Blockchain Technology and the Rule of Code: Regulation via Governance

Primavera de Filippi, Morshed Mannan, Wessel Reijers

Blockchain Technology and the Rule of Code: Regulation via Governance

Primavera De Filippi, CNRS / Harvard

Morshed Mannan, European University Institute

Wessel Reijers, University of Vienna

Abstract:

Blockchain-based systems, by virtue of their technological features, present challenges to the rule of law. These systems work in a transnational and decentralised fashion, often with pseudonymous user identities, executing code autonomously without the possibility of coercion by any single operator. This article argues that blockchain-based systems challenge the rule of law by means of a move towards the rule of code. First, it analyses the analogy between the rule of law and the rule of code, by distinguishing them from the rule by law and rule by code. This analysis evaluates the extent to which the technical features of blockchain-based systems make them particularly difficult to regulate by traditional legal means, contrasting the example of TheDAO with the newer example of BadgerDAO. Second, the article identifies ways in which lawmakers can respond to the rule of code within a global pluralist, polycentric legal system. After distinguishing on-chain and off-chain governance, the paper builds on Lessig's four modes of regulation to offer two pathways for regulating blockchain technologies: the regulation by code approach, which aims to impose legal responsibilities and liabilities on operators of blockchain networks, and the regulation via governance approach, which uses legal pressure points to influence the social norms that govern blockchain communities. *[206 word version]*

Blockchain-based systems work in a transnational and decentralised fashion, often with pseudonymous user identities, executing code without the possibility of coercion by any single operator. This article argues that blockchain-based systems challenge the rule of law by moving towards the rule of code. First, it analyses the analogy between the rule of law and the rule of code, and outlines the technical features that make blockchain systems particularly difficult to regulate by traditional legal means. Second, the article identifies ways in which lawmakers can respond to the rule of code within a global pluralist, polycentric legal system. We build on Lessig's four modes of regulation to offer two pathways for regulating blockchain technologies: the regulation by code approach, which aims to impose legal responsibilities on operators of blockchain networks, and the regulation via governance approach, which uses legal pressure points to influence the social norms that govern blockchain communities. *[150 word version]*

Keywords: blockchain technology, legal theory, rule of law, rule of code, regulation by code, polycentric governance

Introduction

In the early days of the Internet, the academic community introduced the notion of *lex informatica* to illustrate the idea that code is increasingly used as a way to regulate online behaviour.[1] At that time, it was generally believed that regulation by code would ultimately prevail over regulation by law,[2] because the decentralised nature of the Internet network made it initially difficult—if not impossible—for any centralised authority to enforce the law.[3] Internet pioneers, like Timothy May and John Perry Barlow, went as far as to claiming that governments did not have the right nor the legitimacy to regulate cyberspace.[4] Similarly, while investigating the regulation of cyberspace, David Post introduced the notion of 'unregulability' to highlight the complexities inherent in the regulation of a decentralised and transnational network like the Internet.[5] Yet, it soon became clear that many of these claims were overly ambitious: over time, the Internet became an increasingly concentrated system, which is nowadays controlled by a few large incumbents—Internet service providers and large online operators—to which the law can be effectively applied and enforced.[6]

After the Internet, blockchain technologies are now hailed as a new mechanism to escape territorial and governmental regulations. Indeed, if we look at the claims of early blockchain advocates,[7] we may notice that they are quite similar to those of the early Internet pioneers: the decentralisation inherent in the technological design of many blockchain-based systems is such as to promote a more distributed governance, and reduce the risks of surveillance or control from centralised power structures—be they private companies or governmental authorities.[8] Moreover, because of their distinctive characteristics, blockchain platforms are sometimes described as being '*alegal*' in that they—allegedly—operate beyond

[1] Joel Reidenberg, 'Lex Informatica: The Formulation of Information Policy Rules through Technology' (1997) 76 *Texas Law Review* 553, 555.
[2] James Lewis, 'Sovereignty and the Role of Government in Cyberspace' (2010) 16 *The Brown Journal of World Affairs* 55.
[3] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006) xii.
[4] Peter Ludlow, 'New Foundations: On the Emergence of Sovereign Cyberstates and Their Governance Structures' in Peter Ludlow (ed.), *Crypto Anarchy, Cyberstates, and Pirate Utopias* (MIT Press 2001) 1, 4.
[5] David Post, 'Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace' [1995] *Journal of Online Law* 1, para 42.
[6] John Palfrey, 'Four Phases of Internet Regulation' (2010) 77 *Social Research* 981, 990-991.
[7] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) <https://bitcoin.org/bitcoin.pdf> accessed 4 March 2022; Lana Swartz, 'What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology' (2018) 32 *Cultural Studies* 623, 629.
[8] Quinn DuPont, *Cryptocurrencies and Blockchains* (Polity Press,2019) 34, 40-41.

the purview of the law.[9] Both the blockchain protocol and the software code deployed onto a blockchain infrastructure can therefore be regarded as a new means to regulate behaviours: a more powerful form of *lex informatica* which has been referred to as *lex cryptographica*.[10] This article aims to generate a deeper understanding of the new governance structures that emerge out of blockchain-based systems, and formulate ways in which policymakers might address this new mode of non-state regulation.

The main contribution of this article is anchored on its novel approach to describe the rules instantiated by blockchain technology as a new type of regulation governed by the 'rule *of* code' (by analogy with the 'rule of law') that distinguishes itself from the rules established by traditional centralised Internet platforms, which are 'ruled *by* code' (by analogy with the 'rule by law'). Other blockchain scholars have already investigated the specificity of blockchain rules by drawing a distinction between Lessig's 'code is law'[11] and the more blockchain-specific approach to 'law is code'[12]; between the conventional 'code of law' produced and enforced by national legal systems and the emergent "code as law" established by the internal rules of blockchain systems;[13] and between traditional political institutions and blockchain-based systems characterised by the capacity of the 'code to run itself.'[14] Yet, most of the contributions are focused on the distinction between *regulation by law* and *regulation by* (blockchain) *code*, with regard to their intrinsic properties (i.e. natural language vs. formal computable language; amendability vs. immutability; ex-post third-party enforcement vs. ex-ante automated enforcement, etc.). This article builds upon the notion of 'rule of code', first introduced by De Filippi & Wright in *Blockchain and the Law* (2018),[15] and expands it to explore the specificities of blockchain code with regard to its relationship to sovereignty that make it different from more traditional software code. Its aim is to demonstrate that the rules enshrined in a blockchain-based system exhibit an additional feature that distinguish them from other software systems (i.e., those ruled by code) in that these rules apply equally to all (i.e., no one is above the code) rather than being instrumental to the interests of a particular person or company, who stands above the code.

Specifically, this article draws on the scholarship on (global) legal pluralism to argue that blockchain-based systems support the emergence of autonomous legal orders that

---

[9] Primavera De Filippi, Morshed Mannan, and Wessel Reijers, 'The alegality of blockchain technology' (2022) 41 *Policy and Society* 358.

[10] Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (2015) SSRN Research Paper No. 2580664/2015 <https://ssrn.com/abstract=2580664> accessed 4 March 2022.

[11] Lawrence Lessig, 'Code is law' (Harvard Magazine, 1.1.2000), <https://www.harvardmagazine.com/2000/01/code-is-law-html> accessed 15 September 2022.

[12] Primavera de Filippi and Samer Hassan, 'Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code' [2016] 21 *First Monday* <https://doi.org/10.5210/fm.v21i12.7113> accessed 15 September 2022.

[13] Karen Yeung, 'Regulation by blockchain: the emerging battle for supremacy between the code of law and code as law' (2019) 82 *The Modern Law Review* 207.

[14] Wessel Reijers and others, 'Now the code runs itself: On-chain and off-chain governance of blockchain technologies' (2021) 40 *Topoi* 821.

[15] Primavera de Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018).

coexist—and to an extent compete—with the legal order of the state. Adopting a pluralist lens allows for a more nuanced appreciation of how each system shapes the behaviour of network participants, through their own modalities of regulation. Moreover, the literature on legal pluralism shows that instead of one legal order subordinating another, multiple legal orders can coexist and contest over the scope of application of their authority within a given jurisdiction.[16] In light of this, the article argues that, instead of trying to regulate blockchain-based systems with the same regulatory techniques that have previously been used for the regulation of the Internet, endogenous practices of polycentric governance could be regarded as more appropriate.

The article is organised as follows. Part I bridges the literature between Internet governance and blockchain governance by identifying the technical features of blockchain technology that make it harder to regulate than traditional Internet platforms. Through a comparison between the Internet and blockchain technology concerning the extent to which these technologies resist traditional regulation, the paper draws a distinction between two different modes of regulation—*regulation by law* and *regulation by code*—which are often combined in the context of both public and private ordering as an attempt to govern and regulate the digital space. The paper subsequently introduces the notion of the 'rule of code' as an alternative to the notion of the 'rule of law'. It argues that, to the extent that blockchain technology can support the emergence of decentralised platforms that operate autonomously and independently from any centralised authority, the technology introduces a novel modality of regulation (*rule of code*) that is distinct from the more traditional form of regulation by code that pervades the Internet network (*rule by code*).

Part II uses Lessig's analysis of four regulatory levers (law, social norms, market mechanisms and architecture or code) to explore new pathways for policymakers to regulate blockchain-based systems. First, it illustrates the different facets of blockchain governance, focusing in particular on the distinction between "on-chain" and "off-chain" governance, and how regulation can impact each of these different governance structures. Second, the article shows that some of these regulatory pathways might rely on the *rule by code* to replicate the regulatory solutions proposed in earlier efforts to shape Internet governance (i.e., forcing intermediaries to leverage code as a regulatory tool)—in effect, a *regulation by code* approach. An alternate approach would recognise the specificities of the rule of code and therefore use a set of innovative governance practices that acknowledge the advent of blockchain as a transformative regulatory force, leveraging governance as a new mode of regulating blockchain technology. This is the *regulation via governance* approach.

[16] Gunther Teubner, 'Global Bukowina: Legal Pluralism in the World-Society' in G. Teubner (ed.) *Global Law without a State* (Dartmouth, 1997); J-P. Robé, 'Multinational Enterprises: The Constitution of a Pluralistic Legal Order' in G. Teubner (ed.) *Global Law without a State* (Dartmouth, 1997).

I. Blockchain Technology and the Rule of Code

How Blockchain Resists Regulation

A public blockchain can be broadly defined as a decentralised database or public ledger that is replicated on a decentralised peer-to-peer network and that operates without any centralised authority.[17] Most blockchain-based networks were originally public and permissionless, in the sense that anyone could freely join the network and participate in the process of verifying and validating the set of transactions that will eventually be recorded into the decentralised database. Yet, as large companies and commercial operators began to show more interest in adopting the technology, new typologies of blockchain-based networks emerged, which can be private (i.e., only accessible by authorised people) and permissioned (i.e., only a pre-identified set of operators are entitled to participate in maintaining and securing the network). For the purpose of this article, we will focus specifically on public and permissionless blockchains, as it is these that raise the most interesting challenges in terms of both governance and regulation.

Like the Internet, public and permissionless blockchain-based networks are both global and transnational, and they often do not account for national boundaries.[18] As a copy of the blockchain is replicated on the computer of every network node, blockchain-based networks are highly resilient and extremely difficult to shut down. As long as one copy of the blockchain exists, it will be possible to replicate the network from scratch.[19]

Alongside their decentralised and transnational character, blockchain networks are generally considered to be *tamper-resistant*, because, once a piece of information has been recorded on the blockchain, it can no longer be modified or deleted.[20] This is because a blockchain is an append-only data structure, where data can be added according to specific criteria, but can never be edited or removed.[21] Any unilateral modification will be automatically detected by other nodes.[22] As a consequence, no government or other authority can effectively prescribe the erasure or modification of data recorded on a blockchain.

Moreover, as opposed to traditional online platforms, whose internal operations generally remain opaque to the users, most public blockchains are inherently *transparent:* both their protocol and consensus algorithm are known to every node in the network, and generally also to the public at large.[23] This is because the distributed consensus of a blockchain requires network nodes to constantly check and verify the validity and legitimacy

[17] Nakamoto (n 7).
[18] De Filippi and Wright (n 10) 56.
[19] Melanie Swan, *Blockchain: Blueprint for a New Economy* (O'Reilly 2015) x, 32.
[20] Zibin Zheng and others, 'An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends' *2017 IEEE International Congress on Big Data (BigData Congress)* (IEEE 2017) 559.
[21] Nakamoto, (n 7).
[22] Zibin Zheng and others, 'Blockchain Challenges and Opportunities: A Survey' (2018) 14 *International Journal of Web and Grid Services* 352, 357.
[23] Swan, (n 14) 1.

of everyone else's transactions.[24] In addition, as all blockchain transactions are cryptographically signed with the key of the party executing them, they are forever associated with that party.[25] This means that, to the extent that the transaction has been signed by a valid private key, the owner of that key cannot subsequently deny having executed that particular transaction (unless he or she can prove that the key was compromised). Yet, to protect the privacy and confidentiality of transactions, some blockchains—e.g., Monero and Zcash—have adopted specific cryptographic primitives,[26] such as ring signatures or zero-knowledge proofs to guarantee the validity of blockchain transactions without ever disclosing the source, the destination, or even the content of such transactions.[27]

Public and permissionless blockchains are always and necessarily *pseudonymous*, in the sense that anyone can join and operate the network without having to disclose their real identity.[28] People willing to use the network need only to create a public-private key pair in order to generate a public address through which they will be able to pseudonymously interact with the network—even though ownership of cryptocurrency is usually a precondition for executing transactions on the network.[29]

Many blockchains are not limited to recording transaction data or information, they also make it possible to store and execute software code that will run with a *guarantee of execution*—i.e., no one can unilaterally modify, influence or even stop the execution of that code.[30] This makes it possible to create decentralised applications that do not run on a centralised server, but rather are executed in a distributed and deterministic manner by all the network nodes.[31] These applications are generally referred to as 'smart contracts'—a term that refers generically to any snippet of code deployed on a blockchain.[32]

Finally, one important element that characterises public and permissionless blockchain networks is the *lack of coercion* on the part of a single operator. Traditional web

---

[24] Juri Mattila, 'The Blockchain Phenomenon - The Disruptive Potential of Distributed Consensus Architectures' (2016) ETLA Working Paper No. 38, 6-7 <https://www.econstor.eu/bitstream/10419/201253/1/ETLA-Working-Papers-38.pdf> accessed 4 March 2022.

[25] Imran Bashir, *Mastering Blockchain: Distributed Ledgers, Decentralization and Smart Contracts Explained* (Packt 2017) 24.

