RIVISTA ITALIANA
DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 1/2026 • DOI 10.32091/RIID0274 • articolo sottoposto a peer review • pubblicato in anteprima il 19 mag. 2026

Filippo Zatti

Technology-based decentralization and the structural limits of legal attribution: Why adapting the law requires rethinking its foundations

This article examines whether blockchain-based decentralization poses challenges to the legal order amenable to incremental regulatory adaptation, or with structural inadequacies in its very foundations. Legal orders presuppose the identification of subjects – natural persons, legal entities, public authorities – to whom rights and obligations are attributed. Attribution unfolds across three constitutive dimensions: territory, language, and embodied legal subjectivity. Blockchain technology and autonomous decentralized systems – *Decentralized Autonomous Organizations, Decentralized Finance* protocols – destabilize each, operating without identifiable centres of accountable authority. The challenge is therefore structural, not regulatory: as centres of attribution recede, legal categories lose the referent that grounds their meaning. Regulatory responses – the MiCAR Regulation, US enforcement actions – vest accountability in identifiable subjects. Integrating decentralized technologies thus brings to light the need to reconstitute identifiable centres of attribution: not a mere adaptation of the existing normative framework, but an exercise in institutional innovation.

Blockchain technology – Decentralization – Smart contracts – Jurisdiction – Lex cryptographia

Decentralizzazione tecnologica e presupposti strutturali dell'ordinamento. Ripensare i fondamenti del diritto prima di adeguarlo all'innovazione

Il presente contributo esamina se la decentralizzazione di matrice blockchain ponga all'ordinamento sfide risolvibili tramite adeguamento incrementale, o riveli piuttosto un'inadeguatezza strutturale nei suoi stessi fondamenti. Gli ordinamenti giuridici postulano l'individuazione di soggetti – persone fisiche, enti dotati di personalità giuridica, autorità pubbliche – cui attribuire diritti e obblighi. L'attribuzione si dispiega lungo tre dimensioni costitutive: territorio, linguaggio, soggettività giuridica incarnata. La tecnologia blockchain e i sistemi decentralizzati autonomi – organizzazioni autonome decentralizzate, protocolli di finanza decentralizzata – destabilizzano ciascuna di esse, operando senza centri identificabili di autorità responsabile. La sfida è dunque strutturale, non regolatoria: venendo meno i centri di attribuzione, le categorie giuridiche smarriscono il referente che ne fonda il significato. Le risposte regolatorie – il regolamento MiCAR, le decisioni di *enforcement* statunitensi – riconducono la responsabilità in capo a soggetti identificabili. L'integrazione delle tecnologie decentralizzate fa emergere la necessità di ricostituire centri di attribuzione identificabili: non un mero adeguamento del quadro normativo vigente, bensì un'opera di innovazione istituzionale.

Tecnologia blockchain – Decentralizzazione – Smart contract – Giurisdizione – Lex cryptographia

The Author is Associate Professor of Economic Law at the University of Florence, Department of Economics and Management (DISEI), and serves as scientific coordinator of the Blockchain and Artificial Intelligence for Business, Economics and Law (BABEL) Research Unit. He is also Academic Fellow of the European Banking Institute

This paper was developed as part of the PRIN 2022 project "DeTOKoDE – Designing a Governance for the Tokenized Economy in a Decentralized Era" (Protocol No. 20225YEPCT), funded by the Italian Ministry of University and Research (MUR) under the National Recovery and Resilience Plan (NRRP)

1. The decentralization dilemma: reconciling Distributed Ledger Technology with "legal order"

Traditional legal order depends fundamentally on the ability to identify subjects – whether natural persons, legal entities, or state authorities – to whom legal consequences can be attributed. This architectural principle underlies virtually every aspect of law: from criminal responsibility to contractual obligations, from property rights to regulatory enforcement, from territorial jurisdiction to legal personality.

Blockchain technology and decentralized autonomous systems challenge this foundational assumption by operating without identifiable centres or responsible authorities. These systems promise to create legal frameworks that function autonomously, without territorial boundaries, human intermediaries, or the institutional structures that have historically guaranteed legal certainty and enforcement. *Decentralized Autonomous Organisations* (DAOs) make collective decisions through smart contracts and token voting, cryptocurrencies transfer value without banks. *Decentralized finance* (DeFi) provides financial services without the need for licensed institutions. In each case, the system operates – or aspires to operate – without centres to which traditional legal attribution can attach.

This resistance to centres of attribution is not incidental but constitutive: decentralization means the absence of identifiable controlling authorities. Nevertheless, law's basic operations – determining applicable rules, adjudicating disputes, enforcing judgments, allocating responsibility – presuppose the existence of such centres. This creates a fundamental tension, perhaps even an incompatibility, between decentralization's aspirations and law's operational requirements.

How does technology-based decentralization challenge traditional legal paradigms, and can these challenges be reconciled with the law's foundational requirements? More specifically, it examines whether legal systems can adapt their attribution mechanisms to accommodate genuinely centreless systems, or whether ostensibly decentralized systems must ultimately establish identifiable centres to achieve legal recognition and enforceability.

As mentioned above, the analysis employs the concept of "centres of attribution" (*Zurechnungssubjekt*, as defined in Kelsen's terminology) as an organising framework[1]. Based on Kelsen's pure theory of law and Romano's institutional theory[2], it could be argued that law operates solely by attribut-

1. Kelsen 1945.
2. Itzcovich 2020.

ing rights, duties, and legal consequences to specific subjects. These attribution operations take place across three essential dimensions: the first being territory, which refers to the spatial dimension that anchors jurisdiction and enforcement. Another dimension is language, which serves as the symbolic medium for the articulation and interpretation of norms. Lastly, there is the body, which encompasses the embodied subjects that possess legal personality and experience legal consequences.

Decentralization challenges each of these dimensions while simultaneously highlighting their continued necessity. This framework facilitates a systematic analysis of the legal challenges posed by blockchain technology and offers a cohesive theoretical perspective for understanding issues that may appear disparate. The essay employs doctrinal legal analysis, supplemented by engagement with legal theory and empirical observation of blockchain systems. It examines how decentralization disrupts traditional legal concepts, evaluates regulatory responses, and assesses normative claims regarding constitutional benefits and conflicts. The analysis addresses the fundamental theoretical challenges that decentralization poses to law in general, rather than focusing on sector-specific applications. Although particular contexts such as financial regulation, corporate governance, and dispute resolution are referenced, the analysis seeks generality across applications. So, it concentrates on "public" permissionless blockchains rather than private permissioned systems, as these present the most significant challenges to traditional legal assumptions. Geographically, the analysis primarily considers European Union and US legal frameworks, while recognizing the global operation of blockchain.

2. Law without centres: the decentralization challenge

The rise of decentralized technologies, particularly blockchain with the support of smart contracts, presents a profound and multifaceted challenge to the traditional legal paradigm, which is fundamentally built upon centralized institutions, territorial sovereignty, human interpretation, and established frameworks for accountability and liability[3]. The conflict lies in the core principles of decentralization, (pseudo)anonymity, and automation inherent in these technologies, which range from clashing directly with classic juridical standards concerning stability, liability, territory, and social order; to rarely exploring possible alliances with the law to achieve common objectives. The challenges posed by decentralization applications can be examined across several critical areas: the very symbolic foundations of law, the role and sovereignty of the State, the feasibility of enforcement and jurisdiction, and the applicability of traditional liability and regulatory frameworks.

