically, modern organizations function in pyramid structures, where contributions from lower-level members support those of higher levels, ultimately benefiting those at the top who, accumulating the "utility" provided by the other, then redistribute wealth downward. In contrast, decentralized organizations allow each participant to selfishly achieve the "ultimate utility" rather than contributing to a central hierarchy.[4] Benkler [9] through reward mechanisms, members achieve personal utility, and in striving to attain it, they may incidentally create a utility for another subject within the organization who pursue different, non-competitive objectives.[5]

Decisions affecting the organization are made on a widespread basis, with implementation usually requiring majority approval among voters. The ability to initiate a vote generally belongs to all token holders.

A DAO can be simply defined as a decentralized organization managed by an autonomous agent.[6] In other words, it is an organization composed of people and assets, structured without a central authority and managed autonomously (i.e., by a software that operates independently of both participants and programmers) from the individuals who participate in it[7] [10].

[4] DAOs find their roots in the concept of commons-based peer production, a model initially developed by Benkler [9]. Benkler's [9] model describes a system in which individuals work collectively on projects without traditional hierarchy or centralized control. This form of collaborative production enables self-organizing individuals to participate in various projects, as seen in examples like open-source software (e.g., Linux) and community-led platforms (e.g., Wikipedia). In these settings, control is decentralized, and resources are shared among participants without ownership by a central authority, emphasizing community governance and shared contributions. DAOs expand upon Benkler's [9] model by integrating blockchain technology and smart contracts, which provide an additional layer of automation and transparency to decision-making processes. Through blockchain, DAOs enable members to vote and govern collectively, and smart contracts automate key functions, eliminating the need for a central authority altogether.

[5] An example of this is the operation of Bitcoin's blockchain. Considering, for simplicity, two types of participants—the miner and the trader—the former supports the organization by earning bitcoin through mining, while the latter benefits from this activity by trading bitcoin with others. This system is governed by strict protocols within the Bitcoin network, which denies expected utility (e.g., bitcoin rewards or transaction validation) to participants who fail to adhere to the behavioral rules necessary for the organization's proper functioning. According to Buterin [4], Bitcoin's could even be considered on a par with a DAO and not just as a simple decentralized organization.

[6] This is from the words of Buterin [4], according to whom a DAO is "an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do".

[7] The concept of DAOs is not, as one would guess, exclusive to the business world. DAOs, while assuming (as an "organization") the possibility of owning or managing assets, does not have among its "ideological" assumptions the production or distribution of profits. For the purpose of distinguishing DAOs with a properly entrepreneurial vocation from others, the different acronym DAC or "Decentralized Autonomous Corporation" has also been coined.

2.2 Types of DAOs

Although DAO concept dates to 2013 [11], efforts to classify this phenomenon have emerged only recently.

The most important classification is the one based on their function. DAOs can be, indeed, classified into at least three categories: (i) Grant or Social DAO; (ii) Protocol DAO; (iii) Investment DAO [12].

Grant or Social DAOs focus essentially on philanthropic purposes and their goal is to distribute the monies raised when the DAO is established to projects selected by the DAO participants. Examples of grant or social DAOs include MolochDAO, [13] GitCoin DAO [14], Big Green DAO [15]; these projects collect and distribute resources to worthy projects, usually selected by the entire community of token holders.

Protocol DAOs are DAOs that primarily aim to "manage" a decentralized protocol. Examples include projects like Uniswap [16], MakerDAO [17], ICP [18] o Yearn [19] projects.

Uniswap, for instance, in its original version, is one the best example to understand protocol DAOs. Uniswap operates as a so-called "*decentralized exchanges*" (DEX) using a so-called "*automated market maker*" (AMM) model, where users deposit crypto-asset pairs of equal value into so-called "*pools*" managed by smart contracts. These "*liquidity pair*" enable exchanges between assets in each pair without needing to identify, directly, a specific counterparty. In fact, when an exchange order is sent, the smart contract holds the originator's crypto-asset and returns an equivalent value of the crypto-asset requested and present in the liquidity pair. The exchange is based on a mathematical formula embedded in the algorithm implemented in the smart contract; the most popular AMMs employ a formula that ensures that the product of the values in each liquidity pair remains constant before and after each transaction[8] [20]. Users who deposit crypto assets into "*liquidity pools*" participate in the distribution of "*fees*" generated by each exchange in proportion to what they deposit.[9]

The Investment DAO category includes DAOs whose purpose is to raise funds to invest in entrepreneurial projects with the aim of dividing the profits for the benefit of the participants in the DAO itself. Within the latter category falls the first project to have claimed to "take on" the form of a DAO: it dates back to 2016 and is known as the DAO.[10] The DAO is one of the most cited projects in the blockchain community,[11]

[8] For this reason they are also referred to as "Constant Product Market Maker". Variations to this formula involve, for example, the sum of value being constant; others involve "hybrid" or "dynamic" formulas. The reference is to the systems known as Constant Mean Market Maker (CMMM), Constant Sum Market Maker (CSMM), Hybrid Function Market Maker (HFMM) and Dynamic Automate Market Maker (DAMM).

[9] This trading fee is usually between 0.30% and 0.10% of the value of the exchange.

[10] The notoriety of this project may have been caused by the 2017 report of the Security Exchange Commission that, for the first time, sanctioned the applicability to Initial Coin Offerings of the regulations on public offerings of financial instruments.

