CODE IS *NOT* LAW

Carla L. Reyes, Andrea Tosato & Andrew Hinkes

ABSTRACT

In 2022, an image of a “bored ape” accessible through a non-fungible token (NFT) was stolen from actor Seth Green. The thief then sold the bored ape to a good faith purchaser. Had this been a physical painting, the outcome would have been clear: a thief cannot convey title they do not have, and the purchaser would acquire nothing. Yet the ensuing debate proceeded as though the NFT's technical features had altered this settled principle, as though blockchain records could bestow property rights on the new purchaser. They cannot. Ownership rights in digital assets stem from law, not from the software systems that create and maintain them.

When Lawrence Lessig famously proclaimed “code is law,” he meant that code functions as behavioral regulation by imposing technical limitations on users, not that it generates enforceable rights. His insight was descriptive: code shapes what people can do within digital environments, just as physical architecture channels movement through physical space. Yet the advent of blockchain networks, cryptocurrencies, and smart contracts has morphed this observation into the flawed conviction that what code makes possible, the law must recognize as legally enforceable.

While legal scholarship has noted this misconception, it has yet to offer a rigorous framework to resolve it. This Article fills this gap by applying H.L.A. Hart’s legal theory to demonstrate that code acquires legal force only to the extent that positive law grants such power. This investiture occurs through two pathways: public empowerment through legislation, and private empowerment through contracts, trusts, and other ordering instruments. Absent such formal investiture, code remains "soft law," a structural constraint lacking normative force. The relevance of our analysis extends beyond the conceptual malaise affecting the blockchain ecosystem, addressing a foundational conflict poised to reappear with every wave of new technology, from large language models to autonomous robots.

TABLE OF CONTENTS

CODE IS *NOT* LAW

Carla L. Reyes,[*] Andrea Tosato[**] & Andrew Hinkes[***]

INTRODUCTION

In March 2021, an artist offered a pointed lesson about the relationship between code and law. After selling a collection of non-fungible tokens (NFTs),[1] each linked to a stained-glass image of an animal, he used his technical access as the creator to replace the digital artworks associated with those tokens with pictures of rugs. Having executed this literal "rug pull," the artist then took to social media to make his point that despite what buyers may have believed, owning an NFT did not confer ownership of the artwork associated with it, as the two are entirely distinct. The stunt's true impact, however, was to highlight the error of the increasingly commonplace belief that blockchain networks,[2] smart contracts,[3] cryptocurrencies,[4] and other digital assets can, by themselves, generate new legal rights where none existed before.[5]

[*] Associate Professor of Law, SMU Dedman School of Law; Faculty, Initiative for Cryptocurrency and Contracts; Affiliated Faculty, Indiana University Bloomington Ostrom Workshop Program on Cybersecurity and Internet Governance; Research Associate, University College London Center for Blockchain Technology.
[**] Professor of Law, SMU Dedman School of Law.
[***] Partner, Winston & Strawn; Adjunct Professor of Law, New York University School of Law; Adjunct Associate Professor, New York University Stern School of Business.

[1] *See* Edward Lee, *NFTs as Decentralized Intellectual Property*, U. ILL. L. REV. 1049, 1049 (2023) ("An NFT is a virtual token that is created by computer code (what's called a smart contract) that identifies the token as unique—or 'non-fungible'—on a blockchain."); *see also* Christopher K. Odinet & Andrea Tosato, *The Intersection of NFTs and Structured Finance*, 103 B.U. L. REV. 1005, 1018–20 (2023) (describing the two prevalent models for NFT minting and commercialization); Juliet M. Moringiello & Christopher K. Odinet, *The Property Law of Tokens*, 74 FLA. L. REV. 607, 632–47 (2022).

[2] Originally derived from the architecture used by Bitcoin, the term is now broadly used to describe a variety of system architectures that facilitate various types of transactions of digital assets between their users. *See generally* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG (2008), *available at* https://bitcoin.org/bitcoin.pdf (last visited [UPDATE URL DATE]) (describing the functionality of Bitcoin's blockchain); *see also* Carla L. Reyes, *The Language Landmines of Blockchain and Cryptocurrency*, *in* THE CAMBRIDGE HANDBOOK ON LAW AND POLICY FOR NFTS (Nizan Geslevich Packin ed., 2024); Tchatchou v. India Globalization Cap. Inc., No. CV PWG-18-3396, 2021 WL 307415, at 2 (D. Md. Jan. 29, 2021) ("Blockchain is defined as 'a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network.'" (citations omitted)).

[3] *See* Carla L. Reyes, *Creating Cryptolaw for the Uniform Commercial Code*, 78 WASH. & LEE L. REV. 1521, 1541 (2021) ("A smart contract is one type of computer program frequently used in connection with blockchain technology. Like the variance among implementation of DLTs and blockchain protocols, the precise implementation of a smart contract can vary significantly. At base, however, a smart contract is very similar to a 'persistent script'—a standing computer program—that says 'if event x happens, then execute result y.'"); *see also* Carla L. Reyes, *Emerging Technology's Language Wars: Smart Contracts*, 2022 WIS. L. REV. FORWARD 85; Carla L. Reyes, *A Unified Theory of Code Connected Contracts*, 46 J. CORP. L. 981 (2021); Primavera De Filippi, Chris Wray & Giovanni Sileno, *Smart Contracts*, 10 INTERNET POL'Y REV. 1 (2021).

[4] *See* Carla L. Reyes, *Emerging Technology's Language Wars: Cryptocurrency*, 64 WM. & MARY L. REV. 1193, 1197–98 (2023) (explaining cryptocurrencies and the different meanings attributed to the term "cryptocurrency" by legislators, practitioners, and academics).

[5] *Id.*

It would be a mistake to dismiss as a fringe dogma the idea that technical capabilities equate to legal validity, attributing it only to reckless speculators, derisively labeled "crypto-bros." On the contrary, this view has propagated broadly. As Part II documents, federal and state statutes have been enacted that presuppose code has juridical effect,[6] courts have issued opinions that blur system powers with enforceable entitlements,[7] regulators have brought enforcement actions conflating autonomous software with legally responsible actors,[8] and private parties have structured agreements on the flawed premise of code's inherent authority,[9] producing tangible, and at times devastating, consequences.

This painful reality is vividly illustrated by the story of twenty-four-year-old reporter Alison Parker, who was tragically murdered on live television.[10] Because the footage went viral,[11] Ms. Parker's father suffered daily the horror of millions of people watching the violent death of his daughter on perpetual replay. His attempts to remove the video from cyberspace proved an exercise in futility; each successful takedown spawned new uploads elsewhere. His task was made harder still by the fact that he had no rights in the footage.[12] Gray Television, Ms. Parker's employer, owned the copyright to the footage of her death and refused to assign it to him.[13]

As a result, Mr. Parker's new battle plan involved what he describes as a "Hail Mary": minting an NFT and connecting it to the video through the platform Rarible.[14] His hope was that the token would somehow spawn a new copyright in the video, empowering him to force takedowns of the footage and let his daughter rest in peace. This desperate attempt was a heart-rending embodiment of the notion that a technical process can alter rights that belong to someone else or give rise to new ones.[15]

Both the artist's stunt and Mr. Parker's plight illustrate a fundamental misconception about the source of rights in the digital age. While Professor Lawrence Lessig famously observed that "code is law," his crucial insight was descriptive: code acts as a powerful architectural constraint, a form

---

[6] *See* Part II.A.
[7] *Id.*
[8] *See* Part II.B.
[9] *See* Part II.C.1.
[10] Genevieve Carlton, *Alison Parker, The Promising Young Journalist Shot Dead by a Coworker—On Live TV*, ALL THAT'S INTERESTING (Jan. 20, 2022), *available at* https://allthatsinteresting.com/alison-parker; Cristiano Lima-Strong, *To Expunge the Death of His Daughter from the Internet, a Father Created an NFT of the Video*, WASH. POST (Feb. 22, 2022, 8:00 AM), *available at* https://www.washingtonpost.com/technology/2022/02/22/expunge-his-daughters-murder-internet-father-created-an-nft-grisly-video/; Michael D. Shear, Richard Pérez-Peña & Alan Blinder, *Ex-Broadcaster Kills 2 on Air in Virginia Shooting; Takes Own Life*, N.Y. TIMES (Aug. 26, 2015), *available at* https://www.nytimes.com/2015/08/27/us/wdbj7-virginia-journalists-shot-during-live-broadcast.html.
[11] *Id*.
[12] *Id*
[13] *Id*
[14] Lima-Strong, *supra* note 10 (explaining that Mr. Parker minted an NFT of the video); Lee, *supra* note 1 ("An NFT is a virtual token that is created by computer code (what's called a smart contract) that identifies the token as unique—or 'non-fungible'—on a blockchain."); Reyes, *Creating Cryptolaw*, *supra* note 3, at 1541 ("A smart contract is one type of computer program frequently used in connection with blockchain technology. Like the variance among implementation of DLTs and blockchain protocols, the precise implementation of a smart contract can vary significantly. At base, however, a smart contract is very similar to a 'persistent script'—a standing computer program—that says 'if event x happens, then execute result y.'").
[15] *Id*.

of "soft law" that regulates behavior in technology systems by defining the realm of the possible.[16] However, in the context of blockchain systems, this architectural power has been widely misconstrued. Scholars have argued that smart contracts create "de facto property rights" or operate "alegally," beyond traditional legal frameworks.[17] Such claims, even when carefully hedged, risk fostering the misguided conviction that what code makes possible, law must accept as enforceable.

This Article offers a doctrinal counterpoint: code can create or alter rights and correlative duties[18] only to the extent that positive law[19] grants it such power. Technical systems[20] may generate digital assets and enable their users to perform complex operations, but these capabilities do not, in and of themselves, have juridical significance. Although this proposition should be a jurisprudential first principle, the widespread confusion documented above reveals a critical lacuna in legal theory: existing scholarship lacks a rigorous framework to vindicate the claim that code cannot, by itself, constitute a source of legal authority, and to refute assertions to the contrary.

To fill this theoretical vacuum, we draw on H.L.A. Hart's jurisprudence to reveal an ontological gap that separates code from law. The former operates through deterministic execution, imposing architectural constraints on action, while the latter intervenes through normative prescription, engendering enforceable rights and duties.[21] Having established this foundation, we demonstrate

---

[16] *See also* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 2.0 (2006); *see also* KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST 25 (2018) ("The constellation of design decisions that shape a system is known as its 'architecture.' Architecture is power because it defines the limits of human interactions.").

[17] *See, e.g.*, Stefan Bechtold, Giuseppe Dari-Mattiacci, Edoardo D. Martino & Gideon Parchomovsky, *Property Without Law: Personalized Property Rights Through Smart Contracts on the Blockchain*, YALE J. ON REG. (forthcoming 2026) (arguing that smart contracts create "de facto property rights" while acknowledging state involvement remains necessary); HENRY FARRELL & ABRAHAM L. NEWMAN, UNDERGROUND EMPIRE: HOW AMERICA WEAPONIZED THE WORLD ECONOMY 114 (2024) (characterizing blockchain as "alegal" systems that are indifferent to sovereign law and cannot be "punished or taken down"). *See infra* Part I.A.

[18] Wesley Newcomb Hohfeld, *Some Fundamental Legal Conceptions as Applied in Judicial Reasoning*, 23 YALE L.J. 16, 28 (1913) ("[T]he term 'rights' tends to be used indiscriminately to cover what in a given case may be a privilege, a power, or an immunity, rather than a right in the strictest sense . . . [but] it is certain that even those who use the word and the conception 'right' in the broadest possible way are accustomed to thinking of 'duty' as the invariable correlative."); *see also, e.g.*, Mauchlin v. Bier, No. CIVA 07CV02593CMAMEH, 2010 WL 419397, at 7 (D. Colo. Jan. 28, 2010), *aff'd*, 396 F. App'x 519 (10th Cir. 2010) ("A 'right' can be defined as 'a claim recognized and delimited by law for the purpose of securing it.' . . . Thus, the Court will at times refer to clearly established 'law' for the purpose of determining whether a given 'right' has been clearly established, i.e., recognized, as a 'right' by the law." (citation omitted)).

[19] HANS KELSEN, GENERAL THEORY OF LAW AND STATE 8–9 (Anders Wedberg trans., 1949) ("The law created by a legislator, i.e. by an act of will of a human authority, is positive law.").

[20] When this Article refers to "technical systems" it intends to refer to technical artifacts that operate within a social setting. The term technical artifact refers to "a discrete material object consciously produced or transformed by human activity under the influence of the physical and/or cultural environment." Mark C. Suchman, *The Contract as Social Artifact*, 37 LAW & SOC'Y REV. 91, 98 (2003); *see also* Jeffery M. Lipshaw, *The Persistence of 'Dumb' Contracts*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 1, 8 (2019) (applying Suchman's definition to blockchain-based smart contracts). "A technical artifact is one, like a tool or machine that serves a utilitarian, productive purpose." Lipshaw, *supra*, at 98–99 (citing Suchman, *supra*, at 99–100). Technical artifacts do not just stand alone, however. They exist in systems. Such socio-technical systems undoubtedly include a material social component, which gives rise to the concerns underlying this Article. *See* Günter Ropohl, *Philosophy of Socio-Technical Systems*, 4 SOC'Y PHIL. & TECH. Q. ELEC. J. 191, 192 (1999).

[21] *See* JOSEPH RAZ, THE AUTHORITY OF LAW: ESSAYS ON LAW AND MORALITY 30 (1979) (explaining that law "claims authority over its subjects" by creating reasons for action that preempt contrary considerations); Brian Leiter, *Legal*

that code can acquire binding force only through what Hart terms "rules of change."[22] This investiture can occur via two distinct pathways. The first is public empowerment, where lawmakers recognize code-based events as legally effective through legislation, or courts do so through the development of common law.[23] The second is private empowerment, where the law allows individuals to establish rights and obligations using code within contracts, wills, corporate charters, and other private ordering instruments.[24] Outside these pathways, code functions merely as "soft law" that can influence behavior but lacks prescriptive strength. Our framework then identifies the inherent limitations of these two avenues, explaining why code's deterministic logic struggles with concepts that depend on normative judgment, authoritative interpretation, and territorial application. Ultimately, this analysis reveals a relationship defined not by dominance but by distinct domains: while code governs the possible, the law retains the inviolable prerogative to define the permissible.

This Article proceeds in three parts. Part I begins by tracing the intellectual genealogy and subsequent distortion of the "code is law" maxim. We then leverage legal positivism to theorize the essential divide separating technical systems from legal rules and posit our core theoretical claim: this chasm can be bridged only when the legal system deliberately invests code with legal authority through its own rules. Part II diagnoses the grave consequences of misunderstanding the difference between code and law, documenting the resulting uncertainties and failings that pervade legislative, regulatory, and judicial actions, as well as private practice. Finally, Part III explains both the extent to which code genuinely can assume legal validity through either public or private empowerment, and the boundary conditions of these avenues. Our framework not only resolves the malaise affecting the blockchain ecosystem but also provides guidance for navigating the inevitable tensions between technical and legal systems that will arise with each new wave of technology, from large language models to autonomous robots.

I. THE JURISPRUDENCE OF CODE

This Part builds the Article's theoretical foundation in three steps. It first traces how Professor Lawrence Lessig's careful distinction between architectural constraint and legal obligation was progressively collapsed, particularly after the emergence of blockchain networks, into the claim that code possesses normative authority. It then introduces the analytical framework needed to diagnose this error: H.L.A. Hart's theory of primary and secondary rules, which provides the most rigorous method for determining what counts as law within a legal system. Finally, it synthesizes these inquiries to demonstrate that code, absent formal investiture by the legal system's own rules, remains a uniquely powerful form of soft law but lacks the capacity to generate enforceable rights and obligations.

Realism and Legal Positivism Reconsidered, 111 ETHICS 278, 285–87 (2001) (distinguishing law's operation in the space of reasons and justifications from physical constraints operating in the causal realm). *See infra* Part I.C.

[22] *See* H.L.A. HART, THE CONCEPT OF LAW 95–96 (3d ed. 2012) (describing rules of change as secondary rules that "empower[] individuals or bodies of persons to introduce new primary rules" and "to vary or extinguish old ones").

[23] *See infra* Part III.A.

[24] *See infra* Part III.B.

A. From Code is [Soft] Law in Cyberspace to Code is [Actual] Law in Cryptospace

In his influential work on the capacity of society to impose boundaries on activity undertaken via the internet, Professor Lawrence Lessig argued that positive law is but one tool in society's toolbox, and that how each tool is used affects how the others may be employed.[25] Building on work by Professor Joel R. Reidenberg,[26] Lessig argued that positive law represented only one modality through which to restrain or incentivize behavior in cyberspace.[27] While not actually rising to the level of positive law, Lessig pointed out that society and government possessed three other tools with which to constrain behavior in cyberspace: the market, social norms, and architecture, including the architecture of code.[28] Sometimes, one modality's effectiveness prevails over the others, and sometimes use of one modality impairs the use of another.[29]

Lessig explained his theory through the lens of the "pathetic dot," his term for the person or entity subject to regulation.[30] Government can certainly impose a duty on the pathetic dot to behave a certain way by imposing regulation and threatening enforcement for non-compliance.[31] Given, however, practical obstacles to enforcement posed by activity undertaken via the internet, Lessig argued that other modalities could prove equally, if not more, effective in constraining online behavior.[32] The market might entice the pathetic dot to voluntarily change its behavior.[33] Positive law might regulate the market to target specific behaviors, as "[t]he law uses taxes to increase the market's constraint on certain behaviors and subsidies to reduce its constraint on others."[34] Social norms might prevent unwanted actions, and positive law might shape those norms.[35] Lessig believed that architecture was the most overlooked modality in internet contexts.[36] Much of the architecture of cyberspace is built from software created using computer code. For Lessig, the

---

[25] LESSIG, *supra* note 16, at 123.

[26] Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 554 (1998) (arguing that "for network environments and the Information Society . . . law and government regulation are not the only source of rule-making").

[27] Lessig, *supra* note 16, at 123 ("Thus, four constraints regulate this pathetic dot—the law, social norms, the market, and architecture—and the 'regulation' of this dot is the sum of these four constraints. Changes in any one will affect the regulation of the whole.").

[28] Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 549 (1999) ("[M]ore than law alone enables legal values, and law alone cannot guarantee them. If our objective is a world constituted by these values, then it is as much these other regulators—code, but also norms and the market—that must be addressed.").

[29] LESSIG, *supra* note 16, at 123.

[30] *Id*. at 121-22 ("Ther are many ways to think about 'regulation.' I want to think about it from the perspective of someone who is regulated, or, what is different, constrained. That someone regulated is represented by this (pathetic) dot—a creature (you or me) subject to different regulations that might have the effect of constraining (or as we'll see, enabling) the dot's behavior.").

[31] *Id*. at 124 ("[L]aw constrains through the punishment it threatens.").

[32] *Id*. at 124 ("We can use the same [pathetic dot] model to describe the regulation of behavior in cyberspace. Law regulates behavior in cyberspace. . . How well law regulates, or how efficiently, is a different question: In some cases it does so more efficiently, in some cases less.").

[33] *Id*. ("Markets regulate behavior in cyberspace.").

[34] *Id*. at 127.

[35] *Id*. at 129 ("Law can change social norms as well. . . . To say that law plays a role is not to say that it always plays a positive role. The law can muck up norms as well as improve them.").