[26] Eli Ben Sasson and others, 'Zerocash: Decentralized Anonymous Payments from Bitcoin' (2014) *2014 IEEE Symposium on Security and Privacy* (IEEE, 2014) 459; Licheng Wang and others 'Cryptographic primitives in blockchains' (2019) 127 *Journal of Network and Computer Applications* 43, 45-46; Shen Noether, Adam Mackenzie and the Monero Research Lab, 'Ring Confidential Transactions' (2016) 1 *Ledger* 1, 3.

[27] Ronald Rivest, Adi Shamir and Yael Tauman, 'How to Leak a Secret' in Colin Boyd (ed.) *Advances in Cryptology — ASIACRYPT 2001. ASIACRYPT 2001. Lecture Notes in Computer Science, vol 2248* (Springer, 2001); Xiaoqiang Sun and others, 'A Survey on Zero-Knowledge Proof in Blockchain' (2021) 35 *IEEE Network* 198.

[28] Roy Lai and David Chuen, 'Blockchain - From Public to Private' in David Chuen and Robert Deng (eds.) *Handbook of Blockchain, Digital Finance, and Inclusion, vol. 2* (Academic Press 2019) 147, 165.

[29] Tao Feng and others, 'Research on Privacy Enhancement Scheme of Blockchain Transactions' (2019) 2 *Security and Privacy* 1, 2, 12.

[30] Massimo Bartoletti and Livio Pompianu, 'An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns' in Michael Brenner and others (eds.) *Financial Cryptography and Data Security* (Springer 2017) 494.

[31] Siraj Raval, *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology* (O'Reilly 2016) 7.

[32] Nick Szabo, 'Formalizing and Securing Relationships on Public Networks' [1997] 2 *First Monday* <https://doi.org/10.5210/fm.v2i9.548> accessed 15 September 2022.

services are controlled by online operators who are responsible for making the relevant design choices for the interface through which users interact with the platform. As such, they have the power to (often) unilaterally decide to impart changes to the interface to influence what users can or cannot do on these platforms. Because they can impose these choices directly onto their users, users are left with the limited choice of either accepting these changes or leaving the platform altogether.[33] In contrast, the rules of a blockchain-based network cannot be changed without the agreement of the users. Any protocol change requires active participation of the network nodes, who are expected to upgrade their clients in order to abide by the new protocol. Refusal to accept the new protocol rules will result in the maintenance of the original blockchain protocol and/or the emergence of a new blockchain-based network that constitutes a fork of the previous network.

In light of these characteristics, it becomes clear why blockchains, and other decentralised applications, distinguish themselves from more traditional and centralised online applications.[34] As Lessig puts it, in cyberspace, "code is law" because it actually assumes the same functionalities as law.[35] However, in most of the existing online platforms, the code remains under the control of the platform operators, which are required to comply with the law of the jurisdiction they operate in.[36] In the context of blockchain-based applications, code also constitutes a means to regulate behaviours: both the blockchain protocol and the smart contract code will determine what can or cannot be done with a particular blockchain network.[37] The difference is that, given the distinctive features and specificities of blockchain technology, blockchains can be used to create and deploy self-executable systems and autonomous software that operate independently of any centralised operator—and that may, consequently, largely ignore the law.[38] The pseudonymity of those who transact on a blockchain make it difficult for regulators to identify who should be subject to orders and sanctions in the event of a transaction that is deemed to be illegal.[39] Even more critically, given the immutability and tamper-resistant features of a blockchain, the mere act of creating or amending legislation to penalise these blockchain transactions is, on its own, insufficient to reverse them.

The supremacy of blockchain code over the discretionary power of online operators has two important implications for the governance and regulation of blockchain-based systems. First of all, the delegation of power from online operators to blockchain code has led people to describe blockchain technology as a "*trustless*" technology that could reduce the need for online intermediaries or other trusted authorities.[40] The claim is that blockchain technology takes trust away from centralised operators, and distributes it towards the

[33] Morshed Mannan and Nathan Schneider, 'Exit to Community: Strategies for Multi-Stakeholder Ownership in the Platform Economy' (2021) 5 *Georgetown Law Technology Review* 1.
[34] De Filippi and Wright (n 15) 3.
[35] Lawrence Lessig, *Code version 2.0* (Basic Books 2006) 5.
[36] Lawrence Lessig, 'Law Regulating Code Regulating Law' (2003) 35 *Loyola University Chicago Law Journal* 1, 8-9.
[37] De Filippi and Hasan (n 12).
[38] De Filippi, Mannan, and Reijers (n 9).
[39] Georgios Dimitropoulos, 'The Law of Blockchain' (2020) 95 *Washington Law Review* 1117, 1182.
[40] Gili Vidan and Vili Lehdonvirta, 'Mine the Gap: Bitcoin and the maintenance of trustlessness' (2019) 21 *New Media & Society* 42, 47.

underlying peer-to-peer network. Accordingly—the argument goes—as long as we can have "confidence" in the technology (i.e., as long as we can expect that a particular blockchain-based network will operate as planned), we might no longer need to rely on any trusted authority.[41] At the same time, the supremacy of code increases the *autonomy* of blockchain-based systems with regard to traditional forms of authority—whether these relate to government regulation and public ordering, or private ordering via contractual and technological means.[42] Once a new code-based system has been deployed on a blockchain, it can continue to operate autonomously and independently of the will of the parties who have deployed them.[43] The forfeiture or seizure of private keys that allow persons to access their wallets may allow government authorities to seize cryptocurrencies and other tokens, but in and of itself, this does not allow them to wrest control over these applications. While online operators (or regulators) can shut down the centralised interface that provides access to these applications (i.e., the platforms and frontends used to access and interact with the underlying blockchain-based networks), the blockchain applications themselves cannot be shut down: they will remain operative and become accessible again as soon as a new interface is developed.[44] The recent example of a US sanction on the Tornado Cash cryptocurrency 'mixer' illustrates this, as the smart contracts that pool and mix cryptocurrencies can still be accessed by users after the sanctions came into effect and its website went down.[45] In sum, targeting people or intermediary operators—whether through law or through technical measures—will not impact the autonomy of the underlying technical infrastructure.

It is the combination of these two characteristics—the apparently *trustless nature* of blockchain-based systems, and the *operational autonomy* of these systems—that makes them significantly different from the more traditional and centralised online platforms that have emerged from the Internet era. Although this may reduce the risk of an online operator unilaterally modifying the protocol of these decentralised applications, these very same characteristics might also lead to potential conflicts between a state's legal regime—what we refer to as the *rule of law*—and the technological rules enshrined within a particular blockchain-based system that needs to be respected by all network participants—what we refer to as the *rule of code*.[46]

---

[41] Primavera De Filippi, Morshed Mannan and Wessel Reijers, 'Blockchain as a confidence machine: The problem of trust & challenges of governance' (2020) 62 *Technology in Society* 1.
[42] De Filippi, Mannan, and Reijers (n 9).
[43] Usman Chohan, 'The Decentralized Autonomous Organization and Governance Issues' (2022) Critical Blockchain Research Initiative Discussion Paper Series: Notes on the 21st Century, <https://ssrn.com/abstract=3082055> accessed 15 September 2022.
[44] Note that most blockchain-based applications are being accessed (today, at least) by means of centralised web platforms. Even if no one can unilaterally tamper with the operations of these blockchain-based applications, intermediaries ultimately have the power to control what is being displayed on their platforms and how crypto-assets are disposed—and consequently have the ability to affect the manner in which people can or cannot interact with the underlying blockchain network. Yet, this does not preclude third-party operators from developing alternative web interfaces to the same application, or users personally holding cryptocurrencies in their own wallets, enabling people to interact more freely with the underlying network.
[45] US Department of Treasury, 'U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash' (8 August 2022), <https://home.treasury.gov/news/press-releases/jy0916>; gets qt, 'The Downside of Sanctioning Tornado Cash' (CoinDesk, 16 August 2022) <https://www.coindesk.com/layer2/2022/08/16/the-downside-of-sanctioning-tornado-cash/> accessed 2 October 2022.
[46] De Filippi and Wright (n 15) 206.

The Rule of Code vs. the Rule by Code

The concept of the rule of law—as popularised by Dicey—implies that.[47] There is no singular authoritative definition of the rule of law; yet, it is regarded as a fundamental constitutional principle in liberal democracies, which proclaims the supremacy of the law as a means to govern the interactions between individual citizens as well as between the government and its citizens.[48] Given the voluminous literature on the rule of law, it is not possible to provide an exhaustive overview of the subject. Instead, a concise discussion of the concept is provided for the purpose of relating the *rule of law* to the *rule by law* and subsequently, the *rule of code* and the *rule by code*.

The concept of the *rule of law* is often used to mean different things by different people.[49] Under English common law, the *rule of law* is intended to protect citizens against arbitrary political power exercised by the government or other public authorities. One of its main objectives is to separate law from politics.[50] The French and German legal systems also have their own interpretations of the *rule of law*:[51] *L'état de droit* leverages legal rules to limit the exercise of public powers, whereas the *Rechtsstaat* stipulates that all administrative powers are conferred by the law, and are thus also limited by it.[52] As a corollary, it is sometimes considered that one of the preconditions for upholding the *rule of law* is the separation of powers between the legislative, the judiciary, and the executive branches of the government.[53] Laws must be tested by the courts of law, who are responsible to verify that they do not fall afoul of a state's constitution.[54]

In established democracies, the *rule of law* is considered to be a valuable tool for assessing the legitimacy of a government,[55] which requires the internalisation of basic legal and political values by public institutions, and those who work for them.[56] In this context,

---

[47] Albert Dicey, *Introduction to the Study of the Law of the Constitution* (LibertyClassics, 1982 [1885]) 114.

[48] The United Nations provides one definition of the rule of law as: "a principle of governance in which all persons, institutions and entities, public and private, including the State itself, are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency." United Nations Security Council (UN SC) Report of the Secretary General on The Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies (23 August 2004) UN Doc. S/2004/616, 4.

[49] Judith Shklar, 'Political Theory and the Rule of Law' in Allan Hutchinson and Patrick Monahan (eds.) *The Rule of Law: Ideal of Ideology* (Carswell 1987), 1. Shklar highlights the historical relevance of the rule of law in the field of political theory, because of the political objectives it embodied. Today, however, she claims that "the rule of law has become meaningless thanks to ideological abuse and general over-use".

[50] Charles Montesquieu, *Complete Works, vol. 1, The Spirit of Laws* (T. Evans 1748) 198-201.

[51] John Bell, 'Comparative Administrative Law' in Mathias Reimann and Reinhard Zimmermann (eds.) *The Oxford Handbook of Comparative Law* (Oxford University Press 2016).

[52] ibid 1272.

[53] Kay Windthorst, 'Separation of Powers from the German Perspective' (2009) 47 *Duquesne Law Review* 905, 918; Paul Verkuil, 'Separation of Powers, the Rule of Law and the Idea of Independence' (1989) 30 *William & Mary Law Review* 301, 305-307.

[54] David Feldman, 'Democracy, the Rule of Law and Judicial Review' (1990) 19 *Federal Law Review* 1, 13.

[55] Mirko Canevaro, 'The Rule of Law as the Measure of Political Legitimacy in the Greek City States'(2017) 9 *Hague Journal on the Rule of Law* 211.

[56] Feldman (n 47), 11.

assessing whether a particular system complies with the *rule of law* requires accounting for at least the formal and procedural attributes of law: laws must be clear, stable and transparent, and they must be applied fairly, equally and evenly,[57] ideally by an independent judiciary.[58] For Hayek, the transparent announcement and prospective application of the law provides certainty about how authorities will use their coercive powers and thereby allows individuals to plan accordingly.[59] These criteria fulfil the 'thin' conceptions of the *rule of law*.[60] There are also 'thicker' interpretations of the rule of law, which consider substantive aspects of the law, such as social welfare rights, rights of dignity and justice, and the right to own private property.[61] Under that thicker conception, for the *rule of law* to exist, it is not enough that the law prevails over the rule by men,[62] but also that it respects a necessary set of normative conditions (e.g., economic liberalism), which guarantees its legitimacy. This more substantive version of the *rule of law* has been critiqued by Raz, among others, for blurring the distinction between the *rule of law* as a principle, and other concepts such as justice, human rights, etc.[63] It is also unclear which substantive requirements should be included in this thicker conception of the *rule of law*.

For the purpose of this paper, we are primarily concerned with the 'thin' conception of the *rule of law,* taken to entail a government that rules by, and is itself ruled by the law. In this sense, the rule of law can be seen as having both an *enabling* and *constraining* power with regard to the sovereign. It is a principle that requires the law to be obeyed and applied equally to everyone,[64] and it also minimises the risk of arbitrary power being exercised by the sovereign.[65]

The *rule of law* stands in contrast to the rule *by* law,[66] which refers to the instrumentalisation of law as a tool of political power. The *rule by law* has been extensively studied in the field of constitutional and administrative law,[67] often with reference to

[57] Paul Craig, 'Formal and substantive conceptions of the rule of law: an analytical framework' in Richard Bellamy (ed.) *The Rule of Law and the Separation of Powers* (Routledge, 2005), 95, 97; *see also* Jeremy Waldron, 'The Rule of Law and the Importance of Procedure' (2011) 50 *Nomos* 3; Joseph Raz, *The Authority of Law: Essays on Law and Morality* (Oxford University Press 1977); Lon Fuller, *The Morality of Law* (Yale University Press 1964).

[58] David Boies, 'Judicial Independence and the Rule of Law' (2006) 22 *Washington University Journal of Law & Policy* 57, 58; Helmke and Rosenbluth, in contrast, argue that judicial independence is not a precondition for the rule of law nor does it automatically lead to the upholding of the rule of law. Gretchen Helmke and Frances Rosenbluth, 'Regimes and the Rule of Law: Judicial Independence in Comparative Perspective' (2009) 12 *Annual Review of Political Science* 345, 361.

[59] Friedrich Hayek, *The Road to Serfdom* (Routledge 1944) 75-76.

[60] Mathias Siems, *Comparative Law* (Cambridge University Press 2018) 339.

[61] Ugo Mattei and Laura Nader, *Plunder: When the Rule of Law is Illegal* (Wiley-Blackwell 2008) 14; Tom Bingham, *The Rule of Law* (Allen Lane 2010); Brian Tamanaha, *On the Rule of Law: History, Politics, Theory* (Cambridge University Press, 2004), 91, 112; Ronald Cass 'Property Rights Systems and the Rule of Law' in E. Colombatto, (ed.), *The Elgar Companion to the Economics of Property Rights* (Edward Elgar Publications 2004) 131.

