Blockchain Technology and the Rule of Code: Regulation via Governance

Primavera De Filippi, Morshed Mannan & Wessel Reijers[*]

Abstract

Blockchain-based systems, by virtue of their technological features, present challenges to the rule of law. These systems work in a transnational and decentralized 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 toward the rule of code. First, it examines 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 the Decentralized Autonomous Organization Attack with the newer example of Tornado Cash. Second, this Article identifies ways in which lawmakers can respond to the rule of code within a global, pluralist, and polycentric legal system. After distinguishing on-chain and off-chain governance, this Article 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.

Table of Contents

[*] Primavera De Filippi, Director of Research at the National Center of Scientific Research and Faculty Associate at the Berkman-Kein Center for Internet and Society, Harvard University; Morshed Mannan, Lecturer in Global Law and Digital Technologies, Edinburgh Law School, University of Edinburgh; Wessel Reijers, Postdoctoral Researcher at the Department of Media Studies, Paderborn University. This research was funded by the European Research Council under the European Union's Horizon 2020 Research and Innovation Programme (Grant Agreements No. 865856). We would like to thank Larry Backer, Giovanni Sartor, and Matthias Siems for their comments on earlier drafts of this Article. Morshed would especially like to thank the Max Weber Programme at the European University Institute for their support during the 2021–2022 academic year and Alyson Price for her feedback on an earlier version of this manuscript. All three authors contributed equally to this Article.

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 behavior.[1] At that time, it was generally believed that regulation by code would ultimately prevail over regulation by law,[2] because the decentralized nature of the internet network made it difficult—if not impossible—for any centralized authority to enforce the law.[3] Internet pioneers, like Timothy May and John Perry Barlow, went as far as to claim 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 that cyberspace is "unregulatable" to highlight the complexities inherent in the regulation of a decentralized 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.[7] Indeed, the claims of early blockchain advocates are quite similar to

[1] *See* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 Tex. L. Rev. 553, 555 (1998).

[2] *See* James A. Lewis, *Sovereignty and the Role of Government in Cyberspace*, Brown J. World Affs., Spring–Summer 2010, at 55, 60.

[3] Jack Goldsmith & Tim Wu, Who Controls the Internet? Illusions of a Borderless World viii (2006).

[4] *See* Peter Ludlow, *New Foundations: On the Emergence of Sovereign Cyberstates and Their Governance Structures*, *in* Crypto Anarchy, Cyberstates, and Pirate Utopias 1, 4 (Peter Ludlow ed., 2001).

[5] *See* David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. Online L. art. 3, para. 42.

[6] *See* John Palfrey, *Four Phases of Internet Regulation*, 77 Soc. Rsch. 981, 990–91 (2010).

[7] *See* Lana Swartz, *What Was Bitcoin, What Will It Be? The Techno-Economic Imaginaries of a New Money Technology*, 32 Cultural Stud. 623, 627 (2018).

those of the early internet pioneers[8]: the decentralization inherent in the technological design of many blockchain-based systems promotes a more distributed governance and reduces the risks of surveillance or control from centralized power structures—be they private companies or governmental authorities.[9] Moreover, because of their distinctive characteristics, blockchain platforms are sometimes described as being "*alegal*" in that they—allegedly—operate beyond the purview of the law.[10] Both the blockchain protocol and the software code deployed onto a blockchain infrastructure can, therefore, be regarded as a new means to regulate behavior: a more powerful form of *lex informatica* which has been referred to as "*Lex Cryptographia*."[11] 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 nonstate 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 centralized 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"[12] and the more blockchain-specific approach of "law is code";[13] 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;[14] and between traditional political institutions and blockchain-based systems characterized by the capacity of the "code [to] run[] itself."[15]

[8] *See, e.g.*, Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Bitcoin 1 (Aug. 21, 2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/W467-C9F7].

[9] *See* Quinn DuPont, Cryptocurrencies and Blockchains 34, 40–41 (2019).

[10] Primavera De Filippi, Morshed Mannan & Wessel Reijers, *The Alegality of Blockchain Technology*, 41 Pol'y & Soc'y 358, 358 (2022).

[11] Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of* Lex Cryptographia, SSRN 1 (Mar. 12, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [https://perma.cc/K4UF-RSZL].

[12] Lawrence Lessig, *Code Is Law*, Harv. Mag., Jan. 1, 2000, https://www.harvardmagazine.com/2000/01/code-is-law-html [https://perma.cc/R5LH-GHRG].

[13] Primavera De Filippi & Samer Hassan, *Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is Code*, 21 First Monday (Dec. 5, 2016), https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657 [https://perma.cc/Z662-TNEY].

[14] Karen Yeung, *Regulation by Blockchain: The Emerging Battle for Supremacy Between the Code* of *Law and Code* as *Law*, 82 Mod. L. Rev. 207, 207 (2019).

[15] Wessel Reijers, Iris Wuisman, Morshed Mannan, Primavera De Filippi, Christopher Wray, Vienna Rae-Looi, Angela Cubillos Vélez & Liav Orgad, *Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies*, 40 Topoi 821, 822–23, 825, 828 (2021) (emphasis omitted).

Yet most of the contributions are focused on the distinction between *regulation by law* and *regulation by* (blockchain) *code*, concerning 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.[16] This Article builds upon the notion of "rule of code," first introduced in 2018 by Primavera De Filippi and Aaron Wright in *Blockchain and the Law*,[17] and expands it to explore the specificities of blockchain code, concerning its relationship to sovereignty, that make it different from more traditional software code. The aim of this Article 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 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 behavior 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.[18] This Article, thus, argues, instead of trying to regulate blockchain-based systems with the same regulatory techniques that have been previously used for the regulation of the internet, endogenous practices of polycentric governance are more appropriate.

This Article is organized 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 comparing the extent to which internet and blockchain technology resist traditional regulation, this Article draws a distinction between two different modes of regulation—*regulation by law* and *regulation by code*—which are often combined as part of both public and private ordering as an attempt to govern and regulate the digital space. This Article subsequently

[16] *See* PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 187, 196–97, 200 (2018).

[17] *Id.* at 7.

[18] *See* Gunther Teubner, '*Global Bukowina*': *Legal Pluralism in the World Society*, *in* GLOBAL LAW WITHOUT A STATE 3, 4 (Gunther Teubner ed., 1997); Jean-Philippe Robé, *Multinational Enterprises: The Constitution of a Pluralistic Legal Order*, *in* GLOBAL LAW WITHOUT A STATE, *supra*, at 45, 49–50.

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 decentralized platforms that operate autonomously and independently from any centralized 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, Part II 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—e.g., forcing intermediaries to leverage code as a regulatory tool—in effect, a *regulation by code* approach. An alternate approach would recognize 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.

I. Blockchain Technology and the Rule of Code

A. How Blockchain Resists Regulation

A public blockchain can be broadly defined as a decentralized database or public ledger that is replicated on a decentralized peer-to-peer network and that operates without any centralized authority.[19] 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 decentralized database.[20] 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 authorized people—and permissioned—i.e., only a pre-identified set of operators are entitled to participate in maintaining and

[19] *See* Nakamoto, *supra* note 8, at 1.

[20] *See* Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen & Huaimin Wang, *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, 2017 IEEE Int'l Cong. on Big Data 557, 559.

securing the network.[21] This Article focuses specifically on public and permissionless blockchains, as they raise the most interesting challenges for 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.[22] 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.[23] As long as one copy of the blockchain exists, it is possible to replicate the network from scratch.[24]

Alongside their decentralized 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.[25] 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.[26] Any unilateral modification will be automatically detected by other nodes.[27] 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 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.[28] This is because the distributed consensus of a blockchain requires network nodes to constantly check and verify the validity and legitimacy of everyone else's transactions.[29] In addition, as all blockchain transactions are cryptographically signed with the key of the party executing them, they are forever associated with that party.[30] This means, 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 the key was compromised. Yet, to protect the privacy and confidentiality of transactions, some blockchains—e.g., Monero and Zcash—have

[21] *See id.*

[22] *See* Wright et al., *supra* note 11, at 45, 54.

[23] *See* Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen & Huaimin Wang, *Blockchain Challenges and Opportunities: A Survey*, 14 INT'L J. WEB & GRID SERVS. 352, 357 (2018).

[24] *See* MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY, at x, 32 (2015).

[25] *See* Zheng et al., *supra* note 20, at 557.

[26] *See id.*

[27] *See* Zheng et al., *supra* note 23.

[28] *See* SWAN, *supra* note 24, at 1.

[29] *See* Zheng et al., *supra* note 23, at 352.

[30] *See* IMRAN BASHIR, MASTERING BLOCKCHAIN: DISTRIBUTED LEDGERS, DECENTRALIZATION AND SMART CONTRACTS EXPLAINED 24 (2017).

adopted specific cryptographic primitives,[31] 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.[32]

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.[33] People willing to use the network need only 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.[34]

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.[35] This makes it possible to create decentralized applications that do not run on a centralized server but rather are executed in a distributed and deterministic manner by all the network nodes.[36] These applications are generally referred to as "smart contracts"—a term that refers generically to any snippet of code deployed on a blockchain.[37]

Finally, one important element that characterizes public and permissionless blockchain networks is the *lack of coercion* on the part of a single operator. Traditional web services are controlled by online

[31] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer & Madars Virza, *Zerocash: Decentralized Anonymous Payments from Bitcoin*, 2014 IEEE Symp. on Sec. & Priv. 459, 460; Licheng Wang, Xiaoying Shen, Jing Li, Jun Shao & Yixian Yang, *Cryptographic Primitives in Blockchains*, 127 J. Network & Comput. Applications 43, 46 (2019); Shen Noether, Adam Mackenzie & the Monero Research Lab, *Ring Confidential Transactions*, 1 Ledger 1, 3 (2016).

[32] *See* Ronald L. Rivest, Adi Shamir & Yael Tauman, *How to Leak a Secret*, 2001 Int'l Conf. on the Theory & Application of Cryptology & Info. Sec. 553, 553–54; Xiaoqiang Sun, F. Richard Yu, Peng Zhang, Zhiwei Sun, Weixin Xie & Xiang Peng, *A Survey on Zero-Knowledge Proof in Blockchain*, IEEE Network, July–Aug. 2001, at 198, 202–03.

[33] *See* Roy Lai & David Lee Kuo Chuen, *Blockchain—From Public to Private*, *in* 2 Handbook of Blockchain, Digital Finance, and Inclusion 145, 147–48, 153 (David Lee Kuo Chuen & Robert H. Deng eds., 2017).

[34] *See* Tao Feng, Xuan Chen, Chunyan Liu & Xiaoqin Feng, *Research on Privacy Enhancement Scheme of Blockchain Transactions*, Sec. & Priv., Nov.–Dec. 2019, at 1, 7–8, https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.89 [https://perma.cc/EP5V-3LHZ].

[35] *See* Massimo Bartoletti & Livio Pompianu, *An Empirical Analysis of Smart Contracts: Platforms, Applications, and Design Patterns*, 2017 Fin. Cryptography & Data Sec. 494, 494.

[36] *See* Siraj Raval, Decentralized Applications: Harnessing Bitcoin's Blockchain Technology 7–8 (2016).

[37] Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 2 First Monday (1997), https://firstmonday.org/ojs/index.php/fm/article/view/548/469 [https://perma.cc/52MJ-26U4].

operators who are responsible for making the relevant design choices for the interface through which users interact with the platform.[38] 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.[39] In contrast, the rules of a blockchain-based network cannot be changed without the agreement of the users.[40] Any protocol change requires active participation of the network nodes, which are expected to upgrade their clients in order to abide by the new protocol.[41] Refusal to accept the new protocol rules will result in the maintenance of the original blockchain protocol or the emergence of a new blockchain-based network that constitutes a fork of the previous network.[42]

In light of these characteristics, it becomes clear why blockchains, and other decentralized applications, distinguish themselves from more traditional and centralized online applications.[43] As Lawrence Lessig puts it, in cyberspace, "code is law" because it actually assumes the same functionalities as law.[44] 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.[45] Concerning blockchain-based applications, code also constitutes a means to regulate behavior: both the blockchain protocol and the smart contract code determine what can or cannot be done with a particular blockchain network.[46] 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 centralized operator—and may, consequently, largely ignore the law.[47] 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

[38] *See* Juri Mattila, *The Blockchain Phenomenon—The Disruptive Potential of Distributed Consensus Architectures* 6–7 (Rsch. Inst. Finnish Econ., Working Paper No. 38, 2016), https://www.econstor.eu/bitstream/10419/201253/1/ETLA-Working-Papers-38.pdf [https://perma.cc/9MNU-HSMA].