[11] The project saw the light of day in 2016 with the publication on the GitHub site (a development platform frequently employed by computer programmers to make their creations public and receive

often regarded as a landmark crowdfunding experiment due to the significant funds raised in a short period. However, the project was abandoned, both because of a hacker attack,[12] and in relation to a report by the Security Exchange Commission, which acknowledged the nature of "*security*" to the DAO tokens offered to the public.[13]

2.3 DAO Applications in Financial Markets

DAOs have established a transformative role in the financial sector, particularly *Protocols DAO*, enabling and governing decentralized finance (DeFi) [21] protocols, but also in the still slightly less common form of *Investment DAO*. In their first form, DAOs are commonly deployed to manage and operate protocols that offers services that (in a non-juridical way) can be defined as financial services [21].[14] The most common example are decentralized exchanges (DEXs) such as the above-mentioned Uniswap, which facilitates peer-to-peer trading of digital assets without the need for

feedback from the community) of the source code of the smart contracts underlying its operation. On April 30, 2016, these smart contracts were executed on the Ethereum blockchain, and within 15 days the project managed to raise nearly $100 million. Within a month of its publication, some users had identified the existence of some computer errors in the source code on which the operation of the DAO was based. A few days later, before the token holders had time to "vote" on correcting the mentioned errors, a hacker attack, exploiting them, managed to steal about a third of the collected resources. the DAO's protocol, however, stipulated that in order for sums to be withdrawn from the project, it would be necessary to wait 28 days. In order to avoid the subtraction of at least a third of the entire amount collected, the entire Ethereum community was asked to vote on one of the first "forks" of a DLT network in the history of these technologies. Since a DLT network is unchangeable, the only way to avoid sum subtraction was to have all the network's supporters (the so-called "nodes") resume storing information from the version of the registry prior to the subtraction of resources. Some of the nodes that supported the Ethereum blockchain did not agree to "rewind the tape", continuing to record new transactions as if nothing had happened. Most of the miners that supported the blockchain voted to resume recording information from the transaction that preceded the hacker attack. This made it possible to "return" resources to their rightful owners and prevent their theft. From this diversity of behavior, the fork was generated that led to the birth of the Ethereum Classic blockchain (alongside the Ethereum blockchain), which continues to be supported by nodes opposed to the fork.

[12] The attack would appear to have been facilitated by the need to call a vote among all Ethereum token holders to correct a computer error found within a smart contract of the DAO. The execution of a smart contract, in fact, implies that it is no longer modifiable without the consent of a majority of the computing power supporting the underlying DLT network. Thus, the programmers of the the DAO project were forced to call an actual vote even to correct a blatant programming error. This procedure, needing time to be concluded, has meanwhile allowed malicious parties to exploit the same computer errors that should have been corrected, resulting in the near-subtraction of part of the monies collected.

[13] The DAO project aimed to raise capital to be conveyed within entrepreneurial projects based on DLT technology. Specifically, token holders had the power to choose which project the sums raised should be invested in and would receive profits commensurate with the success of the entrepreneurial project in which they invested.

[14] Here the term "financial" is used in its economic meaning and not in its legal one. The reason is that from a legal purpose it is very difficult to classify a protocol as a financial intermediary.

centralized intermediaries. Through DEXs, users can trade tokens directly via smart contracts that execute trades automatically, with liquidity pools managed and funded by individual participants instead of traditional market makers.

Additional example of "financial" protocols are the *lending protocols*, such as Aave [22] or Venus [23], which offer services that are very similar to the one offered by banks, or *yield aggregator protocols* such as Yearn [19], which offer services similar to investment companies, considering their ability to distribute (and so invest) the crypto-asset provided within the protocols offering better returns, giving back crypto-assets to the users with an increase in their amount.

Financial Protocol DAOs export the role of decentralized governance in financial markets. Unlike traditional financial institutions, where corporate boards or regulatory bodies dictate policy, these particular kinds of DAO allow protocol stakeholders—typically token holders—to vote on key decisions [24]. This community-based governance model enables participants to influence aspects like protocol upgrades and fee structures, thus decentralizing control and empowering users [25]. Additionally, DAOs serve as a mechanism for transparency and accountability [2]; by voting on proposed changes and maintaining an open record of decisions, DAOs promote a level of trust and reliability rarely seen in traditional financial institutions.

But one of the most important characteristics of the use of Protocol DAOs in financial markets is their distributed way of functioning that do not just rely in the absence of a central body under which (as it has been said) a fake scheme is created just to avoid regulation [26].[15] DeFi innovation reside in their impossibility to function without a collaborative participation transcending a sort of "mutualistic symbiosis" relation.[16] In DEXs, for instance, liquidity providers earn rewards proportionate to the volume of transactions in their respective pools, creating an incentive for users to supply liquidity and support the protocol's stability. This decentralized, automated approach to liquidity provision would be impractical in traditional finance, where market-making relies on centralized entities and where liquidity supply functions could not be directly offered by investors. By distributing financial markets "tasks" to all possible stakeholders of a financial markets (together with financial incentives that are no more "absorbed" by few big financial intermediaries) among a broad participant base, Financial Protocol DAOs not only enable a scalable and resilient financial ecosystem that adapts organically to market needs [2], but also favor the distribution of wealth within all the stakeholder of a financial markets.

---

[15] This has been argued by [27] and [28], where the authors argue that the notion of decentralization, often portrayed as a core feature of DeFi protocols, is largely illusory. They observe that, while many DeFi projects are marketed as decentralized, significant control over these protocols frequently resides with certain key actors, particularly the developers who design and manage the code. These individuals not only retain the power to modify the protocol but, in some cases, can even disable its functionality. As such, the authors suggest that "decentralization" is more of a strategic tool to avoid regulatory costs than a fundamental aspect of the technology.

[16] In this sense, the function of DeFi protocols can be likened to the framework of mutualistic symbiosis—a form of biological interaction between two organisms of different species, where both parties gain benefits from the relationship. Unlike parasitism, in mutualism, both symbionts contribute positively to each other's welfare, creating a partnership that supports the survival and reproduction of both parties. For the cited notions of biology, please refer to Rózsa and Garay [29].

3 Regulation Obstacles

3.1 A Decentralized Structure…

While DAOs empower participants and reduce entry barriers to "financial" services,[17] they also necessitate a re-evaluation of regulatory frameworks to accommodate their decentralized and autonomous structures within the financial sector.