[62] Alain Supiot, *Governance by Numbers: The Making of a Legal Model of Allegiance* (Hart 2017) 204.

[63] Raz (n 57) 211.

[64] Denise Wohlwend, *The International Rule of Law* (Edward Elgar 2021) 36.

[65] ibid 30.

[66] Tamanaha (n 61), 108.

[67] Ji Li, The Leviathan's Rule by Law (2015) 12 Journal of Empirical Legal Studies 815; Jeremy Waldron, 'Rule by law: a much maligned preposition' (2019) NYU School of Law, Public Law Research Paper No. 19-19, <http://dx.doi.org/10.2139/ssrn.3378167> accessed 2 October 2022.

authoritarian regimes.[68] It may be defined as a system of government in which the law does not apply equally to everyone; one where the sovereign remains 'above the law' and can therefore use the law to exercise its power over the executive, legislative and judicial branches of the government, as well as over the citizens which remain subject to the law. The *rule by law* thus only has an enabling power, but not a constraining power over the sovereign. While both the *rule of law* and the *rule by law* reflect an idealised conception of the relationship between politics and law[69]—whose interrelations are often more intertwined than they appear at first sight[70]—these two concepts remain useful as shorthands to illustrate the core theoretical and practical distinctions between two different regimes: under the rule *by* law, the sovereign (who stands above the law) lays down the rules that will govern society, with no accountability under existing laws;[71] conversely, under the rule *of* law, nobody (not even the sovereign) can rise above the law: 'all citizens are equal before the law and are entitled [...] to equal protection of the law'.[72]

On the Internet, most online platforms are administered by companies which, at their discretion, dictate the rules that underpin our online interactions.[73] These platforms operate like 'monocentric' political systems, where the prerogatives for determining and enforcing the rules are 'vested in a single decision structure that has an ultimate monopoly over the legitimate exercise of coercive capabilities'.[74] In the early days of the Internet, this was only a marginal issue, since the Internet was populated by small online operators, competing with one another in order to provide a more valuable service to the growing population of Internet users. While they had full control over the way in which users could interact on their platform,[75] this was in no way different from the way in which private firms inevitably dictate the rules that people must abide by within their private sphere of influence. It is only in the last decade that the Internet has become an essential infrastructure capable of delivering public services, acting as a complement—or even as a supplement—to those provided by governments or public authorities. And it is precisely at this juncture that the question of the *rule of law* on the Internet becomes pressing.

---

[68] Nóra Chronowski and Márton Varju, 'Two Eras of Hungarian constitutionalism: from the rule of law to rule by law' (2016) 8 *Hague Journal on the Rule of Law* 271; Ratna Balasubramaniam, 'Has rule by law killed the rule of law in Malaysia?' (2008) 8 *Oxford University Commonwealth Law Journal* 211.

[69] Most notably, critical legal scholar Roberto Unger rejects the assumption of a separation between law and politics, and contends that the fundamental assumptions of neutrality, generality, and predictability that underpin the rule of law are mere ideals that can never be achieved in the reality of life. Roberto Unger, *Law in Modern Society: Toward a Criticism of Social Theory* (Free Press, 1976) 179-180.

[70] Martin Shapiro and Alec Sweet, *On Law, Politics, and Judicialization* (Oxford, 2002) 2-3.

[71] Anthony Pereira, 'Of Judges and Generals: Security Courts under Authoritarian Regimes in Argentina, Brazil, and Chile' in Tom Ginsburg and Tamir Moustafa (eds.) *Rule by Law: The Politics of Courts in Authoritarian Regimes* (Oxford University Press, 2008) 50.

[72] Universal Declaration of Human Rights 1948, art 7.

[73] Frank Pasquale, 'Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries' (2010) 104 *Northwestern University Law Review* 105, 105, 112.

[74] Vincent Ostrom, 'Polycentricity', in Michael McGinnis (ed.) *Polycentricity and Local Public Economies: Readings from the Workshop in Political Theory and Policy Analysis* (University of Michigan Press, 1972) 55.

[75] Nathan Schneider, 'Decentralization: An Incomplete Ambition' (2019) 12 *Journal of Cultural Economy* 265, 274.

In the context of the Internet, the *rule of law* can be seen as a set of principles and practices that ensure that online platforms are accountable for the way in which they regulate our online interactions, and that they do so in a way that is consistent with the rule of law. We can recognize at least three main principles that underpin the *rule of law* on the Internet: (1) the principle of *legality*, which requires that the rules governing our online interactions be clear, accessible and predictable; (2) the principle of *proportionality*, which requires that the rules governing our online interactions be appropriate and necessary in light of the aims pursued; and (3) the principle of *accountability*, which requires that online platforms be accountable for the way in which they regulate our online interactions. Legal scholars like Suzor have argued that such principles be reflected in the governance of virtual communities.[76] In order to give effect to these principles, a number of practices have been developed by a variety of online platforms, such as the requirement that users read and expressly consent to the terms of service, the establishment of complaint mechanisms for those unhappy with a decision made by an online operator, and the adjudication of disputes by third-party tribunals.[77]

Yet, when it comes to code, the technical reality is not always consonant with the *rule of law* principles. Large platform operators enjoy significant discretionary powers in establishing the technical rules that govern their platforms:[78] just a "few tweaks to settings in a database can banish a user, silence her, or confiscate all her digital assets".[79] Platform operators can shape how a user interacts with other users, with legal repercussions also outside of the platform.[80] All the while, the contracts users enter into with operators overwhelmingly favour the latter and greatly limit their potential liability.[81] As such, these platforms can be said to be *ruled by code*—code is instrumentalized by the platform operators to determine how users can interact on these platforms.[82] Just like in the *rule by law,* where law is instrumentalised by the sovereign as a means of exercising control over the citizens, in the *rule by code*, the code is instrumentalised by online operators as a means of exercising control over the platform' users. As such, the *rule by code* is a system of online governance in which there exists a sovereign (the online operator—as well as the regulators to which the operator must respond) that stands 'above the code' and therefore uses the code to impose restrictions and constraints over Internet users who are subject to such code.

The *rule by code* can in some cases be problematic in so far as it is incompatible with the *rule of law*. Indeed, many online operators are considered by some as potentially

[76] Nicolas Suzor, 'The Role of the Rule of Law in Virtual Communities' (2010) 25 *Berkeley Technology Law Journal* 1817.
[77] Evelyn Douek, "'What Kind of Oversight Board Have You Given Us?"' [2020] U Chi L Rev Online 1.
[78] Gabriel Hassen, 'Digital Feudalism - An Analysis of Ownership and Control in the Information Age' (2011) 4 *Phoenix Law Review* 1027, 1049-1052.
[79] James Grimmelmann, 'Anarchy, Status Updates, and Utopia' (2014) 35 *Pace Law Review* 135, 138.
[80] Morshed Mannan, 'Theorizing the emergence of platform cooperativism: drawing lessons from role-set theory' (2022) 2 *Ondernemingsrecht Tijdschrift* 64, 65.
[81] Suzor (n 76), 1819.
[82] Code is not only computer code but also a way of codifying policies (e.g., content moderation policy, privacy policy), even when there are people at the edge (e.g., moderators), which are administered by a code-based platform as opposed to a human supervisor.

bypassing the sovereign authority of nation states,[83] especially with regard to their role in regulating commerce and creating or maintaining an inclusive public sphere. Recently, scholars such as Pasquale, Mazzucato, and Schneider[84] have analysed the emergence of new forms of sovereignty stemming from the rise of mega-platforms like Facebook, Amazon and Google. As the new "sovereigns of cyberspace",[85] these platforms are establishing themselves as new "functional sovereigns" reigning over digital fiefdoms.[86] Online platforms have embedded themselves so strongly in the infrastructure of public and commercial life, that they have become quasi-sovereign authorities.[87] Sovereignty, in this context, is not to be understood as the indivisible phenomenon described by Hobbes, but rather as the idea that "two or several authorities may have limited, relative, differential or functional sovereignty over certain areas, groups or resources".[88] While some have argued that these platform juggernauts extend principles and concepts from the jurisdictions where they are headquartered (e.g., common law notions of freedom of contract),[89] these functional sovereigns also have motivations and guiding principles of their own. Applying a constitutional lens to platform governance—as has been argued for previously[90]— through this *rule of law* vs. *rule by law* analysis is useful because it addresses the limitations of a purely contractualist approach to studying platform governance. These limitations range from acknowledging the asymmetries of power between a platform operator and users to recognising the (partial) inalienability of user rights in virtual communities.[91]

Exceptions exist, where platforms seek to emulate the processes by which laws are made in order to acquire ex-ante legitimacy, or even to provide a redress mechanism that can remedy injustices ex-post. Wikipedia, for example, implemented a complex governance system that tries at least to mimic a democracy[92]—despite its limitations in terms of inclusivity and representation.[93] Yet, regardless of the governance structure adopted within

---

[83] Ruth Lapidoth, 'Sovereignty in Transition' (1992) 45 *Journal of International Affairs* 325, 334-336.
[84] Frank Pasquale, 'From Territorial to Functional Sovereignty: the case of Amazon' (*Open Democracy*, 5 January 2018) < https://www.opendemocracy.net/en/digitaliberties/from-territorial-to-functional-sovereignty-case-of-amazon/> accessed 7 October 2022; Mariana Mazzucato, 'Preventing Digital Feudalism' *Project Syndicate* (7 October 2019) at https://www.neweurope.eu/article/preventing-digital-feudalism/; Nathan Schneider, 'Admins, mods, and benevolent dictators for life: The implicit feudalism of online communities' (2021) 24 *New Media & Society* 1965.
[85] Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books 2012).
[86] Pasquale (n 84).
[87] Frank Pasquale, *Digital Capitalism: How to Tame the Platform Juggernauts* (Friedrich-Ebert-Stiftung 2018).
[88] Lapidoth (n 83) 331.
[89] Christopher Marsden, 'Transnational Internet Law' in Christopher Marsden (ed.) *The Oxford Handbook of Transnational Law* (Oxford University Press 2021) 432.
[90] Suzor (n. 76) 1835.
[91] Nicolas Suzor, 'On the (Partially) Inalienable Rights of Participants in Virtual Communities' (2009) 130 *Media International Australia* 90; Brian Fitzgerald, 'Software as Discourse: The Power of Intellectual Property in Digital Architecture' (2000) 18 *Cardozo Arts & Entertainment Law Journal* 337, 384.
[92] Piotr Konieczny, 'Governance, organization, and democracy on the Internet: The iron law and the evolution of Wikipedia' (2009) 24 *Sociological Forum* 162, 189.
[93] Judd Antin and others, 'Gender differences in Wikipedia editing' [2011] *WikiSym '11: Proceedings of the 7th International Symposium on Wikis and Open Collaboration* 11; Eduardo Graells-Garrido, Mounia Lalmas, and Filippo Menczer, 'First women, Second sex: Gender bias in Wikipedia' [2015] *Proceedings of the 26th ACM Conference on Hypertext & Social Media* 165.

the Wikipedia platform, to the extent that it runs on a centralised infrastructure, it is those who control the infrastructure who have the ultimate say as to which technical rules will effectively be implemented in the platform. Moreover, even if online operators have a significant leeway in implementing their own technological rules and governance structures, they also account for external legal pressures that might affect their platform design. As a result, the substantive rules of many online platforms are ultimately determined not only by the whims of the platform operators, but also by the legal norms that these operators are subject to—such as the regulations of the countries in which they are incorporated and where they operate.[94]

The same is not true for blockchain-based systems, where there is no centralised operator or trusted intermediary in charge of managing the system.[95] A public blockchain network is operated in a distributed manner by a multiplicity of nodes, which all contribute, in a small and infinitesimal part, to managing the underlying network. As such, it can be assimilated to a particular type of "polycentric" system[96]—one where "many [...] decision structures are assigned limited and relatively autonomous prerogatives to determine, enforce and alter legal relationships".[97] Such a multifaceted governance structure significantly complicates the governance of these networks, because there is no single entity (or group of entities) that can be regulated as a 'proxy' to regulate the operations of the overall network. At the same time, the polycentric structure of blockchain networks also creates several avenues for regulators and policymakers to exert pressure on the various actors involved in the governance of these networks.

Indeed, despite their (alleged) eagerness to achieve decentralised governance, many blockchain networks and decentralised applications running on top of these networks are relatively centralised when it comes to power distribution. For instance, the major blockchain networks relying on proof-of-work, such as Bitcoin and Ethereum (till 15 September 2022), rely on a few, highly centralised mining-pools that control the majority of the hashing power used to power these networks.[98] Similarly, many of the blockchains that rely on proof-of-stake are also suffering from an extensive concentration of power amongst the

---

[94] External influences are not limited to the need to comply with legal rules, but also extend to political ideologies in specific jurisdictions, such as the belief in free markets and broad protections of freedom of expression. This is well illustrated by Facebook's establishment of an Oversight Board to decide on controversial moderation decisions. While this is intended to implement a transnational, private legal order for content moderation, due to the fact that Facebook's headquarters and a majority of its managers and employees are in the U.S, Facebook's content moderation policy also promotes U.S. free speech norms at an international level. Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 *Harvard Law Review* 1598, 1669. Nevertheless, local regulations, such as the European right to be forgotten, may impinge upon these standards, requiring Facebook not to display specific content to the users of a particular jurisdiction. Vishwas Patil and R.K. Shyamasundar, 'Efficacy of GDPR's Right-to-be-Forgotten on Facebook' in Vinod Ganapathy, Trent Jaeger, R.K Shyamasundar, (eds.) *Information Systems Security*. ICISS 2018. Lecture Notes in Computer Science(), vol 11281 (Springer 2018).

[95] De Filippi, Mannan & Reijers (n 9) 359.

[96] Michael Polanyi, *The Logic of Liberty: Reflections and Rejoinders* (Routledge 2007 [1951]).

[97] Ostrom (n 74) 55.

[98] Ashish Sai and others, 'Taxonomy of centralization in public blockchain systems: A systematic literature review' (2021) *Information Processing & Management* 58, 102584; Sarwar Sayeed and Hector Marco-Gisbert, 'Assessing blockchain consensus and security mechanisms against the 51% attack' (2019) 9 *Applied sciences* 1788.

validators.[99] Yet, although some actors in a blockchain-based network might have more influence than others, they all remain nonetheless accountable to the rules enshrined in the blockchain protocol or smart contract code.[100] Anyone who tries to validate transactions that violate the underlying blockchain protocol will simply see these transactions rejected by the rest of the network. Accordingly, as opposed to monocentric Internet platforms which are essentially *ruled by code*, blockchain-based networks are polycentric systems that can be said to operate according to the "*rule of code*"[101] —as an analogy to the *rule of law* found in many democratic governments.