It is important to note that these challenges are not merely regulatory inconveniences amenable to incremental adaptation. Rather, they strike at the structural presuppositions upon which legal reasoning itself depends. Traditional legal categories – contract, property, personality, jurisdiction – are not free-standing concepts but derive their operational capacity from the existence of identifiable subjects to whom they can be attributed. When that foundational condition is systematically absent, the categories do not merely become difficult to apply; they lose the very referent that gives them meaning[4]. This distinction between difficulty of application and structural inadequacy is central to the argument that follows.

2.1. Displacement of foundational legal symbolics and imaginaries

2.1.1. Lex cryptographia: nomen aut res?

Blockchain technology, through its underlying ideology and technical architecture, initiates a potentially profound displacement of the symbolic and imaginary foundations upon which traditional legal systems have historically relied.

This emerging framework, often termed *lex cryptographia*[5], aspires to emancipate itself from three essential dimensions that have characterised modern legal systems: language, territory, and embodied legal subjectivity. However, whether *lex cryptographia* constitutes an alternative form

3. Coutinho–Pires–Correia Barradas 2024; Becker 2022; Cappiello–Carullo 2021; Lai 2021.
4. This distinction is developed further in Section 3 below. On the structural presuppositions of legal attribution, see Kelsen 1945; on the institutional dimension, Itzcovich 2020.
5. De Filippi–Wright 2018; De Filippi–Wright 2015.

of law or rather a novel regulatory tool operating *within* existing legal frameworks remains a contested question[6].

On one hand, blockchain-based governance exhibits law-like functions – coordinating behaviour, algorithmically resolving disputes, and enforcing compliance through cryptographic constraints – indicating a functional equivalence with traditional legal systems. On the other hand, its reliance on territorial law for ultimate legitimation and enforcement, its lack of interpretive flexibility and institutional structure, and its operation primarily through technical architecture rather than normative authority suggest that it may be more accurately viewed as one regulatory modality among others[7], serving to complement rather than displace state law.

This ambiguity extends beyond mere semantics and carries significant normative implications: to characterise blockchain as "law" may grant it undeserved legitimacy and obscure the private interests embedded within ostensibly neutral technical systems, whereas denying its legal character could close our eyes to genuine innovations in governance and the rise of alternative sources of normative authority. Whether this reflects a completed transformation of law or an ongoing contestation between different regulatory modalities remains an open question that warrants critical examination.

2.1.2. Language as symbolic attribution, code as performative inscription

Natural language provides the law's symbolic medium, enabling the articulation of general norms, their interpretation in specific cases, and the communication of legal meanings across time and contexts.

The most immediate consideration is that traditional law has fundamentally relied on natural language as its primary medium, which is inherently characterised by ambiguity, contextual sensitivity, and opportunities for interpretive flexibility[8]. *Lex cryptographia* aspires to revolutionise this paradigm by substituting linguistic articulation with computer code as the foundational substrate of legal systems. Proponents argue that this shift promises to eliminate subjective interpretation: legal frameworks such as smart contracts purportedly operate according to rigid "if-then" logical principles that would adhere to the rule of noncontradiction[9].

However, this vision of code as determinate and interpretation-free warrants critical scrutiny. As legal scholars have observed, code itself requires interpretation at multiple levels[10]. During its creation, when ambiguities in requirements must be resolved; during execution, when edge cases arise; and during disputes, when questions of intent, error, and enforceability emerge. The notorious collapse of The DAO in 2016, which required human intervention and contentious debate despite operating through ostensibly autonomous code, illustrates the persistence of interpretive questions even within blockchain systems[11].

Furthermore, this framework embodies what might be termed an anti-representational logic. By attempting to collapse the distinction between word and action within the algorithm, the system seeks to eliminate the deliberative space that characterises traditional legal structures – the gap between norm and enforcement that permits negotiation, proportionality, and equitable adjustment[12]. While proponents present this as establishing a more precise and predictable legal environment, critics contend that it risks sacrificing essential legal values: the capacity for contextual judgment, the protection of vulnerable parties, and the democratic contestability of legal outcomes[13].

The normative implications of this shift remain contested. Does the elimination of interpretive

6. Blemus 2018.
7. Lessig 2006.
8. Hart–Green 2012; Fish 1989.
9. Doria–Bassan–Rabitti et al. 2024.
10. Grimmelmann 2021; Scholz 2017.
11. Ungureanu–Bellesia–Cochis 2025; DuPont 2017.
12. Hildebrandt 2018.
13. De Filippi–Mannan–Reijers 2022; Verstraete 2020.

space represent progress toward efficiency and certainty, or does it constitute a dangerous impoverishment of law's capacity to serve justice and adapt to human complexity?

2.2. Deterritorialization and the question of sovereign authority

Decentralized blockchain (infra)structures also challenge traditional legal systems by aspiring to sever the intrinsic connections between law, political sovereignty, and territorial boundaries that have defined the Westphalian order since the seventeenth century[14]. These systems seek to establish legal frameworks that operate independently of the State's symbolic authority, effectively detaching legal validity from territorial jurisdiction.

In this evolving landscape, we observe the emergence of transnational, acephalous systems wherein *lex cryptographia* purports to operate autonomously across borders, emancipated from the cultural and national foundations that have traditionally conferred legal legitimacy[15]. Within these decentralized communities, legal authority remains both formally headless and spatially virtual, complicating conventional understandings of sovereignty, jurisdiction, and the enforcement of judgments.

Additionally, decentralization enables the development of what some theorists term "cloud communities"[16] or state-like non-territorial polities that employ opt-in legal systems. This model ostensibly removes the need for compromise and deliberation on shared values – processes that have historically been regarded as essential to the democratic legitimacy of law[17]. Instead, legal authority would derive from voluntary participation and cryptographic verification rather than democratic authorisation.

However, the deterritorialized aspirations of blockchain systems encounter persistent constraints. Territorial states continue to assert jurisdictional authority over blockchain activities that produce effects within their borders[18]. Regulatory interventions – ranging from China's ban on cryptocurrency exchanges to the European Union's Markets in Crypto-Assets Regulation (MiCAR) and the US Genius Act – demonstrate that territorial sovereignty remains a formidable force shaping blockchain's actual operation, regardless of its ideological commitments[19].

In this context, the European strategy for digital sovereignty deserves particular attention. The European Commission's policy framework – encompassing the Digital Decade Programme, the Data Governance Act, the Digital Services Act, and the AI Act – reflects a deliberate effort to reassert regulatory authority over transnational digital ecosystems, including blockchain-based systems[20]. This strategy proceeds from the premise that territorial governance and digital innovation need not be mutually exclusive, and that the exercise of democratic sovereignty over technological infrastructure constitutes a precondition for the protection of fundamental rights. The digital sovereignty agenda thus provides an important counterpoint to the deterritorialization thesis: far from rendering territorial authority obsolete, the proliferation of decentralized technologies has prompted a renewed assertion of sovereign regulatory capacity, albeit adapted to the specificities of the digital environment.