From a "macro" perspective, governments are limited to exerting only weak controls over DAOs. The intrinsic design of DAOs, which are built and operate on blockchain networks, restricts traditional regulatory powers. Unlike centralized entities that rely on a physical or digital presence easily targeted by enforcement actions, DAOs exist in a decentralized environment where the *locus* of control is dispersed across anonymous, global participants. Since DAOs are hosted on public blockchains, their code and data are not bound to a single geographic location or entity, making enforcement challenging. Authorities cannot simply "shut down" a DAO in the conventional sense, as there is no centralized server or organizational headquarters to target.

The most immediate recourse for governments is to restrict access to the DAO's web interface, often through blocking its associated website domain. However, this measure remains superficial and largely ineffective due to technological workarounds; users can circumvent such restrictions with a simple VPN, masking their location and accessing the DAO interface regardless of imposed bans. Additionally, since DAOs can interact directly with users via blockchain addresses and digital wallets, blocking a website domain has a limited impact on core functionalities. Furthermore, DAOs often have open-source front-ends that can be replicated or "mirrored" across multiple domains, making it nearly impossible to prevent access entirely.

The limited jurisdictional reach of any single government over DAOs highlights an unprecedented regulatory challenge. Traditional enforcement mechanisms fail to account for the unique resilience and fluidity of blockchain-based entities, which can adapt or migrate in response to enforcement actions. This leads to questions of whether alternative regulatory frameworks are needed. In sum, the decentralized architecture of DAOs raises significant barriers to conventional regulatory efforts, calling for innovative regulatory approaches to address these digital and boundaryless entities.

[17] In truth, Atzori [30] critically scrutinizes this profile and posits that Blockchain-based governance is frequently praised for its egalitarian potential, but it often concentrates power among a few key actors—such as developers, miners, and tech entrepreneurs—who influence decision-making within platforms like Bitcoin and Ethereum. This concentration of power raises concerns about transparency and democratic legitimacy, as decision-making tends to fall into the hands of a small elite, challenging the ideal of decentralized, egalitarian control.

3.2 … and an AI Governance

Artificial intelligence (AI) systems, while often integrated into DAO operations for automation and decision-making support, lack the legal capacity to act as agents in the formal and legal sense, meaning they cannot enter into contracts or be held accountable in the way human managers or corporate officers can. Legally, an AI cannot assume the role of a "director", "manager", or "entrepreneur" of a DAO, as these positions require an entity capable of bearing rights and obligations [31, 32]

The most famous active DAOs, such as the Bitcoin protocol infrastructure (considered by some [33] one of the first DAOs to be implemented) and other decentralized finance DAOs like Uniswap or MakerDAO, don't always rely on formal structures. The famous the DAO project itself lacked a formal structure for external representation, operating instead as a mere "IT entity"; its interaction with the external world occurred through DAO.LINK, an entity under Swiss law [34], and a series of agents called "*contractors*", [35] who helped channel funds to selected projects.[18]

At present, no legal system recognizes the personhood of algorithms, nor does this path appear likely to be pursued in the future.

A related issue specific to DAOs is identifying the entity to be sued in the event of damages caused by such decentralized entities: the lack of a centralized legal entity complicates the identification of a responsible party.

In jurisdictions requiring identifiable and accountable leadership for corporate entities, the responsibility gap presents a challenge. Unlike human directors or managers, who can be scrutinized, sanctioned, or held liable, an AI remains outside the reach of traditional corporate governance laws. Without a legal person to hold accountable, regulators face challenges in enforcing compliance standards or penalizing misconduct within DAOs, raising questions about how existing corporate governance frameworks must evolve to address the unique nature of AI governance within DAOs.

The "problem" is so serious that the idea of giving legal personality to artificial agents to establish a center of responsibility for their acts had been considered at the European Level.[19]

However, this stance was soon abandoned by both the legal scholarship and the EU institutions themselves, recognizing numerous obstacles to framing AI in terms

[18] The creation of an entity that merely "assists" the DAO, enabling it to enter into legally binding contracts with the outside world (as opposed to the IT world in which the DAO finds itself), without properly representing its organizational structure, is quite common. Further example can be found in the Aragon DAO [36], a project aimed at developing tools to create other DAOs running on the Ethereum network, which uses the Aragon Association as its "manager" ("*stewardship*").

[19] The European Parliament's Resolution of 16 February 2017, containing Recommendations to the Commission on civil law rules on robotics (2015/2103(INL)), proposed, in paragraph 59(f) to «*creat(e) a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently.*»

of legal personhood.[20] In particular, if a criminal penalty is imposed, there remains the issue that artificial agents cannot fulfill the rehabilitative, general-preventive, or special-preventive functions of a sanction [37].

Similarly, the High-Level Expert Group on Artificial Intelligence (AI HLEG), established by the European Commission in June 2018, in its Report on Liability for Artificial Intelligence and other emerging digital technologies, after determining that «*there is currently no need to give a legal personality to emerging digital technologies*», stated that: «*[h]arm caused by even fully autonomous technologies is generally reducible to risks attributable to natural persons or existing categories of legal persons, and where this is not the case, new laws directed at individuals are a better response than creating a new category of legal person*» [38]. This issue becomes doubly problematic in the context of DAOs, as there is both a general difficulty in determining to which title responsibility for the actions committed by the AI should be attributed and the challenge of identifying any entity upon whom such responsibility might rest: in DAOs, indeed, there is typically no designated, legally accountable individual, and participants are often anonymous or dispersed across multiple global jurisdictions. Therefore, in the context of DAOs, the frequently advocated approach of enhancing human involvement in AI decision-making processes—known as "*human-in-the-loop*"—is impractical.