Many decentralised applications (DApps) or decentralised autonomous organisations (DAOs) running on a blockchain are also only decentralised in theory.[102] In practice, they are often governed by a small number of actors (sometimes referred to as 'whales') holding a huge portion of governance tokens,[103] or—perhaps more critically—they are administered by a few individuals operating a multi-sig,[104] who have the power to operate and upgrade the underlying smart contracts.[105] This notwithstanding, even if the rules underpinning these smart contracts can be modified over time (provided that the system allows for such changes), they can only be changed in accordance with the specified secondary rules (i.e., the rules to change the rules) which have been predefined in advance.[106] No one—not even the creator of the system—has the power to unilaterally or arbitrarily modify the rules of the game, after these rules have been deployed into a blockchain infrastructure. Of course, this is not to say that blockchain networks are perfectly egalitarian or democratic. There are some actors who can exercise significant power when it comes to designing new rules (e.g., blockchain developers) or adopting these rules (e.g., blockchain miners and validators). Yet, once these rules have been adopted and collectively accepted by all participants of a blockchain network, they become an integral part of the infrastructure and can no longer be

---

[99] Nikos Leonardos, Stefanos Leonardos and Georgios Piliouras, 'Oceanic games: Centralization risks and incentives in blockchain mining', in Panos Pardalos and others (eds.) *Mathematical research for blockchain economy* (Springer 2020); Sheikh Saad and Raja Radzi 'Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos)' (2020) 10 *International Journal of Innovative Computing* 27.

[100] Andrej Zwitter and Jilles Hazenberg 'Cyberspace, Blockchain, Governance: How Technology Implies Normative Power and Regulation' in Benedetta Cappiello and Gherardo Carullo (eds.) *Blockchain, Law and Governance* (Springer 2021) 94.

[101] De Filippi and Wright (n 15) 7.

[102] Ashish Sai, 'Towards a holistic assessment of centralization in distributed ledgers' (PhD thesis, University of Limerick 2021).

[103] Olivier Rikken, Marijn Janssen and Zenlin Kwee, 'Governance challenges of blockchain and decentralized autonomous organizations' (2019) 24 *Information Polity* 397; Tom Barbereau and others, 'DeFi, Not So Decentralized: The Measured Distribution of Voting Rights', in Tung Bui (ed.) *Proceedings of the 55th Hawaii International Conference on System Sciences* (HICCS 2022).

[104] Henrik Axelsen, Johannes Jensen and Omri Ross, 'When is a DAO Decentralized?' (2022) 31 *Complex Systems Informatics and Modeling Quarterly* 51.

[105] Mehdi Salehi, Jeremy Clark and Mohammad Mannan, 'Not so immutable: Upgradeability of Smart Contracts on Ethereum' (2022) arXiv preprint <https://doi.org/10.48550/arXiv.2206.00716> accessed 7 October 2022.

[106] To understand the importance of secondary rules for blockchain governance, *see* Marco Crepaldi, 'Why blockchains need the law: Secondary rules as the missing piece of blockchain governance' in *ICAIL '19: Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law* (ACM 2019). This also limits the efficacy of regulating the application layer of blockchain networks, as argued in Hossein Nabilou, 'How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency' (2019) 27 *International Journal of Law and Information Technology* 266, 290.

unilaterally affected by anyone—regardless of their identity or role. Because everyone is subject to the exact same technological rules, there is no sovereign who stands 'above the code'.

We refer here to the *rule of code* as a new regulatory principle introduced by blockchain technology, which distinguishes itself both from the *rule by code* enacted by large Internet platforms, and the *rule of law* endorsed by states. It differs from the former because blockchain-based systems—as decentralised and distributed systems—cannot easily be instrumentalized by centralised authorities or online intermediaries. At the same time, the *rule of code* is only a rough approximation of the *rule of law* because it does not account for all the formal, procedural and substantive requirements which are often associated with it. The *rule of code* is used to stress the fact that technological arrangements can be designed in such a way as to eliminate—or, at least, reduce—the arbitrary influence of any single actor (including the state) over the operations of a technological system as no individual actor can unilaterally dictate actions or changes to the blockchain network, including core developers. In other words, if we continue to use a constitutional lens, no actor has a claim to *sovereign authority* over the network. Accordingly, by analogy to the relationship that subsists between the *rule of law* and the *rule by law*, we can delineate the relationship between the *rule by code*, where code is instrumentalized by platform operators to promote their own economic or political interests; and the *rule of code*, describing a situation where code applies equally to all.[107]

At first glance, the *rule of code* may seem like a preferable alternative to the *rule by code*, because it is intended to preclude abuses of power from a sovereign ruler. The *rule of code* could potentially satisfy many of the formal requirements for a thin conception of the *rule of law*:[108] The rules in a blockchain system are publicly accessible (although not necessarily understandable) to all; they apply prospectively; they are equally applied to all, they are relatively stable, they are non-contradictory by design, and are (for the most part) clearly specified so as to operate properly. Yet, the *rule of code* does not provide normative conditions to guarantee the *legitimacy* of its rules, and could therefore lead to situations that are contrary to the general interest. This is akin to the criticism levelled at the thin and

[107] One could argue, however, that, as opposed to the *rule by code* enacted by large Internet platforms, the *rule of code* enshrined in many blockchain-based systems fails with regard to the scope and potential impact on people's life. Today, the blockchain space is still immature and even the largest blockchain-based systems did not receive enough adoption to systematically impact the life of citizens in the same way as the Internet does. While citizens cannot escape from the *rule of law* without leaving their own country, they also have an increasingly hard time escaping from the *rule by code* established by large online operators, because exiting from mainstream Internet platforms such as Facebook or Google has become extremely costly. *See* Mannan and Schneider (n 33) 3. While there is no guarantee that blockchain architectures will eventually acquire the same significance as today's large Internet platforms, we are already seeing the first glimmers of this potential future, as recently shown by the official adoption of Bitcoin as legal tender by the country of El Salvador, and the use of cryptocurrencies to bypass economic sanctions in Russia. *See* Eric Vázquez, 'The Technical Fix: Bitcoin in El Salvador' (2022) 121 *South Atlantic Quarterly* 600; Emily Flitter and David Yaffe-Bellany, 'Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions' (*New York Times*, 23 February 2022) <https://www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html> accessed 7 October 2022.

[108] Wohlwend (n. 64) 37-46. *But see*, Jan Oster, 'Code is code and law is law—the law of digitalization and the digitalization of law' (2021) 29 *International Journal of Law and Information Technology* 101.

procedural conceptions of the *rule of law* by those who advocate for thicker and more substantive conceptions. In particular, the divergences that may emerge between the *rule of cod*e and the *rule of law* raise important questions concerning the degree to which the law might or might not intervene in case of potential conflicts with the code. From a regulatory perspective, it is generally easier for governments to regulate platforms that are *ruled by code* than it is to govern platforms operating by the *rule of code*. Indeed, while many centralised online platforms are ruled by the whims of their centralised operators, regulation can be more easily enforced on these platforms, insofar as these operators themselves are subject to the laws of a particular jurisdiction and are required to abide by these laws.[109]

Decentralised peer-to-peer networks are also difficult to regulate, because there is no single actor that is in charge of governing these networks. As such, they are not ruled by code. Without tackling the question of whether earlier decentralised peer-to-peer networks (e.g. BitTorrent, Gnutella) are subject to the rule of code—which is beyond the scope of this paper—our claim is that public and permissionless blockchain-based systems, which are not administered by any centralised authority and which are composed of a pseudonymous and globally-distributed group of actors, are the archetypal example of a system governed by the rule of code. This is because all the actions that can be taken on these networks are predefined and specified by the code of the underlying blockchain network (and associated smart contracts). While, in a peer-to-peer network, every node is in charge of running and executing the same software according to their *own* preferences and needs (e.g., deciding to seed a music file), in the case of a blockchain-based system, the software code is executed in a deterministic manner by *every* network node, regardless of who the actors connected to the network are and what their personal preferences may be. There are embedded incentives concerning the coordinated maintenance of a blockchain network which are weaker, or absent, in the case of earlier peer-to-peer networks. In other words, the *rule of code* in the context of a blockchain refers to an objectively identifiable set of rules that every network participant *must* execute as part of its own responsibilities as a network operator.

Yet, in some cases, the *rule of code* might prevail over the rule of law. This might create tension to the extent that the substantive norms of the *rule of code* do not necessarily respect the substantive conditions of the rule of law, such as, for example, the requirements of fairness and equality before the law. Schrepel illustrates this point, by showing how the *rule of law* and the *rule of code* might impose different tradeoffs between potentially conflicting fundamental rights—for instance between privacy and free speech.[110] We analyse the extent of these discrepancies in the following section.

---

[109] Urs Gasser and Wolfgang Schulz, 'Governance of online intermediaries: Observations from a Series of National Case Studies' (2015) Berkman Klein Center for Internet and Society Research Publication 5/2015 <https://ssrn.com/abstract=2566364> accessed 7 October 2022.

[110] Thibault Schrepel, 'Anarchy, State, and Blockchain Utopia: Rule of Law Versus Lex Cryptographia' in Ulf Bernitz and others (eds.) *General Principles of EU Law and the EU Digital Order* (Wolters Kluwer 2020).

Conflict between the Rule of Law and the Rule of Code

Over the years, a variety of blockchain-based applications have come to light, designed with a view to circumvent existing regulations.[111] These applications leverage the pseudonymity of Bitcoin or other cryptocurrencies to facilitate money laundering[112]—often relying on obfuscation tools such as mixers and tumblers, such as the now infamous *Tornado Cash.*[113] Pseudonymity is also exploited in the creation of decentralised marketplaces for illicit goods and services, e.g., in the Silkroad marketplace,[114] or to shield the proceeds of ransomware and cyberattacks. More recently, it also became clear that the tamper-resistant features of blockchain technology can potentially be abused to record illegitimate content on the blockchain—such as copyright infringement, hate speech or links to child pornography.[115] These applications are *illegal*, in that they constitute criminal activities that are expressly punishable under a particular body of law. It is thus to be expected that national law enforcement officials will assert their legal authority in trying to halt and deter these activities.[116] There are, however, also blockchain-based applications that are not strictly illegal per se, but that can nonetheless be designed to ignore existing regulatory frameworks,[117] creating potential discrepancies between the *rule of law* and the *rule of code*.

These discrepancies are particularly apparent in the realm of contracts. Legal scholars, like Schuster, Werbach and Levy, are sensitive to the fact that smart contracts may not comply with the law, and their code cannot capture the complexity of a court's reasoning when interpreting contracts.[118] As some scholars have noted, smart contracts are ambivalent about the actual content of the law and that, more often than not, the traditional legal order

[111] Primavera De Filippi, 'Bitcoin: a regulatory nightmare to a libertarian dream' (2014) 3 *Internet Policy Review* 1, 9.
[112] C. Janze, 'Are Cryptocurrencies Criminals Best Friends? Examining the Co-Evolution of Bitcoin and Darknet Markets' (2017). *AMCIS 2017 Proceedings* 1, 2..
[113] Tornado Cash is is a cryptocurrency mixer that operates on the Ethereum blockchain and indiscriminately facilitates the anonymization of transactions by obfuscating their origin, destination, and counterparties. *See* Alex Wade, Michael Lewellen and Peter van Valkenburgh, 'How does Tornado Cash Work?' (CoinCenter, 25 August 2022) <https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/> accessed 7 October 2022.
[114] Lawrence Trautman, 'Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox?' (2014) 20 *Richmond Journal of Law and Technology* 1, 12.
[115] Roman Matzutt and others, 'A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin', in Sarah Meiklejohn and Kazue Sako (eds.) *Financial Cryptography and Data Security*, FC 2018, Lecture Notes in Computer Science, vol 10957 (Springer 2018) 421; Maurice Schellekens, 'Does regulation of illegal content need reconsideration in light of blockchains?' (2019) 27 *International Journal of Law and Information Technology* 292, 304.
[116] Karen Yeung, 'Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law' (2019) 82 *Modern Law Review* 207, 210.
[117] De Filippi, Mannan and Reijers (n. 9). This is particularly the case of blockchain-based applications that operate—only and exclusively—according to the rules enshrined into their protocol or smart contract code, regardless of whether these rules are compatible with the existing regulatory framework of the parties with which they interact.
[118] Karen Levy, 'Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law' (2017) 3 *Engaging Science, Technology, and Society* 1, 3-4; Kevin Werbach, 'Trust, but Verify: Why the Blockchain Needs the Law' (2018) 33 *Berkeley Technology Law Journal* 487, 528; Edmund Schuster, 'Cloud Crypto Land' (2021) 84 *Modern Law Review* 974, 989-990, 998.

has limited options to unravel a smart contract.[119] To be sure, traditional legal contracts are created according to specific rules defined by contract law and fossilised through terms and conditions agreed *ad idem*, to create a binding agreement between two or more parties. Given that they are written in natural language, the enforcement of these contractual agreements necessitates a third party authority (e.g., a notary or a judge) to exercise judgement in order to interpret the wording of the contractual provisions in light of the actual intent of the parties. In deciding whether or not to enforce the contract, the court will consider, *inter alia,* whether the parties involved in the agreement lack legal capacity, whether the subject matter of the contract renders it illegal, and whether fraud will be committed as a consequence of executing the contract.

Conversely, the provisions of a smart contract are not construed in accordance with the law; they are determined by the execution of the smart contract code.[120] As such, the provisions of a smart contract are automatically executed by the technology, with no opportunity for breach.[121] Despite the benefits they provide in terms of guaranteed execution, one important drawback of such an approach to contracting is that the underlying technology does not account for the intent of the parties nor are the smart contracts necessarily designed to be enforced: the smart contract only abides by the wording of code.[122] Hence, a smart contract might execute a particular set of conditions (defined by code), even if the legal contract which has been enacted—either implicitly or explicitly—by the contracting parties would require a different type of execution, which cannot be enforced by technological means. As a result, smart contracts might create a discrepancy between the contractual provisions established by the traditional legal order (in accordance with contract law) and the conditions established by the technological infrastructure of a blockchain (in accordance with its underlying protocol and smart contract code).

