READY LAYER ONE: FUNCTIONAL REGULATION FOR BLOCKCHAIN INFRASTRUCTURE

Carla L. Reyes[*] & Joseph P. Cutler[**]

I. INTRODUCTION 320

II. TRADITIONALLY, THE LAW TAKES A FUNCTIONAL APPROACH TO OPEN-SOURCE SOFTWARE. 325
- *A. The Seemingly Forgotten History of the Law's Approach to Open-Source Digital Infrastructure Development.* *326*
- *B. Open-Source Layer-1 Distributed Ledger Technology Protocols and Layer-2 Smart Contract Protocols Represent a New Wave of Open-Source Infrastructure Development.* *331*

III. OPEN-SOURCE DISTRIBUTED LEDGER TECHNOLOGY'S INHERENT MISMATCH WITH FINANCIAL REGULATION BUILT FOR INTERMEDIATED FINANCE. 341
- *A. Existing Financial Regulation Assumes an Intermediated Financial System.* *342*
- *B. Applying Existing Financial Regulation to Open-Source Digital Infrastructure Fails to Achieve Stated Policy Goals and Undermines Broader Technology Development.* *349*

IV. THE EMERGING DECENTRALIZED ERA REQUIRES A RETURN TO FUNCTIONAL REGULATION. 355
- *A. Functional Regulation of Layer-1 DLT Protocols and Layer-2 Smart Contract Protocols can be Developed Through Existing Functional Methodologies in Law.* *356*
- *B. Five Key Principles of Functional Regulation Lawmakers Should Internalize as they Continue to Confront Policy Choices in an Increasingly Disintermediated Society.* *361*

The research and writing of this Article were supported by funding from Hedera Hashgraph, LLC, which supports the open-source Hedera hashgraph network.

[*] Associate Professor of Law, SMU Dedman School of Law; Faculty, Institute 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. JD, LLM, MPP, Duke University; BA, Whitworth University. My co-author and I would like to thank Nilmini Rubin, Gregory Schnieder, and Amy Whitsel for their feedback and comments on early drafts of this Article. ORCID ID: 0000-0002-2448-8309

[**] Partner, Perkins Coie, LLP; Firmwide Chair, Fintech Industry Group; Firmwide Lead, Financial Services Compliance, Privacy, and Crime Prevention Vertical; JD, Georgetown University Law Center; BA, University of Washington. I would like to thank Logan Payne for his early research assistance for this Article.

1. The functional method should apply to the substance of regulation rather than the form of regulation. 362
2. Functional regulation should be technology neutral. 364
3. Functional regulation should be grounded in the factual and technical realities of Layer-1 DLT protocols and Layer-2 smart contract protocols. 365
4. Functional regulation should embrace public review and comment of proposed regulations to ensure broad stakeholder participation. 366
5. Open access to digital infrastructure resources should be protected. 368

V. CONCLUSION 370

ABSTRACT

A software developer quietly builds a protocol that connects anyone with a project or a cause directly to other people who might be interested in financially contributing to the project or cause. Known broadly as a crowdfunding platform, this software developer is building something slightly different and new. In particular, his code connects those with project ideas directly to those willing to contribute to those ideas via computer code—enabling peer-to-peer collaboration. No company—such as the well-known Kickstarter—would need to operate the platform, facilitate connections between users of the platform, or custody funds. Rather, the developer is building software that would achieve those functions on an entirely decentralized and disintermediated basis. Before the developer could publish the software and make it available to the public, the Department of Justice brought criminal charges—felonies—against two developers of other decentralized software for unlicensed money transmission—even though the other developers never had custody of, or access to, any funds transacted through the software that they wrote.