[36] Lawrence Lessig, *The Architecture of Privacy: Remaking Privacy in Cyberspace*, 1 VAND. J. ENT. & TECH. L. 56, 62–65 (1999).

computer code enabling internet activity "regulated" behavior by defining the universe of possible actions available to users.[37] This mirrors how physical architecture guides social and economic activity within cities or spaces. As Reidenberg had previously observed, "[t]echnological capabilities and system design choices impose rules on participants" providing policymakers an "extra-legal" tool for achieving policy aims.[38]

Professor Lessig encapsulated this concept with the maxim "code is law."[39] However, Lessig's catchy three-word pronouncement should not be read as "code is [positive] law," but rather as "code is [soft] law." The distinction is critical. Positive law, as legal theorists have long recognized, consists of rules that human institutions create through recognized procedures and enforce through state power. Only rules with this "pedigree" generate legally binding rights and obligations.[40] Soft law, conversely, encompasses "a set of norms that lacks formal legal consequences, but which nevertheless seeks to guide the actions of those to whom it is addressed and may produce some legal effects."[41] While soft law features prominently in the international law discourse,[42] in domestic law it typically attracts attention in areas where positive law is seen as undeveloped, insufficient, or otherwise contested. Scholars exploring the interaction between law and artificial intelligence frequently look to soft law to fill perceived gaps in the regulation of emerging technology.[43] In corporate law, soft law instruments fill gaps left by positive law around issues like corporate social responsibility, organizational ethics, and reputation.[44] Scholars of constitutional law have extensively explored the way soft law, in the form of norms, understandings, and events, applies to constitutional interpretation in deciding new and emerging issues.[45] Similarly, administrative law scholars discuss the use of agency best practices as a form of soft law that induces voluntary compliance with various regulatory schemes.[46] Some even argue

[37] LESSIG, *supra* note 16, at 20.
[38] Reidenberg, *supra* note 26, at 554-556.
[39] LESSIG, *supra* note 16, at 6.
[40] *See infra* Part I.B
[41] *See generally* Stephen Daly, *The Rule of (Soft) Law*, 32 KING'S L.J. 3, 4 (2021).
[42] Gregory C. Shaffer & Mark A. Pollack, *Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance*, 94 MINN. L. REV. 706, 707 (2010) ("There has been a prolific amount of scholarship regarding the use of 'hard' and 'soft' law in international governance."); Kenneth W. Abbott & Duncan Snidal, *Hard and Soft Law in International Governance*, 54 INT'L ORG. 421 (2000); Daniel E. Ho, *Compliance and International Soft Law: Why Do Countries Implement the Basle Accord?*, 5 J. INT'L ECON. L. 647 (2002).
[43] *See, e.g.,* Gary Marchant*, "Soft Law" Governance of Artificial Intelligence*, AI PULSE (Jan. 25, 2019), *available at* https://escholarship.org/content/qt0jq252ks/qt0jq252ks_noSplash_1ff6445b4d4efd438fd6e06cc2df4775.pdf (arguing that AI regulation will be patchwork and leave a governance gap to be filled by soft law, defined as "various types of instruments that set forth substantive expectations but are not directly enforceable by government"); Gary Marchant & Carlos Ignacio Gutierrez, *Soft Law 2.0: An Agile and Effective Governance Approach for Artificial Intelligence*, 24 MINN. J.L. SCI. & TECH. 375 (2023).
[44] *See, e.g.*, Claire A. Hill, *Caremark as Soft Law*, 90 TEMP. L. REV. 681 (2018); Kish Parella, *Improving Human Rights Compliance in Supply Chains*, 95 NOTRE DAME L. REV. 727 (2020); Kish Parella, *Reputational Regulation*, 67 DUKE L.J. 907 (2018).
[45] *See, e.g.*, Ernest A. Young, *The Constitution Outside the Constitution*, 117 YALE L.J. 408 (2007); Eric A. Posner & Adrian Vermeule, *Constitutional Showdowns*, 156 U. PA. L. REV. 991 (2008); Mark Tushnet, *Constitutional Hardball*, 37 J. MARSHALL L. REV. 523 (2004).
[46] David Zaring, *Best Practices*, 81 N.Y.U. L. REV. 294, 307-13 (2006).

that the U.S. Congress uses soft law in the form of congressional resolutions to address controversial, open, and emerging issues suffering from perceived positive law gaps.[47]

Just as soft law addresses gaps in these contexts, Professors Lessig and Reidenberg explored code's potential for guiding behavior in cyberspace. Their point was that "code is law" in the sense that it architects the parameters of possible activity, not that it creates new legal rights from software alone.[48] Even when code enforces compliance with positive law requirements,[49] the code itself does not become positive law.[50] It remains a technical constraint lacking the essential characteristics that transform rules into law: official recognition and state-backed enforcement.[51] Yet, as the internet evolved from a novel frontier into a mundane utility, the urgency of these early jurisprudential debates waned, and the sharp distinction between architectural and legal rules often faded from view. The erosion of analytical precision was further complicated by the persistence of cyber-separatist ideology that had emerged alongside early internet discourse.

During the time that Professor Lessig, Judge Easterbrook, Professor Reidenberg, and others debated the proper approach to law in cyberspace, another group of theorists, sometimes referred to as the cyber-separatists,[52] challenged the idea that positive law should apply in cyberspace at all. In the *Declaration of the Independence of Cyberspace*, John Perry Barlow,[53] who later helped found the Electronic Frontier Foundation,[54] famously proclaimed to the "Governments of the Industrial World, … weary giants of flesh and steel" that they "have no moral right to rule [cyberspace] nor do [they] possess any methods of enforcement [cyberspace has] true reason to fear."[55] Instead, Barlow argued that cyberspace governed itself better through its "culture, ethics or the unwritten codes" that order behavior in cyberspace, and believed that cyberspace would create "a world where anyone anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity."[56] This conception of cyberspace saw the opportunity to claw back personal rights and freedoms believed to have been lost to government overreach.

This cyber-separatist vision found fertile ground in the emerging cypherpunk movement of the late 1980s, where cryptographers, computer programmers, and privacy advocates coalesced around shared convictions about individual liberty and cryptography as a bulwark against state

[47] Jacob E. Gersen & Eric A. Posner, *Soft Law*, 61 STAN. L. REV. 573 (2008).
[48] LESSIG, *supra* note 16, at 20
[49] *See, e.g.*, Carla L. Reyes, *Conceptualizing Cryptolaw*, 96 NEB. L. REV. 384 (2017); Reyes, *Creating Cryptolaw*, *supra* note 3.
[50] Reyes, *Conceptualizing Cryptolaw*, *supra* note 49.
[51] *See infra* Part I.B.
[52] Usha R. Rodrigues, *Law and the Blockchain*, 104 IOWA L. REV. 679 (2019); Carla L. Reyes, *Autonomous Business Reality*, 21 NEV. L.J. 437 (2021).
[53] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), *available at* https://www.eff.org/cyberspace-independence.
[54] JOHN PERRY BARLOW LIBRARY, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/john-perry-barlow (last accessed Jan. 2, 2025).
[55] Barlow, *supra* note 53.
[56] *Id*.

overreach.[57] The cypherpunk ethos of direct technological action, embodied in Eric Hughes's declaration that "cypherpunks write code," merged with Timothy C. May's more radical vision of "Crypto Anarchy," first articulated in his 1988 "Crypto Anarchist Manifesto" and later expanded in the 1994 "Cyphernomicon."[58] May and his fellow crypto-anarchists envisioned cryptography as fundamentally reshaping governmental regulation, economic exchange, and social interaction itself, transforming their technological work into a form of political resistance against state authority and traditional legal constraints.[59]

When Satoshi Nakamoto introduced the Bitcoin protocol in 2008,[60] explicitly building on cypherpunk innovations like Wei Dai's "b-money" and Adam Back's "Hashcash,"[61] these ideological currents converged with technological capability. Bitcoin appeared to offer what Barlow had only imagined and what crypto-anarchists had theorized: a technical infrastructure that could operate autonomously, enforce rules through code rather than law, and remain beyond the reach of state enforcement. This technological embodiment of crypto-anarchist ideology profoundly influenced how early blockchain technology advocates understood the relationship between code and law, creating a predisposition to view technical constraints as legally sufficient in themselves, further muddying the distinction between code as architectural constraint and code as positive legal authority.

Against this backdrop, when scholars began applying Lessig's framework to blockchain technology, cryptocurrencies, and smart contracts, the analytical precision of the original framework was already under strain. As early as 2015, Professors Wright and De Filippi predicted the rise of *lex cryptographia*, under which persons entering into transactions via blockchain networks would be bound by "a set of rules administered through self-executing smart contracts

---

[57] Kelsie Nabben, *Cryptoeconomics as Governance: An Intellectual History from "Crypto Anarchy" to "Cryptoeconomics"*, 7 INTERNET HISTORIES 254 (2023); André Ramiro & Ruy de Queiroz, *Cypherpunk*, 11 INTERNET POL'Y REV. 1 (2022); Craig Jarvis, *Cypherpunk Ideology: Objectives, Profiles, and Influences (1992–1998)*, 6 INTERNET HISTORIES 315 (2022); Eric Hughes, *A Cypherpunk's Manifesto* (Mar. 9, 1993), *available at* https://www.activism.net/cypherpunk/manifesto.html; THOMAS RID, RISE OF THE MACHINES: A CYBERNETIC HISTORY (2016); Enrico Beltramini, *Against Technocratic Authoritarianism: A Short Intellectual History of the Cypherpunk Movement*, 5 INTERNET HISTORIES 201 (2021).

[58] Eric Hughes, *A Cypherpunk's Manifesto* (1993), *available at* http://www.activism.net/cypherpunk/manifesto.html; Timothy C. May, *The Crypto Anarchist Manifesto* (1988); Timothy C. May, *The Cyphernomicon* (1994).

[59] Lana Swartz, *What Was Bitcoin, What Will It Be? The Techno-Economic Imaginaries of a New Money Technology*, 32 CULTURAL STUD. 623 (2018).

[60] In computer science, a "protocol" denotes a formal specification defining the rules and conventions governing communication and data exchange between network participants. In the blockchain context, a protocol establishes the consensus mechanism, transaction validation rules, and communication standards that network nodes must follow to participate in the system. *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), *available at* https://bitcoin.org/bitcoin.pdf (establishing the Bitcoin network's protocol specifications). Throughout this Article, "protocol" is used in this narrow, technical sense—referring to the specification or rule-set itself—as distinct from "system," which denotes the broader socio-technical infrastructure within which protocols are implemented and human actors interact. *See supra* note 20 (defining "technical systems").

[61] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 8 (2008), *available at* https://bitcoin.org/bitcoin.pdf (citing Wei Dai, *b-money* (1998), *available at* http://www.weidai.com/bmoney.txt; Adam Back, *Hashcash - A Denial of Service Counter-Measure* (2002), *available at* http://www.hashcash.org/papers/hashcash.pdf).

and decentralized and potentially autonomous organizations."[62] They theorized this new regime as a combination of code-as-soft-law and private ordering backed by traditional contract law, retaining Lessig's framing largely unaltered. Crucially, however, they predicted that blockchain technology's novel technical capabilities would fundamentally challenge existing legal frameworks. Eventually, they argued, "law and code may merge."[63] Even at this early stage, the language of binding rules administered through technical execution gestured toward code functioning as a source of normative force rather than merely a constraint on behavior.

Over time, this analytical imprecision deepened. By 2016, De Filippi and Hassan argued that blockchain represented a shift from "code is law" to "law is code," where legal rules would be "drafted or elaborated" as code.[64] This formulation no longer treats code as an instrument implementing law, but as the medium in which law itself is constituted. Later work suggested blockchain technology might be "alegal," operating independently of existing legal frameworks.[65] The possibility that code could generate rights and obligations without any investiture by positive law was no longer implicit but explicitly entertained as a structural feature of blockchain governance. Other scholars advanced similar claims with increasing boldness, arguing variously that technical finality could replace state-backed enforcement, that software could become "the sole determinant of enforceability," and that coordination games could produce "authoritative decisions without authoritative decision-makers."[66]

In adjacent fields, scholars of corporate governance and organizational theory built upon the premise that code can substitute for legal structures, treating blockchain-based smart contracts as functional equivalents of "articles of association or bylaws" capable of replacing traditional governance mechanisms.[67] Most recently, some have posited the emergence of "property without

---

[62] Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* 48 (Mar. 12, 2015) (unpublished manuscript), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

[63] *Id.*

[64] Primavera De Filippi & Samer Hassan, *Blockchain Technology as a Regulatory Technology: From Code Is Law to Law Is Code*, 21 FIRST MONDAY (2016), *available at* https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657; Samer Hassan & Primavera De Filippi, *The Expansion of Algorithmic Governance: From Code Is Law to Law Is Code*, 17 FIELD ACTIONS SCI. REPS. 88 (2017).

[65] Primavera De Filippi, Morshed Mannan & Wessel Reijers, *Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance*, 62 TECH. IN SOC'Y 1 (2020); *cf.* Andrew M. Hinkes, *The Limits of Code Deference*, 46 J. CORP. L. 869 (2021) (addressing how users of blockchain-derived systems cannot practically extricate themselves from the purview of extrinsic legal systems).

[66] *See, e.g.,* Pietro Ortolani*, Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin*, 36 OXFORD J. LEGAL STUD. 595 (2016) (describing Bitcoin adjudication as a "self-contained system of dispute resolution" in which technical finality replaces state-backed enforcement); Philipp Paech, *The Governance of Blockchain Financial Networks*, 80 MOD. L. REV. 1073 (2017); Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 382–83 (2016); Stephen Wolfram, *Computational Law, Symbolic Discourse and the AI Constitution*, *in* ETHICS OF ARTIFICIAL INTELLIGENCE 155 (S. Matthew Liao ed., 2020); Wulf A. Kaal & Craig Calcaterra, *Crypto Transaction Dispute Resolution*, 73 BUS. LAW. 109 (2017–2018); Federico Ast & Clement Lesaege, *Kleros: Short Paper v1.0.7* (2020)*,* available at https://kleros.io/whitepaper.pdf.

[67] *See* Mark Fenwick, Wulf A. Kaal & Erik P.M. Vermeulen, *Why "Blockchain" Will Disrupt Corporate Organizations* 17 (Eur. Corp. Governance Inst., Law Working Paper No. 419, 2018) (asserting that "in a truly decentralized system, the code is law"); Mark Fenwick, Wulf A. Kaal & Erik P.M. Vermeulen, *The "Unmediated" and "Tech-Driven" Corporate Governance of Today's Winning Companies* 43–48 (Working Paper No. 2922176, 2017); CHRIS BERG, SINCLAIR DAVIDSON & JASON POTTS, UNDERSTANDING THE BLOCKCHAIN ECONOMY: AN

law," contending that smart contracts can transmute contractual promises into "de facto property rights" through technical enforcement alone, thereby bypassing the numerus clausus principle.[68] Such accounts fundamentally misconceive the nature of legal validity, erroneously assuming that technical mimicry of a property rule is equivalent to the normative investiture provided by a secondary rule of recognition.

These academic arguments found enthusiastic reception in industry. The 2016 launch of The DAO provided the canonical formulation of the fallacy: its terms explicitly stated that "smart contract code governs the Creation of DAO tokens and supersedes any public statements."[69] When an attacker exploited a vulnerability to drain approximately $60 million, defenders argued that because the code permitted the transaction, it was legitimate by definition; the subsequent hard fork that reversed these transactions revealed the practical impossibility of the code-as-law position, yet the ideological commitment persisted.[70] Gavin Wood, co-founder of Ethereum, has consistently advocated "fully automated algorithmic governance," arguing that blockchain technology "directly serves to dilute power" concentrated in legal institutions.[71] This position is not idiosyncratic; it reflects widespread industry sentiment among prominent protocol architects who have implemented "code is law" through deliberate architectural choices.[72] Balaji Srinivasan's *The Network State* extends the fallacy to sovereignty itself, arguing that blockchain-governed

---

INTRODUCTION TO INSTITUTIONAL CRYPTOECONOMICS 2–3 (2020); Sinclair Davidson, Primavera De Filippi & Jason Potts, *Blockchains and the Economic Institutions of Capitalism*, 14 J. INST. ECON. 639 (2018); Aaron Wright, *The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges*, 4 STAN. J. BLOCKCHAIN L. & POL'Y 152, 154–55 (2021).

[68] Bechtold et al., *supra* note 17, at 4–5 (arguing that smart contracts "turn mere contractual rights into de facto property rights" unconstrained by the *numerus clausus* principle).

[69] The DAO, *Explanation of Terms and Disclaimer* (2016), *available at* https://web.archive.org/web/20160513073743/https://daohub.org/explainer.html. The DAO collected approximately 11.5 million Ether, worth roughly $150 million. *See* REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO, Exchange Act Release No. 81207, at 1–2 (July 25, 2017); Christoph Jentzsch, *Decentralized Autonomous Organization to Automate Governance* 1 (2016) (describing The DAO as operating "virtually unstoppably").

[70] *See* Pastebin, *An Open Letter* (June 18, 2016), *available at* https://pastebin.com/CcGUBgDG (purportedly from the attacker, arguing that the exploit was a "rightful" use of "explicitly coded" features); Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 487, 524–27 (2018); Quinn DuPont, *Experiments in Algorithmic Governance*, *in* BITCOIN AND BEYOND: CRYPTOCURRENCIES, BLOCKCHAINS, AND GLOBAL GOVERNANCE 157 (Malcolm Campbell-Verduyn ed., 2018).

[71] *See* Jan Groos, *Crypto Politics: Notes on Sociotechnical Imaginaries of Governance in Blockchain Based Technologies*, *in* DATA LOAM 148, 155 (2020) (describing Wood's vision as "fully automated algorithmic governance"); Gavin Wood, *Remarks at Unfinished Live* (2021), *available at* https://unfinished.com/news/ethereum-co-founder-gavin-wood-blockchain-needs-clear-governance/.

[72] When the Parity wallet hack resulted in losses exceeding $150 million, Wood rejected proposals to fork the blockchain. *See* Michael del Castillo, *The Parity Wallet Freeze: A Postmortem*, COINDESK (Nov. 8, 2017). Other prominent figures embraced similar positions. Andre Cronje, founder of Yearn Finance, normalized the view that smart contract losses are failures of user due diligence, not legal wrongs. *See* Camila Russo, *Andre Cronje: The King of DeFi Has Mass Farmer Appeal*, THE DEFIANT (Sept. 8, 2020). Hayden Adams designed Uniswap's core contracts to be immutable, placing the protocol beyond the technical capacity to comply with external directives. *See* Jacob Horne, *Hyperstructures*, MIRROR (Jan. 2022), *available at* https://jacob.energy/hyperstructures.html. Rune Christensen's "Endgame" plan for MakerDAO envisions "protocol ossification" eliminating human governance entirely. *See* Rune Christensen, *The Endgame Plan*, MAKERDAO F. (May 2022). Jesse Powell, co-founder of Kraken, has argued that cryptographic proof supersedes regulatory oversight. *See* Jesse Powell, *Interview*, UNCHAINED PODCAST (Nov. 2022).

communities will "replace nation-states" and requiring adherents to commit to "trusting AI over human courts and judges."[73]

To be sure, several legal scholars have resisted this drift, maintaining the analytical distinction between code's architectural power and law's normative authority.[74] Yet despite these cogent objections, the fallacy has achieved such cultural and commercial traction that courts must now adjudicate whether it provides a defense to civil liability. In *Banksia Finance Corp. v. Medjedovic*, a defendant who exploited a decentralized finance protocol for approximately $15.8 million invoked "code is law" as a defense, arguing that because he operated within the protocol's technical parameters, his actions were legitimate by definition.[75] The court framed the question as whether Ontario common law supports the "code is law" theory, describing it as a position under which "voluntary participants accept and are bound by the results of the use of the technology."[76] That a court must now engage with whether technical permissibility confers legal validity demonstrates how far the fallacy has traveled from its origins in academic speculation.