Consequently, while code emerges as a novel symbolic referent in this legal framework – one that seeks to displace the trust traditionally invested in state institutions – this displacement remains incomplete and contested. The tension

14. Johnson–Post 1997.
15. Werbach 2018.
16. Orgad 2018.
17. Habermas 1999.
18. Zetzsche–Buckley–Arner–Föhr 2018.
19. Houben–Snyers 2020.
20. On the European digital sovereignty strategy as a framework for asserting regulatory authority over digital ecosystems, see the European Commission's *2030 Digital Compass: the European way for the Digital Decade* (COM(2021) 118) and the broader policy architecture encompassing the *Data Governance Act* (Regulation (EU) 2022/868), the *Digital Services Act* (Regulation (EU) 2022/2065), and the *Artificial Intelligence Act* (Regulation (EU) 2024/1689).

between blockchain's deterritorialized aspirations and the persistent relevance of territorial jurisdiction constitutes a central problematic requiring ongoing empirical and theoretical investigation.

2.3. The elusiveness of jurisdiction and the limits of enforcement

The core difficulty stems from the belief that blockchain technology can "fracture economic and social processes" and operate autonomously, "independently of any government or other centralized authority"[21].

The decentralized and transnational nature of blockchain systems poses profound challenges to traditional concepts of jurisdiction and enforcement. These challenges operate at multiple levels: determining applicable law, establishing jurisdictional authority, and implementing effective enforcement mechanisms.

Traditionally, jurisdiction is defined either by the authority of a court to adjudicate cases or by the territory within which a court or government agency may exercise its power[22]. Decentralized systems deliberately challenge this geographical anchoring, leading to profound conflicts regarding applicable law and judicial authority. The decentralized blockchain structure is said to sever all legal ties to any specific territory[23].

This *a-territorial* and *a-spatial* dimension of the digital space means that decentralized networks operate across national borders, tending to remain scarcely regulated under domestic and supranational laws[24]. The *a-territorial* character of blockchain networks fundamentally disrupts the geographic foundations upon which jurisdictional rules have historically been constructed.

2.3.1. Jurisdictional ambiguity and choice of law

Traditional private international law relies on connecting factors that link legal relationships to specific territories. The Rome I Regulation (EC 593/2008), which governs choice of law for contractual obligations within the European Union, exemplifies this approach. Article 4 establishes a hierarchy of connecting factors, with particular emphasis on the "habitual residence" of the service provider or, in the absence of such identification, the place where the central administration is located.

However, these connecting factors become problematic – indeed, potentially meaningless – when applied to DAO or blockchain-based contractual arrangements. A DAO exists simultaneously everywhere and nowhere: its smart contracts execute on distributed nodes across multiple jurisdictions, its governance tokens may be held by pseudonymous participants globally dispersed, and its treasury may consist of cryptoassets with no physical location. Where is the "habitual residence" of such an entity? Where is its "central administration" when decision-making occurs through on-chain voting mechanisms without any physical headquarters?

The escape clause in Rome I (Article 4(3)) allows courts to apply the law of a country with which the contract is "manifestly more closely connected." However, this provision presupposes the existence of such a country – an assumption that decentralized systems deliberately challenge. The result is jurisdictional ambiguity that creates opportunities for regulatory arbitrage and forum shopping. Projects may structure their token distributions, governance mechanisms, and operational parameters specifically to avoid or minimise connections to jurisdictions with stringent regulatory requirements[25]. This is achieved partly through jurisdictional ambiguity: DAOs are often designed without an official domicile, which complicates the application of corporate, tax, and capital market laws. Furthermore, the complexity of identifying parties in a distributed system makes it "almost impossible" to determine competent jurisdiction in a predetermined manner[26].

21. Hummler 2016.
22. Thysse 2025.
23. Becker 2022.
24. Poncibò 2021.
25. Anus–Allauddin 2025.
26. Coutinho–Pires–Correia Barradas 2024.

Moreover, DAOs present classification challenges that precede choice-of-law analysis. Are they partnerships? Unincorporated associations? Sui generis entities? The answer to this preliminary question determines which choice-of-law rules apply, yet the answer remains contested. This creates what might be termed "double indeterminacy": uncertainty about both the applicable classification framework and the applicable substantive law.

A concrete illustration is provided by the litigation surrounding the bZx Protocol. Following a series of exploits in 2020 that resulted in losses exceeding USD 8 million, affected users faced the threshold question of whom to sue and where. The protocol had no incorporated entity, no registered office, and no identified governing body. Developers were pseudonymous or geographically dispersed, and governance token holders spanned multiple jurisdictions. Traditional connecting factors – domicile of the defendant, place of performance, place of the harmful event – yielded no clear answer, precisely because the system was designed to operate without the territorial anchoring upon which these factors depend[27].

2.3.2. Enforcement challenges in decentralized systems

Even when applicable law can be determined and jurisdiction established, enforcement presents formidable obstacles. Traditional legal enforcement presupposes the existence of identifiable defendants who can be served with process, whose assets can be located and seized, and who can ultimately be compelled to comply with judicial orders. Decentralized systems resist these assumptions at every step.

The concept of the "veil of decentralization" captures this dynamic: just as the corporate veil shields individual shareholders from liability, the architecture of decentralization creates a liability shield – but one without an identifiable entity behind it. There is no "DAO Inc." to sue, no board of directors to hold accountable, no CEO to compel to testify. Legal process confronts a distributed network of pseudonymous participants, none of whom may individually possess the authority or capacity to provide the relief sought.

Smart contract immutability compounds enforcement difficulties. Once deployed to the blockchain, code executes autonomously according to its programmed logic. A court order demanding that a smart contract cease operation, modify its behaviour, or reverse a transaction encounters a fundamental problem. There may be no party capable of implementing such an order. The code operates permissionlessly, continuing to execute regardless of legal judgments. While validators could theoretically coordinate to fork the blockchain and reverse transactions, such interventions contradict the ideology of immutability and face collective action problems.

The Tornado Cash saga offers a particularly instructive example. In August 2022, the US Office of Foreign Assets Control (OFAC) imposed sanctions on Tornado Cash, a decentralized mixing protocol used to anonymise cryptocurrency transactions. The sanctions targeted not an individual or a corporation but a set of smart contract addresses – marking the first time OFAC designated autonomous code as a sanctionable entity. Since the protocol operates autonomously on the Ethereum blockchain, the sanctions could not "shut down" the protocol itself; the smart contracts continued to function. Enforcement instead targeted peripheral human actors: the arrest of developer Alexey Pertsev in the Netherlands, who was subsequently convicted of money laundering by the Rechtbank Oost-Brabant, and the criminal prosecution of co-founder Roman Storm in the Southern District of New York. However, the legal framework underpinning the sanctions themselves proved fragile. In November 2024, the Fifth Circuit held in *Van Loon v. Department of the Treasury* that OFAC had exceeded its statutory authority, as immutable smart contracts lack the hallmarks of ownership and control required to constitute "property" under the International Emergency Economic Powers Act. OFAC subsequently delisted Tornado Cash in March 2025. Storm's trial in August 2025 produced a mixed verdict: the jury convicted him of conspiracy to oper-

27. On the bZx Protocol exploits and the resulting jurisdictional difficulties, see the related litigation in *Sarcuni v. bZx DAO*, No. 22cv00618 (S.D. Cal. 2022), in which the court considered whether holders of the DAO's governance tokens could be treated as general partners of a general partnership for purposes of liability and personal jurisdiction.

ate an unlicensed money transmitting business but deadlocked on the more serious money laundering and sanctions charges, with a retrial requested for October 2026. This sequence vividly illustrates both the limits of traditional enforcement when confronting genuinely decentralized code and the persistent tendency of regulators to re-centralise accountability by focusing on identifiable human actors at the system's periphery – even as courts increasingly question the legal basis for treating autonomous protocols as sanctionable entities[28].