In the wake of these prosecutions, instead of publishing the software, for fear of later facing criminal charges himself, the decentralized crowdfunding software developer sued the Department of Justice, seeking a declaration that it is not illegal to write and publish code that builds tools for use by other people.[1] *The lawsuit stands for more than just pursuit of clarity, however. The lawsuit makes a larger policy point: by targeting open-source code and developers of that code—even though the code only executes software operations and does not take custody of any funds—federal regulatory policy has not only limited access to key existing digital public infrastructure that provides public goods, but has also chilled the willingness of other developers to build additional digital infrastructure. Because decentralized digital infrastructure is needed to usher in the next phase of digital commerce, these legal battles represent more than mere lawsuits. The three cases—two criminal and one civil—represent a battle over individual rights and autonomy and core aspects of national economic and innovation policy.*

1. This opening example is based on the true story of Michael Lewellen and his lawsuit filed on January 16, 2025. *See generally* Complaint, Lewellen v. Bondi, No. 25-cv-00030-Y (N.D. Tex. Jan. 16, 2025) (bringing a declaratory judgment action against the U.S. Attorney General).

Picking up on the policy importance of the issue, in both 2025 and 2026, the Blockchain Regulatory Certainty Act (BRCA) was introduced for consideration by the U.S. Congress, which introduces protections for decentralized software developers so that they no longer need to fear prosecution for developing peer-to-peer open-source software. Up to this point, however, misunderstandings around how the technology works and inapt analogies have prevented regulatory and legal clarity in the DLT industry. Indeed, even as lawmakers considered the BRCA, another proposal circulated on Capitol Hill that would deem developers to be controllers of the open-source software they build for legal liability purposes. This conflict became a point of contention as the Senate worked to build market structure draft bill in 2025 and again in 2026 to correspond with the House's Clarity Act. As a result, developers should not rest comfortably until lawmakers and regulators adopt a broader, and more predictable legal framework that distinguishes the functional roles played by developers of public open-source DLT protocols from centralized businesses that build on top of those protocols and apportions liability accordingly.

To resolve this quandary, this Article proposes a functional regulatory framework that recognizes the inherent characteristics of open-source Layer-1 DLT protocols and open-source Layer-2 smart contract protocols as digital infrastructure. In particular, this Article makes a novel contribution to the on-going scholarly analysis of open-source protocols as digital infrastructure by surveying the functional methods proposed for financial regulation and used in commercial law, comparative law, and legal approaches to artificial intelligence, and crafting five key principles for engaging in functional regulation of the DLT industry. This Article makes this novel proposal in three parts. Part II explores the treatment of the internet and network protocols as infrastructure and argues that open-source Layer-1 DLT protocols and open-source Layer-2 smart contract protocols similarly operate as infrastructure. Ultimately, Part II places open-source DLT protocols and Layer-2 smart contract protocols within this historical context as the next wave of open-source digital infrastructure development. Part III acknowledges that initial regulatory approaches to the DLT industry adopted a functional method, and then traces a shift in the legal treatment of DLT protocols away from a functional regulatory approach to uniform application of financial regulation designed for intermediated finance. As it does so, Part III explores the inherent mismatch between existing highly intermediated financial regulation

and highly disintermediated open-source blockchain protocols. Part IV develops a framework for functional regulation in two respects. First, Part IV recommends regulatory process adjustments that would put the functional approach to work in simple, but impactful and concrete ways. Second, Part IV outlines five key principles of functional regulation for lawmakers and their policy teams to use as they continue to confront the changing landscape presented by an increasingly decentralized and disintermediated commercial era. A final section concludes that embracing functional regulation for the DLT industry will not only preserve access to open-source Layer-1 DLT protocols and Layer-2 smart contract protocols as the digital infrastructure that they are, but may also help lawmakers and regulators craft a careful and coordinated policy for other emerging technologies—including, for example, artificial intelligence—that increasingly play a crucial and strategic role in innovation and economic development in the United States.

I. INTRODUCTION

1.6 billion people around the world use a virtual private network (VPN) when transacting over the internet to protect themselves from tracking and exploitation by fraudsters.[2] Indeed, in the legal field, many consider use of VPN technology to be a key tool in satisfying a lawyers' duty of confidentiality under the Rules of Professional Conduct.[3] And yet, nearly 30 years ago, the law attempted to stomp the foundational technology underlying modern-day VPN software out of existence and jail its creator. Allow us to explain: this is the story of the "Pretty Good Privacy" (PGP) software[4] and the original Cypher Wars, a story that will soon sound all too similar to modern day happenings in decentralized open-source software.