In particular, this concept belongs to the EU's human-centric AI paradigm, which aims to align AI functionality with human objectives[21]: it centers on the notion of trustworthiness, defined by the requirement that intelligent systems must adhere to certain standards to ensure respect for fundamental rights, as well as human freedom and autonomy in interactions with these systems [39]. Human-centric AI has been operationalized through the human-in-the-loop framework, which assigns specific roles and consequent responsibilities to humans in AI-driven processes to address issues related to accountability attribution.

---

[20] At present, not even U.S. laws recognize legal personhood for artificial intelligence. Some recent proposals and discussions have begun to explore the legal responsibilities of advanced AI and algorithms without conferring them the same legal status as natural or legal persons. Reference is made to Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. (2022): it aims to hold companies accountable for the societal impacts of their algorithms, focusing on organizational and developer responsibility rather than AI as an independent entity; and Federal Trade Commission, Aiming for Truth, Fairness, and Equity in Your Company's Use of AI (April 2021): those are guidelines emphasizing the ethical and responsible use of AI, highlighting corporate and individual accountability in AI development. This framework reinforces human and organizational responsibility, implicitly dismissing AI's independent legal status.

[21] Recall Art. 3 of the 2021 Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence, which defined the intelligent system as: "*software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*" The definition was taken verbatim from the 2019 OECD Recommendation on AI and, earlier, from the 2018 Commission Communication Artificial Intelligence for Europe. It is noteworthy that this nuance has been lost in the final version of the AI act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024 laying down harmonized rules on artificial intelligence).

This perspective is not only unsuitable for the aforementioned practical reasons but is also conceptually incompatible with DAOs. The fundamental rationale underpinning DAOs is their design to minimize human intervention, thereby enhancing decentralized governance and autonomy within the system. Imposing a human-in-the-loop framework on DAOs would counteract their core purpose, as DAOs are specifically structured to operate independently of continuous human oversight, relying instead on automated decision-making mechanisms. Consequently, requiring human oversight within DAOs would fundamentally conflict with their intended autonomous operational model and could undermine their functionality and efficiency.

Even regressing back to the time of creation of the DAO in which the AI system is embedded, the imputation of liability to producers or programmers is also problematic: the autonomy of strong AI systems complicates the identification of a causal link between the human subject's inputs and the output produced by the algorithm, due to the opacity of the AI's decision-making process.[22] This increases the risk of creating a sphere of irresponsibility, a phenomenon known as the "*responsibility gap*" [41].

Not even the provisions of the 2022 Artificial Intelligence Liability Directive (AILD)[23] Consulich et al. [42] succeed in resolving some of the most critical issues related to civil liability for damages caused by artificial intelligence systems, particularly due to the ever-growing degree of autonomy and independence of such systems from human users, which gives rise to the well-known *black box* problem.

In fact, although it provides for a relative presumption of causation in cases of fault between the failure to comply with a duty of care and the production or non-production of an output from the AI system that caused the damage,[24] it is still

[22] Actually, someone constructed a liability model based on abstract foreseeability, aligning with the assumption of risk by producers and programmers who have deliberately activated an artificial agent with unpredictable behavior. In this sense Magro [40] asserted the necessity of attributing liability to human actors in any case, maintaining that the lack of predictability and scientific explainability of robotic actions does not absolve the designer from criminal liability for negligence, as, according to the concept of negligence in existing law, abstract foreseeability does not require a detailed or specific prediction of potential harmful outcomes This reconstruction, however, evidently collides with the principle of personal imputation of criminal responsibility: indeed, unlike civil law, which also adopts imputation models of liability on an objective basis, criminal law does not provide similar criteria for objective imputation.

[23] The Artificial Intelligence Liability Directive (AILD) is a European Commission proposal submitted in October 2022 and not yet adopted as binding legislation. This proposal is part of a broader regulatory framework that aims to regulate the safe and responsible use of artificial intelligence technologies within the European Union. In addition to the AILD, this framework also includes the Artificial Intelligence Regulation (AI Act), which entered into force On August 1, 2024. If the AI Regulation focuses on preventing potential harm caused by AI systems, the AI Directive, by contrast, is aimed at harmonizing the liability regime applicable when such systems do cause harm.

[24] Specifically, Article 4(1) of the AI Directive, in light of the difficulty for claimants to demonstrate the causal link between non-compliance with a duty of care and the generation or failure to generate an output from the AI system that caused the damage, provides for a rebuttable presumption of causation in cases of fault; this presumption applies only where the national court deems it excessively difficult for the claimant to fulfill the burden of proof, and the following conditions are met:

incumbent on the injured party to prove the fault of the defendant and the causal link between the damage suffered and the operation of the AI system. This requirement continues to place a significant evidentiary burden on the claimant. Although fault can be established through a breach of duty of care as defined by AI legislation or other EU regulations, the effectiveness of such proof is limited in practice. The specific content of these "duties of care" must ultimately be interpreted by national courts; this carries the risk of interpretive divergence and regulatory fragmentation across the EU, potentially leading to a variety of national approaches that paradoxically undermine the Directive's core objective of harmonization. The same concern applies to the definition of "fault": the Directive does not interfere with national rules in this regard, thus allowing for differing interpretations among Member States. This situation creates additional uncertainty and potential fragmentation, as each state may maintain distinct criteria for determining fault in relation to damages caused by AI systems [43].

Considering all of this, it becomes evident that the primary issue identified with AI is its opacity: as the autonomy of the system increases, there is a growing disconnect between the inputs introduced by the designer, developer, or user, and the outputs produced. Particularly in the case of advanced AI systems, there exists the black box phenomenon, where the logical decision-making path leading to the final output is not traceable and it is complicated the attribution of responsibility.