[39] *See* Morshed Mannan & Nathan Schneider, *Exit to Community: Strategies for Multi-Stakeholder Ownership in the Platform Economy*, 5 Geo. L. Tech. Rev. 1, 3 (2021).

[40] *See* Mattila, *supra* note 38, at 6–7.

[41] *See id.*

[42] *See* De Filippi & Wright, *supra* note 16, at 24.

[43] *See id.* at 3.

[44] Lawrence Lessig, Code version 2.0, at 5 (2006).

[45] *See* Lawrence Lessig, *Law Regulating Code Regulating Law*, 35 Loy. U. Chi. L.J. 1, 8–9 (2003).

[46] *See* De Filippi & Hassan, *supra* note 13.

[47] *See* De Filippi et al., *supra* note 10, at 358.

transaction that is deemed to be illegal.[48] Even more critically, given the tamper-resistant features and immutability of a blockchain, the mere act of creating or amending legislation to penalize these blockchain transactions is, on its own, insufficient to reverse them.[49]

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, 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.[50] The claim is that blockchain technology takes trust away from centralized operators and distributes it toward the underlying peer-to-peer network.[51] Accordingly—the argument goes—as long as people 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.[52] At the same time, the supremacy of code increases the *autonomy* of blockchain-based systems for traditional forms of authority—whether these relate to government regulation and public ordering or private ordering via contractual and technological means.[53] 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 it.[54] 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.[55] Although online operators (or regulators) can

[48] Georgios Dimitropoulos, *The Law of Blockchain*, 95 Wash. L. Rev. 1117, 1182 (2020).

[49] *See* Nakamoto, *supra* note 8, at 1.

[50] Gili Vidan & Vili Lehdonvirta, *Mine the Gap: Bitcoin and the Maintenance of Trustlessness*, 21 New Media & Soc'y 42, 43, 47 (2019).

[51] *See id.* at 41–46. This peer-to-peer network is maintained by a polycentric group of miners, validators, developers, etc. *See* Primavera De Filippi, Morshed Mannan & Wessel Reijers, *Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance*, Tech. in Soc'y, Aug. 2020, 2, 7 (2020), https://www.sciencedirect.com/science/article/pii/S0160791X20303067?via%3Dihub [https://perma.cc/MK3H-DCFG]; *see also* Nigel Dodd, Vires in Numeris*: Taking Simmel to Mt Gox*, *in* The Anthem Companion to Georg Simmel 121, 136 (Thomas Kemple & Olli Pyyhtinen eds., 2016); Nigel Dodd, *The Social Life of Bitcoin*, Theory, Culture & Soc'y, May 2018, at 35, 46–47.

[52] *See* De Filippi et al., *supra* note 51, at 7.

[53] *See* De Filippi et al., *supra* note 10, at 360–64.

[54] *See, e.g.*, Usman W. Chohan, *The Decentralized Autonomous Organization and Governance Issues*, SSRN 5 (Mar. 19, 2022) (on file with author) (defines a decentralized autonomous organization and explains how they operate).

[55] *See, e.g.*, *infra* notes 167–75 and accompanying text (discussing the example of Tornado Cash where, despite sanctions, the U.S. government could not control the application, which continued to process transactions).

shut down the centralized interface that provides access to these applications (i.e., the platforms and front ends 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.[56] The recent example of U.S. sanctions on Tornado Cash (discussed in Section I.C) 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.[57] 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* and *operational autonomy* of blockchain-based systems—that makes them significantly different from the more traditional and centralized online platforms that emerged from the internet era. Although this may reduce the risk of an online operator unilaterally modifying the protocol of these decentralized applications, these very same characteristics might also lead to potential conflicts between a state's legal regime—what this Article refers 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 this Article refers to as the *rule of code*.[58]

B. *The Rule of Code vs. the Rule by Code*

The concept of the rule of law—as popularized by the jurist, Albert Dicey—implies that all citizens and private and public actors, including governmental agencies, are accountable under the law.[59] There is no singular authoritative definition of the rule of law; yet it is regarded as a

[56] *See infra* notes 167–75 and accompanying text. Note that most blockchain-based applications are being accessed (today, at least) by means of centralized 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. *See infra* notes 262–64 and accompanying text. 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.

[57] *See* Press Release, U.S. Dep't of Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916 [https://perma.cc/36VG-PXPS]; gets qt, *The Downside of Sanctioning Tornado Cash*, CoinDesk (June 14, 2024, 12:07 PM), https://www.coindesk.com/opinion/2022/08/16/the-downside-of-sanctioning-tornado-cash/ [https://perma.cc/H8JA-Q5TT].

[58] *See* De Filippi & Wright, *supra* note 16, at 206–08.

[59] *See* A.V. Dicey, Introduction to the Study of the Law of the Constitution 189 (8th ed. 1915).

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.[60] 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, to 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, which is unsurprising as the concept has a history that is at least 4,000 years old.[61] 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.[62] One of its main objectives is to separate law from politics.[63] The French and German legal systems also have their own interpretations of the rule of law:[64] "*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.[65] 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.[66] Laws must be

[60] 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.

U.N. Secretary General, The Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies, ¶ 6, U.N. Doc. S/2004/616 (Aug. 23, 2004).

[61] *See* Judith Shklar, *Political Theory and the Rule of Law*, *in* The Rule of Law: Ideal or Ideology 1, 1 (Allan C. Hutchinson & Patrick Monahan eds., 1987). Shklar highlights the historical relevance of the rule of law in the field of political theory because of the political objectives it embodied. *Id.* However, she notes that "'the [r]ule of [l]aw' has become meaningless thanks to ideological abuse and general over-use". *Id.* On the history of the rule of law, see Fernanda Pirie, The Rule of Laws: A 4,000-Year Quest to Order the World 456 (2021).

[62] *See* Shklar, *supra* note 61, at 4, 6.

[63] *See* 1 Charles Montesquieu, The Complete Works of M. de Montesquieu, 198–201 (1777).

[64] *See* John Bell, *Comparative Administrative Law*, *in* The Oxford Handbook of Comparative Law 1250, 1257 (Mathias Reimann & Reinhard Zimmermann eds., 2d ed. 2019).

[65] *Id.* at 1262–63.

[66] Kay Windthorst, *Separation of Powers from the German Perspective*, 47 Duq. L. Rev. 905, 918 (2009); *see also* Paul R. Verkuil, *Separation of Powers, the Rule of Law and the Idea of Independence*, 30 Wm. & Mary L. Rev. 301, 305–07 (1989).

tested by the courts of law, who are responsible for verifying that they do not fall afoul of a state's constitution.[67]

In established democracies, the rule of law is considered to be a valuable tool for assessing the legitimacy of a government,[68] which requires the internalization of basic legal and political values by public institutions and those who work for them.[69] In this context, 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,[70] ideally by an independent judiciary.[71] For the academic, Friedrich 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.[72] These criteria fulfill the "thin" conceptions of the rule of law.[73] There are also "thick[er]" interpretations of the rule of law, which consider the rule of law to include democratic participation and substantive entitlements, such as social welfare rights, rights of dignity and justice, and the right to own private property.[74] Under that thicker conception, for the rule of law to exist, it is not enough that the law prevails over the rule by men,[75] but also that it respects a necessary set of normative conditions (e.g., economic liberalism), which guarantees its

[67] *See* David Feldman, *Democracy, the Rule of Law and Judicial Review*, 19 FED. L. REV. 1, 13 (1990).

[68] Mirko Canevaro, *The Rule of Law as the Measure of Political Legitimacy in the Greek City States*, 9 HAGUE J. ON RULE L. 211, 211–12 (2017).

[69] *See* Feldman, *supra* note 67, at 11.

[70] Paul Craig, *Formal and Substantive Conceptions of the Rule of Law: An Analytical Framework*, *in* THE RULE OF LAW AND THE SEPARATION OF POWERS 95, 97 (Richard Bellamy ed., 2005); *see also* Jeremy Waldron, *The Rule of Law and the Importance of Procedure*, 50 NOMOS 3, 3 (2011); JOSEPH RAZ, THE AUTHORITY OF LAW: ESSAYS ON LAW AND MORALITY 214–17 (1979); LON L. FULLER, THE MORALITY OF LAW 107 (1964).

[71] *See* David Boies, *Judicial Independence and the Rule of Law*, 22 WASH. U. J.L. & POL'Y 57, 58 (2006). Gretchen Helmke and Frances 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. *See* Gretchen Helmke & Frances Rosenbluth, *Regimes and the Rule of Law: Judicial Independence in Comparative Perspective*, 12 ANN. REV. POL. SCI. 345, 361 (2009).

[72] F.A. HAYEK, THE ROAD TO SERFDOM 75–76 (Bruce Caldwell ed., 2001) (1944).

[73] MATHIAS SIEMS, COMPARATIVE LAW 339 (2d ed. 2018).

[74] *Id.*; *see* Ioannis Kampourakis, Sanne Taekema & Alessandra Arcuri, *Reappropriating the Rule of Law: Between Constituting and Limiting Private Power*, 14 JURIS. 76, 93 (2023); UGO MATTEI & LAURA NADER, PLUNDER: WHEN THE RULE OF LAW IS ILLEGAL 14 (2008); TOM BINGHAM, THE RULE OF LAW 3–4 (2010); BRIAN Z. TAMANAHA, ON THE RULE OF LAW: HISTORY, POLITICS, THEORY 91, 112 (2004); *see also* Ronald A. Cass, *Property Rights Systems and the Rule of Law*, *in* THE ELGAR COMPANION TO THE ECONOMICS OF PROPERTY RIGHTS 222, 222 (Enrico Colombatto ed., 2004).

[75] *See* ALAIN SUPIOT, GOVERNANCE BY NUMBERS: THE MAKING OF A LEGAL MODEL OF ALLEGIANCE 204 (Saskia Brown trans., 2017).

legitimacy.[76] This more substantive version of the rule of law has been critiqued by the philosopher Joseph Raz, among others, for blurring the distinction between the rule of law as a principle and other concepts such as justice, human rights, etc.[77] It is also unclear which substantive requirements should be included in this thicker conception of the rule of law.

For the purpose of this Article, 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 concerning the sovereign. It is a principle that requires the law to be obeyed and applied equally to everyone, and it also minimizes the risk of arbitrary power being exercised by the sovereign.[78] Furthermore, the rule of law is not only a relevant concept for liberal democratic states but has transnational significance as well. Some scholars have argued that transnational rule of law discourse "frames and contextualizes all efforts to manage and regulate law, legitimacy, and conceptions of legality in the sphere of the transnational."[79] The *rule of law* stands in contrast to the *rule by law*, which refers to the instrumentalization of law as a tool of political power.[80] The *rule by law* has been extensively studied in the field of constitutional and administrative law,[81] often with reference to authoritarian regimes.[82] It may be defined as a system of government in which the law does not apply equally to everyone; one in which the sovereign remains above the law and, therefore, can 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.[83] The *rule by law* thus only has an enabling power but not a constraining power over the sovereign. Although both the

[76] *See* RAZ, *supra* note 70, at 143–45.

[77] *See id.* at 211.

[78] *See* DENISE WOHLWEND, THE INTERNATIONAL RULE OF LAW: SCOPE, SUBJECTS, REQUIREMENTS 30, 36 (2021).

[79] Jothie Rajah, *'Rule of Law' as Transnational Legal Order*, *in* TRANSNATIONAL LEGAL ORDERS 340, 343 (Terence C. Halliday & Gregory Shaffer eds., 2015).

[80] *See* TAMANAHA, *supra* note 74, at 108.

[81] *See* Nóra Chronowski & Márton Varju, *Two Eras of Hungarian Constitutionalism: From the Rule of Law to Rule by Law*, 8 HAGUE J. ON RULE L. 271, 272 (2016); Ratna Rueban Balasubramaniam, *Has Rule by Law Killed the Rule of Law in Malaysia?*, 8 OXFORD U. COMMONWEALTH L.J. 211, 211 (2008).

[82] *See, e.g.*, Ji Li, *The Leviathan's Rule* by *Law*, 12 J. EMPIRICAL LEGAL STUD. 815, 815 (2015); Jeremy Waldron, *Rule* by *Law: A Much Maligned Preposition* 1–2 (N.Y. Univ. Sch. of L., Working Paper No. 19-19, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3378167 [https://perma.cc/BVP6-PCB9].