At the dawn of the internet age, personal computers became household items, along with widespread use of modems, fax machines, the internet, email, and cell phones, and a host of other modern technological marvels.[5] But as people reaped the personal and business benefits of modern communications technology, the law struggled to adapt in a variety of ways.[6] In particular, privacy law struggled to adequately address law enforcement's new capacity for surveillance of digital communication.[7] Indeed, the U.S.

---

2. Chauncey Crail, *Top VPN Statistics and Trends*, FORBES: ADVISOR (Feb. 29, 2024, at 09:52 ET), https://www.forbes.com/advisor/business/vpn-statistics/ [https://perma.cc/6LHT-TW5S].

3. *See* Michael Gargiulo, *Protecting Attorney-Client Privilege with a VPN*, FORBES: INNOVATION (Sep. 4, 2019, at 07:30 ET), https://www.forbes.com/councils/forbestechcouncil/2019/09/04/protecting-attorney-client-privilege-with-a-vpn/ [https://perma.cc/NQ3X-RFJU].

4. "PGP is commonly used to secure communication over VPNs . . . which allow users to connect to a private network over the internet. VPNs use PGP to establish an encrypted connection between the client (the user's device) and the server, which helps to protect against snooping and other types of attacks." *PGP*, VPN TRANSPARENCY PROJECT, https://whoisyourvpn.com/glossary/pgp/ [https://perma.cc/M4EN-CY5Y] (last visited July 28, 2025).

5. *See Promotion of Commerce Online in the Digital Era Act of 1996, or "Pro-Code" Act: Hearing on S. 1726 Before the Subcomm. on Sci., Tech., & Space of the S. Comm. on Com., Sci. & Transp.*, 104th Cong. 8 (1996) [hereinafter *Hearing on S. 1726*] (statement of Philip R. Zimmermann, Chairman & Chief Tech. Officer, Pretty Good Privacy, Inc.).

6. *See, e.g.*, Eric C. Hawkins, Note, *General Jurisdiction and Internet Contacts: What Role, If Any, Should the* Zippo *Sliding Scale Test Play in the Analysis?*, 74 FORDHAM L. REV. 2371, 2382–89 (2006); Denis T. Rice & Julia Gladstone, *An Assessment of the Effects Test in Determining Personal Jurisdiction in Cyberspace*, 58 BUS. LAW. 601, 603 (2003); Eric Goldman, *Content Moderation Remedies*, 28 MICH. TECH. L. REV. 1, 20–23 (2021); Kyle Langvardt, *Regulating Online Content Moderation*, 106 GEO. L.J. 1353, 1358 (2018); Philip J. Weiser, *The Future of Internet Regulation*, 43 U.C. DAVIS L. REV. 529, 531–36 (2009).

7. *See Email Privacy Act: Hearing on H.R. 699 Before the H. Comm. on the Judiciary*, 114th Cong. 20–21 (2015) (statement of Rep. John Conyers, Ranking Member, H. Comm. on the Judiciary).

attempted to require communication technology manufacturers to install back-doors into their products to give law enforcement access to data whenever they wanted.[8] In fact, the 1994 Digital Telephony bill required phone companies to install technology that enabled easier wiretapping.[9]

Worried that "new technologies [would] give the government new automatic surveillance capabilities that Stalin could never have dreamed of," software developers searched for privacy-protecting tools that could enable individuals to resist digital encroachment on their privacy rights.[10] In 1991, Phillip Zimmerman created software called "Pretty Good Privacy" or "PGP," which enabled individual internet users to protect their messages and data while communicating online through the use of public-key cryptography.[11] Later that year Zimmermann released PGP to the world as free and open-source[12] software.[13] By 1993, Zimmerman was under federal investigation; he was subjected to a federal criminal investigation for alleged violations of the International Traffic in Arms Regulations, which prohibited the exportation of "munitions," a term broad enough to include cryptographic software like PGP.[14]

8. *See Hearing on S. 1726, supra* note 5, at 10.

9. *See id.*

10. *See id*.