Property rights face a similar type of discrepancy. In the traditional financial system, a variety of centralised operators can reverse an erroneous or illegitimate transaction and an enforcement authority can seize funds from a third-party account following a court order. In contrast, reversing a transaction after it has been recorded on a blockchain is simply not an option. Similarly, as opposed to physical assets which court-ordered bailiffs can unilaterally access by breaking down doors, digital assets held by a smart contract on a blockchain network cannot be seized by any enforcement authority, unless specifically provided by the

---

[119] Ari Juels, Ahmed Kosba, Elaine Shi, 'The Ring of Gyges: Investigating the Future of Criminal Smart Contracts' in Edgar Weippl and others (eds.) *CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (ACM 2016) 283; Max Raskin, 'The Law and Legality of Smart Contracts' (2017) 1 *Georgetown Law Technology Review* 305, 325; James Grimmelmann, 'All Smart Contracts are Ambiguous' (2019) 2 *Journal of Law & Innovation* 1, 3, 15. 21.

[120] Nataliia Filatova, 'Smart contracts from the contract law perspective: outlining new regulative strategies' (2020) 28 *International Journal of Law and Information Technology* 217, 221..

[121] Alexander Savelyev, 'Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law', (2017) 26 *Information & Communications Technology Law* 116, 127; Mateja Durovic and André Janssen, 'The Formation of Blockchain-based Smart Contracts in the Light of Contract Law' (2019) 6 *European Review of Private Law* 753, 756.

[122] Levy (n. 118) 5.

code.[123] Besides, while one could theoretically rely on the traditional legal system to claim monetary compensation for the value of these unseizable assets, the pseudonymity that characterises a large majority of public and permissionless blockchains makes it virtually impossible for a claimant to reclaim their loss.[124]

A clear illustration of this discrepancy can be found in the aftermath of the TheDAO attack.[125] TheDAO was a decentralised investment fund deployed as a smart contract on the Ethereum blockchain. TheDAO managed to raise over $150 million dollars' worth of Ether in less than one month of fundraising. However, a vulnerability in the code enabled an attacker to syphon out one third of these funds, leaving the original investors at loss. Despite the lack of an 'executive branch' or 'board of directors', the investors nonetheless managed to retrieve their funds through an exceptional intervention by the Ethereum community, who collectively agreed to modify the protocol of the Ethereum blockchain to restore the original balance of the TheDAO smart contract. The exceptional character of such a solution was that the decision to change the protocol of the Ethereum blockchain was not the result of a standard upgrade procedure, intended to implement a technical fix or improve the functionalities of the Ethereum blockchain—it was the result of a political decision.[126]

Because of the decentralised character of the Ethereum network, such a coordinated intervention could not be unilaterally executed; its effectiveness required all participating nodes to intentionally update their software. As a result, many attempts were made to gauge the public opinion on this matter, to ensure that there was enough consensus around this type of intervention. Eventually, the large majority of participating nodes agreed to the undertaking, and the funds were successfully retrieved on the main Ethereum network.[127] However, some nodes rejected the change, considering such an intervention impinged upon the principles of immutability and tamper-resistance of the Ethereum blockchain,[128] to the extent that it would ultimately constitute an outright violation of the *rule of code* enshrined in the blockchain protocol.[129]

---

[123] Note that this only applies in the case of non-custodial wallets. If the digital assets are held on a centralised exchange, a court order could order the exchange to freeze the disposal and liquidation of these assets.

[124] This could recently be seen in the Singapore High Court decision of *CLM v. CLN & others* [2022] SGHC 46. The pseudonymity of individuals suspected of theft made it difficult for courts to identify who to sanction, requiring them to place injunctions and worldwide freezing orders on crypto-exchanges to prevent the disposal of digital assets.

[125] This example has already been mentioned many times in the literature, yet it remains one of the best examples (if not the only one) that properly illustrates the governance challenges that may arise when something enshrined in the code of a smart contract does not execute as planned.

[126] Note that the distinction between protocol upgrades of a purely technical nature, and the political response to TheDAO attack is necessarily a blurry one, since many technical upgrades can also be of a political nature. See, for instance, the Bitcoin's blocksize debate, where multiple approaches were proposed as a technical solution to improve the scalability of the Bitcoin network; yet, because some solutions benefited some stakeholders more than others, the question of identifying the right solution was ultimately a political one. *See* Primavera de Filippi and Benjamin Loveluck, 'The invisible politics of bitcoin: governance crisis of a decentralized infrastructure' (2018) 5 *Internet Policy Review* 1.

[127] Voshmgir Shermin, 'Disrupting governance with blockchains and smart contracts' (2017) 26 *Strategic Change* 499, 506-507.

[128] Muhammad Mehar and others, 'Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack' (2019) 21 *Journal of Cases on Information Technology* 1, 2.

[129] De Filippi and Wright (n. 15) 204.

Such an event is considered one of the most important landmarks in the history of blockchain governance, because it has shown that, even if there is no central authority or sovereign on the Ethereum network, the *rule of code* established through the underlying blockchain protocol can nonetheless be violated through a coordinated action of all network nodes.[130] This is particularly likely when it comes to fundamental questions of normative importance, i.e., when the *rule of code* does not respect the normative principles that are (ideally) respected under thicker conceptions of the *rule of law.* In other words, the attack might have been 'legal' under the *rule of code* (i.e., it did not violate the rules enshrined into the smart contract code), but it lacked the legitimacy endowed on lawful behaviour under a thicker conception of the rule of law (e.g., respect for private property rights).

More recent examples, such as the hack of BadgerDAO—a collective focused on offering Bitcoin-focused decentralised finance products—have a passing resemblance to TheDAO attack but differ in several respects. On 2 December 2021, a front-end vulnerability on the BadgerDAO website was exploited by attackers so as to drain funds from DAO members wallets to third-parties' addresses; ultimately leading to losses of over US$120 million—with a lion's share of the loss experienced by the crypto-lender, Celsius Network. As the attack was possible due to a frontend vulnerability and not a problem with the smart contract code, BadgerDAO's insurance provider, NexusMutual, did not provide coverage. Among other things, this required the DAO to vote on a proposal to temporarily 'freeze' their smart contracts and advise their members to decline transactions with blacklisted addresses.[131] While BadgerDAO informed external public authorities in the United States of America and Canada of the attack, its approach to making its members whole was primarily based on solutions crafted through internal governance processes. The method of restitution proposed by BadgerDAO representatives and exploit victims was to, among other things, payout a certain amount of Bitcoin that had been acquired by BadgerDAO through earlier purchases and issue a remBadger token through an 'airdrop' that would be gradually paid out to victims over a two-year period so as to cover the amounts that were not recoverable after the hack.[132] The value of the new remBadger token would derive from the US$ 2 million of BADGER tokens that would be locked in a BadgerDAO 'vault' (valued at $25 dollars in December 2021) and gradually accrue rewards.[133] A central pillar of the restitution plan was that members avoid withdrawing remBadger tokens during the period in which the repayments were taking place, failing which the remaining BADGER token rewards would be forfeited. Celsius, notably, withdraws its allocated tokens, amounting in value to only a

[130] Wessel Reijers and others (n. 14) 828.
[131] Richard Lawler, 'Someone stole $120 million in crypto by hacking a DeFi website' (*The Verge*, 3 December 2021) <https://www.theverge.com/2021/12/2/22814849/badgerdao-defi-120-million-hack-bitcoin-ethereum> accessed 7 October 2022.
[132] BadgerDAO, 'BIP 80 Restitution of non-recoverable assets via remBadger Sett' (Badger Forum, 2 December 2021) <https://forum.badger.finance/t/bip-80-restitution-of-non-recoverable-assets-via-rembadger-sett/5362> accessed 7 October 2022.
[133] BadgerDAO, 'remBADGER' (Badger Gitbook, 2022) <https://docs.badger.com/badger-finance/vaults/vault-user-guides-ethereum/rembadger> accessed 7 October 2022.

fraction of their original loss. BadgerDAO refused to allow Celsius to redeposit and continue receiving repayments.[134]

This case is illuminating for two broad reasons. First, it reveals how a DAO, as the archetypical Web3 application, not only relies on the proper functioning of a blockchain and associated smart contracts (operated by the *rule of code*), but also on the security and reliability of Web 2.0 technologies (e.g., APIs) that enable users to interact with these smart contracts. Because these Web 2.0 interfaces are *ruled by code,* trust in the actors operating these platforms continues to have an important function in buttressing the confidence users have in the blockchain application. This trust was, understandably, shaken in the aftermath of the exploit and one user described the core team as being "sloppy".[135] Second, special or preferential treatment was not given to Celsius, despite the size of loss incurred by the crypto-lending company. This can be seen as a measure intended to regain confidence in the governance of BadgerDAO among its members by adhering strictly to the 'rule of code'.

The Rule of Code in a Pluralist, Polycentric Legal System

Some legal scholars consider the relationship between the *rule of law* and the *rule of code* as inherently conflictual, claiming that the former should always prevail over the latter.[136] They claim that decentralised blockchain-based systems cannot create conditions akin to the *rule of law* because "ruling always necessitates a hierarchy".[137] Others recognise that the *rule of code* cannot only escape from the *rule of law*, but also complement it, or even reinforce it.[138] We adopt here a legal pluralist perspective to underline the fact that multiple legal orders—including those enacted by technological systems—can co-exist in the same jurisdiction.[139] Indeed, historically speaking, legal pluralism has been the norm instead of the monism of state law.[140] Yet, today, when referring to blockchain systems, *lex cryptographica* is often regarded either as an alternative legal order that subsists on its own,[141] or as a separate legal order that should be made compliant with the overarching state legal

[134] Sritanshu Sinha, 'Celsius' crisis exposes problems of low liquidity in bear markets' (CoinTelegraph, 22 June 2022) <https://cointelegraph.com/news/celsius-crisis-exposes-problems-of-low-liquidity-in-bear-markets> accessed 7 October 2022.
[135] Lawler (n. 131).
[136] Robert Herian, *Regulating Blockchain: Critical Perspectives in Law and Technology* (Routledge 2019) 167.
[137] Schuster (n. 118) 993.
[138] Yeung (n 116) 215.
[139] Robé, (n. 16); Teubner (n. 16); David Lefkowitz, 'Global Legal Pluralism and the Rule of Law' in Paul Berman (ed.), *The Oxford Handbook of Global Legal Pluralism* (Oxford: Oxford University Press, 2020); Brian Tamanaha, *Legal Pluralism Explained: History, Theory, Consequences* (Oxford University Press 2021); Anna Jurkevics, 'Democracy in contested territory: on the legitimacy of global legal pluralism' (2022) 25 *Critical Review of International Social and Political Philosophy* 187.
[140] Hans Lindahl, *Authority and the Globalisation of Inclusion and Exclusion* (Cambridge University Press 2018) 64.
[141] Marcella Atzori, 'Blockchain Technology and Decentralized Governance: Is the State Still Necessary?' (2015) SSRN Research Paper No. 2709713/2015 <https://ssrn.com/abstract=2709713> accessed 7 October 2022.

system[142]—without considering the possibility that multiple legal orders can interact and co-exist.

The argument that blockchain-based systems comprise a distinct, gradually emerging legal order within a global plural legal system would not be unfamiliar to earlier scholars of legal pluralism.[143] For Teubner, in particular, legal orders are created not only through the establishment of a body of rules drafted by a legislature and enacted by a sovereign, they can also be created—as 'proto laws'—through self-reproducing legal discourse in global networks (including technological networks) with global validity.[144]

We can observe elements of both 'enacted' and 'interactional' law in the context of *lex cryptographica*. The former refers to laws that are promulgated by an authority, while the latter comes into existence through mutual conduct that gives rise to a series of expectations with regard to third parties' conduct and obligations. The engineers who build the standards for how transactions can take place in a blockchain-based system are akin to lawmakers trying to standardise laws and facilitate legal conduct.[145] At the same time, certain interactions, like those among the stakeholders of a blockchain network which are trying to reach consensus also give rise to certain expectations of conduct[146]—thereby giving expression to the law through "the conduct of men toward one another".[147]

Multinational enterprises provide an illuminating example. Robé describes them as being "islands of law"[148]: they have the character of a legal order due to the way in which their internal rules shape the behaviour and norms of their members, creating the perception that these rules are mandatory, and thereby generating a distinction between lawful and unlawful actions.[149] The private autonomy of these enterprises allows for them to develop their own norms, which may well be informed by the rules of a state's legal order, but nonetheless develop on their own path.[150] In Robé's view, this autonomy was one of the fruits of the creation of the liberal nation-state and a (neo-)liberal international economic order, as the creation and enforcement of property rights and freedom of contract had the effect of both decentralising power to the level of the individual, as well as constraining states from re-centralising this power (e.g., due to constitutional protections, bilateral investment treaties).[151] Indeed, it would not be possible to recentralize power without undermining the

---

[142] Michele Finck, *Blockchain Governance and Regulation in Europe* (Cambridge University Press, 2018) 86; Katrin Becker, 'Blockchain Matters—Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries' (2022) 33 *Law and Critique* 113.
[143] Wibren van der Burg, 'Conceptual Theories of Law and the Challenges of Global Legal Pluralism' in Paul Berman (ed.), *The Oxford Handbook of Global Legal Pluralism* (Oxford University Press, 2020) 320.
[144] Teubner (n 16) 7, 12, 14.
[145] Jake Goldenfein and Andrea Leiter, 'Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct' (2018) 29 *Law and Critique* 141, 143-144.
[146] Van der Burg (n. 143), 325.
[147] Lon Fuller, 'Human Interaction and the Law' (1969) 14 *The American Journal of Jurisprudence* 1, 1; *also see* Gerald Postema, 'Implicit Law' in W. Witteveen and Wibren van der Burg (eds.), *Rediscovering Fuller: Essays on Implicit Law and Institutional Design* (Amsterdam University Press 1999).
[148] Robé, n 16 above, 53.
[149] ibid, 52-53.
[150] ibid, 65.
[151] ibid, 57-62.

fundamental, ideological values of a liberal-democratic state—values which, according to Robé, preceded the creation of these nation-states themselves.[152]

Blockchain-based systems can, by analogy, also be seen as implementing a separate legal order that coexists with the state's legal order, albeit not always peacefully. Whether we refer to it as *lex cryptographi(c)a*,[153] "*cryptolaw*",[154] "*law as code*"[155] or "*code as law*",[156] the *rule of code* implemented by blockchain technology interplays in complex ways with the rule of law. As we will show in the following sections, although the *rule of code* can to some extent be shaped by the *rule of law*, the two remain conceptually distinct because they operate according to different principles. Hence, within the coexisting legal orders of a pluralist system, some legal orders may rely on a hierarchy of authority (e.g., court systems, bureaucratic organisations), while others may rely on "reciprocity and shared but tacit understandings"[157] for decisions to be made; or, in the case of blockchain-based systems, on distributed consensus and *schelling points* (discussed below).