[83] *See* JEREMY WALDRON, THOUGHTFULNESS AND THE RULE OF LAW 237 (2023) ("'Rule by law' means the state uses law to control its citizens but never allows law to be used by the people to control the state.") Although the *rule by law* is often placed in a contrasting, binary relationship

rule of law and the *rule by law* reflect an idealized conception of the relationship between politics and law[84]—whose interrelations are often more intertwined than they appear at first sight[85]—these two concepts remain useful as shorthand 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.[86] 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."[87]

On the internet, most online platforms are administered by companies which, at their discretion, dictate the rules that underpin online interactions.[88] These platforms operate like "monocentric political system[s]," in which the "prerogatives for determining [and] enforcing" the rules are "vested in some single office or decision structure that has an ultimate monopoly over the legitimate exercise of coercive capabilities."[89] In the early days of the internet, this was only a marginal issue because 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.[90] Although they had full control over the way in which users could interact on their platform,[91] 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

with the rule of law, Waldron questions the degree to which the two concepts are distinct as well as the manner in which the former concept is denigrated. *Id.* at 239–49.

[84] 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. *See* Roberto Mangabeira Unger, Law in Modern Society: Toward a Criticism of Social Theory 179–80 (1976).

[85] *See* Martin Shapiro & Alec Stone Sweet, On Law, Politics, and Judicialization 2 (2002).

[86] *See* Anthony W. Pereira, *Of Judges and Generals: Security Courts Under Authoritarian Regimes in Argentina, Brazil, and Chile*, *in* Rule by Law: The Politics of Courts in Authoritarian Regimes 23, 50 (Tom Ginsburg & Tamir Moustafa eds., 2008).

[87] G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 7 (Dec. 10, 1948).

[88] *See* Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 Nw. U. L. Rev. 105, 105, 112 (2010).

[89] Vincent Ostrom, *Polycentricity (Part 1)*, *in* Polycentricity and Local Public Economies 52, 55 (Michael D. McGinnis ed., 1999).

[90] *See* Nathan Schneider, *Decentralization: An Incomplete Ambition*, 12 J. Cultural Econ. 265, 278 (2019).

[91] *Id.* at 274, 277–78.

by governments or public authorities. It is precisely at this juncture that the question of the rule of law on the internet becomes pressing.

Concerning the internet, the rule of law can be seen as a set of principles and practices that ensure online platforms are accountable for the way in which they regulate online interactions and that they do so in a way that is consistent with the rule of law.[92] There are 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.[93] Legal scholars like Nicholas Suzor have argued that such principles should be reflected in the governance of virtual communities.[94] 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.[95]

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[96]: just "[a] few tweaks to settings in a database can banish a user, silence her, or confiscate all her digital goods."[97] Platform operators can shape how a user interacts with other users with legal repercussions outside of the platform.[98] All the while, the contracts that users enter into with operators overwhelmingly favor the latter and greatly limit their potential liability.[99] As such, these platforms can be said to be *ruled by code*: code is instrumentalized by the platform

[92] Nicholas Suzor, *The Role of the Rule of Law in Virtual Communities*, 25 Berkeley Tech. L.J. 1817, 1819 (2010).

[93] *See id.* at 1866–85.

[94] *Id.* at 1818.

[95] *See, e.g.*, Evelyn Douek, *"What Kind of Oversight Board Have You Given Us?*,*"* U. Chi. L. Rev. Online (May 11, 2020), https://lawreview.uchicago.edu/online-archive/what-kind-oversight-board-have-you-given-us [https://perma.cc/82TN-QADW].

[96] *Cf.* Gabriel J. Hassen, *Digital Feudalism—An Analysis of Ownership and Control in the Information Age*, 4 Phx. L. Rev. 1027, 1031, 1049–52 (2011) (describing "the effects of digital media licensing on society and on the economy").

[97] James Grimmelmann, *Anarchy, Status Updates, and Utopia*, 35 Pace L. Rev. 135, 138 (2014).

[98] *See* Morshed Mannan, *Theorizing the Emergence of Platform Cooperativism: Drawing Lessons from Role-Set Theory*, 2022 Ondernemingsrecht Tijdschrift 64, 65.

[99] *See* Suzor, *supra* note 92, at 1819.

operators to determine how users can interact on these platforms.[100] Just like in the *rule by law*, in which law is instrumentalized by the sovereign as a means of exercising control over the citizens, in the *rule by code*, the code is instrumentalized by online operators as a means of exercising control over the platform's 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 *bypassing* the sovereign authority of nation-states, especially with their role in regulating commerce and creating or maintaining an inclusive public sphere.[101] Recently, scholars such as Frank Pasquale, Mariana Mazzucato, and Nathan Schneider have analyzed the emergence of new forms of sovereignty stemming from the rise of megaplatforms like Facebook, Amazon, and Google.[102] As "the new sovereigns of cyberspace,"[103] these platforms are establishing themselves as new "functional sovereign[s]" reigning over digital fiefdoms.[104] Online platforms have embedded themselves so strongly in the infrastructure of public and commercial life that they have become quasi-sovereign authorities.[105] Sovereignty in this context is not to be understood as the indivisible phenomenon described by philosopher Thomas Hobbes in *Leviathan*, but rather as the idea "that two or several authorities may have limited, relative, differential or functional sovereignty over certain areas, groups or resources."[106] Although some have argued that these platform juggernauts extend principles and concepts from the jurisdictions where they are headquartered (e.g., common law

[100] Code is not only computer code but also a way of codifying policies (e.g., content moderation policy, privacy policy) and administering them through a code-based platform as opposed to a human supervisor, even when there are people at the edge (e.g., moderators).

[101] *See* Ruth Lapidoth, *Sovereignty in Transition*, 45 J. Int'l Affs. 325, 334–36 (1992).

[102] *See* Frank Pasquale, *From Territorial to Functional Sovereignty: The Case of Amazon*, Open Democracy (Jan. 5, 2018), https://www.opendemocracy.net/en/digitaliberties/from-territorial-to-functional-sovereignty-case-of-amazon/ [https://perma.cc/D67S-F6G2]; Mariana Mazzucato, *Preventing Digital Feudalism*, Project Syndicate (Oct. 2, 2019), https://www.project-syndicate.org/commentary/platform-economy-digital-feudalism-by-mariana-mazzucato-2019-10 [https://perma.cc/3BEQ-R3XU]; Nathan Schneider, *Admins, Mods, and Benevolent Dictators for Life: The Implicit Feudalism of Online Communities*, 24 New Media & Soc'y 1965, 1965–66, 1974–81 (2022).

[103] Rebecca MacKinnon, Consent of the Networked: The Worldwide Struggle for Internet Freedom xxiv (2012).

[104] Pasquale, *supra* note 102.

[105] *See* Frank Pasquale, *Digital Capitalism—How to Tame the Platform Juggernauts*, WISO Direkt, June 2018, at 1, 1, https://library.fes.de/pdf-files/wiso/14444.pdf [https://perma.cc/4E2W-37Y6].

[106] Lapidoth, *supra* note 101, at 326, 334.

notions of freedom of contract),[107] these functional sovereigns also have motivations and guiding principles of their own. Applying a constitutional lens to platform governance through this *rule of law* vs. *rule by law* analysis is useful because it addresses the limitations of a formal contractualist approach to studying platform governance.[108] These limitations range from acknowledging the asymmetries of power between a platform operator and users to recognizing the (partial) inalienability of user rights in virtual communities.[109]

Exceptions exist when platforms seek to emulate the lawmaking processes to acquire ex ante legitimacy or to provide a redress mechanism that can remedy injustices ex post.[110] Wikipedia, for example, implemented a complex governance system that at least tries to mimic a democracy[111]—despite its limitations concerning inclusivity and representation.[112] Yet, regardless of the governance structure adopted within the Wikipedia platform, to the extent that it runs on a centralized infrastructure, it is those who control the infrastructure who have the ultimate say as to which technical rules will be implemented in the platform. Moreover, even if online operators have 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.[113]

[107] *See* Christopher Marsden, *Transnational Internet Law*, *in* The Oxford Handbook of Transnational Law 419, 432–33 (Peer Zumbansen ed., 2021).

[108] *See supra* note 92 and accompanying text.

[109] *See* Nicolas Suzor, *On the (Partially) Inalienable Rights of Participants in Virtual Communities*, 130 Media Int'l Austl. 90, 90 (2009); Brian F. Fitzgerald, *Software as Discourse: The Power of Intellectual Property in Digital Architecture*, 18 Cardozo Arts & Ent. L.J. 337, 384 (2000). On a more promising approach to social media governance that is grounded in relational contract theory, see Gilad Mills, *A Contractual Approach to Social Media Governance*, 42 Yale L. & Pol'y Rev. 522, 525–27 (2024).

[110] *See, e.g.*, Piotr Konieczny, *Governance, Organization, and Democracy on the Internet: The Iron Law and the Evolution of Wikipedia*, 24 Socio. F. 162, 189 (2009).

[111] *Id.*

[112] *See* Judd Antin, Raymond Yee, Coye Cheshire & Oded Nov, *Gender Differences in Wikipedia Editing*, 7 Int'l Symp. on Wikis & Open Collab. Proc. 11, 11 (2011); Eduardo Graells-Garrido, Mounia Lalmas & Filippo Menczer, *First Women, Second Sex: Gender Bias in Wikipedia*, 26 ACM Conf. on Hypertext & Soc. Media Proc. 165, 165 (2015).

[113] 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. *See* Douek, *supra* note 95. Although this is intended to implement a transnational, private legal order for content moderation, because Facebook's headquarters and a majority of its managers and employees are in the United States,

The same is not true for blockchain-based systems, in which there is no centralized operator or trusted intermediary in charge of managing the system.[114] 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.[115] As such, it can be assimilated to a particular type of "polycentric" system[116]—one in which "many . . . decision structures are assigned limited and relatively autonomous prerogatives to determine, enforce and alter legal relationships."[117] 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 decentralized governance, many blockchain networks and decentralized applications running on top of these networks are relatively centralized when it comes to power distribution. For instance, the major blockchain networks relying on proof-of-work, such as Bitcoin and Ethereum (until September 15, 2022), rely on a few, highly centralized mining pools that control the majority of the hashing power used to power these networks.[118] Similarly, many of the blockchains that rely on proof-of-stake are also suffering from an extensive concentration of power amongst

Facebook's content moderation policy also promotes U.S. free speech norms at an international level. *See* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1602, 1669 (2018). 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. *See* Vishwas T. Patil & R.K. Shyamasundar, *Efficacy of GDPR's Right-to-be-Forgotten on Facebook*, 14 INT'L CONF. ON INFO. SYS. SEC. PROC. 364, 377 (2018).

[114] De Filippi et al., *supra* note 10, at 358–59.

[115] *See* Wright et al., *supra* note 11, at 2.

[116] *See* MICHAEL POLANYI, THE LOGIC OF LIBERTY: REFLECTIONS AND REJOINDERS 170–71 (1951).

[117] Ostrom, *supra* note 89, at 55.

[118] Ashish Rajendra Sai, Jim Buckley, Brian Fitzgerald & Andrew Le Gear, *Taxonomy of Centralization in Public Blockchain Systems: A Systematic Literature Review*, INFO. PROCESSING & MGMT., July 2021, at 1, 1, https://www.sciencedirect.com/science/article/pii/S0306457321000844 [https://perma.cc/RJ94-NX49]; Sarwar Sayeed & Hector Marco-Gisbert, *Assessing Blockchain Consensus and Security Mechanisms Against the 51% Attack*, 9 APPLIED SCIS., Apr.–June 2019, at 1, 4, https://www.mdpi.com/2076-3417/9/9/1788 [https://perma.cc/S278-WHXX]; Yves Renno, *From PoW to PoS: The Ethereum Merge's Game-Changing Impact Explained*, WIREX BLOG (Sept. 15, 2023), https://wirexapp.com/blog/post/from-pow-to-pos-the-ethereum-merges-game-changing-impact-explained-0787 [https://perma.cc/UZU6-225K].

the validators.[119] 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.[120] Anyone who tries to validate transactions that violate the underlying blockchain protocol will simply see these transactions rejected by the rest of the network.[121] 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*"[122]—as an analogy to the *rule of law* found in many liberal democratic states.