Asset seizure – a traditional mechanism for satisfying judgments – becomes equally problematic. When smart contracts manage a DAO's treasury, private keys may be distributed via multi-signature arrangements or threshold cryptography. No single party may possess the unilateral capacity to transfer assets in compliance with a court order. Even if enforcement authorities could identify and compel cooperation from key-holders, cryptocurrency's censorship-resistant properties and the potential for assets to be transferred across chains create additional obstacles.

Cross-border coordination difficulties further undermine the effectiveness of enforcement. Blockchain networks operate globally, yet legal enforcement mechanisms remain primarily national. A judgment issued by a court in one jurisdiction may prove difficult or impossible to enforce in others, particularly when relevant parties or assets reside in jurisdictions with weak international cooperation frameworks or hostile attitudes toward such enforcement actions.

2.4. Disembodiment and the paradox of legal subjectivity

Decentralization significantly challenges traditional conceptions of legal subjectivity, which have historically been constructed around the juridical concept of legal personality. This concept abstracts the legal person from biological particularity while simultaneously depending upon embodied human agency[29]. Within the aspirational framework of *lex cryptographia*, the physical body is conceptually rendered as a non-programmable entity, ostensibly excluded from direct representation in blockchain legal systems, even as these systems continue to produce effects on embodied subjects.

This creates what might be understood as a dual movement: the body loses its authoritative position as the presumptive locus of legal agency while simultaneously being relegated to the status of a mere biological object external to the system's primary operations[30]. Legal personality becomes increasingly detached from human embodiment, potentially migrating instead to algorithmic agents (such as agentic AI), smart contracts, or DAOs that operate according to programmatic logic rather than human will[31].

However, this disembodiment proves paradoxical and incomplete in practice. Bodies remain stubbornly relevant to blockchain systems in multiple ways: through biometric identity verification systems that increasingly govern access; through the embodied labor of developers, miners, and users whose physical actions sustain the infrastructure; through the material consequences of algorithmic decisions that affect nutrition, healthcare, housing, and physical security; and through the legal recourse available when code produces harmful outcomes that territorial legal systems may still remedy[32].

Furthermore, the fantasy of disembodied legal agency obscures important questions about power, inequality, and access. Who possesses the technical literacy, economic resources, and social capital

28. On the Tornado Cash sanctions and subsequent proceedings, see US Department of the Treasury, OFAC, Designation of Tornado Cash (8 August 2022), subsequently delisted on 21 March 2025 following the Fifth Circuit's ruling in *Van Loon v. Department of the Treasury* (26 November 2024); *United States v. Storm*, No. 1:23-cr-00430 (S.D.N.Y. 2023), in which a jury convicted Storm of conspiracy to operate an unlicensed money transmitting business but deadlocked on the money laundering and sanctions charges (6 August 2025), with a retrial requested for October 2026; *Rechtbank Oost-Brabant*, 14 May 2024, ECLI:NL:RBOBR:2024:2069 (conviction of Alexey Pertsev, currently under appeal before the Gerechtshof 's-Hertogenbosch).

29. Naffine 2009.

30. Rouvroy–Berns 2013.

31. Hacker 2024; Scholz 2017.

32. Cengiz 2023; Watters 2023.

to participate meaningfully in supposedly neutral blockchain systems? Whose bodies are rendered more vulnerable by the withdrawal of interpretive flexibility and institutional oversight?[33] The unrepresented but consequential presence of the human body thus creates a constitutive tension within blockchain legal systems – a tension between the ideology of algorithmic autonomy and the persistent materiality of embodied human existence.

This transformation does not simply replace one form of legal subjectivity with another. Instead, it generates a complex field of competing modes of agency: the robotised presence of smart objects seamlessly integrated into algorithmic frameworks coexists uneasily with the excluded-yet-affected presence of biological bodies[34]. Understanding this paradox requires moving beyond technological determinism to examine how different actors negotiate, resist, or are subjected to these new configurations of legal power.

2.5. Regulatory responses

Regulators and courts have begun developing strategies to address these challenges, though the approaches remain experimental and their efficacy is uncertain. Two developments merit particular attention so far: the Ooki DAO enforcement action and the European Union's Markets in Crypto-Assets Regulation.

2.5.1. The Ooki DAO Case

In September 2022, the US CFTC filed an enforcement action against Ooki DAO, marking a significant regulatory development. The CFTC alleged that Ooki DAO offered illegal leveraged trading of digital assets and failed to implement proper KYC and AML procedures[35]. Rather than identifying individual defendants, the CFTC named the DAO itself and, critically, served the DAO's token holders collectively through governance forums and online platforms. The CFTC's theory rested on functional control: token holders who participate in governance effectively control the DAO and therefore bear responsibility for its legal compliance. In June 2023, following Ooki DAO's deliberate non-appearance, the Northern District of California granted a default judgment, finding the DAO to be an unincorporated association under the Commodity Exchange Act and imposing a civil monetary penalty of $643,542 alongside injunctive relief. The decision was hailed by the CFTC as precedent-setting, yet its practical significance remains uncertain. The judgment has not been enforced against individual token holders, and the broader regulatory landscape has shifted markedly: in April 2025, the CFTC Acting Chairman directed enforcement staff to align with the DOJ's "Ending Regulation by Prosecution" memorandum, which instructs prosecutors to cease "superimposing regulatory frameworks on digital assets" and to refrain from targeting platforms for the acts of their end users. The Ooki DAO case thus stands as a cautionary precedent from a regulatory era that may already be receding – though the underlying questions about the extent to which passive governance participants can be held liable for organisational misconduct remain unresolved.

2.5.2. EU MiCAR framework

MiCAR, which became fully applicable on 30 December 2024[36], seeks to identify functional equivalents to traditional financial actors and impose corresponding obligations on them. It establishes a typology of cryptoassets (e-money tokens, asset-referenced tokens, and other crypto-assets) with tailored requirements for each category; creates an authorisation regime for cryptoasset service providers (CASPs), capturing activities such as exchange services, custody, portfolio management, and investment advice; and – most relevant to the enforcement challenges discussed above – requires the identification of responsible "issuers" and "offerors" who bear legal obligations regarding dis-

33. Atzori 2017.

34. Eubanks 2018; Scholz 2017; Hayles 1999.

35. CFTC 2023.

36. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCAR). Titles III and IV on asset-referenced tokens and e-money tokens applied from 30 June 2024; the remaining provisions, including Title V on CASPs, became applicable on 30 December 2024.

closure, governance, and operational standards[37]. For ostensibly decentralized projects, MiCAR's approach involves piercing through the rhetoric of decentralization to identify *de facto* controllers. Projects claiming to lack any responsible party will find such claims receive limited credence. Regulators may identify core developers, foundation entities, large token holders, or others exercising meaningful influence as responsible parties for regulatory compliance purposes[38].

Crucially, however, MiCAR itself acknowledges the limits of this approach. Recital 22 of Regulation (EU) 2023/1114 provides that cryptoasset services provided "in a fully decentralised manner without any intermediary" fall outside the Regulation's scope, and that cryptoassets without an identifiable issuer – such as Bitcoin – are excluded from Titles II through IV governing issuance obligations[39]. Yet the exclusion is far from absolute: CASPs providing services in relation to such cryptoassets remain fully subject to MiCAR's requirements[40], thereby reasserting regulatory control through the intermediary layer even where the underlying protocol eludes direct regulation. This structure confirms the re-centralising dynamic analysed above: regulation gravitates toward the identifiable nodes at the system's periphery. The notion of "full decentralization" is itself indeterminate, as MiCAR provides no definition of the concept, leaving the boundary between regulated and unregulated activity to case-by-case assessment by national competent authorities[41]. The coherence of this framework remains under review: Article 142 of MiCAR mandated the Commission to report, by 30 December 2024, on the "appropriate regulatory treatment of decentralised crypto-asset systems without an issuer or crypto-asset service provider"; EBA and ESMA published their Joint Report contributing to this assessment in January 2025, but the Commission's own report – which may include legislative proposals – had not been published as of early 2026[42].