What emerges from this history is not merely confusion, but a systematic category error: the progressive collapse of the distinction between technical enforcement and legal validity. Across scholarship, industry practice, and now litigation, technical permissibility is increasingly treated as normatively dispositive, as though the ability of code to execute outcomes were sufficient to constitute law. Once this move is made, there is no principled stopping point: contract, property, governance, adjudication, and even sovereignty become candidates for displacement by code. This error reflects a deeper failure to articulate what positive law is, how it differs from soft law, and why neither technical constraint nor algorithmic finality can supply the conditions of legal

---

[73] BALAJI SRINIVASAN, THE NETWORK STATE: HOW TO START A NEW COUNTRY (2022), *available at* https://thenetworkstate.com/; *The Network School, Admissions Requirements* (2024) (requiring commitment to "trusting AI over human courts and judges"); *see also* Nitasha Tiku, *Inside Balaji Srinivasan's "Network School,"* WIRED (Oct. 15, 2024); Editorial, *Network States: The Tech Broligarchy Who Want to Create New Countries*, THE WEEK (Apr. 22, 2025).

[74] *See, e.g.*, Jeffery M. Lipshaw, *The Persistence of "Dumb" Contracts*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 1 (2019) (arguing that code cannot replicate the "infinite regress" of human judgment required for normative legal determination); Kelvin F.K. Low & Eliza Mik, *Pause the Blockchain Legal Revolution*, 69 INT'L & COMP. L.Q. 135, 137–40 (2020) (calling "code is law" a "dangerous fallacy"); Heather Hughes, *Blockchain and the Future of Secured Transactions Law*, 3 STAN. J. BLOCKCHAIN L. & POL'Y 1 (2020); Karen Yeung, *Algorithmic Regulation: A Critical Interrogation*, 12 REGUL. & GOVERNANCE 505 (2018); James J. Park, *Crypto Associations*, 73 UCLA L. REV. (forthcoming 2026); Katrin Becker, *Blockchain Matters—Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*, 33 LAW & CRITIQUE 113 (2022); Carla L. Reyes, *If Rockefeller Were a Coder*, 87 GEO. WASH. L. REV. 373 (2019). *See also* Carla L. Reyes, *A Unified Theory of Code-Connected Contracts*, 46 J. CORP. L. 981 (2021); Kevin Werbach & Nicholas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313 (2017); Juliet M. Moringiello & Christopher K. Odinet, *The Property Law of Tokens*, 74 FLA. L. REV. 607 (2022); Andrea Tosato & Christopher K. Odinet, *Digital Assets and the Property Question*, 78 FLA. L. REV. (forthcoming 2026); Kara Bruce, Christopher K. Odinet & Andrea Tosato, *The Private Law of Stablecoins*, 54 ARIZ. ST. L.J. 333 (2023).

[75] Banksia Fin. Corp. v. Medjedovic, 2021 ONSC 8473 (Can. Ont. Sup. Ct. J.) (granting arrest warrant after defendant failed to appear). The defendant argued that "the people who I traded against and won money from read the same contract I did and were willing to deploy their capital on it." Andean Medjedovic (@ZetaZeroes), TWITTER (Oct. 21, 2021); *see also* Andrew Thurman, *Canadian $15.8M DeFi Theft Case Could Upend "Code Is Law" Convention*, BLOCKWORKS (Dec. 22, 2021); Quinn Emanuel Urquhart & Sullivan, LLP, *"Code is Law"* (Client Alert, 2022), *available at* https://www.quinnemanuel.com/media/u3hbmhhx/client-alert-code-is-law.pdf.

[76] *Banksia*, 2021 ONSC 8473; *see also* Thurman, *supra* note 75; Quinn Emanuel Urquhart & Sullivan, LLP, *supra* note 75.

authority. Before examining how this collapse manifests in doctrine and regulation, it is therefore necessary to recover a clear account of law's normative foundations. Part I.B undertakes that task.

B. A Positivist Framework to Analyze the Relationship Between Code and Law

If the central proposition of this Article is that "code is not law," we must first address a preliminary question: what is "law"? Legal philosophy has offered competing accounts of law's nature, including natural law theory, legal realism, and Dworkinian interpretivism, among others. For the purposes of this Article, we conduct our analysis through a legal positivist framing. Our choice is not based on a claim that positivism is the one true theory of law, but on our conviction that it is the most analytically useful and descriptively accurate framework for addressing the specific question of whether code can create legal rights and obligations. We ground this choice in three principal reasons.

First, positivism, which holds that law is a system of rules grounded in social facts or convention ("the social thesis") and that there is no necessary connection between law and morality ("the separability thesis"),[77] provides the most cogent and widely accepted explanation of our existing legal system. Its descriptive accuracy is so widely recognized that even the leading contemporary natural law theorist John Finnis concedes that positivist theories offer a completely adequate account of "what any competent lawyer…would say are (or are not) intrasystematically valid laws."[78] This descriptive power helps explain why legal positivism is widely regarded as the dominant theory of law in contemporary legal thought,[79] a primacy which extends to practice, where lawmakers, regulators, and practitioners predominantly view law through a positivist lens, focusing on posited rules rather than moral precepts.[80]

Second, positivism is uniquely suited to analyzing questions of legal validity. The "code is law" debate is, at its core, a dispute about what counts as a valid, authoritative source of legal rules. It is not a claim about morality (the focus of natural Law) or about judicial behavior (the focus of legal realism). Legal positivism is the only major school of thought purpose-built to answer this specific question: how do we distinguish rules that are legally binding from those that are not? Its intense focus on the criteria for validity provides the precise analytical toolkit needed to dissect claims that a new technology can generate law.

Third, and most critically, the arguments advanced by proponents of *lex cryptographia* are themselves structurally positivist in nature. As we will see in Part II, the most ambitious proponents of "code is law" argue that blockchain networks create nascent legal orders. They ground their

[77] Brian Leiter, *Legal Positivism*, *in* A COMPANION TO PHILOSOPHY OF LAW AND LEGAL THEORY 241, 244 (Dennis Patterson ed., 2d ed. 2010).
[78] John Finnis, *On the Incoherence of Legal Positivism*, 75 NOTRE DAME L. REV. 1597, 1611 (2000).
[79] Brian Bix, *Legal Positivism*, *in* THE BLACKWELL GUIDE TO THE PHILOSOPHY OF LAW AND LEGAL THEORY 29 (William A. Edmundson & Martin P. Golding eds., 2005) (describing legal positivism as "orthodoxy in desperate need of dissent"); Leiter, *supra* note 77, at 241, 244–46.
[80] Leiter, *supra* note 77, at 241, 244–46 (discussing positivism's prevalence in legal practice and education).

claims in social facts like technical function and community acceptance, rather than in moral principles (as natural law would require), judicial decisions (as legal realism would emphasize), or interpretive coherence with existing legal principles (as Dworkinian theory would demand). In effect, they are advancing a positivist claim that a new set of social conventions has given rise to a new source of law. Therefore, the most rigorous method for evaluating their thesis is to meet it on its own theoretical ground, using the tools of legal positivism to test whether these new social facts satisfy the necessary criteria for what constitutes a mature legal system. If code cannot qualify as law even under the jurisprudential theory that its own proponents implicitly adopt, then the "code is law" thesis fails definitively.

Having established the basis for our analytical approach, we now turn to a fuller exposition of the positivist conception of law. Legal positivism, as a school of thought, seeks to provide a descriptive account of law as a social phenomenon, free from prescriptive judgments about what law ought to be. At its core, positivism advances two central theses that distinguish it from rival theories.[81] The first is the social thesis, which posits that law is fundamentally a product of human social practices and conventions, deriving its existence and content from identifiable social facts such as legislative enactment, judicial decisions, or customary acceptance.[82] The second, the separability thesis, maintains that there is no necessary connection between law and morality; in stark contrast to natural law theories,[83] positivists assert that a rule can be legally valid even if it is morally reprehensible, as its validity depends solely on its conformity to the system's criteria for recognition, not on moral or ethical evaluation.[84] These theses, albeit subject to internal variations, form the bedrock of positivism, enabling a neutral analysis of legal systems as they actually function.

Contemporary positivism owes much to the refinements of H.L.A. Hart, whose work in The Concept of Law constituted a sophisticated evolution from earlier conceptualizations, including those of John Austin[85] and Hans Kelsen.[86] Hart posited that the "key to the science of jurisprudence" lies in understanding law as a union of two different types of rules: primary and secondary.[87] Primary rules are those that impose duties or confer rights upon individuals. They are the rules that govern conduct in a society, specifying what people must do or abstain from doing, such as prohibitions against violence and theft or requirements to pay taxes.[88] A simple, "pre-

[81] Legal positivism emerged from the empiricist tradition of British philosophy, notably from the work of Jeremy Bentham. *See* JEREMY BENTHAM, AN INTRODUCTION TO THE PRINCIPLES OF MORALS AND LEGISLATION (J.H. Burns & H.L.A. Hart eds., 1970) (1789).
[82] See Leiter, *supra* note 77, 242.
[83] See JOHN FINNIS, NATURAL LAW AND NATURAL RIGHTS 23-29 (2d ed. 2011) (articulating the position of natural on this matter).
[84] See Leiter, *supra* note 77, 243.
[85] John Austin's command theory characterized law as orders backed by threats issued by a sovereign whom subjects habitually obeyed. *See* JOHN AUSTIN, THE PROVINCE OF JURISPRUDENCE DETERMINED 18–25 (Wilfrid E. Rumble ed., Cambridge Univ. Press 1995) (1832).
[86] *See* HANS KELSEN, PURE THEORY OF LAW 193–205 (Max Knight trans., Univ. of Cal. Press 1967) (1934) (describing law as a hierarchical system of coercive norms, the validity of which derives from a "basic norm" or *Grundnorm*).
[87] *See* H.L.A. HART, THE CONCEPT OF LAW 94–95 (3d ed. 2012). For an excellent description of Hart's theory, *see generally* JOSEPH RAZ, PRACTICAL REASON AND NORMS 49–58 (2d ed. 1990).
[88] *Id.* at 79-81.

legal" society could exist with only a set of primary rules, but would suffer from three key deficiencies: uncertainty,[89] inability to adapt to change,[90] and inefficient enforcement.[91]

To remedy these, Hart introduced secondary rules, which operate at a meta-level, by specifying the procedures for identifying, altering, and adjudicating the primary rules. First, rules of recognition specify criteria for identifying valid law within the system, solving the problem of uncertainty about which rules are legally binding.[92] This type of rule is not a formally enacted law but rather exists only "as a complex practice of the courts, officials, and private persons in identifying the law by reference to certain criteria."[93] For instance, in the United States, as suggested by Professor Kent Greenawalt, officials recognize as law what the Constitution authorizes, congressional enactments, valid agency regulations, and judicial precedents.[94] Second, rules of change empower authorities or individuals to introduce, modify, or extinguish primary rules, remedying the otherwise static nature of a pre-legal society.[95] These rules confer both public and private powers. Publicly, they grant the authority to legislate. Privately, they empower individuals to create, vary, and extinguish their own rights and duties through legally recognized avenues such as contracts, wills, or trusts.[96] Third, rules of adjudication authorize individuals or bodies to make rulings about whether primary rules have been violated and determine the methods to be followed in this assessment.[97]

This Hartian model underscores positivism's descriptive focus: law exists where primary and secondary rules coexist and are efficacious, independent of moral content. As Brian Leiter elucidates, Hart's approach reconciles positivism with the normative aspect of law by distinguishing the external observer's perspective (describing social facts) from the internal participant's viewpoint (accepting rules as guides for conduct).[98] It rejects natural law's insistence on moral validity as a precondition for law, viewing such claims as conflating "is" and "ought," as well as legal realism's emphasis on judicial behavior as the essence of law.[99]

---

[89] *Id.* at 91-94 (explaining that without an authoritative text or official, doubts would arise as to what the rules are or their precise scope).
[90] *Id.* 91-94 (describing a society with only primary rules as "static" because its rules could only change through slow, undirected processes of custom).
[91] Id. 91–94 (noting that without an official agency for authoritative adjudication, the enforcement of rules would be inefficient and prone to private vendettas).
[92] *Id. at 94–95;* see *Scott Shapiro,* What Is the Rule of Recognition (and Does It Exist)*?,* in THE RULE OF RECOGNITION AND THE U.S. CONSTITUTION 235, 237–40 (Matthew D. Adler & Kenneth Einar Himma eds., 2009) (providing a succinct summary of the criticisms that have been leveled at Hart's conceptualization of the rule of recognition).
[93] *Id.* 94–95.
[94] *See* Kent Greenawalt, *The Rule of Recognition and the Constitution*, 85 MICH. L. REV. 621, 659–60 (1987) (analyzing the complex rule of recognition in the American legal system).
[95] Hart, *supra* note 87, at 94–95; *see also* Shapiro, *supra* note 92, at 243 (describing rules of change as advancing the "dexterity of the law").
[96] *Id.* 95–96.
[97] *Id.* 96–98.
[98] Leiter, supra note 77, at 251–53.
[99] *Id.*

Equipped with this understanding of what constitutes a legal system, we can now examine whether and how computer code might acquire legal force within Hart's framework of primary and secondary rules.

C. The Synthesis: Code is Not Law, Unless Empowered by Secondary Rules

The preceding analysis establishes a critical distinction: Lawrence Lessig's "code is law" describes a system of architectural limitations, while H.L.A. Hart's positivism theorizes a system of legal obligation. The former explains how code *constrains* by defining the boundaries of possible action; the latter explains how law *obligates* by creating enforceable rights and duties. From this foundation emerges our central thesis that code is not law unless it acquires legal force through the legal system's secondary rules. Absent such a formal "investiture," code remains merely a uniquely powerful form of soft law.

The trouble with code is that its extraordinary effectiveness in controlling behavior creates an insidious deception. Like a shadow that appears solid in dim light, code's regulatory power can seem indistinguishable from law's normative force. Professor John Gardner emphasizes that law's nature includes its claim to legitimate authority over other normative systems.[100] As code regulates behavior with such absoluteness and finality, especially in blockchain systems where transactions are tamper-resistant and append-only, it appears to usurp law's throne, not through direct challenge but through sheer indifference. Code does not claim authority; it simply governs the realm of the possible. Yet this is only an illusion of legal authority that cannot obscure the fundamental divide between code and law.

There is an ontological gap that separates architectural constraints from legal rules. Legal rules are not merely patterns of behavior or effective constraints on action. They are normative standards existing within an institutional framework that determines their validity, application, and change.[101] As Joseph Raz argues, law claims authority: it presents itself as creating reasons for action that preempt and exclude contrary considerations.[102] Architecture, by contrast, shapes behavior through physical or digital impossibility, not through normative demand.

When code renders an action possible or impossible, it makes no claim about what ought to occur. It simply determines what can occur through technical means. This represents a fundamentally different mode of regulation than law's normative prescriptions. Brian Leiter's naturalized jurisprudence illuminates this distinction: while law operates in the space of reasons and

[100] *See* JOHN GARDNER, LAW AS A LEAP OF FAITH 138–42 (2012) (discussing law's claim to supremacy over other normative systems).
[101] *See* Hart, *supra* note 87, at 94–95 (distinguishing between social habits and normative rules).
[102] JOSEPH RAZ, THE AUTHORITY OF LAW: ESSAYS ON LAW AND MORALITY 30 (1979) ("The law claims authority over its subjects; they owe allegiance to it."); *see also* JOSEPH RAZ, THE MORALITY OF FREEDOM 35–37 (1986) (developing the concept of exclusionary reasons).

justifications, code operates in the causal realm of physical constraints.[103] The locked door does not tell you that you should not or may not enter; it merely prevents entry.

Code, standing alone, cannot constitute law. Law requires not just behavioral constraints but an institutional structure that validates, changes, and adjudicates those constraints. Code lacks this institutional dimension: it simply exists, without need for validation or interpretation in its basic operation. The fact that code regulates behavior effectively does not make it law any more than the fact that gravity pulls objects downward toward the earth makes it a legal prohibition against flying. Law's distinctive mode of existence, through institutional recognition rather than physical presence, remains essential.

However, this separation is not absolute. Law, through its own institutional mechanisms, can choose to bridge it by formally empowering code. This investiture occurs through two distinct but interlocking pathways derived from Hart's secondary rules. The most direct avenue is through the legal system's "rules of change" that confer power on individuals or institutions to introduce, modify, or extinguish primary rules.[104] The law, through a deliberate act of a recognized authority, proactively creates a bridge from the technical to the legal realm. In doing so, this process maintains the analytical distinction between code and law while creating practical integration: the architectural constraint remains architectural, but law wraps around it, making its implementation obligatory or its effects legally cognizable.

This empowerment operates through both public and private channels. Public powers deserve further differentiation. Legislative empowerment occurs when legislatures mandate specific architectural standards. They do not make architecture into law but rather create legal obligations to implement certain architectural constraints. The architecture remains causally effective, but law provides the normative mandate for its implementation. Administrative delegation, on the other hand, represents a double delegation: from the legal system to the agency, and from the agency to the architectural constraint. When agencies specify technical requirements, molecular or digital architecture becomes legally mandatory through administrative specification.

Private powers operate through a different mechanism. Hart recognized that rules of change grant individuals a form of "limited legislative power" to create binding obligations for themselves.[105] The law of contracts exemplifies this: it is not merely a set of primary duties but a sophisticated system of secondary rules empowering private ordering. Through these secondary rules, individuals can create new primary obligations that the legal system will recognize and enforce. This private legislative power, though limited in scope and subject to legal constraints, represents a genuine delegation of law-making authority to private parties. When extended to code, it allows private actors to create architectural arrangements that carry legal force not through their technical operation but through their legal empowerment.

---

[103] Brian Leiter, *Legal Realism and Legal Positivism Reconsidered*, 111 ETHICS 278, 285–87 (2001) (discussing the causal efficacy of legal rules versus physical constraints).
[104] Hart, supra 87, 95-96.
[105] *Id.* at 96 ("rules which confer on individuals power to vary their initial positions under the primary rules").

A second pathway for code to receive legal investiture is through the rule of recognition. Under this more organic mechanism, legal validity is conferred upon code not by legislative enactment, but by its satisfaction of criteria that emerge from and are sustained by the concordant practice of legal officials.[106]

However, we note that, while jurisprudentially sound, this pathway appears to be more of a theoretical possibility than a present reality. Rules of recognition traditionally identify sources of law such as constitutions, statutes, judicial decisions, and administrative regulations, all of which share certain formal characteristics that code lacks. These sources produce texts that can be interpreted, procedures that can be followed, and institutions the authority of which can be traced.[107] Code operates through deterministic execution rather than interpretable prescription.