11. Ronald Bailey, *Technology: Code Blues*, REASON (May 1, 1994), https://reason.com /1994/05/01/ code-blues/ [https://perma.cc/KPV3-LJ2M].

12. Although often used interchangeably, free software and open-source software are two terms with distinct meanings. *See infra* note 28. PGP is both free software—because Zimmerman gave away the software at no cost—and now open-source software—because the most widely used versions of PGP are built as open-source software compliant with the OpenPGP standard, including GNU Privacy Guard which is distributed under the GNU General Public License by the Free Software Foundation. *See, e.g*., Philip Zimmermann, *PGP Marks 10th Anniversary* (June 5, 2001), http://philzimmermann.com/EN/essays/PGP_10th Anniversary.html [https://perma.cc/Q3WU-WTPT] (describing the day, June 5, 1991, that Philip Zimmermann first gave the PGP software away to his friends for free and how he asked them to post it to certain Usenet newsgroups for others to access it for free); *A Comprehensive Guide to GnuPG on Linux*, LINUXVOX.COM (Jan. 16, 2026), https://linuxvox.com/blog/gnupg-linux/ [https://perma.cc/H572-WHSZ] ("GnuPG (GNU Privacy Guard), often referred to as GPG is a free and open-source implementation of the OpenPGP standard.").

13. Steven Levy, *Cypher Wars: Pretty Good Privacy Gets Pretty Legal*, WIRED (Nov. 1, 1994, at 12:00 ET), https://www.wired.com/1994/11/cypher-wars/ [https://perma.cc/UZM2-DMEV].

14. *See, e.g.*, Sandy Shore, *Feds Target Software Expert Who Developed Code to Encrypt Data*, L.A. TIMES: TECH. & INTERNET (Aug. 14, 1994, at 00:00 PT), https://www.latimes.com/ archives/la-xpm-1994-08-14-me-26991-story.html [https://perma.cc/U9HS-M5EV]; Bailey, *supra* note 11.

The International Traffic in Arms Regulations were enacted as implementing regulations for the Arms Export Control Act of 1976,[15] and were intended to keep U.S. military grade weapons out of the hands of Cold War enemies abroad.[16] Faced with a new threat to its surveillance capacity,[17] law enforcement applied a twenty-year-old law designed to protect military-grade weapons to an entirely new context: open-source software that enabled private digital communications.[18] The public, however, spoke out against the obvious overreach of applying a Cold War-era weapons regulation to an open-source software tool and its developer.[19] Ultimately, the federal government closed its investigation without charges in 1996[20] and PGP became the backbone of modern encryption technology that private individuals and entities use to this day.[21] Unfortunately, these Cypher Wars of the 1990s did not end the fight waged by open-source software against government encroachment upon individual rights to privacy. Indeed, an eerie repeat of the PGP Cypher War is playing out in the modern context of government attempts to apply traditional financial regulation to open-source distributed ledger technology (DLT) protocols.[22]

Open-source DLT protocols and open-source software built on top of such protocols enable private individuals to recapture a measure of financial autonomy by providing the technical infrastructure that enables

15. *U.S. Export Laws*, UNIV. OF MD.: DIV. OF RSCH., https://research.umd.edu/rso/export-control/us-export-laws [https://perma.cc/6PBG-BYMN] (last visited Aug. 30, 2025).

16. *See* Krista Viksnins, *US Bureaucracy Is Blocking Arms for Ukraine*, CTR. FOR EUR. POL'Y ANALYSIS (July 5, 2024), https://cepa.org/article/us-bureaucracy-is-blocking-arms-for-ukraine [https://perma.cc/PST5-B3PU].

17. *See* Levy, *supra* note 13 ("Since its free release into the Net world in June 1991, PGP has become the bane of law enforcement officials, who say it lets criminals and would-be terrorists hide the evidence of their illegal activities.").

18. *See* Gareth Halfacree, *Cryptography Whizz Phil Zimmermann Looks Back at 30 Years of Pretty Good Privacy*, REGISTER, (June 17, 2021, at 17:01 UTC) https://www.theregister.com/2021/06/08/pgp_at_30/ [https://perma.cc/PKC8-NUHY].