Many decentralized applications or decentralized autonomous organizations running on a blockchain are also only decentralized in theory.[123] In practice, they are often governed by a small number of actors (sometimes referred to as "whales") holding a huge portion of governance tokens,[124] or—perhaps more critically—they are administered by a few individuals operating a multi-sig,[125] who have the power to operate and upgrade the underlying smart contracts.[126] 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

[119] Nikos Leonardos, Stefanos Leonardos & Georgios Piliouras, *Oceanic Games: Centralization Risks and Incentives in Blockchain Mining*, 2 INT'L CONF. MATHEMATICAL RSCH. FOR BLOCKCHAIN ECON. 183, 184 (2020); *see also* Sheikh Munir Skh Saad & Raja Zahilah Raja Mohd Radzi, *Comparative Review of the Blockchain Consensus Algorithm Between Proof of Stake (POS) and Delegated Proof of Stake (DPOS)*, 10 INT'L J. INNOVATIVE COMPUTING 27, 28 (2020). Delegated Proof of State ("DPOS") was designed with the intention of improving the processing speed of blockchain protocols. Saad & Radzi, *supra*, at 29. DPOS has also been criticized, however, for reducing the decentralization of blockchains, as this consensus mechanism makes a small number of elected delegates responsible for the validation process. *Id.*

[120] *See* Andrej Zwitter & Jilles Hazenberg, *Cyberspace, Blockchain, Governance: How Technology Implies Normative Power and Regulation*, *in* BLOCKCHAIN, LAW AND GOVERNANCE 87, 94–95 (Benedetta Cappiello & Gherardo Carullo eds., 2021).

[121] *See infra* notes 162–64 and accompanying text.

[122] Wright et al., *supra* note 11, at 7 (emphasis added).

[123] *See* Ashish Rajendra Sai, Towards a Holistic Assessment of Centralization in Distributed Ledgers 15–20, 30 (Jan. 1, 2021) (Ph.D. dissertation, University of Limerick) (on file with University of Limerick).

[124] Olivier Rikken, Marijn Janssen & Zenlin Kwee, *Governance Challenges of Blockchain and Decentralized Autonomous Organizations*, 24 INFO. POLITY 397, 410 (2019); Tom Barbereau, Reilly Smethurst, Orestis Papageorgiou, Alexander Rieger & Gilbert Fridgen, *DeFi, Not So Decentralized: The Measured Distribution of Voting Rights*, 55 HAW. INT'L CONF. ON SYS. SCIS. PROC. 6043, 6050 (2022).

[125] *See* Henrik Axelsen, Johannes Rude Jensen & Omri Ross, *When Is a DAO Decentralized?*, COMPLEX SYS. INFORMATICS & MODELING Q., June–July 2022, at 51, 63.

[126] *See* Mehdi Salehi, Jeremy Clark & Mohammad Mannan, *Not So Immutable: Upgradeability of Smart Contracts on Ethereum*, ARXIV 1, 12 (June 1, 2022), https://doi.org/10.48550/arXiv.2206.00716 [https://perma.cc/2C3X-M8PW].

advance.[127] 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.[128] 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 new 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 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.

This Article refers 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 distributed systems—cannot easily be instrumentally used by centralized 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, 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*, the relationship between the *rule by code*, in which code is instrumentalized by platform operators to promote their own economic or political interests, can be contrasted with the *rule of code*, describing a situation in which code applies equally to all.[129]

[127] To understand the importance of secondary rules for blockchain governance, see generally Marco Crepaldi, *Why Blockchains Need the Law: Secondary Rules as the Missing Piece of Blockchain Governance*, 17 Int'l Conf. on A.I. & L. Proc. 189, 189 (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*, 27 Int'l J.L. & Info. Tech. 266, 290 (2019).

[128] *See* De Filippi et al., *supra* note 10, at 358, 366.

[129] 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 in connection with the scope and potential impact on people's lives. Today, the blockchain space is still immature and even the largest blockchain-based systems did not receive enough adoption to systematically

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*[130]: 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 noncontradictory 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 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, although many centralized online platforms are ruled by the whims of their centralized 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.[131]

impact the lives of citizens in the same way that the internet does. *See* Fernando E. Alvarez, David Argente & Diana Van Patten, *Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador* 1 (Nat'l Bureau of Econ. Rsch., Working Paper No. 29968, 2023), https://www.nber.org/papers/w29968 [https://perma.cc/6G4S-BL7H]. Although 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 et al., *supra* note 39, at 3. Although there is no guarantee that blockchain architectures will eventually acquire the same significance as today's large internet platforms, the first glimmers of this potential future can already be seen, 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* Alvarez et al., *supra*, at 1; Eric Vázquez, *The Technical Fix: Bitcoin in El Salvador*, 121 S. Atl. Q. 600, 600 (2022); Emily Flitter & David Yaffe-Bellany, *Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions*, N.Y. Times (Feb. 24, 2022), https://www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html [https://perma.cc/SC5S-VL3J].

[130] *See* Wohlwend, *supra* note 78, at 37–46. *But see* Jan Oster, *Code Is Code and Law Is Law—The Law of Digitalization and the Digitalization of Law*, 29 Int'l J.L. & Info. Tech. 101, 101–02 (2021).

[131] *See* Urs Gasser & Wolfgang Schulz, *Governance of Online Intermediaries: Observations from a Series of National Case Studies*, *in* Berkman Ctr. for Internet & Soc'y Research Series at 6 (Berkman Ctr. Internet & Soc'y, Research Publ'n No. 2015-5, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2566364 [https://perma.cc/7KAT-HCN3].

Decentralized peer-to-peer networks are also difficult to regulate because there is no single actor in charge of governing these networks. As such, they are not ruled by code. Without tackling the question of whether earlier decentralized peer-to-peer networks such as BitTorrent and Gnutella are subject to the rule of code,[132] which is beyond the scope of this Article, the claim here is that public and permissionless blockchain-based systems, that are not administered by any centralized authority and are composed of pseudonymous and globally distributed 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.[133] Although every node in a peer-to-peer network runs and executes 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 that are weaker, or absent, in the case of earlier peer-to-peer networks. In other words, the rule of code for 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. Thibault Schrepel illustrates this point, by showing how the *rule of law* and the *rule of code* might impose different trade-offs between potentially conflicting fundamental rights—for instance, between privacy and free speech.[134] This Article analyzes the extent of these discrepancies in the following Section.

C. 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.[135]

[132] *See* Raval, *supra* note 36, at 8.

[133] *See supra* notes 122–27 and accompanying text.

[134] *See* Thibault Schrepel, *Anarchy, State, and Blockchain Utopia: Rule of Law Versus Lex Cryptographia*, *in* General Principles of EU Law and the EU Digital Order 367, 377–83 (Ulf Bernitz et al. eds., 2020).

[135] *See* Nikos Sotirakopoulos, *Cryptomarkets as a Libertarian Counter-Conduct of Resistance*, 21 Eur. J. Soc. Theory 189, 195 (2018); Primavera De Filippi, *Bitcoin: A Regulatory Nightmare to a Libertarian Dream*, Internet Pol'y Rev., Apr.–May 2014, at 1, 3.

These applications leverage the pseudonymity of Bitcoin or other cryptocurrencies to facilitate money laundering[136]—often relying on obfuscation tools such as mixers and tumblers.[137] Pseudonymity is also exploited in the creation of decentralized marketplaces for illicit goods and services, e.g., in the Silk Road marketplace,[138] 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.[139] These applications are *illegal* in that they constitute criminal activities that are expressly punishable under a particular body of law.[140] It is thus to be expected that national law enforcement officials will assert their legal authority in trying to halt and deter these activities.[141] 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,[142] 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 Edmund Schuster, Kevin Werbach, and Karen 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.[143] As some scholars have noted, smart contracts are ambivalent about the actual content of the law and, more often than not, the traditional legal order has limited options to unravel a smart contract.[144] To be sure, traditional legal contracts are

[136] Christian Janze, *Are Cryptocurrencies Criminals Best Friends? Examining the Co-Evolution of Bitcoin and Darknet Markets*, Ams. Conf. on Info. Sys., 2017, at 1, 2.

[137] *See infra* notes 166–68 and accompanying text.

[138] Lawrence Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 Rich. J.L. & Tech. 1, 1–2 (2014).

[139] *See* Roman Matzutt, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Müllmann, Oliver Hohlfeld & Klaus Wehrle, *A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin*, 2018 Fin. Cryptography & Data Sec. Proc. 420, 421; Maurice Schellekens, *Does Regulation of Illegal Content Need Reconsideration in Light of Blockchains?*, 27 Int'l J.L. & Info. Tech. 292, 304 (2019).

[140] *See* Yeung, *supra* note 14, at 215–16.

[141] *Id.*

[142] De Filippi et al., *supra* note 10, at 364. 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.

[143] *See* Karen E.C. Levy, *Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law*, 3 Engaging Sci., Tech. & Soc'y 1, 3–4 (2017); Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 Berkeley Tech. L.J. 487, 527–28 (2018); Edmund Schuster, *Cloud Crypto Land*, 84 Mod. L. Rev. 974, 989–90 (2021).

[144] *See* Ari Juels, Ahmed Kosba & Elaine Shi, *The Ring of Gyges: Investigating the Future of Criminal Smart Contracts*, 2016 ACM Conf. on Comput. & Commc'ns Sec. Proc. 283, 283; Max

created according to specific rules defined by contract law and fossilized through terms and conditions agreed *ad idem*, to create a binding agreement between two or more parties.[145] 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 judgment in order to interpret the wording of the contractual provisions in light of the actual intent of the parties.[146] 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.[147]

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.[148] As such, the provisions of a smart contract are automatically executed by the technology with no opportunity for breach.[149] Despite the benefits they provide concerning 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.[150] 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 that 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 centralized operators can reverse an erroneous or illegitimate transaction and an enforcement authority can

Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 322 (2017); James Grimmelmann, *All Smart Contracts Are Ambiguous*, 2 J.L. & INNOVATION 1, 3, 14, 20 (2019).

[145] *See* Raskin, *supra* note 144, at 322.

[146] *See id.* at 314.

[147] *See generally* Levy, *supra* note 143.

[148] *See* Nataliia Filatova, *Smart Contracts from the Contract Law Perspective: Outlining New Regulative Strategies*, 28 INT'L J.L. & INFO. TECH. 217, 221–22, 227 (2020).

[149] *See* Alexander Savelyev, *Contract Law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law*, 26 INFO. & COMMC'NS TECH. L. 116, 126–27 (2017); Mateja Durovic & André Janssen, *The Formation of Blockchain-Based Smart Contracts in the Light of Contract Law*, 6 EUROPEAN REV. PRIV. L. 753, 756 (2019).

[150] *See* Levy, *supra* note 143, at 5.

seize funds from a third-party account following a court order.[151] In contrast, reversing a transaction after it has been recorded on a blockchain is simply not an option.[152] 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 for by the code.[153] Besides, although one could theoretically rely on the traditional legal system to claim monetary compensation for the value of these unseizable assets, the pseudonymity that characterizes a large majority of public and permissionless blockchains makes it virtually impossible for a claimant to reclaim their loss.[154]

A clear illustration of this discrepancy can be found in the aftermath of the Decentralized Autonomous Organization ("DAO") Attack.[155] The DAO was a decentralized investment fund deployed as a smart contract on the Ethereum blockchain.[156] The DAO managed to raise over 150 million dollars worth of Ether in less than one month of fundraising.[157] However, a vulnerability in the code enabled an attacker to siphon out one-third of these funds, leaving the original investors at loss.[158] 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 DAO smart contract.[159] 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

[151] *See Asset Forfeiture*, FBI, https://www.fbi.gov/investigate/white-collar-crime/asset-forfeiture [https://perma.cc/3LWC-MM3D].

[152] *See* Nakamoto, *supra* note 8, at 1.

[153] *See* Wright et al., *supra* note 11, at 21, 55. Note that this only applies in the case of noncustodial wallets. If the digital assets are held on a centralized exchange, a court order could order the exchange to freeze the disposal and liquidation of these assets.

[154] *See, e.g.*, CLM v. CLN, [2022] SGHC 46, 4–5 (Sing.) (the pseudonymity of individuals suspected of theft made it difficult for the Singapore High Court to identify who to sanction, requiring them to place injunctions and worldwide freezing orders on crypto-exchanges to prevent the disposal of digital assets).