The early implementation data offers a preliminary assessment of this framework in operation. By late 2025, over 70 CASP authorisations had been granted across the EEA, with Germany and the Netherlands leading in licence issuance, alongside some 570 cryptoasset white papers submitted to national regulators[43]. However, no MiCAR enforcement actions had been reported as of early 2026, and the transitional regime – under which existing providers may continue operating under national laws until 1 July 2026 – has revealed significant fragmentation, with Member States adopt-

37. See Arts. 4–15 (Title II, public offerings of crypto-assets other than ARTs and EMTs), Arts. 16–47 (Title III, ARTs), Arts. 48–58 (Title IV, EMTs), and Arts. 59–83 (Title V, CASPs), Regulation (EU) 2023/1114. On the general approach of functional equivalence, see Houben–Snyers 2020; Zetzsche–Buckley–Arner–Föhr 2018.

38. Cengiz 2023; De Filippi–Mannan–Reijers 2022. On the concept of "decentralization theatre" in the context of governance structures that claim to be decentralized while retaining effective control by identifiable actors, see Aramonte–Huang–Schrimpf 2021.

39. Recital 22, Regulation (EU) 2023/1114: "Where cryptoasset services are provided in a fully decentralised manner without any intermediary, they should not fall within the scope of this Regulation" See also *ibid*., second sentence: "Where cryptoassets have no identifiable issuer, they should not fall within the scope of Title II, III or IV of this Regulation". Art. 4(2) further exempts from Title II cryptoassets automatically created as a reward for the maintenance of the DLT or the validation of transactions.

40. Recital 22, third sentence, Regulation (EU) 2023/1114: "Cryptoasset service providers providing services in respect of such cryptoassets should, however, be covered by this Regulation".

41. On the interpretive difficulties, see De Filippi–Mannan–Reijers 2022; Aramonte–Huang–Schrimpf 2021. MiCAR does not define "full decentralisation", leaving open the question of at which layer of the DeFi stack an intermediary must operate in order to bring the service within the Regulation's scope.

42. Art. 142, Regulation (EU) 2023/1114. ESMA 2025: The Joint Report found that DeFi remains a niche phenomenon, with value locked in DeFi protocols representing approximately 4% of total crypto-asset market capitalisation globally.

43. Data from ESMA Interim MiCA Register, updated December 2025. On the licensing landscape see also the EBA 2026 Work Programme (published 1 October 2025).

ing grandfathering periods ranging from 6 to 18 months[44]. This disparity undermines MiCAR's harmonising ambition and has created uneven market access across the Union. Moreover, in December 2025, the European Commission announced plans to centralise supervision of the most significant CASPs under ESMA[45] – a development that, if adopted, would further illustrate the re-centralising dynamic at work: even a regulation designed to accommodate decentralized technologies ultimately gravitates toward the identification of accountable centres.

2.5.3. Emerging strategies

These regulatory responses reflect broader strategies to address decentralisation's enforcement challenges.

First, functional analysis: looking beyond formal structures to identify who actually controls systems and allocating responsibility accordingly.

Second, participant liability: extending liability to ecosystem participants – validators, liquidity providers, governance participants – based on their roles and degree of involvement.

Third, service provider regulation: focusing enforcement on centralized points of contact with the traditional financial system, such as exchanges and custodians, even when the underlying protocols remain decentralized.

Fourth, technical mandates: requiring that smart contracts and protocols incorporate compliance functionality, such as transaction monitoring or the ability to respond to legal orders, as a condition of regulatory approval.

These strategies represent adaptations of traditional legal tools to novel technological circumstances. Their long-term efficacy remains uncertain, dependent on international coordination, technical feasibility, and the willingness of courts to accept novel theories of responsibility and control.

3. Law as a system founded on "centres of attribution"

The inevitable question is that the traditional legal paradigm operates fundamentally as a system founded upon and necessitating identifiable "centres of attribution", a structure essential for realising the primary function of law as the main tool for social order. This system of centralized law is typically characterised by being imposed from above by an authoritative institution whose power to rule is both genuine and legitimate, deriving from political action and the will of the rulers. This political authority grants the State, or its designated agencies, the requisite monopoly of coercive power for the ultimate enforcement and application of legal sanctions. This structured exercise of force, balanced against individual rights, constitutes the core mechanism of the rule of law.

The efficacy and certainty indispensable to this traditional legal system rely on defining and fixing these centres across several critical domains. Organisational law provides the necessary "impermeable barriers" and frameworks for groups of people, allowing the system to structure accountability and risk. This institutional anchoring of accountability is non-negotiable within the current paradigm.

Furthermore, this reliance on fixed centres allows the legal system to act as a crucial "supplier of fictional certainty" where technology or reality itself cannot provide absolute deterministic outcomes. This "institutional backstop" is critical, particularly in complex commercial spheres. For instance, concepts fundamental to modern finance, such as achieving absolute "operational finality" in transactions, are acknowledged as nearly impossible[46]; therefore, the law intervenes to impose "legal finality" through presumptions and rules, providing the certainty required to mitigate systemic risks, particularly those arising in insolvency or bankruptcy proceedings[47]. The coherence of the rule of law is thus preserved by defining these ex-

44. Art. 143(3), Regulation (EU) 2023/1114, provides a maximum grandfathering period of 18 months (until 1 July 2026) but allows Member States to reduce or opt out of the transitional regime. Several Member States adopted shorter periods of 6 to 12 months, creating asymmetric market access.

45. European Commission, Market Integration Package within the Savings and Investments Union Strategy, 4 December 2025, proposing to confer on ESMA the supervision of the most significant CASPs.

46. Barresi 2023.

47. Martino–Ringe 2024.

plicit points of connection and control, enabling reliable adjudication and the protection of established rights.

The core challenge posed by technology-based decentralization, and the concept of *lex cryptographia*, lies in their foundational ethos, which seeks radical emancipation from the constitutive legal dimensions: territory, language, and the physical body. The challenge, therefore, is not simply one of regulatory adaptation but of confronting whether law as we have understood it – as a system of centred attribution – can meaningfully operate in a genuinely acephalous, distributed environment, or whether the persistence of legal order necessarily requires the (re)imposition of identifiable centres, even within ostensibly decentralized structures.

It should be acknowledged, however, that not all scholars regard this tension as irresolvable within existing legal frameworks. A significant strand of legal scholarship maintains that the difficulty of applying traditional attribution mechanisms to decentralized systems does not demonstrate their structural inadequacy, but rather the need for creative adaptation. Authors such as Werbach have argued that blockchain systems inevitably produce identifiable *loci* of control – core developers, foundation entities, dominant token holders – and that existing legal tools, properly deployed, can reach these actors[48]. Similarly, the functional analysis employed by regulators in the Ooki DAO case and under MiCAR proceeds from the premise that behind every "decentralized" system there exist human agents exercising meaningful influence, and that legal attribution can attach to their conduct. From this perspective, the problem is not that centres of attribution have disappeared, but that they have become less visible and must be identified through more sophisticated analytical methods. This counter-position deserves serious engagement. The question, however, is whether the centres of attribution that regulators and courts manage to identify within decentralized ecosystems are structurally equivalent to those presupposed by traditional legal paradigms, or whether they represent a qualitatively different – and potentially less stable – form of legal anchoring. The functional identification of *de facto* controllers, while practically useful, may not fully substitute for the formal, institutionally defined centres that underpin the systematic operation of legal order[49].