This concern is echoed in the ESMA 2023 report, which identifies AI as a factor that negatively impacts transparency [44]. In light of this, one proposed solution is to make the decision-making process of AI systems more explainable and less opaque. The ESMA 2023 report provides a definition of the "explainability of artificial intelligence" which, in its narrow sense, refers to a technical and objective understanding of an algorithm's behavior that enables identification of the specific variables and their impact in producing a particular output. In a broad sense, explainability also refers to the comprehensibility of a given AI model for human users. However, ESMA itself acknowledges that this definition is somewhat shallow and lacks broad consensus, leading to uncertainty about the precise meaning of explainability.

Generally, an output is considered explainable if its decision-making process can be linearly traced backward. In contrast, deep neural networks are typically

(a) the claimant has demonstrated, or the court has presumed, the fault of the defendant; (b) it is reasonably probable that the defendant's negligent behavior influenced the generation or failure to generate the AI system's output; (c) the claimant has demonstrated that the damage was caused by the output generated or not generated by the AI system. Additionally, exceptions are provided for systems classified as high risk by the AI Act: the application of the causation presumption is limited under paragraph 2 to cases of non-compliance with certain obligations set out by the AI Regulation, and it does not apply under paragraph 4 if the defendant demonstrates that the claimant had sufficient evidence and expertise available to establish causation. A further exception is provided under paragraph 6 for cases where the AI system was used in the course of a non-professional personal activity: in such cases, the causation presumption applies only if the defendant materially interfered with the conditions of the AI system's operation or if the defendant was under an obligation and was able to determine the conditions of the AI system's operation and failed to do so.

considered to have low explainability due to their highly nested logic, where inputs are combined and transformed at each level, producing outputs that represent entirely new and unpredictable representations. In practice, however, this definition can create ambiguities [44].

4 The Need for a Different Regulatory Approach to Overcome AI and Decentralization Issues

The integration of AI within DAOs introduces an additional layer of complexity to an already intricate set of challenges. This raises a fundamental question: can regulation—or, more broadly, human intervention—effectively address the unique issues arising from the intersection of AI and decentralization?

Starting from the opacity issue, this specific problem could fade out into the specific domain of DAOs, as it operates within a framework characterized by transparency, owing to the features of blockchain technology. Indeed, blockchain provides an immutable record of actions, which is essential for ensuring transparency in DAO operations. In this context, AI can also help improve transparency and regulatory compliance within DAOs by analyzing data recorded on the blockchain and suggesting interventions to maintain adherence to evolving regulations.

This could actually have influence also with reference to the liability problem. In this context, one proposed solution has been to integrate preventive measures within the algorithm's structure, specifically by incorporating a "*deterrence formula*" within the AI system itself [43, 45].[25] This would enforce the certification that the algorithms include mechanisms to inhibit their operation in the event, for instance, of market manipulation risks. This preventive measure, originally proposed by legal scholars in relation to MiFID II[26] and algorithmic trading, in line with its risk-based approach, seems extendable to DAOs. Given the increasing learning capabilities of autonomous algorithms, it is believed that they could soon predict the impact of a specific output, self-restricting their actions in negative circumstances. Such negative conditions could be programmed directly *into-the-code* from the outset or emerge from subsequent learning processes.

[25] Azzutti [45] finds two possible shortcomings encountered in this approach: the first concerns possible technical or legal barriers; the second, assuming there are no technical or legal barriers, concerns the difficulty an autonomous and self-apprehending artificial intelligence would have in adapting to changes in regulations and market dynamics in such a way as to achieve effective deterrence. He believes that this difficulty could only be overcome by moving to more machine-intelligible regulation in terms of objectivity and quantifiability, yet the current European framework is extremely vague and leaves too much room for legal interpretation to be machine learnable. These criticisms have been rejected by other parts of the doctrine: see Annunziata [43], which believes that as far as possible technical or legal barriers are concerned, these have not yet been identified. Instead, for the second objection, it is noted that the European legislation is well specified, with the consequence of being learnable by algorithms.

[26] Directive 2014/65/EU.

This is connected to the idea of using AI to implement automated supervision embedded within DAOs: a concept called "*embedded supervision*" [46]. In this context, AI can monitor actions and transactions within a DAO in real time, reporting suspicious or noncompliant activities directly on the blockchain. This allows for continuous and transparent monitoring of algorithmic intermediaries through the ability to create automated and auditable compliance rules and enables authorities to exercise more effective and timely control than traditional supervisory systems.

Among the examples of the potential application of "*embedded supervision*" [47, 48], one that makes this principle clearer is the one that describes the possibility of verifying compliance with a financial intermediary's capital requirements by monitoring its crypto-wallets in real time [46].

The innovative approach suggested certainly has the advantage of reducing the management and compliance costs of individual intermediaries, while at the same time ensuring better supervision. Activity that, thanks to algorithms, also becomes simpler and more effective for the authorities, who, at the same time, will be able to receive real-time and qualitatively superior information.

However, it is possible to point out that it may be of no use to apply traditional regulation through the concepts of *embedded supervision* to "fully" algorithmic intermediaries. With regard to these, it is already the imposition of "classical" capital requirements that, upstream, loses its meaning. In these cases, the stability of the individual algorithmic intermediary cannot be guaranteed by its capital structure, which is essentially non-existent, but rather by the "stability"[27] of the code it employs. It might, therefore, be useful to espouse the approach of "embedded supervision", but on condition that it focuses on verifying requirements more suited to the management of algorithmic intermediaries' criticalities. These will necessarily be ad hoc requirements (i.e., absence of *bugs* in the computer code used, monitoring aimed at the prevention of attacks by hackers) as they are significantly different from those envisaged by the regulation of "traditional" intermediaries.

The search for new possibilities to innovate the way "decentralized" financial markets are regulated has already seen the emergence of new hypotheses to structure a different regulatory approach for this sector.

Another innovative regulatory approach can be found in what is known as "*polycentric co-regulation*", according to which regulation must be the result of a collaborative approach between authorities, industry players, and other stakeholders. [49] This approach is considered particularly suitable for the regulation of the decentralized finance sector because, given the difficulty of regulating a highly decentralized sector such as this "from above", if regulation also found its source in a decentralized structure, it could gain greater consensus (and thus *compliance*) on the part of the regulated parties [48].