Moreover, if a rule of recognition were to recognize code as having legal force, this would inevitably occur with precision and limitations. The rule of recognition serves to provide certainty about what counts as law. It would not recognize any code executed in any system by any person under any circumstance as having legal authority. At most, recognition would extend to very specific and clearly identified contexts: code executed on particular systems, following specified procedures, by authorized parties.[108] The social practice of legal officials would need to converge on precise criteria for distinguishing legally effective code from mere technical operations.

Thus, code's road to legal status is narrow and precisely delimited. Its mere effectiveness is not a source of legal validity, which derives from "pedigree," not performance.[109] Nor can the convictions of its users bestow legal force, for this would mistake popular consensus for the official, institutional acceptance. Whether through the proactive grant of power by a rule of change or the organic validation by the rule of recognition, it is only an act of positive law that can give code legal force.

This understanding illuminates debates about technological determinism versus legal control in digital spaces. Neither view is complete: code powerfully shapes behavior through architectural constraint, but law retains the capacity to require, prohibit, or channel code's deployment. The relationship is not one of dominance by either modality but of complex interaction mediated by secondary rules. Code governs the possible; law governs the permissible. Their intersection, not their opposition, defines the legal landscape of cyberspace and cryptospace alike.

The next Parts of this Article will explore how misunderstanding this relationship has led to theoretical confusion and costly mistakes, and when code genuinely does carry the force of law

---

[106] See *supra* Part I.B.

[107] *See* Greenawalt, *supra* note 94, at 659–60 (powerfully illustrating this point by mapping out all the sources recognized by the rule of recognition in the U.S.).

[108] For an example of a proposal that falls within the realm of investiture by recognition, *see* Reyes, *Creating Cryptolaw*, *supra* note 3.

[109] *See supra* Part I.B.

through proper empowerment. The theoretical foundation, however, stands firm: code is not law, unless and until law makes it so.

II. MISUNDERSTANDINGS OF CODE AS [ACTUAL] LAW IN CRYPTOSPACE

Part I described the theoretical shift from Lessig's nuanced insights about the capabilities of code as an architectural constraint to claims, rooted in cyber-separatist and cypherpunk ideology, that code is, or should be, actual law. In opposition to this idea, we advanced our central thesis that code is only soft law unless the legal system's secondary rules formally invest it with legal authority.

This is not merely an academic dispute. The true significance of the "code is law" misconception lies in its migration from theory to practice, where it now serves as the flawed foundation upon which the legal and economic frameworks of the cryptospace are being built. This foundational error is the source of tangible legal pathologies, distorting outcomes and creating systemic risk.

This Part, therefore, shifts from jurisprudence to diagnosis. The flawed paradigm we identified in Part I has metastasized throughout the cryptospace legal framework. Legislators enact statutes that conflate technical functionality with legal authority. Regulators issue guidance that assumes code execution generates binding legal rights. Judges struggle to distinguish between what blockchain systems enable technically and what transactions conducted through those systems accomplish legally. Most troublingly, private actors routinely operate under the dangerous misconception that code can create, modify, or extinguish legal rights and obligations through technical execution alone.

A. Legislators and Regulators Charged with Creating Law Occasionally Confuse Code for Law.

The confusion between code's technical capabilities and legal authority pervades legislative and regulatory responses to blockchain technology. Rather than attempt a comprehensive survey of every misguided statute or flawed regulatory guidance, this section examines representative examples that illustrate the fundamental error in each domain. We focus on paradigmatic cases where lawmakers and regulators have conflated what code enables with what law requires, demonstrating how theoretical misunderstanding translates into practical regulatory failure.

The pattern is consistent: when legislators draft laws based on misconceptions about code’s legal status, they create frameworks that achieve neither their intended goals nor legal clarity. When regulators assume that technical functionality automatically generates legal obligation, they produce guidance that confuses rather than clarifies applicable legal standards. These examples reveal not isolated mistakes but systematic confusion about the relationship between architectural constraint and legal authority.

1. Legislation that confuses code for law

State legislatures have operated at the vanguard of digital asset-related lawmaking, enacting bills addressing blockchains, digital assets, and smart contracts well before federal efforts materialized.[110] While ostensibly undertaking these efforts to accommodate emerging technology, these statutes frequently conflate the technical capacities of technological systems with the creation or modification of legal rights. The following examples illustrate this confusion between code and law, serving as case studies that illuminate a deeper and more problematic trend.

In Arkansas, for example, legislators amended the state's Uniform Electronic Transactions Act to include several digital asset-related definitions and rather unusual assertions regarding smart contracts.[111] Specifically, the statute asserts that the term smart contract means "business logic that runs on a blockchain" or "[a] software program that stores rules on a shared and replicated ledger and uses the stored rules for: (i) Negotiating the terms of a contract; (ii) Automatically verifying the contract; and (iii) Executing the terms of a contract."[112] The statute further provides that "[a] smart contract shall be considered a commercial contract,"[113] and declares that any smart contract that "relates to a transaction shall not be denied legal effect, validity, or enforceability."[114]

The Arkansas statute's proposition that all smart contracts are commercial contracts reflects a fundamental misunderstanding. A contract, at its core, is a legally enforceable agreement: "a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty."[115] Its formation requires offer, acceptance, consideration, and mutual assent: elements that exist in the normative realm of legal obligation between identifiable parties.[116] A smart contract, by contrast, is a computer program deployed on a blockchain that executes predetermined operations upon receiving specified data inputs.[117] The former is a creature of law; the latter is an artifact of code. A smart contract may, under certain circumstances, serve as the vehicle through which parties form or perform a legally enforceable agreement, but it does not constitute one by virtue of its technical operation alone.[118] By equating the software script with the legal obligation, the Arkansas statute conflates the architectural constraint with the binding legal agreement, collapsing the very distinction between code and law that our theoretical framework identifies as essential.

---

[110] Federal legislative efforts addressing digital assets emerged later, with significant proposals appearing only after 2022. *See, e.g.*, Financial Innovation and Technology for the 21st Century Act, H.R. 4763, 118th Cong. (2023); Responsible Financial Innovation Act, S. 2281, 118th Cong. (2023).
[111] ARK. CODE ANN. § 25-32-122 (2023).
[112] *Id*. § 25-32-122(a)(3).
[113] *Id*. § 25-32-122(d)(1).
[114] *Id*. § 25-32-122(d)(2).
[115] RESTATEMENT (SECOND) OF CONTRACTS § 1 (Am. L. Inst. 1981).
[116] *See id.* §§ 17, 22, 24, 71.
[117] *See supra* note 3 and accompanying text (defining smart contracts); *see also* Reyes, *Unified Theory*, *supra* note 3, at 987 (explaining that a smart contract is very similar to a "persistent script"—a standing computer program—that says "if event x happens, then execute result y").
[118] *See supra* Part I.C (explaining that code acquires legal force only through investiture by secondary rules); *see also infra* Part III.B.1 (discussing the conditions under which smart contracts can serve as vehicles for legally enforceable contractual arrangements).

Wyoming provides a second illustration. The state legislature has worked diligently to make its legal framework receptive to digital assets and blockchain technology, enacting significant changes to the state's Uniform Commercial Code (UCC). While many of these modifications follow the UCC tradition of building rules that match technical function (rather than specific technology) and commercial activity (rather than a specific business model), one provision is particularly problematic. With regard to perfecting a security interest in digital asset collateral, the statute provides that perfection "must be achieved through possession."[119]

This requirement erroneously equates a creditor's technical custody of a digital asset, such as holding the relevant private keys, with the legal state of possessing a tangible good.[120] This conflation reflects a fundamental category error. In personal property law, "possession" is a term of art presupposing tangibility: it denotes physical dominion over a corporeal thing, distinguishing *choses in possession* from *choses in action*.[121] Digital assets, however, are intangible; they exist as data entries on distributed ledger systems and are not susceptible to physical taking.[122] Consequently, requiring "possession" of an inherently intangible asset creates a doctrinal impossibility.

Read literally, the statute renders it impossible for businesses that lend against digital asset collateral to perfect their security interests, a result that directly contradicts the legislature's intent. Why would the legislature make it impossible for such lenders to obtain the benefits that result from being a secured creditor, especially if it was trying to attract digital asset commerce to Wyoming? The answer is, Wyoming would not have intentionally made it harder for cryptocurrency-related lending to thrive. Instead, the legislature confused technical system control with legal possession. A person who holds the private keys to a digital asset enjoys certain technical powers: the ability to obtain substantially all the benefit from the asset, to exclude others from doing so, and to transfer those powers to another.[123] While these capabilities mimic the *effects* of possession, they are not possession in a legally cognizable sense; they are architectural constraints imposed by code, not legal entitlements conferred by positive law. Technical system control may serve as evidence bearing on legal determinations of ownership or possession, but it cannot, standing alone, alter the fundamental principles that govern those determinations.

---

[119] WYO. STAT. ANN. § 34-29-103(a) (2023).

[120] Carla L. Reyes, *Emerging Technology's Unfamiliarity with Commercial Law*, 119 NW. U. L. REV. ONLINE 31 (2024).

[121] This is the conception implicit throughout the Uniform Commercial Code. *See* U.C.C. § 9-313(a) (Am. L. Inst. & Unif. L. Comm'n 2010) (permitting perfection by possession only for tangible or quasi-tangible collateral, including goods, instruments, money, and tangible chattel paper).

[122] *See* Andrea Tosato & Christopher K. Odinet, *Digital Assets and the Property Question*, 78 FLA. L. REV. (forthcoming 2026) (analyzing the intangible nature of digital assets and their classification within American property law), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5151907.

[123] The 2022 Amendments to the Uniform Commercial Code address this issue by introducing "control" as a functional analog of possession for intangible digital assets. Under the Amendments, "the key policy choice . . . is that control of a [controllable electronic record] is accorded similar legal significance and effects as the possession of a tangible good." Tosato & Odinet, *supra* note 74, at 4. *See* U.C.C. §§ 12-102, 12-105, 9-107A (Am. L. Inst. & Unif. L. Comm'n 2022) (defining "control" functionally by reference to the powers a person holds over a controllable electronic record). *See infra* Part III.A.

A third example arises in the context of business formation statutes. Several states have enacted legislation specifically designed to attract a form of blockchain-based business venture known as a decentralized autonomous organization, or "DAO."[124] In 2021, Wyoming adopted a law creating a new option for those seeking to form a limited liability entity: namely, a decentralized autonomous organization organized as a limited liability company.[125] Wyoming specifies that such a DAO can be "algorithmically managed" with the formal management powers of the entity vested in a smart contract.[126] The problem here is that smart contracts are fundamentally passive: reactive, not proactive.[127] A smart contract must be told that a condition X has occurred before it will execute result Y.[128] Smart contracts do not exercise independent judgment, and as a general rule, are not themselves the source of predictive analytics or other artificial intelligence that could approximate such judgment.[129] In the context of a limited liability company, however, "management" is not mere execution; it denotes the exercise of discretion and fiduciary judgment on behalf of the entity and its members.[130] It is therefore not clear how a smart contract, which can only process predetermined instructions in response to external inputs, can be credited with performing this function. The statute appears to confuse the use of code to execute decisions taken by people with the activity of management itself, activity that requires a normative and evaluative capacity that deterministic code does not independently possess.

The state of Tennessee fell into this trap, enacting LLC provisions for "decentralized organizations" in 2022.[131] In its attempt to modify the LLC statute to accommodate blockchain-based entities, the law proclaims that the articles of organization "and the smart contracts for a decentralized organization govern…rights and duties under this chapter of a person in that person's capacity as a member;…[and] rights and voting rights of members," among other things.[132] Smart contracts cannot "govern" rights and duties. They may serve as a medium through which people exercise their rights and perform their duties,[133] but they do not generate new rights and duties through technical operation alone.

Although these are but three examples, they reveal a consistent pattern: state legislatures have enacted statutes that assume code's technical operation carries inherent legal force, importing into

---

[124] The confusion embedded in these DAO-enabling statutes is mirrored by the behavior of private actors who form and participate in DAOs on the flawed assumption that the technical asset-shielding features of a DAO provide the legal protection of limited liability. *See infra* Part II.C.3.

[125] WYO. STAT. ANN. § 17-31-104(a) (2021) (defining a "decentralized autonomous organization" as "a limited liability company organized under this chapter"). *See also* WYO. STAT. ANN. § 17-31-102(a)(iv).

[126] WYO. STAT. ANN. § 17-31-109 (2021).

[127] Reyes, *Unified Theory*, *supra* note 3, at 987.

[128] HENNING DIEDRICH, ETHEREUM 167–68 (2016) (explaining that smart contracts move assets after a condition has been filled and that "[t]he condition can be internal to the blockchain or fed in from the outside").

[129] *Id.* at 170 (explaining that relying on external data "is the usual situation for smart contracts, they will be tied to external events and they are set in motion by receiving a signed transaction expressing what the outcome of a specific event was" (emphasis omitted)).

[130] *See, e.g.*, REVISED UNIF. LTD. LIAB. CO. ACT § 409 (Unif. L. Comm'n 2006) (imposing duties of loyalty and care on managers of an LLC).

[131] TENN. CODE ANN. §§ 48-250-101 to -115 (2022)

[132] TENN. CODE ANN. § 48-250-105(b)(3), (5) (2022).

[133] Reyes, *Unified Theory*, *supra* note 3, at 987 ("many simply use smart contracts to achieve more efficient performance of traditional contractual obligations").

positive law the very confusion that Part I identified as a conceptual error. As Part III will demonstrate, legislatures can properly empower code, but only through the deliberate exercise of rules of change.[134]

2. *Regulators that confuse code for positive law*

The SEC's approach to digital asset enforcement provides a powerful illustration of how regulators confuse code for positive law. Over nearly a decade, the Commission developed an enforcement posture that treated the technical characteristics of digital assets as proxies for securities status, conflating code and law.

To understand this error requires a brief examination of the governing legal framework. "Investment contract" is included in the definition of "security" in the Securities Act of 1933.[135] The Supreme Court's approach to identify an investment contract, established in *SEC v. W.J. Howey Co.*, requires an investment of money, in a common enterprise, with the expectation of profits derived from the managerial and entrepreneurial efforts of others.[136] This test focuses on the scheme, arrangement, or set of representations surrounding a transaction, not on the intrinsic characteristics of any asset delivered as part of that scheme.[137] Howey itself illustrates this principle: the transaction at issue involved parcels of a citrus grove sold together with a services agreement for the cultivation and marketing of the oranges. The parcels of land were not inherently securities; they were real property. What transformed the transaction into an unauthorized securities offering was the accompanying arrangement that created investor expectations of profit from the promoter's entrepreneurial and managerial efforts.[138] The thing delivered with an investment contract does not itself become a security merely by its inclusion in such a transaction, unless an independent provision of law classifies that thing as a security on its own terms.[139]

---

[134] *See infra* Part III.A.

[135] *Id.*

[136] SEC v. W.J. Howey Co., 328 U.S. 293, 298 (1946). Given that an "investment contract" does not require the typical elements of contract formation or enforceability, common interpretations of the investment contract elements suggest that the analysis hews closer to a detrimental reliance theory than to contract theory.

[137] *Id.* at 298–99 (defining the investment contract as "a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party"). Notably, other law, including contract law, may separately provide parties who make representations to each other with legal rights.

[138] *Id*. at 295–96 (describing the transaction involving parcels of citrus land sold with a service agreement for cultivation and marketing).

[139] SEC v. Ripple Labs, Inc., 673 F. Supp. 3d 432, 448 (S.D.N.Y. 2023) (collecting cases and describing the various assets that have featured in investment contract schemes); *see also* Lewis Cohen et al., *The Ineluctable Modality of Securities Law: Why Fungible Crypto Assets Are Not Securities* 12 (Nov. 10, 2022) (unpublished manuscript), *available at* https://ssrn.com/abstract=4282385 (noting the lack of precedent to support a finding that the property transferred with an investment contract should itself be classified as a security); *cf.* Glen-Arden Commodities, Inc. v. Constantino, 493 F.2d 1027, 1034–35 (2d Cir. 1974) (whiskey warehouse receipts); Hocking v. Dubois, 885 F.2d 1449, 1457 (9th Cir. 1989) (en banc) (condominiums).

Against this backdrop, the SEC's enforcement posture regarding digital assets and blockchain networks departed from the scheme-focused inquiry that *Howey* demands. In April 2019, the Commission's Division of Corporation Finance issued a "Framework for 'Investment Contract' Analysis of Digital Assets" that, while invoking *Howey*, directed substantial attention toward the technical characteristics of digital assets themselves.[140] For example, the Framework suggested that the design and functions of a digital asset could create expectations of appreciation, and that their transferability could generate investment incentives.[141] This granular focus on code architecture, rather than on contractual arrangements between identifiable parties, blurred the boundary between what a digital asset's code enables and what the surrounding legal arrangements establish. The consequences of this analytical drift were most acute in the secondary market context, where the Framework's asset-focused approach encouraged the conclusion that securities status persisted through every subsequent trade solely because of the token's design.

This drift reached its apex in June 2023, when the SEC filed enforcement actions against Coinbase and Binance, the two largest cryptocurrency exchanges in the United States.[142] The complaints revealed a systematic pattern of treating tokens' technical design features as proxies for securities status in secondary market transactions. In the Coinbase action, for instance, the Commission alleged that Solana's native token, SOL, constituted a security based in significant part on the protocol's deflationary token-burning mechanisms, Solana Labs' use of pooled proceeds to fund development, and ongoing technical upgrades that purportedly created expectations of appreciation among secondary market purchasers.[143] The parallel Binance complaint advanced a similar theory, treating consensus mechanisms, supply schedules, and ecosystem roadmaps as evidence that every subsequent exchange transaction constituted an investment contract.[144] The operative assumption was that a digital asset's technical design embeds securities status within the asset itself, so that the investment contract travels with the token through every secondary market trade. This is the category error in its purest form: the SEC treated architectural constraints as though they generated normative force binding on parties who had no relationship to the original issuer.

The legal system's corrective mechanisms eventually exposed the conflation. Weeks after the Coinbase and Binance complaints, the court in *SEC v. Ripple Labs, Inc.*, building on foundations laid in earlier decisions,[145] held that institutional sales of XRP constituted investment contracts

---

[140] *Framework for "Investment Contract" Analysis of Digital Assets*, U.S. SEC. & EXCH. COMM'N (Apr. 3, 2019), *available at* https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

[141] *See id.* (directing analysis toward whether the digital asset's design creates an expectation of appreciation, and whether the asset's transferability and trading markets generate investment incentives).

[142] Complaint, SEC v. Binance Holdings Ltd., No. 1:23-cv-01599 (D.D.C. filed June 5, 2023); Complaint, SEC v. Coinbase, Inc., No. 1:23-cv-04738 (S.D.N.Y. filed June 6, 2023)

[143] Complaint ¶¶ 233–44, *Coinbase*, No. 1:23-cv-04738 (describing the Solana blockchain and alleging that the "burning" of SOL tokens led investors to reasonably view their purchase as having the potential for profit).

[144] Complaint ¶¶ 348–51, 356–60, *Binance*, No. 1:23-cv-01599 (describing "Common Features" of the crypto assets and alleging that staking and consensus mechanisms created expectations of profit).