[155] This example has already been mentioned many times in the literature. *See, e.g.*, Muhammad Izhar Mehar, Charles Louis Shier, Alana Giambattista, Elgar Gong, Gabrielle Fletcher, Ryan Sanayhie, Henry M. Kim & Marek Laskowski, *Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack*, J. CASES ON INFO. TECH., Jan.–Mar. 2019, at 19, 21. 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.

[156] *See id.*

[157] *Id.* at 20.

[158] *Id.*

[159] *Id.*

functionalities of the Ethereum blockchain—it was the result of a political decision.[160]

Because of the decentralized 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.[161] 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.[162] Eventually, the large majority of participating nodes agreed to the undertaking and the funds were successfully retrieved on the main Ethereum network.[163] However, some nodes rejected the change, considering that such an intervention impinged upon the principles of immutability and tamper resistance of the Ethereum blockchain[164] to the extent that it would ultimately constitute an outright violation of the *rule of code* enshrined in the blockchain protocol.[165]

The DAO Attack 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.[166] 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*. The attack might have been legal under the *rule of code*—as it did not violate the rules enshrined into the smart contract code—but it lacked the legitimacy endowed on lawful behavior under a thicker conception of the *rule of law*, such as respect for private property rights.

Another compelling example that delineates the intricate conflict between the *rule of code* and the *rule of law* is the case of Tornado

[160] Note that the distinction between protocol upgrades of a purely technical nature and the political response to The DAO Attack is necessarily a blurry one, since many technical upgrades can also be of a political nature. For instance, in the Bitcoin's blocksize debate, 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 & Benjamin Loveluck, *The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure*, INTERNET POL'Y REV., Sept. 2016, at 1, 16, https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure [https://perma.cc/CJ7E-C6HY].

[161] *See* Mehar et al., *supra* note 155, at 26.

[162] *See* Voshmgir Shermin, *Disrupting Governance with Blockchains and Smart Contracts*, 26 STRATEGIC CHANGE 499, 506 (2017).

[163] *Id.*

[164] *See* Mehar et al., *supra* note 155, at 20.

[165] *See* DE FILIPPI & WRIGHT, *supra* note 16, at 204.

[166] *See* Reijers et al., *supra* note 15, at 828.

Cash—a blockchain-based system designed to enhance the privacy of cryptocurrency transactions.[167] Users can send cryptocurrency to the Tornado Cash smart contract from one address and withdraw it to a different address, thereby obfuscating the identity of the cryptocurrency holder and making it difficult to trace the origin of the cryptocurrency transaction.[168] Although Tornado Cash can be used for both legitimate and illegitimate purposes, the legality of its operations remains a subject of contention in various jurisdictions.[169]

From the rule of code standpoint, Tornado Cash executes transactions in a deterministic manner, as dictated by the code of its smart contract and the underlying blockchain network. Tornado Cash neither discriminates nor judges the source or purpose of the funds it receives, adhering to the automated procedures embedded in its programming. This strict adherence to the rule of code might, however, lead to a potential misalignment with traditional legal frameworks, which often require transparency and traceability in financial transactions to combat money laundering and other illicit activities. Indeed, many jurisdictions require financial intermediaries to implement anti-money laundering ("AML") and know-your-customer ("KYC") procedures to ensure compliance with the *rule of law*. Tornado Cash enables users to bypass such regulatory requirements, raising concerns about its ability to facilitate illicit financial activities and evasion of legal obligations.

Yet the decentralized and deterministic nature of Tornado Cash, which—just like many other blockchain systems[170]—operates independently of any central authority, complicates the enforcement of laws and regulations. Traditional centralized online platforms that are ruled by code can be more easily regulated by existing authorities to the extent that they can hold online operators accountable for illicit activities occurring on these platforms.[171] The disintermediated nature of Tornado Cash not only disperses accountability but also introduces a layer of anonymity as users engage with the platform pseudonymously. This pseudonymity, coupled with the privacy features of Tornado Cash transactions, creates an additional barrier for law enforcement agencies

[167] Primavera De Filippi & Morshed Mannan, *Tornado Cash: The End of Blockchain Neutrality*, Zora Zine (Dec. 6, 2022), https://zine.zora.co/tornado-cash-primavera-de-filippi-morshed-mannan [https://perma.cc/HR5U-LMAK].

[168] *Id.*

[169] *E.g.*, Protos Staff, *Coin Center Loses Tornado Cash Lawsuit, Intends to Appeal*, Protos (Nov. 2, 2023), https://protos.com/coin-center-loses-tornado-cash-lawsuit-intends-to-appeal [https://perma.cc/3W9E-PHQX]; Jerry Brito & Peter Van Valkenburgh, *Analysis: What Is and What Is Not a Sanctionable Entity in the Tornado Cash Case*, Coin Center (Aug. 15, 2022), https://www.coincenter.org/analysis-what-is-and-what-is-not-a-sanctionable-entity-in-the-tornado-cash-case [https://perma.cc/C623-Z666].

[170] *See* Nakamoto, *supra* note 8, at 1.

[171] *See supra* note 131 and accompanying text.

attempting to trace and prosecute illicit activities facilitated by the platform.

On August 8, 2022, the U.S. Office of Foreign Assets Control ("OFAC") imposed sanctions on Tornado Cash.[172] The rationale behind these sanctions was the allegation that Tornado Cash facilitated a North Korean hacker group's laundering of proceeds from their illicit activities.[173] The sanctions made it illegal for any U.S. person to engage in transactions with the smart contract addresses associated with Tornado Cash—thereby demonstrating that, even when the *rule of law* cannot prevail over the *rule of code*, it can nonetheless dissuade people from engaging with a particular blockchain-based system. Significant consequences ensued in response to the OFAC sanctions, including the removal of the GitHub repositories, the shutting down of the Tornado Cash decentralized autonomous organization, the arrest of one of Tornado Cash's core developers, and, recently, the issuance of indictments against two Tornado Cash founders.[174] Despite all of this, the Tornado Cash smart contracts remain operative, and continue to process anonymous transactions.[175] This underscored the inherent resilience of decentralized blockchain-based systems to external intervention, further emphasizing the challenges authorities may encounter when attempting to regulate or shut down systems operating according to the rule of code.

D. *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.[176] They claim that decentralized blockchain-based systems cannot create conditions akin to the *rule of law* because "*ruling* always necessitates a hierarchy."[177] Others recognize that the *rule of code* cannot only escape the *rule of law* but also complement it or even reinforce it.[178] This Article adopts a legal,

[172] Press Release, U.S. Attorney's Off., S. Dist. of N.Y., Tornado Cash Founders Charged with Money Laundering and Sanctions Violations (Aug. 23, 2023), https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations [https://perma.cc/C9A9-KDD3].

[173] *Id.*

[174] *Id.*

[175] In the first half of 2024, more than 1.9 billion U.S. dollars was deposited in Tornado Cash. *See* Adrian Zmudzinski, *Ethereum Mixer Tornado Cash Has Received Almost $2 Billion in 2024 Despite Sanctions*, DECRYPT (July 20, 2024), https://decrypt.co/240603/ethereum-mixer-tornado-cash-has-received-almost-2-billion-in-2024-despite-sanctions [https://perma.cc/Q38B-C2JJ].

[176] *See* ROBERT HERIAN, REGULATING BLOCKCHAIN: CRITICAL PERSPECTIVES IN LAW AND TECHNOLOGY 167 (2019).

[177] Schuster, *supra* note 143, at 993.

[178] *See* Yeung, *supra* note 14, at 215.

pluralist perspective to underline the fact that multiple legal orders—including those enacted by technological systems—can coexist in the same jurisdiction.[179] Indeed, historically speaking, legal pluralism has been the norm instead of the monism of state law.[180] Yet, today, when referring to blockchain systems, *lex cryptographica* is often regarded either as an alternative legal order that subsists on its own[181] or as a separate legal order that should be made compliant with the overarching state legal system[182]—without considering the possibility that multiple legal orders can interact and coexist.

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.[183] For Gunther 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, but they can also be created—as "proto-law"—through self-reproducing legal discourse in global networks (including technological networks) with global validity.[184]

Elements of both "enacted" and "interactional" law can be observed as part of *lex cryptographica*.[185] 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 concerning third parties' conduct and obligations.[186] The engineers who build the standards for how transactions can take place in a blockchain-based system are akin to lawmakers trying to standardize laws and facilitate legal conduct.[187] At the same time, certain interactions, like those among the stakeholders of a blockchain network who are trying to reach

[179] *See* Robé, *supra* note 18, at 49–50, 52–53; Teubner, *supra* note 18, at 2; David Lefkowitz, *Global Legal Pluralism and the Rule of Law*, *in* The Oxford Handbook of Global Legal Pluralism 364, 381–82 (Paul Schiff Berman ed., 2020); Brian Z. Tamanaha, Legal Pluralism Explained: History, Theory, Consequences 1 (2021); Anna Jurkevics, *Democracy in Contested Territory: On the Legitimacy of Global Legal Pluralism*, 25 Critical Rev. Int'l Soc. & Pol. Phil. 187, 189–90 (2022).

[180] Hans Lindahl, Authority and the Globalisation of Inclusion and Exclusion 64 (2018).

[181] *See* Marcella Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, 6 J. Governance & Regul. 45, 47–48 (2015).

[182] *See* Michèle Finck, Blockchain Regulation and Governance in Europe 86 (2019); Katrin Becker, *Blockchain* Matters—*Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, 33 Law & Critique 113, 127–28 (2022).

[183] *See* Wibren van der Burg, *Conceptual Theories of Law and the Challenges of Global Legal Pluralism: A Legal Interactionist Approach*, *in* The Oxford Handbook of Global Legal Pluralism, *supra* note 179, at 319, 320.

[184] Teubner, *supra* note 18, at 5, 7, 12.

[185] van der Burg, *supra* note 183, at 325.

[186] *Id.*

[187] *See* Jake Goldenfein & Andrea Leiter, *Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct*, 29 Law & Critique 141, 143–44 (2018).

consensus, also give rise to certain expectations of conduct[188]—thereby giving expression to the law through "the conduct of men toward one another."[189]

Multinational enterprises provide an illuminating example. Jean-Philippe Robé describes them as being "island[s] of law";[190] they have the character of a legal order due to the way in which their internal rules shape the behavior and norms of their members, creating the perception that these rules are mandatory, and thereby generating a distinction between lawful and unlawful actions.[191] 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.[192] 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 because the creation and enforcement of property rights and freedom of contract had the effect of both decentralizing power to the level of the individual as well as constraining states from recentralizing this power (e.g., due to constitutional protections or bilateral investment treaties).[193] Indeed, it would not be possible to recentralize power without undermining the fundamental, ideological values of a liberal-democratic state—values which, according to Robé, preceded the creation of these nation-states themselves.[194]

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 "[l]*ex [c]ryptographica*,"[195] "cryptolaw,"[196] "law as code,"[197] or "code *as* law,"[198] the *rule of code* implemented by blockchain technology interplays in complex ways with the *rule of law*. As this Article shows 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 organizations),

[188] *See* van der Burg, *supra* note 183, at 325.

[189] Lon L. Fuller, *Human Interaction and the Law*, 14 Am. J. Juris. 1, 1 (1969); *see also* Gerald J. Postema, *Implicit Law*, 13 L. & Phil. 361, 363–66 (1994).

[190] Robé, *supra* note 18, at 53.

[191] *Id.* at 52–53.

[192] *See id.* at 65.

[193] *See id.* at 57–62.

[194] *Id.* at 62.

[195] Wright et al., *supra* note 11, at 4.

[196] Carla L. Reyes, *Conceptualizing Cryptolaw*, 96 Neb. L. Rev. 384, 387 (2017).

[197] De Filippi & Hassan, *supra* note 13.

[198] Yeung, *supra* note 14, at 209.

while others may rely on "reciprocity and shared but tacit understandings" for decisions to be made;[199] or, in the case of blockchain-based systems, on distributed consensus and Schelling points.[200]

This Article contends that, although 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*.[201] 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.[202] In that regard, this Article is situated 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,[203] it can effectively eliminate human agency and generate an automated robotic form of law that is self-enforcing in the case of blockchain.[204] 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,[205] 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.