The concept of *co-regulation* has seen an evolution into the different principle known as "participatory regulation" [48] in which market participants collaborate with the regulator from the development stages of the technology, which thus seems to lose its "traditional" characteristic of neutrality [50].

[27] Stability in this context must be understood as resistance to cyber-attacks.

In general, therefore, there are several hypotheses on how to renew and innovate today's regulatory approach to decentralized finance. Hypotheses and approaches all share the idea that the rules that should be enacted for algorithmic intermediaries should be significantly different from those currently in place for traditional intermediaries. On the contrary, the approach used today by the European legislator within the regulations already in force does not differ significantly from the ways in which traditional intermediaries are already regulated. The reference is to Regulation (EU) 2023/1114 (so-called MiCAR), which regulates crypto-asset service *providers* (so-called *crypto-asset service providers* or CASPs) by almost completely transposing the regulations envisaged for traditional financial intermediaries [21].

Despite these considerations, two legal issues arising from the absence of legal personality for AI systems within DAOs remain unresolved: the establishment of a responsibility regime and the capacity to enter into contracts.

Specifically, all the above-mentioned approaches do not address the issue of responsibility: assuming the inclusion of a deterrence formula (embed within the code and being the result of a co-regulation process) should it fail, an AI cannot be held legally responsible for its actions, which in a DAO context typically involve autonomous decision-making and operational tasks. This creates a concerning regulatory gap, as there is no legally accountable entity[28] to which claims for damages or violations can be directed. The gravity of the situation is heightened by the fact that DAOs themselves lack a formal structure for external representation: due to this lack, there is no clear, legally responsible entity that can interface with the outside world; when the management is handled by AI, which also lacks legal personality, it doubles the accountability vacuum: there's no legal person to answer for, or represent, the organization in case of disputes or breaches.[29]

[28] In the context of DAOs, it has been suggested that any token holder could be held liable, similar to the structure of a general partnership. However, this is not a general approach for several key reasons: (1) not all DAOs are organized or operate like traditional businesses. Many DAOs lack of the formal structure or activities of a traditional enterprise. In these cases, the application of such liability frameworks is complicated; (2) in many DAOs token holders and participants remain anonymous or operate under pseudonymous identities. In these cases, applying liability rules that assume identifiable individuals, such as those used in general partnerships, becomes practically and legally problematic. (3) DAOs are typically decentralized across multiple jurisdictions. Legal enforcement becomes a significant issue when participants are based in multiple regions with differing laws on liability and corporate governance. If token holders are located in jurisdictions with less stringent regulations on DAOs, or where DAOs are not explicitly recognized by law, holding them liable could be ineffective [8].

[29] As an attempt to regulate the phenomenon, mention should be made of the State of Vermont (USA), which sought to bridge the legal gap between traditional entities and decentralized organizations such as DAOs through an amendment to its LLC (Limited Liability Company) legislation. With this 2020 amendment, the creation of blockchain-based LLCs was permitted, allowing for the use of technology in governance. In this context, LLCs can be programmed to operate through smart contracts, with a voting and management system utilizing blockchain technology, while still maintaining the limited liability protection typical of an LLC. Nonetheless, given that DAOs are global entities, it would be beneficial to develop an international regulatory framework that enables greater interoperability between different jurisdictions and establishes common principles regarding the liability, governance, and transparency of DAOs [51].

Secondly, without legal personality, an AI cannot own assets, enter into contracts, or exercise property rights—essential functions for the operation of DAOs. As a result, DAOs managed by AI must rely on legal workarounds, such as delegating activities to developers or DAO members, which contrasts with the principle of decentralization and increases the risk of manipulation or conflicts of interest, undermining the DAO's core objective of operating without centralized authority.

All the above being true, a solution could be to stop trying to regulate DAOs in a "traditional" manner, namely, by insisting on identifying a "classical" responsible party. Indeed, even if a "scapegoat" were identified through legal means, the outcome would likely remain unsatisfactory.

For instance, if this should be identified with the programmers of the algorithm providing the service, the risk would be that of extending to them a potentially indefinite liability considering the impossibility of guaranteeing that an algorithm is free from computer programming errors and that it will remain so, given its many possible uses, its diverse and unpredictable interactions, and the possible subsequent innovations of the underlying technology. Not to mention the fact that *software* is considered by the sector's legislation as creative works of the intellect and that their "programming" liability could even collide with freedom of expression.

It would be different, however, to reverse the "liability" (and so the related risk) regime on users. Several years of *overprotective* regulation of the investor have had no effect on his growth and preparation.[30] Indeed, there is no legal obstacle to holding accountable a user that deliberately exploits an undiscovered computer error for personal gain at the expense of others. Such actions, driven by intent and resulting harm, fall within the scope of existing liability frameworks, ensuring that malicious exploitation does not evade legal repercussions. This principle underscores the importance of distinguishing between accidental interactions with flawed systems and intentional misuse aimed at deriving unfair advantages. In this context, blockchain technology is particularly well-suited for tracking, with significant advancements being made through the development of increasingly sophisticated blockchain forensic tools.

These considerations could lead to the possibility of giving a different "legal status" to DAO and, in particular, to Protocol DAOs. Indeed, considering DAOs as enterprises, with corresponding governance and accountability implications, it something that suits most Investment DAOs. Such organizations often resemble traditional enterprises, as they involve a collective entrepreneurial effort aimed at generating and distributing revenues. This process is typically preceded by a contribution, often used to acquire tokens that confer both administrative rights and a stake in the organization.