To address this need for research, it is necessary to verify that decentralization does not hinder but rather facilitates the achievement of the constitutional objectives of centralized legal systems. In addition, it is key to ensure that this technological decentralization does not erode the fundamental principles and values upon which Constitutions are founded. In a technologically decentralized context, power is not merely granted but rather intercepted through solutions that begin with fragmentation and ultimately converge towards unity. This approach stands in contrast to the more conventional top-down approach, where power is assumed and then organised to serve the community.

3.1. The theoretical facilitation of constitutional ideals

Having examined the fundamental challenges that decentralization poses to traditional legal paradigms – the displacement of foundational symbolics, the deterritorialization of authority, the elusiveness of jurisdiction, the paradoxes of legal subjectivity, and the resistance to centres of attribution – we must now consider the normative claims made on behalf of blockchain technology. Proponents argue that decentralized systems may facilitate certain constitutional ideals even as they challenge traditional legal structures. This subsection examines these claims while maintaining critical awareness of tensions with the preceding critique.

48. Werbach 2018, particularly chapters 4–6, where the author argues that blockchain systems generate new forms of trust rather than eliminating the need for institutional anchoring. See also Cengiz 2023, who observes that the governance structures of ostensibly decentralized protocols consistently converge towards identifiable centres of decision-making.

49. For a nuanced analysis of the gap between functional and formal centres of attribution, see De Filippi–Mannan–Reijers 2022, who characterise blockchain technology as "alegal" – operating in a space that is neither fully within nor fully outside the legal order, and therefore requiring novel conceptual tools rather than mere adaptation of existing ones.

Decentralization, in its ideal form, embodies features that resonate strongly with modern constitutional and democratic ideals, particularly concerning transparency, efficiency, and participation.

One primary objective of any modern legal system is to ensure predictable, fair, and accountable governance. Decentralization proponents argue that the technology achieves this through algorithmic transparency and the elimination of traditional "Single Points of Failure" associated with human-centric centralized institutions. According to this perspective, the use of open-source code and on-chain records in decentralized systems ensures data is publicly verifiable and difficult to manipulate. This enhances accountability by allowing real-time monitoring of decisions and financial flows, an objective that many state-based systems struggle to meet, especially in complex bureaucratic or financial operations[50]. Decentralization would aim to disperse power away from a central entity that might otherwise be susceptible to regulatory capture, corruption, or misuse of power. This would align with the constitutional goal of preventing authoritarian drift and ensuring that the government is subject to the rule of law[51].

Moreover, decentralized applications (dApps) and DAOs, which promote models of direct and collaborative decision-making, would offer new ways to realise the constitutional ideals of political participation and effective justice. DAOs and platforms like *Kleros* and *Jur* would enable liquid democracy and collective dispute resolution, leveraging consensus mechanisms to govern resource allocation and resolve conflicts. This can be interpreted as facilitating participatory governance, enhancing citizen involvement beyond traditional representative structures. Decentralized dispute resolution systems specifically target low-value, high-volume transactions, providing affordable mechanisms to solve "micro-claims" that often lack affordable recourse in traditional, expensive court systems. This expands access to justice, a core constitutional objective.

3.2. The fundamental conflict with constitutional prerequisites

Despite these potential benefits, the core claim of technological decentralization fundamentally clashes with essential constitutional objectives, particularly those concerning sovereignty, legal certainty, and accountability.

Constitutional systems presuppose the existence of ultimate authority – a sovereign capable of making binding collective decisions and resolving conflicts authoritatively. Decentralized systems resist this requirement. By design, they lack ultimate authority: no entity can unilaterally modify protocols, reverse transactions, or resolve disputes authoritatively. This refusal of sovereignty is presented as a virtue – liberation from hierarchical power. Nevertheless, it creates fundamental problems for constitutional governance. How are constitutional amendments adopted? How are irreconcilable conflicts resolved? How is the boundary between permissible and impermissible conduct authoritatively determined?

Constitutional authority traditionally operates through territorial jurisdiction: the State exercises sovereign power within defined borders. As seen, Blockchain aspires to transcend such territorial limitations, creating legal orders without geographic anchoring. However, this deterritorialization should eliminate one of constitutionalism's foundational mechanisms: the definition of a political community bound together by shared subjection to common authority.

Moreover, governance rights derive from token ownership, which reflects economic power rather than equal citizenship. The initial distribution of tokens typically occurs through sales or airdrops that favour early participants, insiders, or those with capital to invest – not through any process claiming democratic legitimacy. Subsequent distributions through the market further concentrate tokens in the hands of those with greater resources. "Governance by numbers"[52] replaces deliberative democracy with algorithmic aggregation of preferences but eliminates the deliberative process through which preferences are formed, refined,

50. Nabben 2023; De Filippi–Wright 2018; Werbach 2018.

51. Reijers–Mannan–De Filippi 2024; Atzori 2017; De Filippi–Loveluck 2016; Mumford 1964.

52. Rouvroy–Berns 2013.

and synthesised into collective judgments. Cloud communities and opt-in systems allow fragmentation: those who disagree can exit rather than compromise. While this may satisfy individuals' preferences, it abandons the constitutional project of constructing shared frameworks for collective life despite disagreement.

Empirically, ostensibly decentralized systems often exhibit significant power concentration. Core developers exercise disproportionate influence over protocol evolution: while anyone can formally propose changes, practical authority resides with those possessing technical expertise and credibility within developer communities. Their decisions about which improvements to implement, which bugs to prioritise, and how to respond to crises shape system evolution more profoundly than token holder votes. Token distribution patterns reveal similar concentration. "Whales" – holders of prominent token positions – dominate governance outcomes when they choose to participate. Analysis of DAO voting patterns consistently shows highly unequal participation and influence[53].

These distributional inequities may give rise to oligarchic governance structures beneath decentralization's egalitarian rhetoric[54]. The plutocratic character of token voting means that those who already possess wealth can entrench their advantages by controlling protocol governance, putting them in a position to evade accountability. By disclaiming the existence of any controlling party, they deny that anyone owes fiduciary duties. Token holders disclaim responsibility despite exercising governance rights. Developers claim merely to propose code changes that others are free to reject. Platform operators assert they simply facilitate access to decentralized protocols. Everyone disclaims control, yet collectively the system operates and produces consequences for participants. This structure creates a moral hazard: those who exercise effective control over systems escape the legal obligations traditionally accompanying such power. They enjoy the benefits of governance participation – the ability to shape protocols in ways that advantage their interests – without bearing corresponding responsibilities to those affected by their decisions.

The enforcement blind spots discussed in Section 2 compound these accountability deficits. Even when legal duties theoretically attach, enforcement proves difficult or impossible when responsible parties cannot be identified or when their pseudonymity and distributed coordination frustrate the legal process.