This Article provides an alternative perspective, one that sees blockchain systems as capable of automating the execution of specific actions or interactions, without being able to guarantee absolute and ineluctable execution.[206] Indeed, as the DAO attack has demonstrated, actions determined by the self-executing code of smart contracts are still subject to human intervention.[207] It is exactly this space of intervention that can be leveraged by lawmakers to regulate blockchain systems.

[199] Sally Engle Merry, *Legal Pluralism*, 22 L. & Soc'y Rev. 869, 878 (1988).

[200] *See infra* Section II.A.

[201] For an approach that similarly notes the failures of existing regulatory approaches and calls for greater attention to be paid to the internal self-regulatory mechanisms of cryptocurrencies, see Immaculate Dadiso Motsi-Omoijiade, Cryptocurrency Regulation: A Reflexive Law Approach (2022). On tensions generated within a pluralistic legal order, see, for example, Peer Zumbansen, *The Rule of Law, Legal Pluralism, and Challenges to a Western-centric View: Some Very Preliminary Observations*, *in* Handbook on the Rule of Law 57, 65 (Christopher May & Adam Winchester eds., 2018).

[202] *See* Yeung, *supra* note 14, at 215.

[203] *See* Laurence Diver, Digisprudence*: The Design of Legitimate Code*, 13 L., Innovation & Tech. 325, 330 (2021).

[204] Antoine Garapon & Jean Lassègue, Justice Digitale: Révolution Graphique et Rupture Anthropologique 146 (2018).

[205] *See* Schuster, *supra* note 143, at 989–99.

[206] *Cf.* Crystal Hall, Eric Chown & Fernando Nascimento, *A Critical, Analytical Framework for the Digital Machine*, 46 Interdisc. Sci. Revs. 458 (2021).

[207] Quinn DuPont, *Experiments in Algorithmic Governance: A History and Ethnography of "The DAO," A Failed Decentralized Autonomous Organization*, *in* Bitcoin and Beyond:

Yet only a proper understanding of the underlying operations of decentralized 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,[208] their influence cannot be absolute. Polycentric systems are, indeed, often regarded as a means to support and uphold the rule of law.[209] First, the dispersion of legal authority contributes to mitigating arbitrary uses of sovereign power.[210] Second, the existence of a common set of rules recognized by all the participants provides for a more decentralized law enforcement system, distributed across multiple power structures.[211] Hence, regulating these systems cannot be done in a top-down manner,[212] 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.

Part II delineates the specificity of blockchain governance to shed light on the various levers of influence that can be adopted by regulators and policymakers. Specifically, the next Part 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

A. Blockchain Governance

This Article relies on Lessig's four regulatory levers—*law, market dynamics, social norms, and architecture or code*,[213] shown in Figure 1 below[214]—to analyze the interdependencies between state governance and blockchain governance. Wright and De Filippi, De Filippi and Hassan, and Yeung have already undertaken a similar analysis, which examines the interplay between conventional law (the *code of law*) and the internal rules of blockchain systems which take the form of

Cryptocurrencies, Blockchains, and Global Governance 157, 159 (Malcolm Campbell-Verduyn ed., 2018).

[208] Josephine van Zeben, *Polycentricity as a Theory of Governance*, *in* Polycentricity in the European Union 9, 13 (Josephine van Zeben & Ana Bobić eds., 2019). *See generally* Polanyi, *supra* note 116; Ostrom, supra note 89.

[209] *See* Paul D. Aligica & Vlad Tarko, *Polycentricity: From Polanyi to Ostrom, and Beyond*, 25 Governance 237, 237 (2012).

[210] *See id.* at 245; Polanyi, *supra* note 116, at 196–97.

[211] *See* Aligica et al., *supra* note 209, at 245.

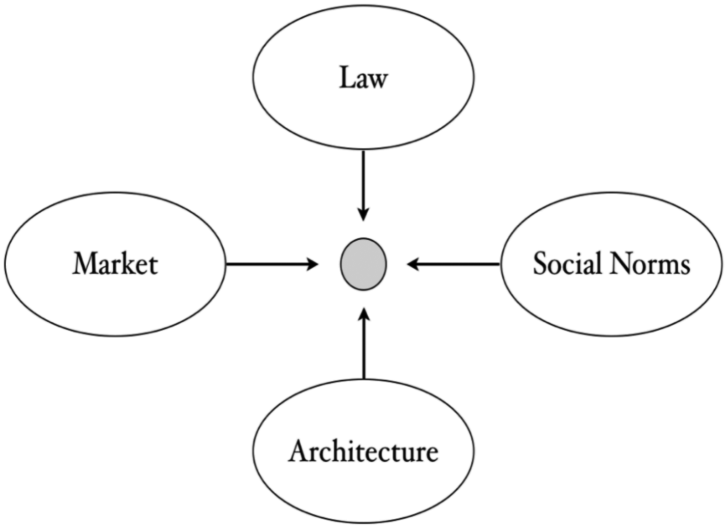
[212] *See* van Zeben, *supra* note 208, at 14.

[213] Lessig, *supra* note 44, at 122–23.

[214] *Id.*

executable software code and technical protocols (*code as law*).[215] Yet these previous contributions mostly focus on the different attitudes that blockchain-based systems might adopt concerning the legal system—and how these attitudes may shape their relationships with the law.[216] This Article focuses on the various means available to state law in order to control or influence the operations of technology.

FIGURE 1. LESSIG'S FOUR MODES OF REGULATION, ADAPTED FROM LAWRENCE LESSIG, CODE: VERSION 2.0[217]



Blockchain governance is a multilayered endeavor 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.[218] 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.[219] Finally, there are

[215] *See* Wright et al., *supra* note 11; De Filippi & Hassan, *supra* note 13; Yeung, *supra* note 14, at 209.

[216] Wright et al., *supra* note 11; De Filippi & Hassan, *supra* note 13; Yeung, *supra* note 14, at 209.

[217] LESSIG, *supra* note 44, at 123.

[218] Jack Parkin, *The Senatorial Governance of Bitcoin: Making (De)Centralized Money*, 48 ECON. & SOC'Y 463, 470–71 (2019).

[219] *See* Matthew A. Zook & Joe Blankenship, *New Spaces of Disruption? The Failures of Bitcoin and the Rhetorical Power of Algorithmic Governance*, 96 GEOFORUM 248, 251 (2018).

the users of these systems—cryptocurrency or tokenholders, smart contract programmers, and all those who have a reason to interact with the network, e.g., to transact with these smart contracts[220]—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").[221] *On-chain* governance "refers to rules that have been encoded directly into the underlying infrastructure of blockchain systems," and which can be "automatically enforced by the underlying technology."[222] As such, the focus of *on-chain* governance is the enforcement of formal and codified rules, rather than the elaboration of these rules.[223] *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.[224] Although *on-chain* governance rules are, by their very nature, clear and formalized, *off-chain* governance rules are, with a few exceptions, much more fluid and informal—and, therefore, more difficult to discern with accuracy and precision.[225] Indeed, although some blockchain communities have implemented a somewhat formalized procedure for discussing protocol upgrades (e.g., Bitcoin Improvement Proposals and Ethereum Improvement Proposals ("EIP")), 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.[226] Off-chain governance generally entails the participation of different stakeholders, with competing interests and ideological views, who are globally distributed and pseudonymous.[227] Although this makes the formalization of off-chain governance all the more necessary, it remains, however, an uphill task.

Initially, and understandably, those analyzing the governance of blockchain communities were mostly focused on the on-chain aspects of blockchain governance. These include the blockchain protocol,

[220] *See id.* at 254.

[221] PRIMAVERA DE FILIPPI & GREG MCMULLEN, GOVERNANCE OF BLOCKCHAIN SYSTEMS: GOVERNANCE OF AND BY DISTRIBUTED INFRASTRUCTURE 4 (2018), https://hal.archives-ouvertes.fr/hal-02046787/document [https://perma.cc/3G24-6EHL].

[222] *Id.* at 5.

[223] *See id.*

[224] *See id.* at 6.

[225] *See* Ellie Rennie, Michael Zargham, Joshua Tan, Luke Miller, Jonathan Abbott, Kelsie Nabben & Primavera De Filippi, *Toward a Participatory Digital Ethnography of Blockchain Governance*, 28 QUALITATIVE INQUIRY 837, 837 (2022).

[226] *See* DE FILIPPI & MCMULLEN, *supra* note 221, at 19.

[227] *See id.* at 18–19.

consensus algorithms, or the code of a particular smart contact.[228] A blockchain based on proof-of-work (e.g., Bitcoin)[229] will give rise to a very different governance structure than a blockchain based on proof-of-stake (e.g., Tezos, Ethereum since September 15, 2022),[230] or proof-of-authority (e.g., VeChain).[231] The incentive schemes of a particular blockchain (e.g., block-rewards and transaction fees) will also impact the behaviors of the different stakeholders maintaining the network.[232]

Yet events such as the DAO 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.[233] Off-chain governance is particularly relevant with "forking." Indeed, as described in the previous Section, blockchain networks exhibit different power dynamics than traditional internet platforms because there are no centralized operators that can impose a unilateral decision on their users.[234] 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.[235]

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.[236] 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

[228] *See* Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen & Dong In Kim, *A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks*, 7 IEEE Access 22328, 22334, 22339 (2019).

[229] *See supra* note 118 and accompanying text.

[230] *See supra* note 119 and accompanying text.

[231] *See Consensus Deep Dive*, VeChain Docs, https://docs.vechain.org/introduction-to-vechain/about-the-vechain-blockchain/consensus-deep-dive [https://perma.cc/9BB5-RPDQ].

[232] *See* De Filippi & McMullen, *supra* note 221, at 14.

[233] *See* Reijers et al., *supra* note 15, at 829–30.

[234] *See supra* note 161 and accompanying text.

[235] *See* Bronwyn E. Howell, Petrus H. Potgeiter & Bert M. Sadowski, *Governance of Blockchain and Distributed Ledger Technology Projects*, EconStor 3, 15–16 (2019), http://hdl.handle.net/10419/201737 [https://perma.cc/3VZV-BB6E].

[236] *See* Michael Abramowicz, *The Very Brief History of Decentralized Blockchain Governance*, 22 Vand. J. Ent. & Tech. L. 273, 278–80 (2020).

choice will ultimately depend both on their own personal preferences and on the perception or expectation of what others will choose.[237] This is often referred to as a "Schelling point"—i.e., the choice that everyone thinks many others will make.[238]

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; any 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.[239] All these actors contribute, in their own way, to steering the behavior of users, tokenholders, and all other network participants toward 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.[240] 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.[241] *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.[242] 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.[243] 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.[244] There are, however, a variety of exogenous off-chain rules—such as laws and regulations—that might

[237] *Id.*

[238] *Id.*

[239] *See* De Filippi & McMullen, *supra* note 221, at 15; Schneider, *supra* note 102, at 1965–66.

[240] *See infra* note 256 and accompanying text.

[241] De Filippi & McMullen, *supra* note 221, at 16.

[242] *See* Shermin, *supra* note 162, at 507.

[243] *See* De Filippi & McMullen, *supra* note 221, at 18–20.

[244] *See id.*

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 for 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 that are part of these blockchain communities.[245] Schelling points are further analyzed in the following Sections.

B. Regulation by Code

An overview of the history of internet governance might help provide a better understanding of the interplay between *regulation by code* and *regulation by law*, as it applies to both centralized and decentralized internet platforms.[246] Many of the rules embedded in the technological infrastructure of online platforms are elaborated by large multinational companies, for the most part, interested in maximizing the adoption and the economic returns that they can derive from these platforms.[247] Yet these rules might sometimes turn out to be incompatible with national laws—such as the data protection regulations of many European countries[248]—and it is thus necessary to find ways to ensure the proper application of national laws on these global and transnational internet platforms.[249]

As described above, 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,[250] which often introduces additional

[245] *See* Julie Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210, 255 (2007); Suzor, *supra* note 92, at 1833.

[246] *See, e.g.*, INTERNET GOVERNANCE: INFRASTRUCTURE AND INSTITUTIONS (Lee Bygrave & Jon Bing eds., 2009).

[247] *See* Alice Marwick, *Silicon Valley and the Social Media Industry*, *in* THE SAGE HANDBOOK OF SOCIAL MEDIA 314, 314–17 (Jean Burgess et al. eds., 2018); JOSÉ VAN DIJCK, THE CULTURE OF CONNECTIVITY: A CRITICAL HISTORY OF SOCIAL MEDIA 21 (2013).