On the other hand, Protocol DAOs are more akin to infrastructures. For example, a protocol like a DEX can be compared to a public "iron bridge". It functions as a neutral platform facilitating interactions among diverse stakeholders and it shall be distinguished from the private entity (usually an enterprise) holding a concession to operate the bridge and that use it as its principal business asset. The DEX itself is

[30] Suffice it to say that Italy is still among the countries with the lowest levels of financial literacy [52].

an asset—an infrastructural tool—and should be assessed and qualified from a legal perspective as such.

From this standpoint, attempting to assign legal personality to (certain) DAOs is an unproductive exercise, analogous to trying to attribute legal personality to an inanimate object, like a rock.

In other words, if the combination of AI and blockchain technology results in the creation of mere assets or infrastructures—entities capable of interacting with humans but that are not, themselves, human—the regulatory framework designed for these new *res* will need to adapt accordingly. Specifically, it may require the removal of certain regulatory obligations that are inherently inapplicable to autonomous infrastructures as such.

Another conceivable (and less anarchic) solution would be to subject only the code that makes up the algorithms used by the protocols to prior authorization, in the specific same way as it is done by the rules that provide how to build the above-mentioned iron bridge.

Although it does not resolve them completely, this approach may provide more opportunities for the regulatory "management" of these entities. Focusing the audits on the code of these entities rather than on the "human" part of the organization already seems to be more in line with the essence of these IT entities.

Notwithstanding the fact that their international nature could not prevent the creation of Protocol DAO in countries that will not adopt such rules, the impossibility of showing the public the obtaining of the authorization (for instance with a *label*[31] confirming the consistency of the algorithms employed with the regulatory standards) would certainly favor spontaneous *compliance* due to the greater trust that obtaining the *label* would convey to investors.

In this case, a potential investor deciding to interact with a Protocol DAO that has not received the authorization *label* will bear full risk and responsibility of his acts (as it happens to investors deciding to interact with financial intermediaries having their seat in off-shore countries).

With reference to investors that will interact with authorized Protocol DAO, a sort of insurance system could be created and imposed by the regulator for obtaining the authorization, considering the possibility of this being financed by part of the fee collected by the Protocol itself [53].[32]

---

[31] For example, in France, the "digital asset service providers" who wish to offer services related to the custody of crypto assets, exchange with other crypto assets or with fiat currency, the management of an exchange or other services related to crypto assets, can optionally obtain a license issued by the Autorité des marchés financiers (AMF). This license merely allows them to display the "label" proving their possession to the public.

[32] However, it should be noted that while an insurance system may help mitigating potential risks, it also raises concerns regarding "*moral hazard*": this concept pertains to the risk that subjects covered by insurance may engage in reckless behavior. In the context of DAOs and AI, users might feel less accountable for associated risks, thereby incentivizing riskier actions. Consequently, insurance could inadvertently diminish the incentive for DAO developers and users to implement adequate precautions. Furthermore, traditional insurance models are poorly equipped to deal with the complexities of risks posed by DAOs, unique and often dynamic, while simultaneously offering coverage at a reasonable cost.

At the end of the day, given the decentralized nature of these entities and the inherent difficulty in "imposing" rules on them, the preferred regulatory approach would likely focus on demonstrating the benefits of compliance. This strategy aims to encourage voluntary adherence by highlighting its practical value to such organizations.

5 Considering DAO as Infrastructure to Solve Regulatory Uncertainty

This paper tries to contribute to the definition of DAO legal status by analyzing the regulatory issues that characterize this phenomenon.

Indeed, the attempt to regulate DAOs as if they were conventional financial market entities reveals a fundamental flaw deeply connected with their legal status: it assumes that DAOs operate as (and *are*) traditional "businesses". In reality, the concept of a DAO encompasses a broader range of organizational forms, many of which do not align with traditional business structures. As shown in various classifications, only Investment DAOs resemble enterprises, while most active DAOs (Protocol DAOs) today function more like infrastructures.

This shift in perspective calls for an innovative regulatory approach tailored to these new phenomena. Rather than imposing rigid "top-down" solutions, regulatory frameworks should embrace flexibility and incentivize DAOs toward voluntary compliance. Considering a DAO's inherent ability to evade conventional regulatory control, a more effective approach could involve incentive-based regulations that encourage DAOs to adopt standards for secure code development, maintain "cyber insurance", and adhere to best practices for risk management.

Moreover, the classification of DAOs as infrastructure aligns with their inherent challenges, such as the lack of legal personhood, which complicates accountability and regulatory compliance. A forward-thinking regulatory model could leverage these unique qualities, aiming to foster voluntary adherence to standards rather than enforce rigid oversight.

References

1. Wikipedia: Decentralized autonomous organization. https://en.wikipedia.org/wiki/Decentralized_autonomous_organization, last accessed 2025/04/14
2. Wang, S., Ding, W., Li, J., Yuan, Y., Ouyang, L., Wang, F.: Decentralized autonomous organizations: concept, model, and applications. IEEE Trans. Comput. Soc. Syst. **6**(5), 876 (2019)
3. Borgogno, O., Martino, E.: Decentralised autonomous organizations: targeting the potential beyond the hype. European Banking Institute Working Paper Series No. 161 (2024)