[145] *See* SEC v. Telegram Grp. Inc., 448 F. Supp. 3d 352, 379 (S.D.N.Y. 2020) (characterizing digital assets as "little more than alphanumeric cryptographic sequences"); SEC v. Kik Interactive Inc., 492 F. Supp. 3d 169, 177–80 (S.D.N.Y. 2020) (analyzing the promotional scheme surrounding the Kin token distribution rather than the token's technical features). Both decisions applied the scheme-focused *Howey* analysis and declined to treat the intrinsic characteristics of the digital assets as determinative of securities status.

because the surrounding arrangements satisfied *Howey*, while programmatic exchange sales did not, because secondary market purchasers lacked any nexus with the issuer's efforts.[146] The same token carried different legal significance depending entirely on the surrounding arrangements. The SEC ultimately conceded as much, acknowledging in September 2024 that "crypto asset securities" had been merely "shorthand," that it was "not referring to the crypto asset itself as the security," and expressing "regret" for "any confusion it may have invited."[147]

The significance of this episode, however, extends beyond the SEC's belated course correction. That a sophisticated federal regulator, applying a legal test established nearly eighty years ago with dedicated enforcement resources at its disposal, could sustain this category error for the better part of a decade illustrates the insidious quality of the confusion diagnosed in Part I: code regulates behavior with such completeness that its architectural power becomes difficult to distinguish from normative authority, even for those specifically charged with policing the boundary.

B. Judicial Arbiters Occasionally Confuse Code for Law

As legal disputes over cryptocurrency, blockchain technology, and related products and services begin to appear before courts with greater frequency, it has become apparent that those charged with interpreting law in order to resolve disputes, whether a judge or jury, sometimes confuse code for positive law. This confusion not only paves the way for precedential cases being created using flawed legal foundations, but also increases dispute resolution inefficiencies and heightens legal risk for participants in cryptospace. Examining two examples—one in which a judge mistook code for law leading to his decision being reversed, and one in which a jury was so confused about which was code and which was law that a mistrial was declared—illustrates both the jurisprudential and practical risks that surface when arbiters of disputes confuse code with law.

In the high-profile case of *Van Loon v. Department of the Treasury*,[148] the U.S. District Court for the Western District of Texas confused smart contracts with legally enforceable contracts.[149] In that case, plaintiff Joseph Van Loon sued the Department of the Treasury, alleging that Treasury wrongfully placed the smart contract-based software program known as Tornado Cash on the Specially Designated Persons sanctions list.[150] Early in the background portion of the decision, the Court variously described smart contracts as "software programs deployed directly onto the Ethereum network,"[151] and "computer code that is stored directly on the Ethereum blockchain, and

[146] *Ripple Labs*, 673 F. Supp. 3d at 453–55. The court found that secondary market purchasers "could not have known if their payments of money went to Ripple, or any other seller of XRP," and therefore lacked the requisite nexus with the issuer's managerial efforts. *Id.* at 455.
[147] Plaintiff Securities and Exchange Commission's Memorandum of Law in Support of Motion for Leave to Amend the Complaint at 6 n.6, SEC v. Binance Holdings Ltd., No. 1:23-cv-01599 (D.D.C. Sept. 12, 2024), ECF No. 273. The Commission further conceded that it was "not advancing" the argument that tokens offered during initial coin offerings "remain securities into perpetuity." *Id.*
[148] Van Loon v. Dep't of Treasury, 122 F.4th 549 (5th Cir. 2024), *rev'g* 688 F. Supp. 3d 454 (W.D. Tex. 2023).
[149] *Van Loon*, 688 F. Supp. 3d at 467–68, *rev'd*, 122 F.4th 549.
[150] *Id*. at 458.
[151] *Id*. at 459.

which automatically executes all or parts of an agreement, pursuant to its specifications."[152] However, when the Court evaluated Treasury's claim that the Tornado Cash smart contracts were properly placed on the sanctions list because they were property, the Court moved away from its earlier technologically accurate descriptions of smart contracts to one that confuses code with contract law.[153]

Specifically, Treasury can list property that belongs to sanctioned entities on the sanctions list.[154] Having found that a DAO could be an entity under the sanctions regulations,[155] the Court considered Treasury's claim that the smart contracts were property of the DAO because they fit the regulations' definition of property, which included "contracts of any nature whatsoever."[156] The Court agreed with Treasury because "as other courts have recognized—smart contracts are merely a code-enabled species of unilateral contracts."[157] The cases that the Court relied upon described smart contracts as: "self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code,"[158] enabling "the parties to define the terms of their contract and submit the crypto-assets contemplated in the contract to a secure destination,"[159] "programs that verify and enforce the negotiation or performance of binary contracts,"[160] and as a legally enforceable agreement.[161]

Perhaps recognizing that its reliance on these characterizations of smart contracts as a legally enforceable agreement contradicts the descriptions of the Tornado Cash smart contracts it recited earlier in its own opinion, the Court hedged its analysis by saying that "[e]ven if not every smart contract can be considered a contract, the record shows that Tornado Cash promoted and advertised the contracts and its abilities and published the code with the intention of people using it—hallmarks of a unilateral offer to provide services."[162] However, if the whole of the service constituted a unilateral contract, then the individual smart contracts – the software through which the services were provided, could not individually be a contract. In other words, even after taking great pains to recite a fairly accurate technical description of the Tornado Cash software, the Court confused smart contract code with the legal force of contract law. This confusion contributed to an analytical path that the Fifth Circuit ultimately rejected, reversing the decision and remanding the case for further proceedings.[163]

In a different context altogether, similar confusion about the relationship between code and law brought a criminal prosecution to a standstill. In May 2024, the Department of Justice indicted 24-year-old Anton Peraire-Bueno and 28-year-old James Peraire-Bueno for conspiracy to commit

[152] *Id*. at 460.
[153] *Id*. at 648.
[154] *Id*. at 465.
[155] *Id*. at 466.
[156] *Id*. at 468.
[157] *Id*.
[158] Rensel v. Centra Tech, Inc., No. 17-24500-CIV, 2018 WL 4410110, at 10 (S.D. Fla. June 14, 2018).
[159] In re Bibox Grp. Holdings Ltd. Sec. Litig., 534 F. Supp. 3d 326, 330 (S.D.N.Y. 2021).
[160] Williams v. Block.one, No. 20-cv-2809, 2022 WL 524189, at 2 n.19 (S.D.N.Y. Aug. 15, 2022).
[161] Snyder v. STX Techs., Ltd., No. 19-6132, 2020 WL 510672, at *2 (W.D. Wash. Aug. 31, 2020).
[162] *Van Loon*, 688 F. Supp. 3d at 468.
[163] *Van Loon*, 122 F.4th 549.

wire fraud, wire fraud, and conspiracy to commit money laundering.[164] Prosecutors alleged that the two brothers used their MIT-taught computer science skills to "tamper with and manipulate the protocols relied upon by millions of Ethereum users across the globe."[165] How did the two achieve this "tampering and manipulation"? In brief, the alleged scheme operated as follows: Validators of blocks in the Ethereum protocol can re-order transactions and insert other transactions into a block right up until the block becomes part of the chain.[166] Doing so allows the validator to obtain the maximal extractable value (MEV) from users.[167] Because MEV extraction is viewed as a practice that can distort the well-functioning of the protocol, 90% of validators use software known as MEV-Boost, which puts validators on equal MEV footing and makes MEV tactics more transparent so that all users benefit rather than a select few traders that excel at frontrunning trades.[168]

The Peraire-Bueno brothers built code that interacted with MEV-Boost in a way that diverted funds from MEV-Boost blocks to validating nodes they operated.[169] The Department of Justice argued that building and executing code that interacted with widely used software in this way was fraudulent conduct because it diverged from accepted community norms around MEV and MEV-Boost.[170] The Peraire-Bueno defense team argued at trial that the brothers did not act outside of what the Ethereum protocol and the MEV-Boost software code allowed. Rather, the brothers claimed that they simply outsmarted frontrunning tactics used by most validators: they had outmaneuvered the validators at their own game.[171] In other words, the defense claimed that as long as the trades made by the Peraire-Bueno brothers were permitted by the Ethereum protocol, the trades were legal. Meanwhile, the prosecution argued that even if the trades were technically permissible, they might still not be legal. The case was a "code is law" vs. "code is not law" debate come to life. Ultimately, the debate left the jurors confused, and the case ended in a mistrial.[172]

The *Van Loon* case reveals that once confusion about the relationship between code and law seeps into judicial opinions, it carries precedential value that can distort future legal reasoning. The lower court in *Van Loon* accurately described the technical reality of smart contracts at the outset of its

---

[164] Indictment, United States v. Peraire-Bueno, No. 1:24-cr-00293 (S.D.N.Y. unsealed May 15, 2024); *see also* Press Release, Dep't of Justice, *Two Brothers Arrested for Attacking Ethereum Blockchain and Stealing $25M in Cryptocurrency* (May 15, 2024), *available at* https://www.justice.gov/archives/opa/pr/two-brothers-arrested-attacking-ethereum-blockchain-and-stealing-25m-cryptocurrency.

[165] *Id*.

[166] Margaux Nijkerk, *How MIT Brothers Allegedly Cheated a Noxious-But-Accepted Ethereum Practice for $25M*, COINDESK (May 16, 2024), *available at* https://www.coindesk.com/tech/2024/05/16/how-2-brothers-allegedly-cheated-a-noxious-but-accepted-ethereum-practice-for-25m.

[167] *Id*.

[168] *Id*.

[169] *Id*.

[170] *Id*.

[171] Ritu Singh, *Crime or Clever Trading? MIT-Educated Brothers Face Trial for $25 Million Crypto Heist*, MSN, *available at* https://www.msn.com/en-us/news/crime/crime-or-clever-trading-mit-educated-brothers-face-trial-for-25-million-crypto-heist/ar-AA1OuE4r.

[172] Christopher Beam, *Mistrial Shows Difficulty in Applying Law to Crypto*, BLOOMBERG (Nov. 17, 2025), *available at* https://www.bloomberg.com/news/newsletters/2025-11-17/crypto-mistrial-shows-difficulty-in-applying-law-to-blockchain-trades; *see also* Tim Craig, *'Massive Overstep': Mistrial Declared for 'MEV Brothers' Accused of $25 Million Fraud on Ethereum*, THE BLOCK (Nov. 8, 2025), *available at* https://www.theblock.co/post/378101/massive-overstep-mistrial-declared-for-mev-brothers-accused-of-25-million-fraud-on-ethereum.

opinion. Yet it then relied upon precedent that conflated the technical aspects of smart contracts with legal consequences, reaching a conclusion that differed markedly from the Court's own understanding of the relationship between technology and law. The Peraire-Bueno mistrial, for its part, reveals that litigants are aware of the confusion about the relationship between code and law and can use that confusion to their advantage during litigation. Neither of these outcomes helps judicial proceedings accurately or efficiently arrive at just results when disputes arise. Achieving that result requires the kind of foundational realignment advanced by this Article in understanding how law interacts with code.

C. Private Actors Frequently Confuse Code with Binding Legal Arrangements

While lawmakers, regulators, and courts have struggled to properly distinguish between what blockchain systems enable technically and what transactions conducted through those systems accomplish legally, the most profound and widespread confusion occurs among the private actors who build, use, and transact within the cryptospace. Operating under the powerful misconception that technical execution alone can create, modify, or extinguish legal rights, these market participants routinely structure their affairs on a foundation of legally ineffective arrangements. This section examines this phenomenon through three prominent examples: the mistaken belief that non-fungible tokens (NFTs) can embody and transfer legal rights in digital works, the failure to recognize that blockchain transactions and smart contract executions alter system-level control over assets without, standing alone, affecting legal title or creating enforceable obligations, and the dangerous assumption that the technical asset-shielding features of decentralized autonomous organizations (DAOs) confer the legal protection of limited liability.

1. *The Illusion of Code-Based Rights in NFT Markets*

One of the most vivid examples of how private actors misunderstand the relationship between code and law is found in the market for non-fungible tokens (NFTs) purportedly linked to works of art.[173] Differing from fungible cryptocurrencies such as Bitcoin, NFTs are unique digital assets recorded on distributed ledger networks, such as Ethereum, Solana, and many others.[174] These digital assets contain only a small amount of data, typically metadata with a hyperlink that *points* or refers to a distinct digital file such as an image, video, or text, generally maintained on a separate resource.[175]

---

[173] *See generally* Joshua A.T. Fairfield, *Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property*, 97 IND. L.J. 1261 (2022); Juliet M. Moringiello & Christopher K. Odinet, *The Property Law of Tokens*, 74 FLA. L. REV. 607 (2022); Christopher K. Odinet & Andrea Tosato, *The Intersection of NFTs and Structured Finance*, 103 B.U. L. REV. 1005 (2023); Juliet M. Moringiello & Christopher K. Odinet, *NFTs in Commercial Transactions*, *in* THE CAMBRIDGE RESEARCH HANDBOOK OF EMERGING ISSUES AT THE INTERSECTION OF COMMERCIAL LAW AND TECHNOLOGY (Nancy Kim & Stacy-Ann Elvy eds., 2025); Joshua Fairfield, *Digital Property Cycles*, 80 WASH. & LEE L. REV. 1115 (2023); Brian L. Frye, *Luxury Tokens* (Aug. 16, 2023), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4541913.

[174] Moringiello & Odinet, *supra* note 173, at 632–47; Odinet & Tosato, *supra* note 173, at 1011–17.

[175] Moringiello & Odinet, *supra* note 173.

NFTs were initially conceived as technological proofs-of-concept to demonstrate that blockchain networks could create and maintain uniquely identifiable data objects.[176] The 2017 launch of CryptoKitties marked the first glimpse of mass-market potential, with NFTs pointing to cartoon renderings of cats that would vary in their appearance and other attributes based on inherited traits akin to genetic code.[177] The early success of Cryptokitties[178] led to the insight that such technology could be utilized in connection with diverse forms of creative works.[179]

The market response was explosive. By 2021, speculative fervor reached monthly trading volumes of $2.8 billion, including high-profile sales such as "Nyan Cat" for $580,000 and Beeple's "Everydays: the first 5000 Days" selling at Christie's auction for $69 million.[180] This growth was propelled by claims that NFTs provided a novel way to establish and transfer ownership over digital works and related intellectual property rights.[181] These ideas reflected the erroneous belief that code alone could create and convey legal rights, even where positive law provided no such recognition.

NFTs purportedly linked to artistic works are created and distributed through two predominant models, both of which demonstrate systematic confusion between code's technical capabilities and law's normative authority. The first, the *standardized model*, involves individuals, typically with limited technical expertise, relying on minting platforms such as OpenSea, Mintable, and Rarible that offer infrastructure and modularized services to create and sell NFTs.[182] The second, the *bespoke model*, features issuers like Yuga Labs and Dapper Labs deploying tailored smart contracts to mint and distribute their NFTs while controlling most aspects of the process directly.[183] Despite their technical differences, both approaches reveal a profound misunderstanding of the essential distinction between code's capacity to define technical possibilities and law's power to create enforceable rights and obligations, reflecting the dangerous misconception that technological implementation can substitute for legal recognition under positive law.

The standardized model offers the most straightforward illustration of this confusion, as these platforms provide user-friendly websites that create the mirage of legal effect without satisfying the underlying legal requirements. Mintable offers a particularly telling example. On its NFT platform, a user seeking to create an NFT can upload a digital artwork, add a description, and then, before finalizing the listing, is presented with a simple checkbox: "Transfer Copyright when

[176] *See* Joshua A.T. Fairfield, *Bitproperty*, 88 S. CAL. L. REV. 805, 825–28 (2015).
[177] Elisa Campaci, *The Story of the CryptoKitties, the NFTs That Wrote Blockchain History*, YOUNG PLATFORM (Dec. 2, 2022), *available at* https://youngplatform.com/en/blog/news/cryptokitties-guide-history-nft-flow-blockchain/.
[178] *Id.*
[179] *See* Moringiello & Odinet, *supra* note 173, at 632–47 & n.4.
[180] Erin Griffith, *Why an Animated Flying Cat with a Pop-Tart Body Sold for Almost $600,000*, N.Y. TIMES (May 27, 2021), *available at* https://www.nytimes.com/2021/02/22/business/nft-nba-top-shot-crypto.html; Jay Peters, *Beeple Sold an NFT for $69 Million*, THE VERGE (Mar. 11, 2021), *available at* https://www.theverge.com/2021/3/11/22325054/beeple-christies-nft-sale-cost-everydays-69-million.
[181] *See supra* Part III.A.
[182] Odinet & Tosato, *supra* note 173, at 1018–22.
[183] *Id.*

purchased?".[184] Mintable's interface explains that selecting this option grants the purchaser "the rights to use the file commercially."[185]

This streamlined, code-driven process misleadingly suggests that copyright ownership can be transferred through simple user interactions, exemplifying how private actors conflate architectural constraints with legal authority. The checkbox functions perfectly within Mintable's technical system: it modifies metadata, triggers display changes, and influences user behavior. However, under Section 204(a) of the U.S. Copyright Act, such a transfer "is not valid unless an instrument of conveyance, or a note or memorandum of the transfer, is in writing and signed by the owner of the rights conveyed."[186] A simple, unsigned checkbox click on a web interface fails to meet this strict statutory formality. No matter what the platform's code is designed to represent, it cannot unilaterally override a mandatory provision of positive law. Users experience the illusion of legal efficacy while remaining entirely outside the actual framework that governs copyright assignments.[187] The purported transfer is legally void.

NFT issuers using the bespoke model exhibit an even deeper and more troubling conflation of code and law. The Bored Ape Yacht Club (BAYC), created by Yuga Labs, serves as a paradigmatic case study. BAYC is a collection of 10,000 NFTs linked to unique cartoon ape images that have commanded multi-million-dollar prices and become celebrity status symbols.[188] Yuga Labs' terms of service for these digital assets contain explicit and flawed rejections of legal authority in favor of code-based governance.

First, Yuga Labs attempts to displace fundamental property law by declaring that "Ownership of the NFT is mediated entirely by the Smart Contract and the Ethereum Network: at no point may we seize, freeze, or otherwise modify the ownership of any Bored Ape."[189] This statement reflects a profound misunderstanding of property law's foundational principles. Ownership is a legal concept determined by applicable property law. It is not "mediated," or otherwise structurally modified by blockchain technology, smart contracts or any technological system. For example, if the owner of an NFT dies, title passes to their heirs according to inheritance law, regardless of what the blockchain ledger indicates; a technical transaction of the NFT is not necessary for title to change.

---

[184] *See How Do NFT Copyrights Work?*, MINTABLE EDITORIAL (2021), *available at* https://editorial.mintable.com/how-do-nft-copyrights-work/ (last visited 2/3/2026).

[185] *Id.*

[186] 17 U.S.C. § 204(a) (2024).

[187] *See* Radio Television Espanola S.A. v. New World Ent. Ltd., 183 F.3d 922, 927 (9th Cir. 1999) ("Section 204's writing requirement is not unduly burdensome; it necessitates neither protracted negotiations nor substantial expense. The rule is really quite simple: If the copyright holder agrees to transfer ownership to another party, that party must get the copyright holder to sign a piece of paper saying so."); *see also* 17 U.S.C. § 101 (defining "transfer of copyright ownership").