19. *See, e.g.*, Bailey, *supra* note 11.

20. *See Feds Drop Charges in Encryption Case*, CNET (Jan. 11, 1996, at 16:30 PT), https://www.cnet.com/tech/services-and-software/feds-drop-charges-in-encryption-case/ [https://perma.cc/88V6-DM3K].

21. *See What Is a PGP Encryption*, MEDIUM (Oct. 28, 2022), https://nfting.medium.com/what-is-a-pgp-encryption-460acb8c143 [https://perma.cc/DDS7-VZRW].

22. The term Distributed Ledger Technology protocol or DLT protocol refers to the broad category of technology that blockchain protocols, as well as protocols such as R3's Corda or Hedera's hashgraph network that do not strictly fit the blockchain protocol model of a chain of "linked blocks" of state change data. For further explanation of the technology and the features that make functional regulation the appropriate approach to related law and policy, see *infra* notes 60–80 and accompanying text.

disintermediated digital financial transactions.[23] The modern-day federal government routinely attempts to apply financial regulation designed for an intermediated financial system to open-source DLT protocols that create peer-to-peer infrastructure.[24] Instead of justifying this approach with worries about affording communications privacy to Russian spies, the modern enforcement apparatus justifies applying financial regulation to open-source software in order to prevent criminals and terrorists from exploiting it for illicit finance.[25] Just as export control laws were an ill-fitting tool for combatting the cold war in the internet era, modern financial regulation is an ill-fitting tool for combatting illicit digital finance in today's decentralized digital era.

Instead of using a system of regulation designed for an intermediated industry as a one-size-fits-all solution to regulation, this Article argues that the increased adoption of decentralized infrastructure for digital activity requires functional regulation.[26] Functional regulation requires crafting regulation by first "examining the functionality of a process or application

23. Carla L. Reyes, *Law's Detrimental Reliance on Intermediaries*, 92 GEO. WASH. L. REV. 1343, 1354–57 (2024).

24. Press Release, U.S. Dep't of Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916 [https://perma.cc/G7T6-WEEK]; Sealed Indictment at 31–34, United States v. Storm, No. 23-CRIM-430 (N.D.N.Y. Aug. 21, 2023) (charging two of the software developers who began the Tornado Cash open-source software project with conspiracy to commit money laundering, operating an unlicensed money transmission business, and sanctions violations); *Cyber-Related Designation: Specially Designated Nationals List Update,* U.S. DEP'T OF THE TREASURY: OFF. OF FOREIGN ASSETS CONTROL (Aug. 8, 2022), https://ofac.treasury.gov/recent-actions/20220808 [https://perma.cc/W3FH-XUE8] (original designation of Tornado Cash); Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 Fed. Reg. 72701, 72702 & n.18, 72707–09 (proposed Oct. 23, 2023); Samuel D. Boro et al., *CFPB Proposes Rule to Expand Regulation E to Crypto and Gaming Accounts*, PERKINS COIE: UPDATES (May 21, 2025), https://perkinscoie.com/insights/update/cfpb-proposes-rule-expand-regulation-e-crypto-and-gaming-accounts [https://perma.cc/XV2A-5E98].

25. *See* U.S. GOV'T. ACCOUNTABILITY OFF., GAO-23-105346, BLOCKCHAIN IN FINANCE: LEGISLATIVE AND REGULATORY ACTIONS ARE NEEDED TO ENSURE COMPREHENSIVE OVERSIGHT OF CRYPTO ASSETS 23–25 (2023).

26. In an earlier work, one of the authors suggested that functional regulation could offer a path forward, saving elaboration on that proposal for later research. *See* Reyes, *supra* note 23, at 1389–90. This Article aims to begin the deeper conversation about what functional regulation for blockchain infrastructure might look like in more concrete terms. Indeed, one of the authors has been urging the use of the functional method when evaluating issues at the intersection of law and blockchain since 2016. Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191, 224–27 (2016). To advance the theory and address an ever-pressing real-world problem, this Article moves beyond the generalizations of this earlier work and examines more specifically why and how to approach functional regulation in relation to open-source Layer One protocols as an alternative to financial regulation specifically.

without worrying about the details of its internal structure."[27] A functional legal regime would calibrate its regulatory approach to the function that actors and technology play in commerce. For example, open-source software that acts as digital infrastructure to support any number of different types of activity, including disintermediated financial transactions, would not be subject to rules designed for financial intermediaries, while broker-dealers who use the infrastructure to transact on behalf of others would be subject to such rules. Using open-source Layer-1 DLT protocols and open-source Layer-2 smart contract protocols as case studies, this Article unpacks a framework for functional regulation, in three Parts.