4. Buterin, V.: DAOs, DACs, DAs and more: an incomplete terminology guide. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/, last accessed 2025/04/14
5. Proietti, G.: Definire l'indefinibile? I sistemi di intelligenza artificiale alla ricerca di un inquadramento sistematico. Contratto e impresa **3**, 832–925 (2024)
6. Searle, J.R.: Minds, brains, and programs. Behav. Brain Sci. **3**(3), 417–457 (1980)
7. Russell, S., Norvig, P.: Artificial Intelligence: A Modern Approach, 4th edn. Pearson, Boston (2021)
8. De Filippi, P., Wright, A.: Blockchain and the Law. Harvard University Press, Cambridge (2018)
9. Benkler, Y.: The Wealth of Networks: How Social Production Transforms Markets and Freedom. Yale University Press, New Haven (2006)
10. Kaal, W.A.: Decentralized autonomous organizations—internal governance and external legal design. Ann. Corp. Governance, Univ. of St. Thomas Legal Studies Research Paper No. 20–14, 6–7 (2021)
11. Ortolani, P.: Decentralized autonomous organizations: inquadramento giuridico de jure condito e prospettive de jure condendo. In: Battaglini, R., Giordano, M.T. (eds.) Blockchain e Smart Contract, pp. 404–420. Giuffrè Francis Lefebvre, Milano (2019)
12. Moduoran, C.: The complete guide to crypto DAO. https://milkroad.com/dao/, last accessed 2025/04/14
13. MolochDAO official website. https://molochdao.com/, last accessed 2025/04/14
14. Gitcoin official website. https://www.gitcoin.co/, last accessed 2025/04/14
15. Big Green DAO official website. https://dao.biggreen.org/home, last accessed 2025/04/14
16. Uniswap official website. https://uniswap.org/, last accessed 2025/04/14
17. MakerDAO official website. https://makerdao.com/, last accessed 2025/04/14
18. Internet Computer official website. https://internetcomputer.org/, last accessed 2025/04/14
19. Yearn Finance official website. https://yearn.fi/, last accessed 2025/04/14
20. Mohan, V.: Automated market makers and decentralized exchanges: a DeFi Primer. Financ. Innov. **8**, 20 (2022)
21. Furnari, S.L.: La Finanza Decentralizzata. Cripto-attività, protocolli, questioni giuridiche aperte. Editrice Minerva Bancaria, Roma (2023)
22. Aave official website. https://aave.com/, last accessed 2025/04/14
23. Venus Protocol official website. https://venus.io/, last accessed 2025/04/14
24. Dupont, Q.: Cryptocurrencies and blockchains. Wiley, Cambridge (2019)
25. Powell, W.W.: Neither market nor hierarchy: network forms of organization. Res. Organ. Behav. **12**, 295–336 (1990)
26. Bank for International Settlements: The crypto ecosystem: key elements and risks, p. 9 (2023)
27. Anker-Sørensen, L., Zetzsche, D.: From centralized to decentralized finance: the issue of "Fake-DeFi". Working Paper (2021)
28. Aramonte, S., Huang, W., Schrimpf, A.: DeFi risks and the decentralisation illusion. BIS Q. Rev., December (2021)
29. Rózsa, L., Garay, J.: Definitions of parasitism, considering its potentially opposing effects at different levels of hierarchical organization. Parasitol. **150**(9), 761–768 (2023)
30. Atzori, M.: Blockchain technology and decentralized governance: is the state still necessary? J. Govern. Regul. **6**(1), 45–62 (2017)
31. Tullio, P.: Diritto societario degli algoritmi. E se I robot diventassero imprenditori commerciali? Anal. giur. econ. **1**, 225–246 (2019)
32. Mosco, G.D.: Roboboard. L'intelligenza artificiale nei consigli di amministrazione. Anal. giur. econ. **1**, 247–258 (2019)
33. Voshmigir, S.: DAOs & Purpose-Driven Tokens. Elvas (2024)
34. DAO Link—Blockchain and real-world business. https://blog.slock.it/announcing-dao-link-the-bridge-between-blockchain-and-brick-and-mortar-companies-9510ba04d236#.z0z9xwbpa, last accessed 2025/04/14

35. On Contractors and Curators. https://blog.slock.it/on-contractors-and-curators-2fb9238b2553, last accessed 2025/04/14
36. Aragon Association official website. https://aragon.org/association, last accessed 2025/04/14
37. Cappellini, A.: Machina delinquere non potest? Brevi appunti su intelligenza artificiale e responsabilità penale. disCrimen (2019)
38. Expert Group on Liability and New Technologies: Report on Liability for Artificial Intelligence and other emerging digital technologies. European Commission (2019)
39. High-Level Expert Group on AI: Ethics Guidelines for Trustworthy AI. European Commission (2019)
40. Magro, M.B.: Decisione umana e decisione robotica. Legislazione penale, 10 May (2020)
41. Consulich, F., Maugeri, M., Milia, M., Poli, T.N., Trovatore, G.: AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie? Quad. Giuridici, CONSOB 29 (2023)
42. Proietti, G.: Responsabilità civile, inadempimento e sistemi di intelligenza artificiale. Giust. Civile.com, 07.02.2023
43. Annunziata, F.: Artificial Intelligence and Market Abuse Legislation. Edward Elgar, Cheltenham (2023)
44. ESMA: Artificial intelligence in EU securities markets. ESMA TRV, 1 February 2023, ESMA50-164-6247
45. Azzutti, A.: AI-driven Market Manipulation and Limits of the EU law enforcement regime to credible deterrence. ILE Working Paper Series No. 54, Univ. of Hamburg (2022)
46. Auer, R.: Embedded supervision: how to build regulation into blockchain finance. BIS Working Paper No. 811 (2019)
47. Lessig, L.: Code and Other Laws of Cyberspace. Basic Books, New York (1999)
48. Ostercamp, P.: From 'Code is Law' to 'Code and Law': Polycentric Co-Regulation in Decentralized Finance (DeFi), SSRN working paper (2022)
49. Flick, M.: Digital Regulation: Designing a Supranational Legal Framework for the Platform Economy. LSE Law, Society and Economy Working Papers 15/2017, 23–28 (2017)
50. Bassan, F.: Digital Platforms and Blockchains: The Age of Participatory Regulation. Eur. Bus. Law Rev. (2023)
51. Wright, A.: The rise of decentralized autonomous organizations: opportunities and challenges. Stanford J. Blockchain Law Policy (2021)
52. Eurobarometer: https://europa.eu/eurobarometer/surveys/detail/2953, last accessed 2025/04/14
53. Faure, M., Li, S.: Artificial Intelligence and (Compulsory) Insurance. J. Eur. Tort Law **13**(1), 1–24 (2022)