[188] *See* NFTing, *The History of BAYC: A Billion-Dollar Ecosystem of Cartoon Apes*, MEDIUM (Aug. 23, 2022), *available at* https://nfting.medium.com/the-history-of-bayc-a-billion-dollar-ecosystem-of-cartoon-apes-fcc67e032408; *see also* Shanti Escalante-De Mattei, *Eminem and Snoop Dogg Performed as Their Bored Ape Yacht Club Avatars at the VMAs*, ARTNEWS (Aug. 29, 2022), *available at* https://www.artnews.com/art-news/news/eminem-snoop-dogg-bored-ape-yacht-club-vmas-1234637677/.

[189] Yuga Labs LLC, *Bored Ape Yacht Club License Terms*, BORED APE YACHT CLUB, *available at* https://www.boredapeyachtclub.com/licenses/bayc (last visited Jun. 3, 2025).

Second, Yuga Labs' intellectual property licensing framework compounds this confusion. At the outset, BAYC's terms state "When you purchase an NFT, you own the underlying Bored Ape, the Art, completely."[190] This statement is, however, immediately contradicted by the simultaneous granting of a separate license, which would be superfluous if owners of the NFT were also being assigned the copyright for the Art outright. The licensing terms themselves reveal profound confusion about the relationship between code and law. The agreement fails to specify critical elements: whether the license is exclusive, how it is granted to new NFT owners, and under what conditions it terminates.[191] Most problematically, while the terms suggest the license is "subject to continued compliance," they provide no mechanism for identifying when compliance failures occur or how license rights transfer when NFTs change hands.[192]

These deficiencies create real-world legal uncertainty, as demonstrated by the 2022 theft of actor Seth Green's Bored Ape #8398.[193] Green had been developing an animated television show featuring the ape image associated with his Bored Ape NFT when he lost system control over the NFT through a phishing attack.[194] The incident raised profound questions about ownership of NFTs and license continuity: did Green retain ownership of the NFT? Did Green retain commercial rights despite losing NFT control? Would the thief acquire rights provided by the license granted to Green despite obtaining the NFT surreptitiously? If the stolen NFT reached a good faith purchaser, would Green's commercial ventures suddenly become infringing?[195] BAYC's terms provide no answers to these critical questions because they attempt to merge distinct legal concepts, property ownership and copyright licensing, through technological implementation rather than proper legal frameworks.

Thus, these case studies ultimately reflect the same fundamental error: the misconception that code can substitute for positive law in creating and transferring legal rights. Whether through simple checkboxes or elaborate smart contracts, these approaches demonstrate how private actors' misunderstanding of the relationship between code and law leads to arrangements that are legally ineffective, failing to achieve their intended outcomes, fostering erroneous beliefs among consumers and exposing them to unforeseen risks.

---

[190] *Id.*
[191] *Id.* (failing to specify licensing terms with requisite precision).
[192] *Id.*
[193] *See* Ryan Hogg, *Seth Green Pays $260,000 Ransom for a Stolen Bored Ape Ethereum NFT Meant to Feature in His New TV Show*, BUS. INSIDER (June 11, 2022, 10:58 AM), *available at* https://www.businessinsider.com/seth-green-pays-260000-return-stolen-bored-ape-ethereum-nft-2022-6.
[194] *See* Riddhi Setty, *Seth Green's Stolen 'Bored Ape' Muddles NFT Legal Ownership*, BLOOMBERG L. (June 8, 2022) (discussing the distinction between possession of the NFT and legal ownership of the underlying IP); *see also NFTs: Usage Rights and Legal Fights*, BROWNSTEIN CLIENT ALERT (June 28, 2022), *available at* https://www.bhfs.com/insight/client-alert-nfts-usage-rights-and-legal-fights/ (analyzing Green's loss of control over the token versus his retention of legal title).
[195] *See* Andrea Tosato & Christopher K. Odinet, *Digital Assets and the Property Question*, 78 FLA. L. REV. (forthcoming 2026) (explaining the issues raised by the commercial circulation of digital assets, including NFTs, and the significant of the good faith purchaser protection introduced by the 2022 Amendments to the Uniform Commercial Code), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5151907.

2. *Smart contracts are software code, not legally enforceable agreements*

When lawyers hear the phrase "smart contracts," they often intuitively interpret it to mean "artificially intelligent legally enforceable agreements."[196] Indeed, both legal scholars and practitioners have devoted a significant number of pages to examining whether, when, and under what circumstances smart contracts themselves serve as an enforceable agreement by making and accepting an offer through code, with sufficient evidence of mutual consideration and meeting of the minds.[197] Unfortunately, both as a technical matter and in the context of commercial use, smart contracts are not by default legally enforceable agreements.[198] Instead, a smart contract is just one type of computer program commonly used in connection with blockchain technology.[199] When smart contracts are deployed on a blockchain protocol, the term "smart contract" really just refers to computer software that takes some action after receiving some pre-defined data input,[200] and then reflects the resulting change in the transaction history of the blockchain protocol.[201] In other words, smart contracts are simply instructions to computers.[202]

As a very general matter then, "smart contracts are computer code that says, 'if data is received that X has occurred, Y will execute.'"[203] Creative developers use these computer programs in many ways, including as part of decentralized applications, decentralized organizations, and protocols that protect financial privacy for transactions conducted through blockchain networks. The divide between the historical legal focus on smart contracts in the contract law context and the technical reality that developers use smart contracts as they would any computer program to power complicated software is an example of confusion about when smart contracts act as positive law by embodying contract law in code, and when smart contracts serve as code that shapes user

[196] Carla L. Reyes, *Emerging Technology's Language Wars: Smart Contracts*, 2022 WIS. L. REV. FORWARD 85, 90.
[197] Jeremy M. Sklaroff, Comment, *Smart Contracts and the Cost of Inflexibility*, 166 U. PA. L. REV. 263 (2017); Jeffrey M. Lipshaw, *The Persistence of "Dumb" Contracts*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 1 (2018); CARDOZO BLOCKCHAIN PROJECT, *"Smart Contracts" & Legal Enforceability* (Oct. 16, 2018), *available at* https://larc.cardozo.yu.edu/cgi/viewcontent.cgi?article=1000&context=blockchain-project-reports; NORTON ROSE FULBRIGHT, *Smart Contracts* (Nov. 2019), *available at* https://www.nortonrosefulbright.com/en/knowledge/publications/1bcdc200/smart-contracts#section4.
[198] HENNING DIEDRICH, ETHEREUM 167 (2016); WILLIAM MOUGAYAR, THE BUSINESS BLOCKCHAIN: PROMISE, PRACTICE AND APPLICATION OF THE NEXT INTERNET STRATEGY 42–43 (2016) ("Smart contracts are software code representing business logic" . . . "Even in the Ethereum implementation, smart contracts run as quasi-Turing complete programs.").
[199] Diedrich, *supra* note 198, at 176 ("In Ethereum, 'smart contract' often just means 'a Solidity script.'"); ANDREAS M. ANTONOPOULOS & GAVIN WOOD, MASTERING ETHEREUM: BUILDING SMART CONTRACTS AND DAPPS 127 (2018) ("In the context of Ethereum, the term . . . . 'smart contracts' . . . refer[s] to immutable computer programs that run deterministically in the context of an Ethereum Virtual Machine as part of the Ethereum network protocol—i.e., on the decentralized Ethereum world computer.").
[200] *See* Diedrich, *supra* note 198, at 167 ("Smart contracts are decentralized code that [executes] after a condition is fulfilled."); Mougayar, *supra* note 198, at 42–43 ("Smart contracts…are triggered by some external data that lets them modify some other data. They are closer to an event-driven construct more than artificial intelligence.").
[201] Reyes, *Language Wars: Smart Contracts*, *supra* note 196, at 93.
[202] A Andrew M. Hinkes, *The Limits of Code Deference*, 46 J. CORP. L. 869, 870–72 (2021).
[203] Reyes, *Unified Theory*, *supra* note 3, at 987 (citing Richard Gendal Brown, *A Simple Model for Smart Contracts* (Feb. 10, 2015), *available at* https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/).

behavior in the cryptospace.[204] Smart contracts are only legal contracts when the law recognizes them as having legal effect; otherwise they are simply code used to automate technical acts to be conducted on computer systems.

To illustrate this point, we start by considering the legal significance of a transaction of a digital asset on a blockchain. The records of transactions maintained by blockchain systems determine if a transfer of technical, system-level control of a given asset occurred. Transactions of digital assets on blockchains do not record or affect legal title to those assets in the absence of exogenous facts. A system-level transaction that modifies system control may be related to but is generally not dispositive of the question of whether a change of legal title has occurred. To determine if a change to legal title has occurred requires information, including the intent and actions of the transferor and transferee, and the relevant legal system's recognition of that intent and those actions. For example, a transaction of a digital asset from the control of a wallet's public key address to another public key address may occur as part of a legal sale, a gift, a theft, or may be legally insignificant in the case of a user transacting an asset from one wallet address that they control to another that they control.

A transaction conducted via a smart contract deployed on a blockchain address that receives technical control of an asset from another address and transacts another asset back to the sender of the initial asset likewise may or may not be legally significant based on exogenous facts. The difference between a user-initiated transaction and a smart contract-initiated transaction is the automation of the smart contract; the smart contract code and oracle supplying data to the smart contract determine when a transaction and what transaction may occur. Unlike the user-initiated transaction, the scope of the transactions that may be performed by a smart contract is fixed by its code. The execution of a smart contract may alter system powers over an asset but may not affect legal title to a given asset. For instance, a smart contract may be used to transact a digital asset from a wallet controlled by A to a custodian who is contracted to provide services to A under specified conditions. Like a user-initiated transaction, a smart contract may divest the user of technical system control over an asset without that user losing legal title over that asset. A smart contract is not a legal person or entity; no U.S. law recognizes a smart contract as a legal person.[205] The smart contract cannot itself be a legal counterparty to any transaction. Thus, while a smart contract's execution may alter system powers over assets, the legal meaning of that smart contract's execution, if any, is a function of the application of law to the transaction.

Maker is a protocol composed of smart contracts that allow its users to engage in transactions that may appear similar to regulated leveraged commodities transactions. The Maker system itself creates data structures called "vaults" that allow its users to "borrow DAI" by "locking up assets as collateral."[206] A dramatically oversimplified view of Maker suggests that a user transacts

[204] Reyes, *Language Wars: Smart Contracts*, *supra* note 196, at 102–06 (collecting linguistic evidence of the confusion between smart contracts as contract law and smart contracts as code-based architecture).

[205] A smart contract may be deployed as an instrumentality or "agent" intended to act on behalf of a third party. To identify such an instrumentality or agent would require exogenous information not present on the face of the smart contract itself.

[206] *See generally Maker Protocol 101*, *available at* https://docs.makerdao.com/build/dai.js/single-collateral-dai/collateralized-debt-position.

system control of an asset (*i.e.*, the "collateral")[207] to a smart contract that calls other smart contracts which allow the user to take control of a calculated amount of another asset (DAI). A user of Maker who sends an asset (*i.e.* ETH) to a smart contract and receives access to another asset (*i.e.* DAI) may have engaged in technical acts that function like a margin loan or leveraged commodity transaction under US law, but the transaction itself is entirely different. Users of Maker are not offered or required to agree to any express legal covenants that are typical of loans or retail commodity transactions. Users of Maker do not interact with a legal counterparty. While the use of Maker's smart contracts may affect the user's ability to control the assets transacted as collateral and to control an amount of DAI, the transaction does not alter the user's legal title to the digital assets transacted to the protocol as "collateral," or create new title in DAI, unless relevant law determines that those technical actions have legal significance. There is no debtor/creditor relationship established by any user and any other person. Without contracts and without law that characterizes technical acts as having legal significance, a user is simply calling code functions to cause the computer system to change the user's control over digital assets.[208]

A digital asset may cause the public key address that controls that asset to receive additional assets in the future. While the transaction of new assets to that address may appear similar to a dividend paid to a holder of equity in a legal entity, the mere fact that the technology system transacts new assets to an address that controls a digital asset does not mean that the initial asset is equity or the newly transacted asset is a dividend. An equity interest is defined by law.[209] A digital asset may be issued by a technology system rather than a legal person- many digital assets are issued as a result of the operation of smart contracts. The transaction of new assets to the address that controls the initial asset may not have any legal significance, it may merely be a system function. Of course, parties to a legal agreement to create an equity in a tokenized form could attempt to use smart contract technology to pay dividends to holders of that equity.[210] Under those circumstances, because the issuer of that tokenized representation of equity (hypothetically) complies with relevant law, the digital assets would be viewed as equity, and the additional transactions may be viewed as the payment of a dividend. Absent legal recognition, the mere transaction of new or additional assets by a smart contract to an address that controls a digital asset is not, alone, legally significant.

3. The Illusion of Code-Based Limited Liability in Decentralized Autonomous Organizations

---

[207] *Id.*

[208] The language used by developers, promoters, and users of these systems further confuse the issue; although marketing incentives may favor comparing transactions facilitated by digital assets with their traditional contract laden analogues, those communications only further muddle the reality of the transactions which in the absence of law recognizing acts as legally meaningful, lack legal significance.

[209] *See* 17 C.F.R. § 240.3a11-1 (2023).

[210] *See, e.g.,* Overstock.com Digital Voting Series A-1 Preferred Stock, which were issued as digital assets and which paid owners of those shares a digital dividend. Robert Anzalone, *Overstock Pays Blockchain-Powered Dividend, 4 Million Shares Now Trading*, FORBES (May 20, 2020), *available at* https://www.forbes.com/sites/robertanzalone/2020/05/20/overstock-pays-ostko-over-4-million-shares-now-trading/?sh=43e0ed73248b.

In the cryptospace, when individuals who do not know each other and do not necessarily trust each other want to collaborate for some common purpose, they sometimes coordinate activity through smart-contract-enabled code often referred to as a decentralized autonomous organization (DAO).[211] Although the purposes, technical architecture, and degree of human activity vary widely from one DAO to another,[212] a DAO, at its most basic technical foundation, is a set of interlocking smart contracts (interacting software programs) that operate on a blockchain protocol.[213] Sometimes, a DAO is nothing more than complex, open-source code with a community of developers to maintain it.[214] On other occasions, entrepreneurs choose to operate a business through a DAO, often referred to as a "venture" or "investment" DAO.[215] In these latter organizations, venture DAO operators frequently conflate the capacity of the technology to give exclusive control over digital assets to the DAO with the limited liability that law attributes to certain formally created entity structures.

For a long time, venture DAO creators built DAOs without considering potential entity law implications. Then a variety of scholars pointed out the potential problem: when a group of people join together to pursue a business for profit and they do not form some other entity, they may form a general partnership by default.[216] General partners do not enjoy a limited liability shield, but rather, can be held personally liable on a joint and several basis for the liabilities of the business.[217] Despite these warnings from legal experts, many venture DAO creators chose not to create a "legal wrapper" for the code through a formal business entity, believing the technical control of DAO assets by the code itself would act as a sufficient liability shield. Some such venture DAO creators have begun to confront the harsh reality that mistaking the control over assets enabled by technical systems for legal asset shielding can result in detrimental consequences.

Samuels v. Lido DAO provides the most direct illustration of this confusion: the defendants argued that because the DAO was merely software, it could not constitute a legal association of persons capable of forming a partnership. In 2020, three individual software developers created the Lido

---

[211] Carla L. Reyes & Christine Hurt, *DeFi, DAOs, and the Corporation*, 76 FLA. L. REV. 735, 750 (2024) (citing Primavera De Filippi & Samer Hassan, *Decentralized Autonomous Organizations*, INTERNET POL'Y REV. (2021) ("A DAO is a blockchain-based system that enables people to coordinate and govern themselves mediated by a set of self-executing rules deployed on a public blockchain, and whose governance is decentralized (i.e., independent from central control).")).

[212] *Id.* at 750 ("Many people can use the same term—DAO—and intend to mean very different concepts. Some insist that all DAOs rest upon human activity. Others focus on highly decentralized and extremely automated DAOs, to the exclusion of other models. In other words, people often use the term DAO when they have a specific technical archetype in mind, but in reality, DAOs—both in terms of their technical architecture and purposes—are not monolithic.").

[213] *Id*. at 751.

[214] *Id*. at 751-52.

[215] *Id*. at 752.

[216] *See, e.g.*, Carla L. Reyes, *If Rockefeller Were a Coder*, 87 GEO. WASH. L. REV. 373 (2019); Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 108 NW. U. L. REV. 1485 (2014); Shawn Bayern, *The Implications of Modern Business-Entity Law for the Regulation of Autonomous Systems*, 19 STAN. TECH. L. REV. 93 (2015); Shawn Bayern, *Implied Organizations and Technological Governance*, 64 WM. & MARY L. REV. 959 (2023); Rodrigues, *supra* note 52; Reyes & Hurt, *supra* note 211.

[217] Reyes & Hurt, *supra* note 211, at 758.

DAO to facilitate an Ethereum staking service.[218] To participate in the Lido DAO staking services, an Ethereum user exchanges ether for LDO tokens.[219] LDO token-holders then enjoy the right to vote on certain Lido DAO decisions, including selecting the Lido DAO participants who will serve as Ethereum validators.[220] Once selected, the Lido DAO validators "stake the ether pooled by Lido" and perform validator services for the Ethereum protocol.[221] Any ether rewards earned for performing those services are split among the DAO (5%), the validator (5%) and the LDO token holders (remaining 90%).[222] In December 2023, Andrew Samuels sued the Lido DAO and four institutional investors in Lido: Paradigm Operations, Andreessen Horowitz, Dragonfly Digital Management, and Robot Ventures.[223] Samuels alleged that he purchased LDO tokens in May 2023 and sold them at a loss in June 2023.[224] Samuels sued to recoup his losses, arguing that the Lido DAO should have registered LDO tokens as securities, and that because it did not, each member of Lido was jointly and severally liable for his losses because they were each general partners in a general partnership.[225]

Lido DAO never appeared in the litigation, but the institutional investor defendants moved to dismiss the complaint, arguing that Lido DAO was merely "a set of executable software programs…stored at and openly accessible on a specific set of public addresses on the Ethereum blockchain" and as a result, "[t]he Lido system identified in the Complaint is not owned or operated by any particular entity or group and is not authoritative or exclusive."[226] Ultimately, the institutional investors argued that Lido DAO could not be a general partnership because it "is another smart contract system, not a legal entity or natural persons."[227] The court disagreed, holding that operating an Ethereum staking service that keeps a percentage of the resulting revenue is the equivalent of carrying on, as co-owners a business for profit—the quintessential definition of a general partnership.[228] Although the court admitted that it remained unclear, at the motion to dismiss stage, who exactly constituted a partner in the partnership, the complaint sufficiently alleged the existence of a Lido DAO partnership for the case to continue forward.[229] The result is that, no matter how the case ultimately concludes, anyone holding LDO tokens faces liability risk stemming from Samuels' case. This is a liability risk that token-holders believed they had already mitigated through the technology alone.

Houghton v. Leshner reveals a deeper dimension of the problem: even sophisticated institutional investors, represented by experienced counsel, did not initially contest the partnership characterization on the merits. In that case, Amanda Houghton and several others sued the

[218] Samuels v. Lido DAO, 767 F. Supp. 3d 951, 957 (N.D. Cal. 2024) ("In 2020, Vasiliy Shapovalov, Konstantin Lornashuk and Jordan Fish created Lido, one such staking service.").
[219] *Id*.
[220] *Id*. at 958.
[221] *Id*.
[222] *Id*.
[223] *Id*. at 956.
[224] *Id*. at 960.
[225] *Id*.
[226] *Id*. at 960.
[227] *Id*.
[228] *Id*. at 962.
[229] *Id*.