4. The necessity of hybridisation and legal anchoring

This analysis demonstrates that pure decentralization risks undermining constitutional accountability mechanisms. Consequently, pragmatic approaches favor hybrid arrangements that leverage blockchain's technical advantages while preserving essential legal safeguards.

DLTs require institutional and legal anchors to function responsibly within the broader economy. As a result, the approach so far has primarily been for law to engage actively with these new organisational solutions, as the Ricardian contract approach confirms, enabling smart contracts to function seamlessly within established legal frameworks. Another adaptation is to evolve regulatory frameworks to ensure that technological innovations can coexist with traditional legal functions. Jurisdictions are tasked with defining rules that establish the functional equivalence of these technologies, all while safeguarding fundamental rights. An exemplary initiative highlighting this need is the EU's DLT Pilot Regime, which mandates the presence of an identifiable and liable operator for DLT market infrastructures[55]. This requirement underscores the importance of having a centralized, accountable entity that can interface with the legal system, even within decentralized contexts. Another solution to gain traction is to address governance through a polycentric lens[56]. This means recognising that multiple governing

53. Fritsch–Müller–Wattenhofer 2024; Nabben 2023.

54. Messias–Ide 2025; Weidener–Laredo–Kumar–Compton 2025; Messias–Pahari–Chandrasekaran et al. 2023.

55. Regulation (EU) 2022/858; Zaccaroni 2022.

56. European University Institute 2024; Gazi–Treccani–Morini–Sahdev 2022; Carlisle–Gruby 2019; Aligica–Tarko 2012; Ostrom 2010.

bodies – spanning local, national, international, and private decentralized networks – must interact and coordinate effectively. Establishing clear rules for how on-chain regulations align with off-chain national or international laws becomes crucial in this framework.

Concrete examples from the financial sector illustrate the practical necessity of such hybridisation. The experience of decentralized lending protocols such as *Aave* and *Compound* demonstrates that, even within architectures designed to eliminate intermediaries, governance structures progressively re-centralise around identifiable actors. *Aave*'s governance framework, for instance, relies on a delegated voting system in which a small number of prominent delegates exercise disproportionate influence over protocol parameters. Similarly, blockchain-based supply chain management initiatives – such as those deployed in the agri-food sector for traceability and food safety certification – have required the identification of responsible data custodians and legal guarantors to satisfy regulatory requirements under EU food safety law (Regulation (EC) 178/2002). These cases confirm that the integration of decentralized technologies into legally regulated domains invariably demands the reconstitution of identifiable centres of attribution[57].

Nevertheless, efforts to harness the benefits of decentralization without reverting to a pre-political state dominated by unaccountable private interests require deliberate and constructive cooperation with existing legal structures. Such cooperation should prioritize regulations that mandate governance transparency, enforce accountability, and protect fundamental rights. Embracing decentralization should be viewed as an organizational theory that enhances the effectiveness of the legal order, rather than as a standalone political theory capable of supplanting it.[58] The solution is necessarily multi-layered, involving both the adaptation of existing legal frameworks and the strategic introduction of new, technology-aware legal and institutional mechanisms. This approach seeks to balance the code-based *lex cryptographia* with the state-based rule of law.

5. Beyond functional equivalence: the imperative of institutional innovation

The nature of decentralized systems, transcending territorial boundaries and relying on code for execution, would demand flexibility in legal classification and execution.

For tokenization, legal fitness requires moving beyond rigid conceptual definitions towards a functional analysis. Tokens are often polyhedric, potentially fulfilling multiple legal roles depending on their characteristics and the context[59]. While technological neutrality and functional equivalence provide the indispensable lens for jurists to analyse and classify new digital phenomena, they function best when the latest technology aligns with existing institutional logic (e.g., highly centralized, entity-based DLTs). When encountering truly disruptive elements – such as the inherent probabilistic finality of PoW consensus[60], the anonymity of users, or the anti-institutional ethos of DAOs – these principles reveal their inadequacy. They provide a descriptive analysis (what the technology *does* economically) but falter in prescribing solutions for the new normative concerns (how to assign accountability and ensure justice when political and territorial constraints are deliberately circumvented).

The theoretical and practical implications suggest that regulatory frameworks need to adopt a nuanced approach. First and foremost, it is essential to embrace functional regulatory standards. However, it is not a convincing argument that regulations should focus on the economic activities being performed rather than the technological specifics, such as defining a token as a security irrespective of its underlying code. Additionally, there is a need to mandate legal bridges that address the challenges posed to core legal principles like property rights, liability, and finality. The law should actively work to create these "legal links", which may involve establishing new legal categories for decentralized entities and categories or explicitly connecting on-chain technical realities to off-chain legal frameworks through complete tokenization.

57. On the re-centralisation dynamics in DeFi governance, see Fritsch–Müller–Wattenhofer 2024.

58. Achebe–Onyeka–Anyanwu–Umeh 2024.

59. ESMA 2019.

60. Barresi 2023; Nakamoto 2008.

Moreover, legal intervention must acknowledge the inherent trade-offs involved in these scenarios. Efforts to impose conventional accountability mechanisms, such as requiring a liable operator, could unintentionally undermine decentralization that these technologies aim to achieve, leading to increased centralization[61]. Therefore, the objective is not to achieve total technological integration but rather to foster a constructive dialogue in which legal safeguards are introduced to uphold fundamental values, such as human dignity and fairness, within these emerging transnational regimes.

In conclusion, technological norms and functional equivalence are far from obsolete; instead, they need to be thoughtfully balanced with the introduction of tailored legal rules and institutional requirements, particularly in areas where technological design choices pose unique and unacceptable societal risks.

References

V.C. Achebe, M.C. Onyeka, A.C. Anyanwu, A.C. Umeh (2024), *Blockchain as a Legal Compliance Infrastructure: Reinventing Corporate Governance and Internal Control Systems*, in "International Journal of Scientific Research in Science and Technology", vol. 11, 2024, n. 4

P.D. Aligica, V. Tarko (2012), *Polycentricity: From Polanyi to Ostrom, and Beyond*, in "Governance", vol. 25, 2012, n. 2

M. Anus, A. Allauddin (2025), *The Legal Fiction Of "Decentralization": How DAOs Are Accidentally Creating Unregulated Financial Entities*, in SSRN, 2025

S. Aramonte, W. Huang, A. Schrimpf (2021), *DeFi Risks and the Decentralisation Illusion*, in "BIS Quarterly Review", 2021

M. Atzori (2017), *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, in "Journal of Governance and Regulation", vol. 6, 2017, n. 1

R.G. Barresi (2023), *The Evolution of the Finality of Payment or "How RTGSs, Instant Payment Systems, and DLT Platforms Change the Concept of Money"*, in F. Zatti, R.G. Barresi (a cura di), "Digital Assets and the Law", Routledge, 2023

K. Becker (2022), *Blockchain Matters – Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, in "Law and Critique", vol. 33, 2022, n. 2

S. Blemus (2018), *Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide*, in SSRN, 2018

B. Cappiello, G. Carullo (2021), *Introduction: The Challenges and Opportunities of Blockchain Technologies*, in B. Cappiello, G. Carullo (a cura di), "Blockchain, Law and Governance", Springer, 2021

K. Carlisle, R.L. Gruby (2019), *Polycentric Systems of Governance: A Theoretical Model for the Commons*, in "Policy Studies Journal", vol. 47, 2019, n. 4

F. Cengiz (2023), *Blockchain Governance and Governance via Blockchain: Decentralized Utopia or Centralized Dystopia?*, in "Policy Design and Practice", vol. 6, 2023, n. 4