Our claim is that, while the state's legal order can influence blockchain-based systems, it does not necessarily follow that the *rule of law* will (or should) necessarily prevail over the *rule of code*.[158] That the *rule of code* could prevail in certain circumstances becomes especially relevant when blockchain-based applications are intended to alleviate the transactional frictions that are generally imposed by the law.[159] In that regard, we situate our argument between two extreme perspectives on the legality of blockchain-based systems. On the one hand, there is a view that, because code does not leave room for interpretation,[160] it can effectively eliminate human agency and as such generate an automated, 'robotic' form of law that is self-enforcing in the case of blockchain.[161] On the other hand, there is a view that blockchain technologies cannot enact any form of effective legality, especially if they try to interact with the physical world,[162] because as soon as they do so, they lose their ability to effectively and autonomously govern people's actions. State law, in other words, needs to intervene in order to guarantee the efficacy of these systems in the physical world.

We provide here an alternative perspective—one that sees blockchain systems as capable of automating the execution of specific actions or interactions, without however being able to guarantee absolute and ineluctable execution.[163] Indeed, as the TheDAO attack

[152] ibid, 62.
[153] Wright and De Filippi (n. 10).
[154] Carla Reyes, 'Conceptualizing Cryptolaw' (2017) 96 *Nebraska Law Review* 384.
[155] De Filippi and Hassan (n. 12).
[156] Yeung (n. 116) 209.
[157] Sally Merry, 'Legal Pluralism' (1988) 22 *Law & Society Review* 869, 878.
[158] Peer Zumbansen, 'The rule of law, legal pluralism, and challenges to a Western-centric view: Some very preliminary observations' in Christopher May and Adam Winchester (eds.) *Handbook on the Rule of Law* (Edward Elgar Publishing 2018) 65.
[159] Yeung (n. 116) 215.
[160] Laurence Diver, 'Digisprudence: The Design of Legitimate Code' (2021) 13 *Law, Innovation and Technology* 325.
[161] Antoine Garapon and Jean Lassègue, *Justice digitale: Révolution graphique et rupture anthropologique* (Presses Universitaires de France, 2018) 146.
[162] Schuster (n. 118).
[163] Crystal Hall, Eric Chown and Fernando Nascimento, 'A critical, analytical framework for the digital machine' (2021) 46 *Interdisciplinary Science Reviews* 458.

has demonstrated, actions determined by the self-executing code of smart contracts are still subject to human intervention.[164] It is exactly this space of intervention that can be leveraged by lawmakers to regulate blockchain systems.

Yet, it is our belief that only a proper understanding of the underlying operations of decentralised blockchain-based systems—in particular their governance structure—will enable governments to properly interface with these systems. Importantly, in their attempt at regulating these systems, governments must acknowledge that, in a polycentric and plural legal system,[165] their influence cannot be absolute. Polycentric systems are, indeed, often regarded as a means to support and uphold the *rule of law*.[166] First, because the dispersion of legal authority contributes to mitigating arbitrary uses of violence. Second, because the existence of a common set of rules recognized by all the participants provides for a more decentralised law enforcement system, distributed across multiple power structures. Hence, regulating these systems cannot be done in a top-down manner,[167] it requires governments to act as one out of many other nodes of decision-making (rather than act as a central coordinator), thereby dynamically responding to the interests and needs of all relevant stakeholders.

We delineate in the following section the specificity of blockchain governance in order to shed light on the various levers of influence that can be adopted by regulators and policymakers. Specifically, the next section will discuss how regulators and policymakers could respond to the deficiencies of the *rule of code*, regulating it via two alternative, yet interconnected approaches: "regulation by code" or "regulation through governance".

II. Regulation of Blockchain Technology

Blockchain Governance

We rely on Lessig's four regulatory levers—*law, market dynamics, social norms, and architecture or code* (Fig 1)[168]—to analyse the interdependencies between state governance and blockchain governance. A similar analysis has already been undertaken by De Filippi & Wright, De Filippi & Hassan (2018), and Yeung (2018), which analyses the interplay between conventional law (the "*code of law"*) and the internal rules of blockchain systems which take the form of executable software code and technical protocols ("*code as law"*).[169] Yet, while these previous contributions mostly focus on the different attitudes that blockchain-based systems might adopt with regard to the legal system—and how these attitudes may shape

[164] Quinn DuPont 'Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization' in Malcolm Campbell-Verduyn (ed.) *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (Routledge 2017).
[165] Michael Polanyi (n. 96); Josphine van Zeben, 'Polycentricity as a Theory of Governance' in Josephine van Zeben and Ana Bobić (eds.) *Polycentricity as a Theory of Governance* (Cambridge University Press 2019) 13.
[166] Paul Aligica and Vlad Tarko, 'Polycentricity: From Polanyi to Ostrom, and Beyond' (2012) 25 *Governance* 237.
[167] van Zeben (n. 129) 14.
[168] Lessig (n. 35) 122-123.
[169] De Filippi and Wright (n. 29); De Filippi and Hassan (n. 12); Yeung (n. 89) 209.

their relationships with the law—we focus here on the various means available to state law in order to control or influence the operations of blockchain technology.

[FIGURE 1 ABOUT HERE]

Blockchain governance is a multi-layered endeavour that requires constant and recurrent interaction within a large variety of stakeholders involved in the development, operations or maintenance of a blockchain system. On the one hand, there are the core developers, who propose the choices or protocol changes that network participants will select from.[170] On the other hand, there are the network participants (miners and validators), who must choose and discriminate between the possible solutions offered by the core developers.[171] Finally, there are the users of these systems—cryptocurrency or token holders, smart contract programmers, and all those who have a reason to interact with the network (for e.g., to transact with these smart contracts)—who ultimately contribute to the value of the overall blockchain network.

To understand the operations of a blockchain network, it is useful to distinguish between two types of governance: governance *by* the infrastructure (on-chain) and governance *of* the infrastructure (off-chain).[172] *On-chain* governance refers to the rules which have been baked directly into the technological infrastructure of a blockchain-based system, and which can thus be automatically enforced by the technology. As such, the focus of on-chain governance is on the enforcement of formal and codified rules, rather than on the elaboration of these rules. *Off-chain* governance refers instead to the social and institutional mechanisms allowing for these rules to be defined and elaborated, as well as the procedures put in place in order to apply, enforce, or possibly change these rules. While on-chain governance rules are—by their very nature—clear and formalised, off-chain governance rules are, with a few exceptions, much more fluid and informal—and therefore more difficult to discern with accuracy and precision.[173] Indeed, while some blockchain communities have implemented a somewhat formalised procedure for discussing protocol upgrades (e.g., Bitcoin and Ethereum Improvement Proposals: BIPs, EIPs), the majority of them did not set up any formal process for many other aspects of off-chain governance, including the processes of delegating duties and powers, deliberation, decision-making, and sanctioning. Off-chain governance generally entails the participation of different stakeholders, with competing interests and ideological views, who are globally distributed and pseudonymous. While this makes the formalisation of off-chain governance all the more necessary, it remains, however, an uphill task.

---

[170] Jack Parkin, 'The senatorial governance of Bitcoin: making (de)centralized money' (2019) 48 *Economy and Society* 463, 470-471.

[171] Matthew Zook and Joe Blankenship, 'New spaces of disruption? The failures of Bitcoin and the rhetorical power of algorithmic governance' (2018) 96 *Geoforum* 248, 251.

[172] Primavera de Filippi and Greg McMullen, 'Governance of Blockchain Systems: Governance of and by Distributed Infrastructure' (2018) Blockchain Research Institute and COALA Research Report, 4 <https://hal.archives-ouvertes.fr/hal-02046787/document> accessed 7 October 2022..

[173] Ellie Rennie and others 'Toward a Participatory Digital Ethnography of Blockchain Governance' 28 *Qualitative Inquiry* 837.

Initially, and understandably, those analysing the governance of blockchain communities were mostly focused on the *on-chain* aspects of blockchain governance. These include the blockchain protocol, consensus algorithms or the code of a particular smart contact.[174]A blockchain based on proof-of-work (e.g., Bitcoin) will give rise to a very different governance structure than a blockchain based on proof-of-stake (e.g., Tezos, Ethereum since 15 September 2022), or proof-of-authority (e.g., VeChain). The incentive schemes of a particular blockchain (e.g., block-rewards and transaction fees) will also impact the behaviours of the different stakeholders maintaining the network.

Yet, events such as the TheDAO attack and other instances of failed on-chain governance made it clear that one cannot understand the governance of any blockchain-based system without accounting for the mechanisms of off-chain governance at play within these systems.[175] Off-chain governance is particularly relevant in the context of 'forking'. Indeed, as described in the previous section, blockchain networks exhibit different power dynamics than traditional internet platforms, because there are no centralised operators that can impose a unilateral decision on their users. Hence, in order to implement any change to a particular blockchain network, active network participants (e.g., miners and validators) need to explicitly agree to the proposed protocol change, and upgrade their clients accordingly, without any opportunity to exercise coercive power on the other participants. Accordingly, even if a majority of miners chose to implement a particular protocol change, network participants always have the choice to stay on the previous version of the protocol—thereby 'forking' the network into two separate and concurrent networks, which operate side by side.[176]

Off-chain governance in this context refers to the activities of different stakeholder groups (often with their own vested, and potentially competing, interests) trying to influence each other in choosing one particular protocol over the other, in the absence of third-party enforcement or coercion. Yet, in light of the network effects inherent in the value and practicality of any given blockchain system, the choice of each network participant cannot be done on a purely individual basis—the choice will ultimately depend both on their own personal preferences and on the perception or expectation of what others will choose.[177] This is often referred to as a 'schelling point'—i.e., the choice that everyone thinks many others will make.

A variety of stakeholders contribute to establishing the schelling point in any given blockchain network: the mining pools aggregating the hashing power of multiple miners; cryptocurrency exchanges; blockchain explorers; custodian wallet providers; or any

---

[174] Wenbo Wang and others, 'A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks' (2019) 7 *IEEE Access* 22328.
[175] Wessel Reijers and others (n. 14) 829-830.
[176] Bronwyn Howell, Petrus Potgeiter and Bert Sadowski, 'Governance of Blockchain and Distributed Ledger Technology Projects' (2nd Europe-Middle East-North African Regional Conference of the International Telecommunications Society (ITS): "Leveraging Technologies For Growth", Aswan, 18-21 February 2019) 3 <http://hdl.handle.net/10419/201737> accessed 7 October 2022.
[177] Michael Abramowicz, 'The Very Brief History of Decentralized Blockchain Governance' (2020) 22 *Vanderbilt Journal of Entertainment and Technology Law* 273, 279.

commercial operator accepting cryptocurrencies, whose choice will influence their customers' choices; and specific individuals, such as charismatic leaders who have high credibility in the space or social media influencers whose opinions can reach a larger number of people.[178] All these actors contribute, in their own way, to steering the behaviour of users, token holders and all other network participants towards that particular schelling point that best suits their own interests. To be sure, the fact that governance is distributed does not mean that power is equally distributed: certain actors have significantly more influence (and stake) over the network than others—as discussed further below. As such, the schelling point of a blockchain network is somewhat difficult to predict, because it depends on a mixture of private economic interests, financial incentives, social norms and ideological values, which might diverge from one category of stakeholders to another.

In that regard, it is important to distinguish between endogenous rules, developed *by* the community and *for* the community, and exogenous rules, imposed by a third party over a particular community.[179] *On-chain* rules are mostly endogenous to a particular community—they are generally elaborated by a small and close-knit community of developers and they must be adopted by all relevant network participants[180]—yet they also rely on exogenous market dynamics in order to establish the relevant economic incentives for people to participate in the network. Similarly, *off-chain* governance rules can be both endogenous and exogenous to a particular blockchain community. At first, much of the attention was given to endogenous off-chain rules, which include the social norms and various institutional arrangements by which blockchain developers, miners, validators, or other community members participate in the deliberation and decision-making processes of that particular blockchain community. There are, however, a variety of exogenous off-chain rules—such as laws and regulations—that might indirectly affect the operations of a particular blockchain system and ultimately lead to the establishment of a different *schelling* point. As has been argued previously with respect to power dynamics in virtual communities, the establishment of a schelling point is not just of a theoretical interest but bears directly on the material interest of people part of these blockchain communities.[181] We analyse these in the following sections.

Regulation by Code

An overview of the history of Internet governance[182] might help provide a better understanding of the interplay between *regulation by code* and *regulation by law,* as it applies to both centralised and decentralised Internet platforms. Many of the rules embedded in the technological infrastructure of online platforms are elaborated by large multinational companies, for the most part interested in maximising the adoption and the economic returns

[178] De Filippi and McMullen (n. 126) 15; Schneider (n. 84).
[179] De Filippi and McMullen (n. 172) 18-20.
[180] Shermin (n. 98) 507.
[181] Julie Cohen, 'Cyberspace as/and Space' (2007) 107 *Columbia Law Review* 210, 255; Suzor (n. 76) 1833.
[182] *See, e.g.,* Lee Bygrave and Jon Bing (eds.) *Internet governance: Infrastructure and Institutions* (Oxford University Press 2009).

that they can derive from these platforms.[183] Yet, these rules might sometimes turn out to be incompatible with national laws—such as the data protection regulations of many European countries[184]—and it is thus necessary to find ways to ensure the proper application of national laws on these global and transnational Internet platforms.[185]

As described earlier, code is increasingly used as a complement or a supplement to existing laws. This has led to the establishment of a new system of private ordering,[186] which often introduce additional constraints to those actually prescribed by the law.[187] Yet, while it is true that—at least in the case of centralised online platforms—regulation by code has progressively taken over regulation by law,[188] it would be wrong to conclude that laws no longer have a role to play in the regulation of online behaviours. To the contrary, in the context of centralised platforms which are effectively *ruled by code*,[189] the *rule of law* could ultimately have a major role to play, as governments use law to regulate the code of these platforms by exerting pressure on the online operators which are managing and operating the code (Fig. 2).[190] As a result, over the last two decades, online operators have progressively been turned into private executive bodies responsible for policing the Internet and enforcing both public and private ordering.[191]

[FIGURE 2 ABOUT HERE]

At the outset, it might be tempting for regulators to try and address the issues of blockchain regulation similarly to how they have addressed the regulation of the Internet network: focusing on the low-hanging fruit (i.e., those players who can be more easily regulated) and leveraging the growing centralisation and concentration of power in the hands of a few powerful intermediaries, in order to influence the operations of the overall network. As a result, regulators and policy-makers may attempt to impose responsibilities or liabilities onto these actors who have the ability to (albeit partially) influence the operations of a

[183] Alice Marwick, 'Silicon Valley and the Social Media Industry' in Jean Burgess, Alice Marwick and Thomas Poell (eds.) *The SAGE Handbook of Social Media* (SAGE 2018) 314; José Van Dijck, *The Culture of Connectivity: A Critical History of Social Media* (Oxford University Press 2013) 21.