Compound DAO, two individuals, and several institutional investors, alleging that they suffered losses when the defendants sold them unregistered securities in the form of COMP tokens.[230] Specifically, Houghton alleged that Compound Labs created a crypto-lending business that they later transferred to the Compound DAO, which continued to operate the business.[231] Houghton alleged that Compound DAO was a general partnership under California law, controlled by the individuals and institutions that controlled the majority of the COMP tokens: the named defendants.[232] Accordingly, Houghton alleged that the defendants were general partners with joint and several liability for the losses she and the other plaintiffs suffered as a result of the Compound DAO's failure to comply with securities regulations.[233] When the defendants moved to dismiss, they did not initially rest their arguments on a theory that the Compound DAO was not a partnership.[234] Rather, the defendants reserved their arguments on the partnership law question for later in the proceedings, arguing that "even if they are found to be formal partners in the Compound DAO 'partnership,'" a characterization the defendants contested, "and liable for some [or] all of the Compound DAO's acts, they cannot be liable for acts that predate their entry into the partnership."[235] Because the partnership questions rested so heavily on questions of fact, the court agreed with the defendants that those issues were better left for examination at the summary judgment stage.[236]

The remaining cases extend the analysis beyond securities liability to negligence, illustrating the full breadth of legal exposure that flows from the code-liability confusion. In at least two other cases, victims of a software hack sued DAO participants for negligent cybersecurity practices on the theory that the defendants were partners in a general partnership.[237] An examination of one of those cases, *Sarcuni v. bZx DAO*,[238] further illustrates the significant legal risk that arises when actors mistake code as soft law for code as positive law." Christian Sarcuni and eighteen other plaintiffs sued various individuals as partners in a general partnership in order to recover losses suffered when one of the partners negligently caused a cybersecurity incident.[239] The plaintiffs alleged that the bZx DAO operated the bZx protocol, which offered various cryptocurrency trading services and products.[240] One of the software developers who contributed to the bZx protocol

[230] Houghton v. Leshner, No. 22-cv-00781-WHO, 2023 WL 6826814 (N.D. Cal. Sept. 20, 2023).
[231] *Id*. at 1.
[232] *Id*.
[233] *Id*. at 6.
[234] *Id*.
[235] *Id*.
[236] *Id.* Note that both the Samuels and Houghton cases, along with a separate case involving the Ooki DAO involved further motion practice regarding how best to serve a DAO alleged to be a general partnership. *See, e.g.*, Houghton v. Leshner, No. 22-cv-007781-WHO, 2024 WL 5154071 (N.D. Cal. Nov. 25, 2024); Samuels v. Lido DAO, No. 23-CV-06492-VC, 2024 WL 4231598 (N.D. Cal. June 27, 2024); Commodity Futures Trading Comm'n v. Ooki DAO, No. 3:22-CV-05416-WHO, 2022 WL 17822445 (N.D. Cal. Dec. 20, 2022). None of these service-related decisions are discussed at length here because they did not touch on the merits issues of whether the participants in each DAO actually formed a partnership, or whether or which DAO token holders were partners in the alleged partnership.
[237] Sarcuni v. bZx DAO, 664 F. Supp. 3d 1100 (S.D. Cal. 2023); Fabian v. LeMahieu, No. 19-CV-54-YGR, 2019 WL 4918431 (N.D. Cal. Oct. 4, 2019).
[238] Sarcuni v. bZx DAO, 664 F. Supp. 3d 1100 (S.D. Cal. 2023).
[239] *Id.* at 1108.
[240] *Id*. at 1109.

received a phishing email on his personal computer in November 2021.[241] When the developer fell for the phishing scheme, he compromised the security of the bZx protocol, and the hacker stole around $55 million worth of cryptocurrency tokens belonging to bZx protocol users.[242] The plaintiffs brought an action for negligence, arguing that each general partner was liable for the negligence of their fellow general partners.[243]

The defendants moved to dismiss on various grounds, including that the bZx DAO was not a partnership, and that even if it was, the named defendants themselves were not partners of the partnership.[244] Explaining that under California law (as is true in every state), "unless persons associated to do business together establish a formal entity like a corporation, the association is deemed to be a partnership regardless of the parties' intent,"[245] the court methodically evaluated the factors that make an association of people a partnership. First, the court explained that at the motion to dismiss stage, all that is required of the plaintiff is that the complaint make "specific factual allegations demonstrating: (1) the right of the purported partners to participate in the management of the business; (2) the sharing of profits and losses among the purported partners; and (3) contributions of money, property, or services by the purported partners to the partnership."[246] The court determined that Sarcuni and the other plaintiffs had met this pleading standard by alleging that the bZx DAO was an association of two or more persons with the right to participate in the management of the DAO, that the DAO generated profits through the cryptocurrency services and products it offered to the public, and that the defendants, as token-holders of the DAO had the right to share in those profits.[247] As a result, even though the founders of the bZx DAO initially created it because they believed that the technology could build limited liability for their activity without creating a legal entity, that very misunderstanding about the relationship between code and law created new legal risk.[248]

These cases illuminate no fewer than four areas in which confusing technical capabilities with the effect of legal rules can expose individual entrepreneurs and investors to significant legal and monetary risk. First, functionally locking-in capital through smart contracts used by a DAO is not the same as the asset shielding and capital lock-in achieved through legally recognizable business entities. Second, participants in venture DAOs who opt not to create a formal legal wrapper for a DAO face general partnership liability risk. Third, determining who is a partner in such partnerships is fact-intensive and may require costly discovery. Fourth, even when good arguments exist for legally limiting general partnership risk exposure, those arguments may not save DAO participants from the expenses associated with defending a lawsuit, including class action lawsuits, through at least the summary judgment stage. In other words, when private parties conflate

[241] *Id*. at 1110.
[242] *Id*. at 1111.
[243] *Id*.
[244] *Id*. at 1114.
[245] *Id*. at 1115.
[246] *Id*. at 1115.
[247] *Id*. at 1115-19.
[248] *Id.* at 1110 (quoting the founders as having said that creating the bZx DAO was about "really preparing for the new regulatory environment by ensuring bZx is future-proof. …really what we're going to do is take all the steps possible to make sure that when regulators ask us to comply, that we have nothing we can really do because we've given it all to the community.").

technical system attributes with legal limited liability, they often do so to their detriment. In terms of our theoretical framework, these cases confirm that the technical constraints imposed by DAO code, however effective at controlling access to digital assets, operate exclusively in the architectural domain; limited liability, by contrast, is a normative creation available only through the legal system's secondary rules of change, when parties comply with applicable entity formation statutes.

III. Only Positive Law Can Make Code Law

The preceding Parts of this Article have established a foundational proposition and diagnosed its widespread neglect. Part I advanced our central thesis: a categorical divide separates the architectural constraints of code from the normative force of law, a gap that can only be bridged when the legal system itself, through its secondary rules, formally invests code with legal authority. Part II demonstrated the tangible legal pathologies that arise from confusing code's technical capabilities with legal power, revealing how this foundational error distorts outcomes for legislators, judges, and private actors alike. We now turn to the pathways through which code might acquire legal significance, distinguishing between successful investiture that grants code legal effect and the conceptual impossibility of code becoming an autonomous source of law.

The analysis proceeds through two distinct inquiries. First, we consider investiture through rules of change. This occurs either when legislatures enact statutes that grant legal effect to code-based systems (public empowerment) or when private ordering instruments, such as wills, trusts, bailments, and contracts, empower individuals to create binding arrangements in which code generates enforceable legal consequences (private empowerment). These mechanisms successfully attach legal consequences to code-based facts, demonstrating how positive law can make code legally significant. Second, as a thought-experiment, we examine whether code could theoretically be recognized as an autonomous source of legal norms through a rule of recognition, revealing why such an approach is implausible if not conceptually incoherent given code's inability to generate prescriptive rules.

This Part validates the analytical power of our proposed framework. It demonstrates that our thesis is not merely a theoretical abstraction but a descriptive tool to explain how and the limited extent to which code acquires legal authority in a world governed by positive law.

A. Investiture Through Legislative Empowerment

The most direct pathway to bridge the chasm between code and law is through public empowerment. This occurs when a recognized law-making authority exercises its power under a secondary rule of change to enact legislation. Such laws operate by identifying specific, verifiable code-based states or technical conditions and then formally investing them with binding consequences. This process, however, does not grant inherent legal authority to code. Instead, the law deliberately envelops a technical system, imbuing the states or outcomes that code produces with juridical effect. The code remains a set of architectural constraints; the legislation in question

is the exclusive source of normative power. Authority thus flows from the law to the code, never the reverse.

Real property recording systems provide a familiar example of how technical record-keeping systems acquire legal significance through statutory empowerment. Control or possession of real property does not automatically confer legal rights; only positive law can convert physical occupation into legally cognizable ownership. Recording statutes transform technical acts, such as filing documents in government registries, into legally dispositive evidence of title. The recording system itself operates through purely administrative and clerical processes: clerks receive documents, assign recording numbers, and maintain chronological files. Yet these operations carry profound legal consequences because statutes grant legal effect to recorded information, including priority of filing, identity of titleholders, and descriptions of affected parcels. These statutory provisions create rules that determine property rights and resolve disputes between competing claimants. Without such statutory frameworks, these recording systems would remain mere administrative conveniences rather than sources of legal authority. The legal significance flows not from the sophistication of the recording process, but from legislative decisions to invest those recorded facts (or, more accurately, technical states) with binding consequences. This demonstrates the essential pattern: law strategically enlists technical systems while retaining ultimate control over when and how they generate legally enforceable outcomes.

Moving from analog recording systems to digital technologies, electronic signature legislation exemplifies the first major instance of public empowerment applied to code-based systems. At the turn of the 21st century, responding to the growing prevalence of electronic transactions, Congress passed the Electronic Signatures in Global and National Commerce Act in 2000 ("E-Sign"),[249] while states concurrently adopted the ULC Uniform Electronic Transactions Act (UETA).[250] These statutes represent paradigmatic examples of legislatures exercising secondary rules of change to grant legal significance to specific technical conditions.

The core mechanism operates precisely as our theoretical framework predicts: these legislative instruments identify verifiable code-based elements (including cryptographic signatures, digital authentication processes, and electronic document formats) and formally invest them with binding legal authority. E-Sign provides that no signature or contract may be denied enforceability solely because it exists in electronic form.[251] UETA goes further by establishing that electronic records satisfy writing requirements and electronic signatures fulfill statutory signature mandates;[252] moreover, this act even empowers electronic notarization, eliminating requirements for physical stamps or seals.[253]

Moving past electronic signature laws, a particularly significant example of public empowerment in the digital realm is the 2022 set of amendments to the Uniform Commercial Code (UCC), which

[249] Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, 114 Stat. 464 (2000) (codified at 15 U.S.C. §§ 7001–7031 (2023)).
[250] UNIF. ELEC. TRANSACTIONS ACT (Unif. L. Comm'n 1999).
[251] 15 U.S.C. § 7001(a).
[252] UNIF. ELEC. TRANSACTIONS ACT §§ 7, 9.
[253] *Id.* § 11.

introduced the new Article 12.[254] This legislative project represents a deliberate and nuanced exercise of secondary rules of change, designed to create a predictable legal framework for a novel class of property, digital assets, that had previously existed in a state of legal uncertainty. Recognizing that the common law regime for intangible assets was ill-suited for the high-velocity, pseudonymous nature of the blockchain ecosystem, the Uniform Law Commission and the American Law Institute developed a new legal architecture to accommodate emerging practices and the expectations of market participants.[255] Article 12 does not, however, represent a blind deference to technology or a generalized endorsement of the "code is law" maxim; instead, it carefully defines which technological facts will be granted legal significance and precisely what their juridical status will be.

The first step in this legislative process was to define the specific object of this new statute. Article 12 introduces the concept of a "controllable electronic record" (CER), a record stored in an electronic medium that can be subjected to "control."[256] The concept of control is the linchpin of the entire framework, and it is defined in UCC § 12-105 as a verifiable, code-based state. A person has control over an electronic record if they possess a trio of technical powers: the power to avail themselves of substantially all the benefit from the record, the power to prevent others from doing so, and the power to transfer these powers to another person.[257] This functional definition remains technology-neutral, focusing on capabilities rather than the technical details of specific implementations.[258] Nevertheless, it is a pure assessment of fact, not legal right. It is a determination of whether the code-based system affords a particular person these capabilities. By isolating "control" as the key technological fact, the legislature created a clear, objective trigger for the attachment of legal consequences.

The most powerful of these statutory effects is the creation of the "qualifying purchaser." Section 12-104 establishes a potent "take-free" rule: a purchaser who obtains control of a CER for value, in good faith, and without notice of a competing property claim acquires their rights in the asset free from any such claims.[259] This rule, which cloaks CERs in the mantle of negotiability, is a deliberate act of legal investiture.[260] The law attaches a profound juridical effect, the ability to take clean title even from a transferor with defective title, directly to the technical fact of obtaining control, albeit limited by specified conditions. This is the clearest possible example of the theoretical framework in action: the legal system is not deferring to the code's outcome but is

[254] *For the official text of the final amendments, see* UNIF. L. COMM'N & AM. L. INST., UNIFORM COMMERCIAL CODE AMENDMENTS (2022), *available at* https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=d5bcf850-366f-b4b5-e7d6-6749ba2382c6.

[255] *See* Andrea Tosato, Diane Lourdes Dick, & Christopher K. Odinet, *Debt Tokens*, 173 U. PA. L. REV. 1150, 1150–52 (2025) (detailing the history of the 2022 amendments to the UCC).

[256] U.C.C. § 12-102(a)(1) (Am. L. Inst. & Unif. L. Comm'n 2022).

[257] For example, a Bitcoin holder who possesses the private keys can spend the Bitcoin (benefit), prevent others from spending it (exclusion), and transfer the private keys to another person (transferability).

[258] The statute does not specify whether control must be achieved through private keys, multi-signature arrangements, smart contracts, or other technical means. Instead, it identifies the functional outcomes that must be achievable and leaves the technological implementation open.

[259] *See* Tosato et al., *supra* note 255, at 1154–56.

[260] This approach mirrors the negotiability principles found in Articles 3 and 7 of the UCC, which similarly protect good faith purchasers of negotiable instruments and documents of title.

instead empowering the technical state of control by granting the acquirer a privileged legal status that serves the established commercial law goals of certainty and finality.

Article 12 provides another explicit example of public empowerment in its choice-of-law provision. Section 12-107 establishes a multi-step structure, a "waterfall," to determine the governing law for a CER. At the top of the hierarchy, the statute empowers a code-based state: if the CER or its associated records expressly designate a jurisdiction, that designation controls.[261] This is a direct investiture of legal authority in a set of data embedded in the digital asset. However, the law does not stop there. If this technical fact is absent, the waterfall descends through a series of traditional legal inquiries, culminating in a default rule that designates the District of Columbia as the governing jurisdiction.[262] This waterfall elegantly blends different sources of authority, creating a seamless interplay between code-based facts and traditional legal rules. It demonstrates that law can deliberately harness technology while retaining its ultimate authority to resolve uncertainty. It is a perfect illustration of the legal system harnessing code without ceding its own power.

Perhaps the most sophisticated public empowerment of code found in Article 12 is represented by "controllable accounts" and "controllable payment intangibles."[263] These are new categories of personal property introduced by the 2022 UCC Amendments. A controllable account represents a traditional account receivable, such as a software company's right to payment for a SaaS subscription or an e-commerce platform's claim to commission fees from marketplace transactions, that is evidenced by a CER, with the account debtor agreeing to pay whoever controls that digital asset.[264] Similarly, controllable payment intangibles involve payment rights evidenced by a CER where the account debtor's principal obligation is monetary and the debtor has agreed to pay the person in control of that digital asset.[265] In essence, these legal devices are a legislatively sanctioned form of "tokenization" for payment rights.[266]

The concept of tokenization, the practice whereby one asset is used to represent rights in another, has a long history in commercial law, from negotiable instruments like promissory notes to share certificates and bills of lading.[267] Each of these instruments required specific legal frameworks to become effective, demonstrating that tokenization has always depended on deliberate acts of public empowerment.[268] The foundational property law principle of *numerus clausus* restricts the creation of new forms of property to a closed list recognized by law; private parties cannot simply agree that a piece of paper or a digital asset represents rights in another asset in a way that binds

[261] U.C.C. § 12-107(a); *see also id*. § 12-107 cmt. 2 ("This subsection gives effect to an express designation of jurisdiction contained in the controllable electronic record itself or in a record attached to or logically associated with it.").
[262] U.C.C. § 12-107(b)-(d); *id.* § 12-107 cmt. 3 (describing the fallback sequence when no express jurisdictional designation exists).
[263] *See* U.C.C. § 9-102(a)(27A), (27B).
[264] U.C.C. § 9-102(a)(27A)
[265] U.C.C. § 9-102(a)(27B)
[266] *On tokenization see generally* Moringiello & Odinet, *supra* note 1; Tosato et al., *supra* note 255; Tosato & Odinet, *supra* note 195.
[267] *See* Moringiello & Odinet, *supra* note 1; Tosato & Odinet, *supra* note 195.
[268] *See* Moringiello & Odinet, *supra* note 1; Tosato & Odinet, *supra* note 195.

the rest of the world.[269] For tokenization to be effective, a law must establish that the representative asset can legally embody the underlying rights and that its transfer effects a transfer of those rights.[270] Article 12's creation of controllable accounts and payment intangibles is precisely this deliberate legislative act, defining new property categories and specifying the legal consequences of controlling their associated CERs.

The necessity of this statutory investiture is best illustrated with a hypothetical. Consider two parties who attempt to use a standard NFT to represent an account receivable. They could create a sophisticated digital asset with metadata containing all information about the receivable, including a statement from the debtor undertaking to pay whoever controls the NFT. The blockchain would enable seamless transfer of this NFT. Yet, despite this technical sophistication, the arrangement would lack the legal force of negotiability. A good-faith purchaser of the NFT would acquire no greater rights than the transferor possessed and would not be protected from defenses the debtor could assert against the original creditor. The code enables the technical operations, but without the specific statutory framework of Article 12, the digital representation remains legally inert for property law purposes. Only the public investiture through legislation transforms this technical capability into a legally enforceable property right.

Having demonstrated how public empowerment operates through legislative delegation to code-based systems, we now turn to the second pathway through which code can acquire legal force: private empowerment, where the law delegates authority to individuals to create their own binding legal arrangements.

B. Investiture Through Private Empowerment

We now turn to the second pathway identified in our theoretical framework: private empowerment. This mechanism operates through the same Hartian secondary rules of change that enable public legislation, but with a crucial difference in scope and application. While public empowerment involves legislative authorities granting legal significance to technical systems, private empowerment occurs when the legal system confers "limited legislative power" upon private parties. When Hart described this capacity of individuals to "create, vary, and extinguish their own rights and duties," he was identifying something more profound than mere contractual freedom. He recognized that the legal system delegates genuine law-making authority to private parties. This delegation transcends passive permission. Through established institutional frameworks, the legal system actively empowers individuals to create new primary obligations. Courts will then recognize and enforce these privately generated obligations as binding law, provided the parties have properly exercised their delegated authority.