CFTC (2023), *Statement of CFTC Division of Enforcement Director Ian McGinley on the Ooki DAO Litigation Victory*, 2023

F.P. Coutinho, M.L. Pires, B. Correia Barradas (2024), *Blockchain and the Law: Dogmatics and Dynamics*, T.M.C. Asser Press, 2024

P. De Filippi, B. Loveluck (2016), *The Invisible Politics of Bitcoin*, in "Internet Policy Review", vol. 5, 2016, n. 3

61. Werbach 2018.

P. De Filippi, M. Mannan, W. Reijers (2022), *The Alegality of Blockchain Technology*, in "Policy and Society", vol. 41, 2022, n. 3

P. De Filippi, A. Wright (2018), *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018

P. De Filippi, A. Wright (2015), *Decentralised Blockchain Technology and the Rise of Lex Cryptographia*, in SSRN, 2015

M. Doria, F. Bassan, M. Rabitti, A. Sciarrone Alibrandi, U. Malvagna (2024), *Caratteristiche degli smart contracts*, in "Questioni di Economia e Finanza (Occasional Papers)", 2024, n. 683

Q. DuPont (2017), *Experiments in Algorithmic Governance*, in "Bitcoin and Beyond", Routledge, 2017

ESMA (2025), *Joint EBA-ESMA Report on the recent developments in crypto-assets (Article 142 of MiCAR)*, in esma.europa.eu, 2025

ESMA (2019), *Advice on Initial Coin Offerings and Crypto-Assets*, in esma.europa.eu, 2019

V. Eubanks (2018), *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St. Martin's Press, 2018

European University Institute (2024), *Blockchain Technology and Polycentric Governance*, Publications Office of the European Union, 2024

S.E. Fish (1989), *Doing What Comes Naturally: Change, Rhetoric, and the Practice of Theory in Literary and Legal Studies*, Duke University Press, 1989

R. Fritsch, M. Müller, R. Wattenhofer (2024), Analyzing Voting Power in Decentralized Governance: Who Controls DAOs?, in "Internet Computing", vol. 28, 2024, n. 3

S. Gazi, M. Treccani, M. Morini, N. K. Sahdev (2022), *Blockchain as Commons: Applying Ostrom's Polycentric Approach to Blockchain Governance*, in SSRN, 2022

J. Grimmelmann (2021), *All Smart Contracts Are Ambiguous*, in "Journal of Law & Innovation", vol. 2, 2021, n. 1

J. Habermas (1999), *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*, MIT Press, 1999

P. Hacker (2024), *Proposal for a Directive on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence: Complementary Impact Assessment,* European Parliamentary Research Service Study, PE 762.861, 2024

H.L.A. Hart, L. Green (2012), *The Concept of Law*, 3rd edn, Oxford University Press, 2012

N.K. Hayles (1999), *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics*, University of Chicago Press, 1999

M. Hildebrandt (2018), *Algorithmic Regulation and the Rule of Law*, in "Philosophical Transactions of the Royal Society A", vol. 376, 2018, n. 2128

R. Houben, A. Snyers (2020), *Crypto-Assets – Key Developments, Regulatory Concerns and Responses*, PE 648.779, European Parliament, 2020

K. Hummler (2016), *Blockchain – der nächste Wohlstandsschock*, in "Neue Zürcher Zeitung", 2016

G. Itzcovich (2020), *"Something More Lively and Animated Than the Law": Institutionalism and Formalism in Santi Romano's Jurisprudence*, in "Ratio Juris", vol. 33, 2020, n. 2

D.R. Johnson, D.G. Post (1997), *Law And Borders – The Rise of Law in Cyberspace*, in SSRN, 1997

H. Kelsen (1945), *General Theory of Law and State*, Harvard University Press, 1945

T. Lai (2021), *Blockchain, Law and Governance: General Conclusion*, in B. Cappiello, G. Carullo (eds.), "Blockchain, Law and Governance", Springer, 2021

L. Lessig (2006), *Code: Version 2.0*, 2nd edn, Basic Books, 2006

E.D. Martino, W.G. Ringe (2024), *The Social Cost of Blockchain: Externalities, Allocation of Property Rights, and the Role of the Law*, Institute of Law and Economics Working Paper 2024 No. 80, 2024

J. Messias, A. Ide (2025), *Fairness in Token Delegation: Mitigating Voting Power Concentration in DAOs*, in arXiv, 2510.05830, 2025

J. Messias, V. Pahari, B. Chandrasekaran, K.P. Gummadi, P. Loiseau (2023), *Understanding Blockchain Governance: Analyzing Decentralized Voting to Amend DeFi Smart Contracts*, in arXiv, 2305.17655, 2023

L. Mumford (1964), *Authoritarian and Democratic Technics*, in "Technology and Culture", vol. 5, 1964, n. 1

K. Nabben (2023), *Blockchain Governance: Accountability in Decentralised Technology Communities*, in Kelsie – on the cataclysmia of digital infrastructure – Substack, 2023

N. Naffine (2009), *Law's Meaning of Life: Philosophy, Religion, Darwin and the Legal Person,* Bloomsbury Publishing, 2009

S. Nakamoto (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008

L. Orgad (2018), *Cloud Communities: The Dawn of Global Citizenship?*, in Globalcit, 2018

E. Ostrom (2010), *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, in "American Economic Review", vol. 100, 2010, n. 3

C. Poncibò (2021), *Blockchain and Comparative Law*, in B. Cappiello, G. Carullo (eds.), "Blockchain, Law and Governance", Springer, 2021

W. Reijers, M. Mannan, P. de Filippi (2024), *The Emergence of Blockchain Constitutionalism*, in G. De Gregorio, O. Pollicino, P. Valcke (eds.), "The Oxford Handbook of Digital Constitutionalism", Oxford University Press, 2024

A. Rouvroy, T. Berns (2013), *Gouvernementalité Algorithmique et Perspectives d'émancipation*, in "Réseaux", vol. 177, 2013

L.H. Scholz (2017), *Algorithmic Contracts*, in "Stanford Technology Law Review", vol. 20, 2017

W. Thysse (2025), *Decentralized Law: The Power of Blockchain to Transform the Broken Legal System*, Thysse Publishing, 2025

P. Ungureanu, F. Bellesia, C. Cochis (2025), *Dealing with Blame in Digital Ecosystems: The DAO Failure in the Ethereum Blockchain*, in "Technological Forecasting and Social Change", vol. 215, 2025

M. Verstraete (2020), *The Stakes of Smart Contracts*, in "Loyola University Chicago Law Journal", vol. 50, 2020, n. 3

C. Watters (2023), *When Criminals Abuse the Blockchain: Establishing Personal Jurisdiction in a Decentralised Environment*, in "Laws", vol. 12, 2023, n. 33

L. Weidener, F. Laredo, K. Kumar, K. Compton (2025), *Delegated Voting in Decentralized Autonomous Organizations: A Scoping Review*, in "Frontiers in Blockchain", vol. 8, 2025

K. Werbach (2018), *The Blockchain and the New Architecture of Trust,* MIT Press, 2018

G. Zaccaroni (2022), *Decentralized Finance and EU Law: The Regulation on a Pilot Regime for Market Infrastructures Based on Distributed Ledger Technology*, in "European Papers", vol. 7, 2022

D.A. Zetzsche, R.P. Buckley, D. W. Arner, L. Föhr (2018), *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*, in SSRN, 2018