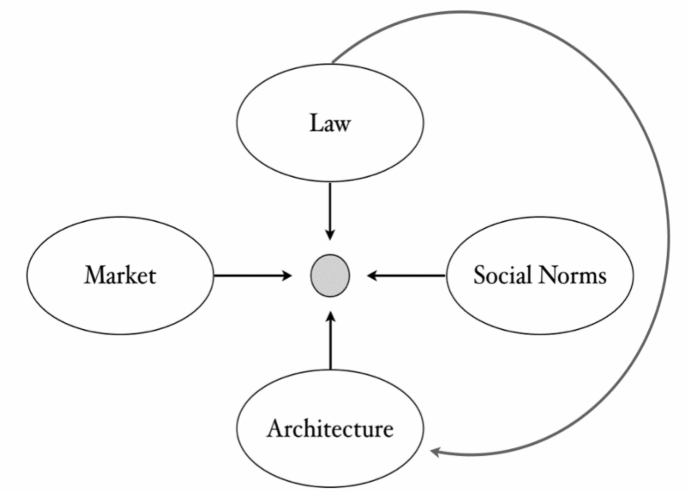
[248] *See* Luciano Floridi, *Soft Ethics, the Governance of the Digital and the General Data Protection Regulation*, PHIL. TRANSACTIONS ROYAL SOC'Y A: MATHEMATICAL, PHYSICAL & ENG'G SCIS., Oct. 2018, at 1, 2–4; Jim Isaak & Mina J. Hanna, *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*, COMPUTER, Aug. 2018, at 1, 56. For Robert Herian, the European Union's General Data Protection Regulation shares a common conceptual and psychological origin with certain blockchain applications as they are respectively legal and technical means for securing individual control over data that has been mismanaged and misused by commercial actors. Robert Herian, *Blockchain, GDPR, and Fantasies of Data Sovereignty*, 12 L., INNOVATION & TECH. 156, 156–57 (2020).

[249] *See* Philip J. Weiser, *The Future of Internet Regulation*, 43 U.C. DAVIS L. REV. 529, 534 (2009); Molly Land, *The Problem of Platform Law: Pluralistic Legal Ordering on Social Media*, *in* THE OXFORD HANDBOOK OF GLOBAL LEGAL PLURALISM, *supra* note 179, at 974, 977.

[250] *See* David Baron, *Private Ordering on the Internet: The eBay Community of Traders*, 4 BUS. & POL. 245, 245 (2002).

constraints to those actually prescribed by the law.[251] Yet, although it is true that—at least in the case of centralized online platforms—*regulation by code* has progressively taken over *regulation by law*,[252] it would be wrong to conclude that laws no longer have a role to play in the regulation of online behavior. To the contrary, concerning centralized platforms which are effectively *ruled by code*,[253] 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 that are managing the code, as seen in Figure 2 below.[254] 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.[255]

Figure 2. Lessig's Four Modes of Regulations, Adapted from Lawrence Lessig, Code: Version 2.0[256]



[251] *See* Tim Wu, *When Code Isn't Law*, 89 Va. L. Rev. 679, 707–08 (2003); Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 Or. L. Rev. 81, 83–84 (2010).

[252] *See* Lawrence Lessig, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, 5 CommLaw Conspectus 181, 191 (1997); Lawrence Lessig, *Law Regulating Code Regulating Law*, 35 Loy. U. Chi. L.J. 1, 11–12 (2003); *see also* Lessig, *supra* note 44, at 24.

[253] *See* James Grimmelmann, Note, *Regulation by Software*, 114 Yale L.J. 1719, 1728–29 (2005).

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

[255] *See* Joel R. Reidenberg, *States and Internet Enforcement*, 1 U. Ottawa L. & Tech. J. 213, 221, 226 (2003); Niva Elkin-Koren, *After Twenty Years: Revisiting Copyright Liability of Online Intermediaries*, *in* The Evolution and Equilibrium of Copyright in the Digital Age 29, 39–40 (Susy Frankel & Daniel Gervais eds., 2014).

[256] Lessig, *supra* note 44, at 123.

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 centralization 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 policymakers may attempt to impose responsibilities or liabilities onto these actors who have the ability to (albeit partially) influence the operations of a 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.[257]

In contrast to the legal pluralist view,[258] this approach favors 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 toward 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.[259] Over time, this might lead to a progressive shift—which we already observed with the internet network—in which blockchain networks become increasingly *ruled by code*, rather than subject to the *rule of code*. Accordingly, although 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 licenses were granted in the 2019 to 2020 period in order to legalize operations which had previously been undertaken in a "climate of fear," the government declared a ban on all Bitcoin mining activities to protect cities against potential blackouts.[260] Furthermore, as the U.S. sanction on Tornado Cash

[257] Yeung, *supra* note 14, at 218.

[258] *See supra* notes 179–88 and accompanying text.

[259] *See, e.g.*, Commission Regulation 2023/1114, 2023 O.J. (L 150) 40, 56–57 ("MiCA Regulation").

[260] Paddy Baker, *Over 1,000 Bitcoin Miners Granted Licenses in Iran*, CoinDesk (Jan. 27, 2020, 8:02 AM), https://www.coindesk.com/policy/2020/01/27/over-1000-bitcoin-miners-granted-licenses-in-iran-report [https://perma.cc/3ZKD-TEN2].

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 to them.[261]

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.[262] 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.[263] Because 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 Recommendation No. 15, have already imposed stringent KYC and AML or Counter Terrorist Financing regulations onto these actors with a view to addressing public policy concerns.[264] In the future, they could push regulations further and require them to only accept or execute transactions from, or to, specific addresses or blockchain wallets which have been whitelisted according to stringent due diligence requirements. Conversely, certain addresses or blockchain wallets may be blacklisted through the application of worldwide freezing orders.[265] 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 of the software they create. Such

[261] *See* Vishal Chawla & Tim Copeland, *At Least 23% of Ethereum Blocks Are Complying With US Sanctions*, The Block (Sept. 28, 2022, 10:34 AM), https://www.theblock.co/post/173417/at-least-23-of-ethereum-blocks-are-complying-with-us-sanctions [https://perma.cc/4QCS-Q5HG].

[262] *See* Dirk Wiegandt, *Blockchain, Smart Contracts and the Role of Arbitration*, 39 J. Int'l Arb. 671, 687–88 (2022). Indeed, as Faria's ethnographic research indicates, some cryptocurrency exchanges actively seek regulation so as to establish greater "legitimacy" and thereby "grow outside niche communities, get funding and be insured against volatile unregulated crypto markets." Inês Faria, *Blockchain in the EU: Transforming Imaginaries and the Social Making of Financial Regulation*, 39 Anthropology Today 21, 21, 23 (2023).

[263] *See* Eric Alston, *Digital Currency Industry Self-Regulation: Not All Consensus Is Automatic*, 27 Va. J.L. & Tech. 1, 4 (2023).

[264] *See* Faria, *supra* note 262, at 22.

[265] *See supra* note 154.

an approach was proposed by Angela Walch, who contends that the developers of existing public blockchain networks like Bitcoin should hold fiduciary duties toward the users or third-party operators that rely on these networks.[266] Yet, in addition to reevaluating 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[267]—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 the update of the protocol.[268] Thus, as opposed to centralized 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.[269]

The ability of blockchain developers to impose changes on a blockchain network is a core issue in an ongoing case in England and Wales concerning the alleged theft of crypto assets. In the *Tulip Trading Ltd.*[270] cases, the England and Wales High Court, and subsequently the England and Wales Court of Appeal, considered, inter alia, the question whether Bitcoin core developers have a fiduciary duty toward particular users of the Bitcoin blockchain network (and forked networks from the original Bitcoin blockchain) that included a positive obligation to help Bitcoin owners recover stolen assets.[271] In the first instance, Justice Falk held that they did not owe such a duty because their relationship to a subgroup of Bitcoin owners did not require single-minded loyalty toward them.[272] Moreover, as "developers are a fluctuating body 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

[266] Angela Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains*, *in* REGULATING BLOCKCHAIN: TECHNO-SOCIAL AND LEGAL CHALLENGES 58, 58–59 (Philip Hacker et al. eds., 2019).

[267] *See* ROD DIXON, OPEN SOURCE SOFTWARE LAW 103–04 (2004); *see also* Carla L. Reyes, *(Un) Corporate Crypto-Governance*, 88 FORDHAM L. REV. 1875, 1908 (2020); Bryan H. Choi, *Software as a Profession*, 33 HARV. J.L. & TECH. 557, 566–67 (2020).

[268] *See* Raina S. Haque, Rodrigo Seira Silva-Herzog, Brent A. Plummer & Nelson M. Rosario, *Blockchain Development and Fiduciary Duty*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 139, 177–78 (2019).

[269] *See id.* at 181.

[270] [2022] EWHC 667 (Ch) [1, 6].

[271] *Id.*

[272] *Id.* ¶ 74.

so."[273] Evidently, Bitcoin owners could not "realistically be described as entrusting their property to a fluctuating, and unidentified, body of developers of the software."[274] In contrast, on appeal, Lord Justice Birss held that as core developers appeared to be the only actors in the network that can patch software bugs, entrustment by Bitcoin owners can be implied and a positive fiduciary duty arises from this "*de facto* power" to offer a remedy.[275] Although this case had been sent for a full trial on the facts by the Court of Appeal, this lawsuit was discontinued in April 2024 after a judge in a separate trial ruled that there was "overwhelming" evidence that Craig Wright, the founder of Tulip Trading, is not Satoshi Nakamoto.[276]

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. Although 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. For instance, the OFAC sanctions against Tornado Cash make it illegal for any U.S. citizen, resident, or company to transact with the smart contract addresses associated with that blockchain-based service.[277] 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.[278] Such sanctions have been heavily criticized by the blockchain community because they apply to a general-purpose technology which also comes with legitimate uses (e.g., safeguarding financial privacy).[279]

Moreover, criminalizing 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 centralized platform where one needs to intentionally create an account in order to interact with the platform (e.g., PayPal)—on a blockchain, users might receive tokens on their wallet from a particular smart contract application without them even being aware of it.[280] This is what happened,

[273] *Id.* ¶ 75.

[274] *Id.* ¶ 73.

[275] *See* Tulip Trading Limited v. Bitcoin Association for BSV [2023] EWCA Civ 83, [77–80] (appeal taken from Eng.).

[276] *Craig Wright Discontinues Tulip Trading Case in Major Win for Bitcoin Developers*, Bitcoin Legal Def. Fund (Apr. 17, 2024), https://bitcoindefense.org/craig-wright-discontinues-tulip-trading-case-in-major-win-for-bitcoin-developers [https://perma.cc/D7EK-PAFJ].

[277] *See* Brito et al., *supra* note 169.

[278] *See id.*

[279] *See id.*

[280] *See* Mat Di Salvo, *Tornado Cash User 'Dusts' Hundreds of Public Wallets—Including Celebs Jimmy Fallon, Steven Aoki and Logan Paul*, Decrypt (Aug. 9, 2022), https://decrypt.co/107090/tornado-cash-dusts-public-wallets-jimmy-fallon-brian-armstrong-steve-aoki-logan-paul [https://perma.cc/CHW3-TAER].

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 chief executive officer Brian Armstrong.[281] The point was to show that if OFAC requires that every U.S. person refuse any transaction stemming from a sanctioned entity, this simply cannot be done for an open and decentralized 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 they might not even be informed of having received them.[282] 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 decentralized application or decentralized autonomous organization (whether or not they are aware of being in possession of these tokens) may qualify as a co-administrator (or "general partner") of a decentralized autonomous organization and be, therefore, regarded as jointly and severally liable with all the other tokenholders for any illicit action taken by the decentralized autonomous organization.[283] 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 these decentralized autonomous organizations.[284] 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 decentralized autonomous organizations simply because they are the holders of a particular amount of governance tokens.[285]

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

[281] *See id.*

[282] *See id.*

[283] *See, e.g.*, Sarcuni v. bZx Dao, 664 F. Supp. 3d 1100, 1108, 1114 (S.D. Cal. 2023) (plaintiffs alleging that the governance tokenholders of bZx DAO and its successor Ooki DAO, comprised an association of two or more persons operating together for profit and were, consequently, a general partnership with joint and several liability for the putative partners).

[284] *See id.* at 1116 (court clarifying that unequal governance rights among tokenholders does not divest a general partnership of its essential nature as such partnerships can involve the delegation of management powers to one partner).