The legal system propagates this empowerment through multiple instruments: contracts, trusts, wills, bailments, and corporate governance documents, among others. Each offers a distinct pathway for private law-making, yet all share an essential characteristic: they grant individual persons considerable discretion in determining which rights and obligations they wish to create, modify, or extinguish, and in selecting the mechanisms for doing so. Crucially, the underlying legal principle remains constant: legal force derives from the parties' valid exercise of their

[269] *See* Tosato & Odinet, *supra* note 195.
[270] *Id*.

delegated authority, not from the particular technical mechanisms they employ, regardless of their sophistication or effectiveness as architectural constraints.

This inherent flexibility has historically enabled private parties to incorporate emerging technologies into their binding arrangements. From wax seals authenticating medieval contracts to printing presses standardizing commercial terms, from telegraph systems enabling remote formation to electronic signatures facilitating digital commerce, each innovation has been absorbed into private ordering through existing legal frameworks. The law's adaptability demonstrates that private empowerment instruments are technology-agnostic: they care not about the medium but about the parties' intent and the satisfaction of legal requirements.

Blockchain networks, digital assets, and smart contracts are the latest evolution in this historical pattern. Yet these tools offer capabilities that make them uniquely powerful for private empowerment, surpassing previous technologies in ways that fundamentally transform the effectiveness of private legal arrangements. Unlike earlier developments that primarily improved communication or documentation, blockchain technology combines multiple features within a single system. Smart contracts can autonomously manage digital assets according to predetermined conditions. Blockchain-enabled immutable ledgers create tamper-resistant, permanent records of transactions and state changes. This distributed architecture eliminates single points of failure while providing transparency to all participants. Most significantly, programmability enables virtually unlimited complexity in conditional logic, allowing parties to encode sophisticated arrangements that respond automatically to specified triggers.

The transformative potential of blockchain technology becomes especially apparent when considering its application in two areas where private parties enjoy considerable empowerment under existing legal frameworks: first, in contracts, where parties can harness smart contracts and digital assets to automate formation, performance, and enforcement of their agreements; and second, in organizational governance, where parties can employ code-based mechanisms within decentralized autonomous organizations to coordinate collective decision-making and resource management according to predetermined rules.

1. Code-Based Contracts

Consider first contractual arrangements. When parties incorporate smart contracts and digital assets into their binding agreements, they do not create new forms of law but rather exercise their established private legislative power in novel ways. These technologies enable automation across the entire contract lifecycle, starting with formation, where code can embody the fundamental elements of offer and acceptance.

Nick Szabo's prescient vending machine analogy illuminates this mechanism of automated contract formation.[271] Just as a vending machine presents a standing offer that customers accept

[271] Nick Szabo, *Smart Contracts: Formalizing and Securing Relationships on Public Networks*, FIRST MONDAY (Sept. 1997), *available at* http://firstmonday.org/article/view/548/469.

by inserting coins, smart contracts can create binding arrangements through predetermined triggers. For example, suppose a person deploys a smart contract on Ethereum that transfers an NFT with specific features upon receiving an amount of ether tokens. The code itself constitutes a standing offer by the token holder, while the sender's transmission of the specified cryptocurrency amount constitutes acceptance. This arrangement creates binding obligations not because code has inherent legal authority, but because the parties have exercised their power under contract law to make offers and manifest acceptance through their conduct. Indeed, courts have begun to formally recognize this principle, confirming that automated systems can form binding contracts within established legal frameworks.[272]

Beyond formation, blockchain technology profoundly transforms how parties perform contractual obligations, regardless of how those contracts were initially created. Parties can agree that code execution constitutes proper performance of their contractual duties, potentially eliminating traditional friction in contract fulfillment. Smart contracts can enable escrow arrangements where digital assets are automatically released upon satisfaction of verifiable conditions, removing the need for trusted intermediaries. Conditional transfers can be triggered by oracle-provided data, such as parametric insurance payouts activated by weather data or derivative settlements based on price feeds. Time-based payment schedules execute automatically, ensuring precise compliance with agreed payment terms. In each case, the legal framework remains traditional contract law. Parties simply agree that successful code execution satisfies their performance obligations. The innovation lies not in new legal principles but in the reliability and automation that code brings to contractual performance.

The application of blockchain technology to contractual remedies illustrates both its potential and its boundaries. While parties possess some freedom to structure remedies through their private legislative power, this freedom operates within strict legal confines. Contract law permits parties to pre-agree to certain automated responses, particularly where they align with recognized remedial structures. A supply chain contract might escrow liquidated damages that automatically transfer to the buyer if oracle data confirms late delivery. Collateral arrangements can self-liquidate upon predetermined default triggers. Arbitration agreements may specify that code will automatically implement arbitral awards by transferring disputed assets. These arrangements derive legal force from the parties' agreement that such automated responses constitute valid enforcement of pre-authorized contractual remedies. The code executes what parties have agreed, transforming abstract remedial rights into immediate technical operations. Through this mechanism, private parties use their delegated authority to create arrangements that are simultaneously self-executing and legally enforceable.

2. Code-Based Organizational Governance

[272] The Singapore High Court's recognition in *Quoine Pte Ltd v B2C2 Ltd* that algorithmic trading systems can form binding contracts confirms that automated formation mechanisms operate within established contract law frameworks. *See* Quoine Pte Ltd. v. B2C2 Ltd., [2019] SGHC(I) 03 (Sing.).

Beyond bilateral agreements, private empowerment finds a still more potent application in the realm of collective governance. The same principles of delegated authority that animate contracts also underpin the legal frameworks for partnerships, corporations, and unincorporated associations. This move from individual contracts to collective action allows an exploration of the rich middle ground between traditional hierarchical firms and the futuristic, fully autonomous entities that dominate scholarly debate. Blockchain technology provides a powerful new toolkit for this purpose by enabling parties to translate their governance arrangements into transparent, automated code.

This private empowerment allows for the creation of what can be termed "Distributed Business Entities" (DBEs): organizations that use technology to automate the "mediating hierarchy" of middle management and, in doing so, fundamentally challenge the traditional separation of ownership and control.[273] These blockchain-based tools offer robust solutions to classic collective action problems. Governance can be executed through code-enforced voting mechanisms, treasury management can be automated with smart contracts disbursing funds only after a valid vote, and economic entitlements can be linked directly to digital assets, creating a clear and technically enforced structure. By embedding these operational rules in an immutable ledger, such systems reduce trust requirements and lower coordination costs, making them exceptionally effective instruments for private ordering.

The legal significance of these code-based systems is realized when parties use established legal instruments to adopt them as their chosen method of governance. The specific configuration of these tools is not technologically determined but is rather the result of conscious "design trade-offs" made by founders to achieve particular organizational goals.[274] The real-world application of this principle is already evident; for instance, the Dash network used a New Zealand-based irrevocable trust to legally structure its masternode-governed system, while the software developer collective dOrg formed as a Vermont Blockchain-Based Limited Liability Company (BBLLC) to formalize its code-based rules for work and profit allocation.[275] In each scenario, the code's authority is not inherent; it derives from the members' agreement, memorialized in a legally cognizable instrument. Through their exercise of private legislative power, the parties voluntarily and formally bind themselves to the outcomes produced by the code.

This delegated authority is powerful but not absolute. The boundaries of private empowerment remain firmly within established legal constraints. Code can execute ministerial functions, but it cannot override the mandatory rules of organizational law. Directors and trustees cannot abdicate fiduciary duties to algorithms; fundamental corporate changes still require traditional statutory procedures; and members retain non-waivable rights such as judicial dissolution and books and

[273] Carla L. Reyes, *Autonomous Business Reality*, 21 NEV. L.J. 437, 474–77 (2021) (defining "Distributed Business Entities" as businesses that automate the "mediating hierarchy" and discussing how automation can change the level of separation between ownership and control).

[274] *Id.* at 462 (explaining that "stakeholders in many fields must make design tradeoffs when undertaking activity to achieve one goal inhibits their ability to achieve another goal"); *see also* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 164 (2018) ("The tradeoff thesis . . . applies more generally to any situation in which we're trying to maximize a set of values, . . . at least some of the time.").

[275] *Id.* at 442, 467–68 (describing the specific legal wrappers chosen by the Dash and dOrg projects to gain formal legal recognition and structure their operations).

records inspection. This limitation confirms our central thesis: code operates with the force of law only to the extent that positive law, through secondary rules empowering private ordering, permits parties to delegate specific decisions to technical systems.

Ultimately, blockchain-based governance represents an evolution in the exercise of private ordering, not a revolution against law itself. Whether it is a traditional shareholder vote in a general meeting or a vote cast by remote token holders participating in a distributed organization, the source of legal rights and obligations is identical: the voluntary exercise of private legislative power through instruments that the law recognizes as creating binding commitments. The technology provides unprecedented tools for implementing these arrangements, but the legal authority flows from human agreement formalized through recognized legal instruments, not from code itself.

3. The Inherent Limitations of Code-Based Private Ordering

The preceding sections demonstrate how private parties can use their delegated legislative power to create code-based arrangements with genuine legal force. Yet this investiture remains structurally limited by the distinction between law and code identified in Part I. Law operates in the realm of normative obligation, determining what ought to be, while code factually creates architectural constraints on what can be done. Even when law empowers code through private ordering, this fundamental difference generates systemic boundaries on the extent to which code can effectively serve as a source of legal rights and obligations. While not exhaustive, five prominent limitations illustrate these structural constraints.

First, while code might approximate evaluative standards through proxies and metrics, law will not accept such deterministic approximations as authoritative interpretations of inherently contextual concepts. Legal standards like "reasonable efforts," "good faith," or "materiality" require human judgment that weighs factors no algorithm can fully capture. Even sophisticated code using multiple data sources can only create mechanical substitutes for these evaluative concepts. The legal system preserves these standards precisely because they require the kind of contextual, value-laden assessment that resists algorithmic reduction.[276] Thus, parties who code their arrangements must either accept mechanical proxies that imperfectly capture their intentions or maintain parallel legal agreements that preserve evaluative flexibility.

Second, the append-only architecture of blockchain networks creates a fundamental mismatch with law's concept of nullification. When code executes on a blockchain, it creates an immutable technical record that persists even when law declares the underlying transaction void. While blockchain systems can reverse economic effects through offsetting transactions, this forward-moving correction differs fundamentally from legal nullification *ab initio*. A blockchain system

[276] For this reason, many such systems use smart contracts as a coordinating tool, aggregating votes of users who themselves, using the code as their instrumentality, determine the outcome of claims among or between users of those systems. *See* Hinkes, *supra* note 202, at 888 (discussing the voting schema used by the MetaCartel Pact to resolve disputes between members of the MetaCartel DAO).

generally can only add new records to its record set. A court declaring a transaction void for fraud erases its legal existence retroactively, affecting tax consequences, creditor priorities, and third-party rights in ways that no subsequent blockchain transaction can replicate. This architectural reality means code-based systems can only approximate, never fully implement, legal concepts like rescission or avoidance that require erasing rather than offsetting past events.

Third, while code-based systems can implement dispute resolution mechanisms, they cannot provide the authoritative interpretation that law requires. Decentralized arbitration protocols and automated resolution systems may determine outcomes within their technical parameters, but when parties dispute whether those parameters correctly embodied their legal intentions, only courts can provide binding interpretation.[277] Whether code properly implemented a settlor's intent, honored testamentary wishes, or fulfilled fiduciary duties requires examining evidence and applying legal principles that exist outside any technical system.[278] The limitation is not that code cannot resolve disputes, but that it cannot authoritatively determine whether its own execution aligned with the parties' exercise of private ordering powers.

Fourth, the global nature of blockchain networks collides with the territorial boundaries of legal systems. A smart contract may execute simultaneously across multiple jurisdictions, each with different requirements for contract formation, electronic signatures, and legal capacity. While parties might specify governing law in their code or associated documentation, this choice remains subject to mandatory local laws that cannot be contracted away. Consumer protection statutes, usury limits, and public policy restrictions apply regardless of the parties' coded intentions. Moreover, enforcement ultimately depends on courts in particular jurisdictions, and judges may refuse to recognize automated transactions that violate local formality requirements, such as witnessing, notarization, or written documentation, even if the code executed flawlessly.

Fifth and finally, efforts by creators of DAOs to create "code deference," that is, to limit resolution of disputes between users of technical systems to system-native dispute resolution systems, ultimately fail. DAOs and similar organizations have attempted to compel their participants to resolve disputes regarding the DAO's operation and the participants' powers and expectations using a variety of approaches, including contractual provisions limiting the right to sue, self-executing system-native dispute resolution processes, and the imposition of system-native remedies.[279] However, none of these strategies can absolutely bar a participant from seeking redress through the conventional legal system, nor can they preclude the imposition of a judicial remedy on other participants.[280] The legal system is designed to be readily accessible to any party; both the code and its participants remain subject to legal systems, and neither code nor contract can absolutely

[277] Hinkes, *supra* note 202 (recognizing that the resolution of a dispute by system-native technical processes may always be questioned by redress to the dispute resolution apparatus of the exogenous legal system, and that technical attempts to limit or restrict access to the exogenous legal system are ineffective).
[278] *See* James Grimmelmann, *All Smart Contracts Are Ambiguous*, 2 J.L. & INNOVATION 1 (2019) (”Smart contracts can be ambiguous, too, because technical facts depend on socially determined ones.”).
[279] Hinkes, *supra* note 202.
[280] *Id.* at 872.

bind a party to the outcome of system-native dispute resolution or restrict access to judicial processes and remedies that may overturn or vary outcomes reached through such mechanisms.[281]

C. Investiture Through Rule of Recognition

Having demonstrated how code can be invested with legal force through both public and private empowerment, we now consider a final, more theoretical, possibility: whether the rule of recognition of a legal system could evolve to treat a blockchain network as an autonomous source of law.

As explained in Part I, Hart posits that the rule of recognition serves as the ultimate criterion for identifying valid law within a legal system.[282] It exists not as enacted law but as a social fact constituted by convergent official practice, particularly among judges who accept and employ common criteria for determining which norms they must recognize and apply.[283] Through this mechanism, legal systems solve what Hart called the problem of "uncertainty," providing a definitive test to distinguish legally binding rules from mere social norms, moral principles, or invalid enactments.

Since Hart's initial formulation, positivist scholars have vigorously debated important aspects of the rule of recognition, questioning whether it must be a singular rule or might be multiple,[284] if it generates genuine normativity or merely describes official practice,[285] and its fundamental character, with some re-conceptualizing it as a "shared plan" that constitutes a system's political order.[286] Nevertheless, a functional consensus emerges from these discussions on two points that are fundamental to our inquiry. First, legal systems must necessarily contain a mechanism that identifies which rules count as binding.[287] Second, the rule of recognition must confer legal authority to sources capable of generating prescriptive norms that can articulate what legal subjects ought or ought not do.

In our view, this functional consensus is precisely what makes a code-based rule of recognition conceptually untenable. Consider Hart's paradigmatic example of a rule of recognition: "What the Queen in Parliament enacts is law."[288] This formulation identifies Parliament as a source capable of generating prescriptive rules. To test whether a technical system could serve a similar function,

---

[281] Id. at 896.
[282] *See* Part I.B.
[283] *See* Part I.B.
[284] Joseph Raz, *The Identity of Legal Systems*, 59 CALIF. L. REV. 795, 806–08 (1971).
[285] Jules L. Coleman, *Negative and Positive Positivism*, 11 J. LEGAL STUD. 139, 157 (1982).
[286] Shapiro, *supra* note 92, at 268
[287] Notably, Shapiro argues that Hart's specific conception of the rule of recognition as a duty-imposing convention among officials is questionable. *See* Shapiro, *supra* note 92, at 268. However, Shapiro immediately substitutes his own "planning theory" which serves the identical function of identifying valid law through social facts about official practice and shared understandings. *Id.* at 265–67. As Shapiro acknowledges, both Hart's rule of recognition and his shared plan "play the same role, namely, the resolution of normative uncertainty" about what counts as law.
[288] Hart, *supra* note 22, at 36.

consider the following, parallel rule of recognition: "What the Bitcoin blockchain records is law" or "The states validated on the Ethereum network constitute binding legal rules."

Such a formulation would fail the second functional requirement identified above. Blockchain networks, however sophisticated, record factual states rather than prescriptive norms. The Bitcoin ledger documents that a transaction, signed with Alice's private key, has designated a set of unspent transaction outputs (UTXOs) as now spendable by Bob's address; Ethereum records that particular functions executed with specific parameters; these systems memorialize computational events and cryptographic proofs. These are descriptions of what has occurred on the network, not prescriptions of what ought to occur in the world. Unlike Parliament's statutes or judicial precedents, which articulate prescriptive norms that can be interpreted and applied, a blockchain system remains a deterministic state machine incapable of normative expression.

One might object that blockchain records do appear prescriptive—when the Bitcoin ledger shows Alice holding tokens, does this not prescribe that others must respect her ownership? This objection conflates the technical record with the legal concept it might evidence. The blockchain records only that certain cryptographic operations occurred: that a private key signed a transaction moving unspent outputs to a new address. "Ownership," with its attendant rights to exclude others, to transfer, and to use, is a legal concept that positive law may choose to attach to these technical facts. The blockchain itself generates no concept of property, no rights, and no obligations; it generates merely cryptographic proofs of computational events.

Alternatively, one might argue that the "If X, then Y" logic at the heart of a smart contract is itself a prescriptive norm. This mistakes a rule of computation for a rule of conduct. A smart contract's conditional logic is a statement of executional necessity: "If event X occurs, the code *will* execute function Y." This is a descriptive statement about a machine's predetermined operation. A prescriptive norm, by contrast, provides a human agent with a reason for action: "If event X occurs, you *ought* to do Y." The former is a statement of causal certainty enforced by the network's protocol; the latter is a normative standard whose authority derives from a recognized legal source. The smart contract's logic is not the source of a legal rule; it is the technical trigger that a pre-existing legal rule might recognize.

This conceptual impossibility differs fundamentally from the successful investiture examined in Parts III.A and III.B. There, positive law attaches specific legal consequences to particular code states; for instance, UCC Article 12 provides that control of a digital asset confers property rights. The law remains the source of the normative rule; code merely supplies the triggering facts. By contrast, recognizing code as an autonomous source of law would require blockchain systems themselves to generate prescriptive content, a function for which these systems of technical execution are conceptually unsuited.

CONCLUSION

The confusion between code and law did not originate with blockchain technology, and it will not end there. Each generation of technological innovation tempts lawmakers, courts, and market participants to mistake architectural power for normative authority. This Article has offered a

jurisprudential framework to resist that temptation. By applying Hart's theory of primary and secondary rules, we demonstrated that an ontological gap separates code's capacity to constrain behavior from law's power to create enforceable rights and obligations. Because code records factual states rather than prescriptive norms, it is structurally incapable of bridging that gap on its own. The gap can be bridged, but only through the deliberate exercise of legal authority, whether by legislatures investing code-based states with juridical effect or by private parties incorporating code into recognized ordering instruments. The boundary is not always easy to police, as the costly consequences visited upon legislators, investors, and market participants documented in these pages attest. Yet maintaining the distinction remains essential. As technical systems grow ever more sophisticated in regulating human conduct, the foundational insight endures: code governs the possible; only law determines the permissible.