[184] Luciano Floridi, 'Soft ethics, the governance of the digital and the General Data Protection Regulation' (2018) 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 1, 2-4; Jim Isaak and Mina Hanna, 'User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection' (2018) 51 *Computer* 56.

[185] Philip Weiser, 'The Future of Internet Regulation' (2009) 43 *UC Davis Law Review* 529, 534; Molly Land, 'The Problem of Platform Law: Pluralistic Legal Ordering on Social Media' in Paul Berman (ed.) *The Oxford Handbook of Global Legal Pluralism* (Oxford University Press, 2020) 977.

[186] David Baron, 'Private ordering on the Internet: The eBay community of traders' (2002) 4 *Business and Politics* 245.

[187] Tim Wu 'When code isn't law' (2003) 89 *Virginia Law Review* 679, 707-708; Annemarie Bridy, 'Graduated response and the turn to private ordering in online copyright enforcement' (2010) 89 *Oregon Law Review* 81, 83-84.

[188] Lawrence Lessig, 'The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation' (1997) 5 *Commlaw Conspectus* 181, 191; Lawrence Lessig, 'Law Regulating Code Regulating Law' (2003) 35 *Loyola University Chicago Law Journal* 1, 11-12; Lessig (n. 30) 24.

[189] James Grimmelmann, 'Regulation by Software' (2005) 114 *Yale Law Journal* 1719, 1728-1729.

[190] Andrew Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge, 2007) 34.

[191] Joel Reidenberg, 'States and Internet Enforcement' (2003) 1 *University of Ottawa Law & Technology Journal* 213, 221, 226; Niva Elkin-Koren, 'After twenty years: revisiting copyright liability of online intermediaries' in Susy Frankel and Daniel Gervais (eds.) *The Evolution and Equilibrium of Copyright in the Digital Age* (Cambridge University Press 2014).

blockchain (e.g., cryptocurrency exchanges, custodian wallets, core developers, mining pools, etc.) in order to influence their governance decisions—whether or not it is morally or ethically appropriate to hold them responsible.[192]

In contrast to the legal pluralist view described above, this approach favours a monist, hierarchical view of the legal system. In fact, as an attempt to subordinate the legal order of blockchain-based systems (*rule of code*) to the state's legal order (*rule of law*), this approach seeks to subordinate the operations and technical infrastructure of a blockchain-based network to the hegemony of a political sovereign. This is done by enacting regulations which push towards further centralization of the actors participating in a blockchain network (e.g. miners, cryptocurrency exchanges, etc.) so as to acquire more influence over the operations of the network. Over time, this might lead to a progressive shift—which we already observed with the Internet network—where blockchain networks become increasingly *ruled by code*, rather than subject to the *rule of code.* Accordingly, while the regulation of mining activities, cryptocurrency exchanges, and blockchain developers can be effective for achieving certain purposes, if poorly conceived they could have unintended consequences that inhibit the growth of blockchain networks.

One example of a state seeking to subject the operation of a blockchain-based network to a state's positive law is the regulation of mining activities on the Bitcoin network in specific jurisdictions. For instance, in Iran, after thousands of commercial mining licences were granted in the 2019-2020 period in order to legalise operations which had previously been undertaken in a "climate of fear",[193] the government declared a ban on all Bitcoin mining activities to protect cities against potential blackouts. Furthermore, as the US sanction on Tornado Cash demonstrates, the imposition of a sanction by a state on an entity, person or even smart contract address in a blockchain network can have a collateral effect on validators in the network who may begin censoring transactions originating from sanctioned addresses by default out of a desire to appear legally compliant, even when the sanction is inapplicable.[194]

Cryptocurrency exchanges and custodian wallets are another interesting target for litigation and regulation because of the influence they have in the governance of blockchain networks.[195] Indeed, even if they do not have the power to decide which transactions get recorded onto a blockchain (a right exclusive to network miners and validators), these intermediary operators—acting as the 'on-ramps' and 'off-ramps' to the blockchain ecosystem—have a significant weight in the governance of blockchain networks. Because

---

[192] Yeung (n. 116) 218.

[193] Paddy Baker, 'Over 1,000 Bitcoin Miners Granted Licences in Iran' (*CoinDesk,* 2020) <https://www.coindesk.com/policy/2020/01/27/over-1000-bitcoin-miners-granted-licenses-in-iran-report/> accessed 7 October 2022.

[194] Vishal Chawla and Tim Copeland, 'At least 23% of Ethereum blocks are complying with US sanctions' (*The Block*, 28 September 2022) <https://www.theblock.co/post/173417/at-least-23-of-ethereum-blocks-are-complying-with-us-sanctions> accessed 7 October 2022.

[195] Dirk Wiegandt, 'Blockchain and Smart Contracts and the Role of Arbitration' (2022) 39 *Journal of International Arbitration* 671, 687-688.

they control the private keys of their users, they have the power to decide with whom these users can or cannot transact, as well as to which fork of the blockchain the transactions will effectively be broadcasted. Policymakers in many jurisdictions, pursuant to transnational soft laws like the Financial Action Task Force's (FATF) Recommendation No. 15, have already imposed stringent Know-Your-Customer (KYC) and Anti-Money Laundering (AML) or Counter Terrorist Financing (CTF) regulations onto these actors with a view to addressing public policy concerns. In the future, they could push regulations further and require them to only accept or execute only transactions from, or to, specific addresses or blockchain wallets which have been 'white listed' according to stringent due diligence requirements. Conversely, certain addresses or blockchain wallets may be 'black listed' through the application of worldwide freezing orders.[196] More radically, they might force these intermediary actors to choose a particular fork over another, thereby indirectly gaining the ability to influence the adoption (or removal) of specific features into a blockchain-based network.

Another potential pressure point is blockchain developers, who could be held liable for the usage made of the software they create. Such an approach was first proposed by Walch, who contends that the developers of existing public blockchain networks like Bitcoin should hold fiduciary duties towards the users or third-party operators that rely on these networks.[197] Yet, in addition to re-evaluating existing liability frameworks for software developers—whereby open source software developers are generally exempt from liability for the software they produce, if provided with the necessary warranty disclaimers[198]—this solution also reflects a common misunderstanding of how blockchain networks operate. Even if blockchain developers have the ability to propose certain changes to the underlying blockchain protocol, they do not have the power to *impose* these changes onto the network, given that each network participant must individually agree to switch to the new protocol.[199] Thus, as opposed to centralised platform operators who may decide, at any point in time, to change the design and architecture of their platforms (and directly implement these changes without seeking users approval), the developers of a blockchain-based network only have limited capacity to affect the network. In a recent judgement, which considered, *inter alia,* the question whether core Bitcoin developers had a fiduciary duty towards particular users of the blockchain network, Falk J. held that they did not owe such a duty, because their relationship to a sub-group of bitcoin owners did not require single-minded loyalty towards them. Moreover, as "developers are a fluctuating group of individuals [...] it cannot realistically be argued that they owe continuing obligations to, for example, remain as developers and make future updates whenever it might be in the interests of [bitcoin] owners to do so.[200] Besides,

---

[196] *CLM* (n. 96)

[197] Angela Walch, 'In Code(rs) we Trust: Software Developers as Fiduciaries in Public Blockchains' in Philip Hacker and others (eds.) *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford University Press 2019) 59.

[198] Rod Dixon, *Open Source Software Law* (Artech House 2004) 103-104; Carla Reyes, '(Un)Corporate Crypto Governance' (2020) 88 *Fordham Law Review* 1875, 1908; Bryan Choi, 'Software as a Profession' (2020) 33 *Harvard Journal of Law & Technology* 557, 566-567.

[199] Raina Haque and others 'Blockchain Development and Fiduciary Duty' (2019) 2 *Stanford Journal of Blockchain Law and Policy* 139, 141.

[200] *Tulip Trading Limited v. Bitcoin Association For BSV & Ors* [2022] EWHC 667 (Ch) (25 March 2022, para 75. This judgment is currently before the England & Wales Court of Appeal.

"bitcoin owners could not realistically be described as entrusting their property to a fluctuating, and unidentified, body of developers of the software".[201]

As a last resort, when everything else fails, governments could turn to end-users, imputing liability to those who use or interact with a particular blockchain-based system. While it might be difficult to identify these users—in light of the pseudonymity of public and permissionless blockchain networks—some countries have already begun to experiment with such draconian measures. In the U.S., for instance, the U.S. Treasury Department has recently imposed sanctions on the popular cryptocurrency mixer Tornado Cash—which was allegedly used to facilitate money laundering. These sanctions make it illegal for any U.S. citizen, resident or company to transact with the smart contract addresses associated with that blockchain-based service, which currently hold more than $400 million worth of Ether. Anyone contravening these sanctions will be held criminally liable under a strict liability regime—meaning that there is no need to demonstrate intent or knowledge of these sanctions. Such sanctions have been heavily criticised by the blockchain community, because they apply to a general-purpose technology which also comes with legitimate uses (e.g. safeguarding financial privacy).[202]

Moreover, criminalising users for the mere act of interacting with, or having governance power over a blockchain-based infrastructure might be problematic to the extent that—as opposed to a centralised platform where one needs to intentionally create an account in order to interact with the platform (e.g. Paypal or Lydia)—on a blockchain, users might receive tokens on their wallet from a particular smart contract application, without them even being aware of it. This is what happened, for instance, with Tornado Cash, where—following the establishment of the sanctions—anonymous users began to send small amounts of Ether from Tornado Cash to wallets controlled by public figures, such as American television host Jimmy Fallon and Coinbase CEO, Brian Armstrong. The point was to show that if the U.S. Office of Foreign Assets Control (OFAC) require that every U.S. person refuse any transaction stemming from a sanctioned entity, this simply cannot be done in the context of an open and decentralised network like Ethereum, on which Tornado Cash runs, as receivers of the funds do not have the power to accept or reject the transaction, and thy might not even be informed of having received them.[203] Hence, anyone could theoretically send Ether from Tornado Cash to a U.S. person, without their approval, thereby subjecting them to potential liability.

The same applies for governance tokens. Anyone whose wallet is controlling tokens that can be used to engage in the governance of a particular DApp or DAO (whether or not

---

[201] ibid [73].

[202] Jerry Brito and Peter van Valkenburgh, 'Analysis: What is and what is not a sanctionable entity in the Tornado Cash case' (*CoinCenter*, 15 August 2022) <https://www.coincenter.org/analysis-what-is-and-what-is-not-a-sanctionable-entity-in-the-tornado-cash-case/> accessed 7 October 2022.

[203] Mat Di Salvo, 'Tornado Cash User 'Dusts' Hundreds of Public Wallets—Including Celebs Jimmy Fallon, Steve Aoki and Logan Paul' (DeCrypt, 9 August 2022) <https://decrypt.co/107090/tornado-cash-dusts-public-wallets-jimmy-fallon-brian-armstrong-steve-aoki-logan-paul> accessed 7 October 2022.

they are aware of being in possession of these tokens) may qualify as a co-administrator (or 'general partner') of this DAO, and be therefore regarded as jointly and severally liable with all the other token holders, for any illicit action taken by the DAO.[204] Yet, some users might not even be aware of being in possession of these tokens (as in the case of 'airdrops'), while others may be aware of holding these tokens, but might not possess a sufficiently significant share to influence the decisions taken by the DAOs. As a result, it may be problematic, and indeed unjust in some instances, to hold these users responsible for the decisions which have been taken collectively by the DAO, by the mere fact of being the holders of a particular amount of governance tokens.

Paradoxically, given that governments can only impute liability on individuals or companies over which they have jurisdiction, they might hold these parties accountable for the decisions taken by the overall blockchain system, even if they only marginally contributed to these decisions. In doing so, governments might ultimately dissuade actors located in their own jurisdiction from engaging in the process of blockchain governance, by fear of legal liability.[205] This might further undermine governments' ability to influence the operations of these blockchain-based systems, since only those who operate outside of their jurisdiction will effectively engage in the blockchain governance process. This has been described by Yeung as the 'cat and mouse' approach to regulation, as harsher regulations may encourage regulated entities to explore new pathways to escape regulation—by either moving into less regulated jurisdictions, or by relying on more decentralised tools.[206]

An alternative approach, intended to encourage more participation and experimentation of local companies in the blockchain ecosystem, entails the creation of regulatory sandboxes,[207] in which specific legal requirements and taxation schemes are inapplicable. Such sandboxes for experimentation have been created in countries as diverse as Thailand and Uganda, to build blockchain-based securities clearing infrastructure and new decentralised applications.[208] Pushing further in that direction, these regulatory sandboxes could also be used to encourage blockchain companies to explore the use of blockchain technology as a regulatory technology (RegTech), coming up with innovative solutions that rely on the technological guarantees provided by blockchain technology as an alternative way to meet specific regulatory requirements or to achieve specific policy objectives,[209] which are

---

[204] See, e.g., the complaint filed on 22 September 2022 in *Commodity Futures Trading Commission v. Ooki DAO (formerly d/b/a bZx DAO), an unincorporated association*, Civil Action No: 3:22-cv-5416 alleging that the governance token-holders of Ooki DAO, as members of an unincorporated association, had violated the Commodity Exchange Act, 7 U.S.C. §§ 1-26, and Commission Regulations ("Regulations"), 17 C.F.R. pts. 1-190 (2021) and were thus jointly and severally liable for this violation.

[205] Dirk Zetzsche, Ross Buckley and Douglas Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2018) *University of Illinois Law Review* 1361, 1391.

[206] Yeung (n. 116) 219-220.

[207] Denisa Kera, 'Sandboxes and Testnets as "Trading Zones" for Blockchain Governance' in Javier Prieto and others (eds.) *Blockchain and Applications* (Springer 2020).

[208] Baker McKenzie, *International Guide to Regulatory Fintech Sandboxes* (*Baker McKenzie*, 2018) 13 <https://www.bakermckenzie.com/en/-/media/files/insight/publications/2018/12/guide_intlguideregulatorysandboxes_dec2018.pdf>; *The Free Zones (Declaration of Block Chain Technologies Free Zone) Instrument, 2020*, The Uganda Gazette, No. 42, Volume No. CXIII, dated 17 July 2020.