[285] *See id.* at 1118–19 (deeming participation in management to be a particularly important factor in determining whether an association is a general partnership). It remains to be seen if other courts will follow the same approach.

actors located in their own jurisdiction from engaging in the process of blockchain governance for fear of legal liability.[286] 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 Karen 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 decentralized tools.[287]

An alternative approach, intended to encourage more participation and experimentation of local companies in the blockchain ecosystem, entails the creation of regulatory sandboxes, in which specific legal requirements and taxation schemes are inapplicable.[288] Such sandboxes for experimentation have been created in countries as diverse as Australia, Thailand, and Uganda, so as to build blockchain-based securities clearing infrastructure and new decentralized applications.[289] 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, 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,[290] which are currently dealt with through expensive formalities and reporting obligations.[291] 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.[292] Yeung describes this approach as seeking an "efficient

[286] *See* Yeung, *supra* note 14, at 217–20.

[287] *Id.*

[288] Denisa Reshef Kera, *Sandboxes and Testnets as "Trading Zones" for Blockchain Governance*, *in* Blockchain and Applications: 2nd International Congress 3, 4 (Javier Prieto et al. eds., 2020).

[289] *See* Baker McKenzie, International Guide to Regulatory Fintech Sandboxes 5, 15 (2018), https://www.bakermckenzie.com/en/-/media/files/insight/publications/2018/12/guide_intlguideregulatorysandboxes_dec2018.pdf [https://perma.cc/X9PR-46WA]; The Free Zones (Declaration of Block Chain Technologies Free Zone) Instrument, 2020, No. (42) 113 Uganda Gazette Statutory Instruments Supplement No. (25) (July 17, 2020).

[290] *See* De Filippi et al., *supra* note 10, at 368.

[291] Alexis Collomb, Primavera De Filippi & Klara Sok, *Blockchain Technology and Financial Regulation: A Risk-Based Approach to the Regulation of ICOs*, 10 Eur. J. Risk Regul. 263, 289 (2019).

[292] 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

alignment" intended to create mutually beneficial interactions between the rule of code and the rule of law.[293]

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, 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.[294] Moreover, some of the operations undertaken on top of a blockchain network (e.g., interacting or contracting with a decentralized autonomous organization, issuing crypto assets) cannot be easily encompassed by the law, and—even if they could—law enforcement would remain a significant challenge.[295]

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[296] in public sector agencies or other institutional frameworks,[297] 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.[298] These new regulatory pathways are identified in the next Section.

C. *Regulation via Governance*

As discussed above, and summarized in Table 1, 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

have engaged into a transaction that does appear on the blockchain. *See* Alston, *supra* note 263, at 44.

[293] Yeung, *supra* note 14, at 215, 220–22.

[294] *See* De Filippi et al., *supra* note 10, at 368.

[295] *See* Yuliya Guseva, *When the Means Undermine the End: The Leviathan of Securities Law and Enforcement in Digital-Asset Markets*, 5 STAN. J. BLOCKCHAIN L. & POL'Y 1, 3, 11 (2022).

[296] Tommy Koens, Pol van Aubel & Erik Poll, *Blockchain Adoption Drivers: The Rationality of Irrational Choices*, 33 CONCURRENCY & COMPUTATION: PRAC. & EXPERIENCE, Apr. 25, 2021, at 1, 1.

[297] *See* Adam Sulkowski, *Blockchain, Business Supply Chains, Sustainability, and Law: The Future of Governance, Legal Frameworks, and Lawyers?*, 43 DEL. J. CORP. L. 303, 310–19 (2019).

[298] *See* Werbach, *supra* note 143, at 534.

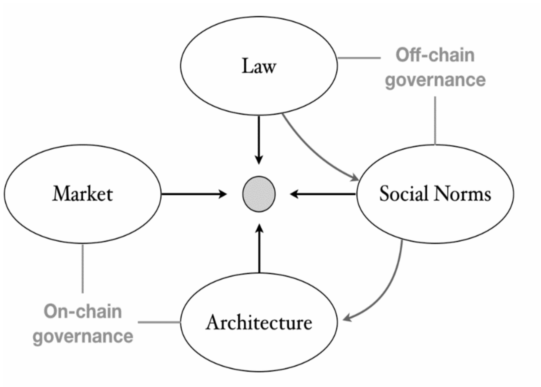
norms.[299] Combined, endogenous on-chain and off-chain governance (i.e., blockchain code and social norms) constitutes a separate, transnational legal order that remains distinct from any one state's legal order but is nonetheless affected by exogenous regulatory forces (i.e., market dynamics and national laws) that remain outside of the control of the relevant blockchain community.

TABLE 1. REGULATORY FORCES THAT SHAPE BLOCKCHAIN GOVERNANCE

Regulatory forces	**Endogenous**	**Exogenous**
On-chain	*Architectural rules*	*Market dynamics*
Off-chain	*Social norms*	*Laws & regulations*

If the regulation of the internet 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 shape their design choices, as seen in Figure 3 below.

FIGURE 3. LESSIG'S FOUR MODES OF REGULATIONS, ADAPTED FROM LAWRENCE LESSIG, CODE: VERSION 2.0[300]



[299] *See* AVINASH K. DIXIT, LAWLESSNESS AND ECONOMICS: ALTERNATIVE MODES OF GOVERNANCE 6–7 (2004).

[300] LESSIG, *supra* note 44, at 123.

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.[301] The Bitcoin network is characterized 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 with the emergence of several competing networks (or forks) with slightly different technical characteristics—e.g., Bitcoin Cash, Bitcoin SV, Bitcoin Gold.[302]

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.[303] This was well illustrated in the aftermath of the DAO 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.[304]

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 multisignature wallets on the Ethereum blockchain.[305] The exploitation of the vulnerability in that code has led to the freezing of over $150 million worth of Ether at the time, locked into these wallets with

[301] *See* Wessel Reijers, Fiachra O'Brolcháin & Paul Haynes, *Governance in Blockchain Technologies & Social Contract Theories*, 1 Ledger 134, 136 (2016).

[302] *See* De Filippi & Loveluck, *supra* note 160, at 8.

[303] *See* Wessel Reijers & Mark Coeckelbergh, *The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies*, 31 Phil. & Tech. 103, 121–23 (2018).

[304] According to Paul Dylan-Ennis and colleagues, the majority of the community agreed to subordinate the norms of decentralization and immutability to preserving the economic sustainability of the Ethereum network. *See* Paul Dylan-Ennis, Donncha Kavanagh & Luis Araujo, *The Dynamic Imaginaries of the Ethereum Project*, 52 Econ. & Soc'y 87, 97 (2023).

[305] *See* Giuseppe Destefanis, Michele Marchesi, Marco Ortu, Roberto Tonelli, Andrea Bracciali & Robert Hierons, *Smart Contracts Vulnerabilities: A Call for Blockchain Software Engineering?*, 1 IEEE Int'l Workshop on Blockchain Oriented Software Eng'g Proc. 21–23 (2018).

no possibility of withdrawal.[306] Just as with the DAO 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 standardized 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[307]—including risks of fiduciary liability.[308] Although bug fixes and protocol upgrades are dealt with via standardized procedures (e.g., EIPs), there is no formalized procedure to discuss contentious protocol changes of a nontechnical nature.[309] 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. Blockchain engineers generally do not want to assume responsibility for these decisions.[310] 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 as 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 DAO attack.

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

[306] *Id.*

[307] 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 EIP over a standardized format for lost fund recovery would potentially violate Japanese law. Rachel-Rose O'Leary, *Ethereum Developer Resigns as Code Editor Citing Legal Concerns*, CoinDesk (Feb. 15, 2018, 6:00 AM), https://www.coindesk.com/markets/2018/02/15/ethereum-developer-resigns-as-code-editor-citing-legal-concerns [https://perma.cc/F7Y8-AEHU].

[308] *See* Haque et al., *supra* note 268, at 185; Walch, *supra* note 266, at 66.

[309] *See* Dupont, *supra* note 207, at 11–12.

[310] *See* Haque et al., *supra* note 268, at 177; Law Commission, Decentralized Autonomous Organisations (DAOs): A Scoping Paper 80 (2024), https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2024/07/DAOs-scoping-paper-110724.pdf [https://perma.cc/33SY-J7WP].

internal governance practices of any given blockchain community.[311] 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 DAO 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.[312] At the same time, the Parity incident has shown that exogenous rules of a nontechnical 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. Although, on the one hand, people whose funds have been frozen could theoretically have sued Parity 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 decentralized 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 behaviors of individuals or companies through a series of sanctions and rewards.[313] By understanding the multiple and intricate dynamics of blockchain governance (i.e., governance by architecture,

[311] *See* Thomas John & Mantri Pam, *Complex Adaptive Blockchain Governance*, 223 MATEC WEB CONFS. 13 (2018); Philipp Hacker, *Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations*, *in* REGULATING BLOCKCHAIN: TECHNO-SOCIAL AND LEGAL CHALLENGES 140, 148 (Philip Hacker et al. eds, 2019).

[312] 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. *See* DE FILIPPI & WRIGHT, *supra* note 16, at 47–48.

[313] *See* De Filippi at al., *supra* note 10, at 4. There is resistance to the idea that blockchain-based systems are alegal, with the court in the recent *Sarcuni* case, for instance, contending that recognizing the bZx DAO as a general partnership *would not* be a "radical expansion and alteration of long-standing principles of partnership law." Sarcuni v. bZx DAO, 664 F. Supp. 3d 1100, 1117 (S.D. Cal. 2023) (quoting the case docket). Existing laws and legal precedent would suffice. Yet, as argued in this Article, in certain ways, these blockchain-based systems reveal the limitations of the factual assumptions that undergird specific legal regimes and prompt the reconceptualization of the goals of said regimes and reconfiguration of the institutions governing said regimes. On the need for reassessing legal regimes in the face of tech-enabled social change, see

market mechanisms, and social norms), policymakers can generate new regulatory pressure points that will affect the social norms of blockchain communities and, therefore, also indirectly affect 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 decentralized 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 centralized platforms—e.g., Google, Facebook, Twitter (X), YouTube—that collect most internet traffic. Hence, internet governance is currently facing a very different set of challenges than it did twenty years ago.[314] 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 centralized sovereign authority.[315] Today, we are witnessing the emergence of functional sovereigns with the proliferation of large centralized online platforms that transcend national boundaries and are controlled by private corporations operating across multiple jurisdictions.[316] Accordingly, the main challenge of internet governance today is to guarantee that these platforms remain subject to national sovereignty and the rule of law.

Just like the internet, the global and decentralized 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 as part of today's internet governance—holding intermediary operators responsible for whatever happens on the platforms they control—are not readily applicable for open and decentralized 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 decentralized network.

BJ Ard & Rebecca Crootof, *Legal Responses to Techlaw Uncertainties*, *in* Research Handbook on Law and Technology 28 (Bartosz Brożek et al. eds., 2024).

[314] *See* Mannan et al., *supra* note 39, at 3.

[315] *See* Richard Collins, Three Myths of Internet Governance: Making Sense of Networks, Governance and Regulation (2009); Milton L. Mueller, Networks and States: The Global Politics of Internet Governance 25 (2010).

[316] *See* Laura DeNardis, The Global War for Internet Governance 154–57 (2014); Pasquale, *supra* note 102.

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 centralized operator or trusted authority in charge of managing or regulating public and permissionless blockchain networks, the autonomy of these networks remains 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 minimize the risks of legal liability.[317]

Whether this is done by imposing fiduciary duties on blockchain developers, regulating commercial operators like cryptocurrency 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 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 decentralization, 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?[318] What do theories on polycentric governance and collective action have to offer in further developing

[317] Dirk A. Zetzsche, Ross P. Buckley & Douglas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, U. Ill. L. Rev. 1361, 1391–92 (2018).

[318] *See* Eric Alston, *Constitutions and Blockchains: Competitive Governance of Fundamental Rule Sets*, 11 J.L., Tech. & Internet 131, 167 (2020).

or improving such policy proposals?[319] Crucially, how can we combine on-chain and off-chain governance systems in order to ensure the legitimacy of blockchain-based systems, concerning both community members and society at large? We hope to explore this in future work.

[319] *See* Primavera De Filippi, Morshed Mannan, Sofia Cossar, Tara Merk & Jamilya Kamalova, Blockchain Technology and Polycentric Governance (May 2024), https://hdl.handle.net/1814/77030 [https://perma.cc/J4TV-8S28].