[209] De Filippi, Mannan and Reijers (n. 9).

currently dealt with through expensive formalities and reporting obligations.[210] For instance, the transparency of blockchain technology, combined with the resilience and tamper-resistance of many blockchain-based networks, could enable the emergence of new means of regulatory compliance that do not require the same formalities or the same degree of regulatory scrutiny, because of the technological guarantees embedded directly into the technological infrastructure.[211] Yeung describes this approach as seeking an 'efficient alignment' intended to create mutually beneficial interactions between the rule of code and the rule of law.[212]

There are, however, elements of a blockchain that resist, and thus cannot be reduced to a particular legal order. For instance, public and permissionless blockchains are likely to remain beyond the reach of the law,[213] because they are—by their very nature—nearly impossible to shut down and will thus continue to operate even if one or more governments were to force all the nodes within their jurisdiction to shut down. Moreover, some of the operations undertaken on top of a blockchain network (e.g., interacting or contracting with a DAO) cannot be easily encompassed by the law, and—even if they could—law enforcement would remain a significant challenge.

Yet, even if the traditional means of regulation are not readily applicable in the blockchain space, there are other ways in which intervention is possible. In particular, as the adoption of blockchain technology increases,[214] public sector agencies or other institutional frameworks,[215] it will become increasingly necessary to identify new avenues to control or influence existing blockchain-based systems, so as to preserve the rule of law in the global arena.[216] We identify these new regulatory pathways below.

Regulation via Governance

As discussed earlier, when assessed in light of Lessig's framework, *on-chain* governance can be described as a combination of endogenous *architectural rules* ("code is law") and exogenous *market dynamics* (based on mechanism design and game theoretical incentives), whereas *off-chain* governance can be described as including both endogenous *social norms* (i.e., that particular set of rules and procedures established and promoted by a relevant blockchain community) and exogenous pressures established by *law and regulation*, which may possibly affect or influence a community's social norms.[217] Combined,

[210] Alexis Collomb, Primavera de Filippi and Klara Sok, 'Blockchain Technology and Financial Regulation: A Risk-Based Approach to the Regulation of ICOs' (2019) 10 *European Journal of Risk Regulation* 263.
[211] For example, if all transactions are executed on a public blockchain, one cannot claim to have undertaken a transaction that does not appear on the blockchain, or—vice versa—to not have engaged into a transaction that does appear on the blockchain.
[212] Yeung (n. 116) 220-222.
[213] De Filippi, Mannan and Reijers (n. 9).
[214] Tommy Koens, Pol van Aubel and Erik Poll, 'Blockchain adoption drivers: The rationality of irrational choices' (2020) 33 *Concurrency and Computation: Practice and Experience* 1 .
[215] Adam Sulkowski, 'Blockchain, Business Supply Chains, Sustainability, and Law: The Future of Governance, Legal Frameworks, and Lawyers?' (2019) 43 *Delaware Journal of Corporate Law* 303, 310-319.
[216] Werbach (n. 118) 520, 534.
[217] Avinash Dixit, *Lawlessness and Economics: Alternative Modes of Governance* (Princeton University Press 2004) 6-7.

endogenous on-chain and off-chain governance (i.e., blockchain code and social norms) constitutes a separate, transnational legal order that remains distinct from any one state's legal order, but are nonetheless affected by exogenous regulatory forces (i.e., market dynamics and national laws) that remain outside of the control of the relevant blockchain community.

[TABLE 1 ABOUT HERE]

If the regulation of the Internet network has been mostly achieved through the regulation of intermediary operators—who had the ability to design and modify the technological infrastructure of their online platforms—the same approach cannot easily be undertaken in the case of a public and permissionless blockchain network, given that no regulatory authority has the power to control or change the on-chain governance rules enshrined within the technological infrastructure of the network. Accordingly, if the code of a blockchain-based network cannot be unilaterally modified by any given authority, a more effective means of intervention would be to focus on the off-chain governance rules, i.e., influencing the set of social norms promoted and endorsed by a particular blockchain community in order to influence their design choices (Fig 3).

[FIGURE 3 ABOUT HERE]

The importance of social norms, and their role in the governance of existing blockchain-based systems can be illustrated by comparing the social norms of Bitcoin with those of Ethereum.[218] The Bitcoin network is characterised by a desire to achieve almost perfect immutability, drawing from the "code is law" paradigm. As a result, despite the unavoidable technical fixes that it has gone through, the Bitcoin protocol has essentially failed to evolve to address the core scalability issues,[219] with the emergence of several competing networks (or forks) with slightly different technical characteristics—e.g. Bitcoin Cash, Bitcoin SV, Bitcoin Gold.

The Ethereum community, in contrast, puts more emphasis on the notion of "distributed consensus" and has been shown to be much more willing to modify the protocol of the Ethereum blockchain in order to reverse the effect of certain transactions that might have a negative impact on the network, or society more generally.[220] This was well illustrated in the aftermath of the TheDAO attack, which has shown that whenever on-chain governance fails—either because of a bug, or because of an unforeseen and unexpected event that had not been previously foreseen—off-chain governance represents an opportunity for the community to intervene and resolve the issue. The solution, in this specific case, had been deliberated and implemented endogenously, in accordance with the social norms of the broader Ethereum community.

---

[218] Wessel Reijers, Fiachra O'Brolcháin and Paul Haynes, 'Governance in Blockchain Technologies & Social Contract Theories' (2016) 1 *Ledger* 134.
[219] De Filippi and Loveluck (n. 126).
[220] Wessel Reijers and Mark Coeckelbergh, 'The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies' (2018) 31 *Philosophy & Technology* 103, 123-124.

A few months later, the Ethereum community encountered a second incident due to another on-chain governance failure, which, this time, was addressed by taking into account both endogenous and exogenous factors. This second incident was due to a flaw in the code of a smart contract library (developed by *Parity*) used in the deployment of multi-signature wallets on the Ethereum blockchain.[221] The exploitation of the vulnerability in that code has led to the freezing of over USD $300 million worth of Ether at the time, locked into these wallets with no possibility of withdrawal. Just as with the TheDAO attack, this incident raised a series of heated debates within the Ethereum community, who had to decide whether or not the protocol should be changed—once again—in order to release those funds. Ultimately, in this instance, the decision was made not to intervene.

An interesting aspect of this decision is that it was partially motivated by exogenous rules. Indeed, even if several community members (including those whose funds had been locked) were advocating for the implementation of a standardised procedure for lost fund recovery, some of the core developers and prominent members of the Ethereum Foundation were concerned about the potential legal liability they might incur as a result of such an intervention[222]—including risks of fiduciary liability.[223] While bug fixes and protocol upgrades are dealt with via standardised procedures (e.g., EIPs), there is no formalised procedure to discuss contentious protocol changes of a non-technical nature. The reason is that the establishment of such a procedure would inevitably require vesting specific individuals (blockchain engineers, for the most part) with the power to suggest, approve, amend or reject protocol changes of a political nature. Not only are many blockchain engineers unqualified to make these types of decisions, they generally also do not want to assume any responsibility for these decisions. Hence, the decision not to change the Ethereum protocol to allow for the recovery of these funds was motivated as much by the desire to signal the fact that the Ethereum blockchain is, and should remain, an immutable tamper-resistant record of transactions, than by the desire to protect community members from any risk of legal liability. These motivations overrode other considerations—such as the desire to make victims whole—which may have called for recovering the funds, as it was decided in the TheDAO attack.

One important lesson that can be derived from both the TheDAO attack and the Parity bug is that blockchain governance is a complex phenomenon that cannot be understood by

---

[221] Giuseppe Destefanis and others, 'Smart contracts vulnerabilities: a call for blockchain software engineering?' in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, (IEEE 2018) 21-23.
[222] For instance, Yoichi Hirai was an Ethereum code editor who resigned from his position in the aftermath of the Parity bug, following personal concerns that an Ethereum Improvement Proposal (EIP) over a standardised format for lost fund recovery would potentially violate Japanese law. Rachel-Rose O'Leary, 'Ethereum Developer Resigns as Code Editor Citing Legal Concerns' (*CoinDesk*, 2018) <https://www.coindesk.com/markets/2018/02/15/ethereum-developer-resigns-as-code-editor-citing-legal-concerns/> accessed 7 October 2022.
[223] Haque and others (n. 199); Walch (n. 197) 66.

looking solely at the internal governance practices of any given blockchain community.[224] Even though the governance of blockchain-based systems is generally defined by a particular set of endogenous rules (both on-chain or off-chain), exogenous rules can directly or indirectly affect the operations of these endogenous practices.

At the technical level, the TheDAO attack has shown that a blockchain community (Ethereum, in this case) can directly affect the operations of any smart contract deployed on top of that blockchain, simply by modifying the rules of the underlying blockchain protocol.[225] At the same time, the Parity incident has shown that exogenous rules of a non-technical nature—such as the laws and regulations of a particular jurisdiction—may have an impact on the internal governance and decision-making processes of existing blockchain communities. While, on the one hand, people whose funds have been frozen could theoretically have sued Parity in their own jurisdiction with a view to recover damages (although, in practice, no one did), on the other hand, the law of national jurisdictions nonetheless impacted the situation, as community members did at least partially motivate their decisions on how to proceed with the case based on the threat of legal liability. This is a demonstration of how the exogenous legal orders of national jurisdictions can influence the rules and norms established within a particular blockchain community.

This highlights the fact that policymakers are not powerless when it comes to the regulation of decentralised public and permissionless blockchain-based systems. Although they are not capable of directly and unilaterally affecting their internal operations, policymakers can respond to the (alleged) *alegality* of these systems by shaping or influencing the behaviours of individuals or companies, through a series of sanctions and rewards.[226] By understanding the multiple and intricate dynamics of blockchain governance (i.e., governance by architecture, market mechanisms, and social norms), policymakers can generate new regulatory pressure points that will affect the social norms of blockchain communities, and therefore, indirectly, also their technical design. This approach constitutes an indirect legal response to the *alegal* properties of blockchain systems.

Conclusion

The widespread adoption of Internet technologies in the 1990s has brought to the forefront the complexity associated with the regulation of a global and decentralised communication network that transcends geographical boundaries and national jurisdictions. That regulatory challenge was eventually resolved through the progressive concentration of power in the hands of a few centralised platforms (e.g., Google, Facebook, Twitter, YouTube) that collect most Internet traffic. Hence, Internet governance is currently facing a very

---

[224] Thomas John and Mantri Pam, 'Complex Adaptive Blockchain Governance' in Erik Puik and others (eds.), *MATEC Web Conference, vol. 223, The 12th International Conference on Axiomatic Design (ICAD 2018)* (EDP Sciences 2018); Philip Hacker, 'Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations', in Philip Hacker and others, *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford University Press 2019).

[225] Similarly, decisions made at the Internet governance level (e.g., packet filtering or national firewalls) might indirectly impact the operations of a blockchain-based network. De Filippi and Wright (n 15) 47-48.

[226] De Filippi, Mannan and Reijers (n 9).

different set of challenges than it did 20 years ago.[227] Originally, the main concern was to ensure the application of the rule of law among a distributed network of actors, often with divergent interests, who had to coordinate their activities with no recourse to any centralised sovereign authority.[228] Today, we are witnessing the emergence of *functional sovereigns* with the proliferation of large centralised online platforms that transcend national boundaries and are controlled by private corporations operating across multiple jurisdictions.[229] Accordingly, the main challenge of Internet governance today is that of guaranteeing that these platforms remain subject to national sovereignty and the rule of law.

Just like the Internet, the global and decentralised nature of blockchain networks has challenged the ability of governments and other regulatory authorities to impose their sovereignty over these networks. Yet, the strategies adopted in the context of today's Internet governance—holding intermediary operators responsible for whatever happens on the platforms they control—are not readily applicable in the context of open and decentralised blockchain-based networks, whose operations are mostly disintermediated and dictated by distributed consensus. As a result, the challenges faced by existing blockchain-based networks are more similar to those of early Internet governance, when the Internet was still regarded as an open and decentralised network.

Although the coercive power of the law cannot be readily applied to regulate blockchain-based systems, existing laws and regulations can nonetheless influence the operations of these code-based platforms—albeit indirectly. Indeed, despite the lack of a centralised operator or trusted authority in charge of managing or regulating public and permissionless blockchain networks, the autonomy of these networks remain limited: governments retain the ability to implement specific regulatory and policy pathways to counteract the alleged *alegality* of blockchain technology. To be sure, even if many blockchain-based networks operate outside of the reach of the law, the various actors involved in the governance of these networks (i.e., those who collectively manage and maintain the network) are not, themselves, immune from the law and may—under the threat of litigation—be more inclined to behave in such a way as to minimise the risks of legal liability.[230]

Whether this is done by imposing fiduciary duties on blockchain developers, regulating commercial operators like crypto-currency exchanges and custodian wallet providers, establishing liability regimes for miners or validators, different regulatory strategies can contribute to influencing the governance of the overall network—albeit only partially or indirectly. These approaches suffer from two important limitations. On the one the hand, they only work to the extent that there is a sufficient degree of centralization and intermediation within a particular blockchain-network. On the other hand, they have the

[227] Mannan and Schneider (n. 33) 3.
[228] *See, e.g.,* Richard Collins, *Three Myths of Internet Governance: Making Sense of Networks, Governance and Regulation* (University of Chicago Press 2009); Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (MIT Press 2010) 25.
[229] Laura DeNardis, *The Global War for Internet Governance* (Yale University Press, 2014) 154-157; Pasquale (n. 84) above.
[230] Dirk Zetzsche and others (n 205).

performative effect of further reinforcing the centralization and concentration of power in the hands of a few regulated intermediaries, as has happened before with the Internet. Together, this undermines the space for a rule of code in a pluralist, polycentric legal system.

This opens up a fresh set of research questions to explore in future work: if there is value in decentralisation, what are the possible combinations of on-chain governance rules (i.e., endogenous protocol or constitutional rules and exogenous market incentives or mechanism design) and off-chain governance rules (i.e., endogenous social norms and exogenous legal provisions) that need to undergird future policy proposals to ensure that the blockchain ecosystem does not follow the same path as the Internet, and that the distributed nature of blockchain technology is preserved over time?[231] What do theories on polycentric governance and collective action have to offer in further developing or improving such policy proposals? Crucially, how can we combine on-chain and off-chain governance systems in order to ensure the legitimacy of blockchain-based systems, with respect to both community members and society at large? We hope to explore this in future work.

[231] *See, e.g.,* Eric Alston, 'Constitutions and Blockchains:Competitive Governance of Fundamental Rule Sets' (2020) 11 *Case Western Reserve Journal of Law, Technology & the Internet* 131.