Part II outlines the history of law's interaction with open-source software, highlighting law's tradition of approaching open-source software functionally and the long-familiar open-source ethos of creating rights-protecting software infrastructure as new technology changes the face of commerce. In particular, Part II examines the treatment of the internet and network protocols as infrastructure and argues that open-source Layer-1 DLT protocols and open-source Layer-2 smart contract protocols similarly operate as infrastructure. Ultimately, Part II places open-source DLT protocols and Layer-2 smart contract protocols within this historical context as the next wave of open-source digital infrastructure development and uncovers how regulatory efforts related to DLT initially followed a functional approach by focusing on activity undertaken using infrastructure but maintaining open access to the infrastructure itself.

Specifically, various financial regulation enforcement agencies initially seemed to acknowledge the infrastructural nature of Layer-1 DLT protocols and certain Layer-2 smart contract protocols by adopting regulatory guidance that centered on activity and excepted infrastructure. Part III traces the shift in the legal treatment of DLT protocols from a functional regulatory approach that governed activities of individuals and entities to the application of financial regulation designed for intermediated finance directly to code. Part III explores the inherent mismatch between the existing highly intermediated financial regulatory regime and highly disintermediated open-source DLT protocols. Further, Part III uses several case studies to argue that blindly applying existing financial regulation to DLT protocols both fails to achieve stated policy goals and undermines long-term technological innovation.

Part IV develops a framework for functional regulation in two respects. First, Part IV recommends regulatory process adjustments that would put the functional approach to work in simple, but impactful and concrete ways. Second, Part IV outlines five key principles of functional financial regulation

27. Steven L. Schwarcz, *Regulating Financial Change: A Functional Approach*, 100 MINN. L. REV. 1441, 1445 (2016).

for lawmakers and their policy teams to use as they continue to confront the changing landscape of finance in an increasingly decentralized and disintermediated era. A final section concludes that embracing functional regulation, first for open-source Layer-1 DLT protocols and open-source Layer-2 smart contract protocols, and then more broadly for other emerging technology may offer an underappreciated avenue for combatting systemic risks to both traditional and emerging decentralized technology systems.

II. TRADITIONALLY, THE LAW TAKES A FUNCTIONAL APPROACH TO OPEN-SOURCE SOFTWARE.

The long and fruitful U.S. history with open-source software development offers lessons for developing a modern-day legal regime for open-source Layer 1 blockchain protocols and certain open-source Layer-2 smart contract protocols. Specifically, the law's approach to open-source software and their communities as a form of commons resulted in a functional approach to issues at the intersection of law and open-source software. This Part examines the history of free and open-source software development in the United States, emphasizing the mostly hands off approach law adopted with regard to the code itself. This Part also highlights the impact that understanding and characterizing open-source network protocols (like the internet) as digital infrastructure had on policy debates. This Part then considers the technical realities of open-source Layer-1 distributed ledger technology (DLT) protocols and open-source Layer-2 smart contract protocols and argues that they fit the various definitions of infrastructure resources and infrastructural services that justified the preservation of open-access digital technologies during the early policy debates at the emergence of the internet. Layer-1 DLT protocols and Layer-2 smart contract protocols represent the next wave of open-source digital infrastructure development. As the law develops with regard to DLT protocols, it should be guided by the same functional approach historically used for activity conducted via the internet and other open-source software protocols.

A. The Seemingly Forgotten History of the Law's Approach to Open-Source Digital Infrastructure Development.

Free and open-source software[28] enjoy a lengthy commercial, economic, and legal history in the United States.[29] Indeed, during the last four decades,[30] open-source software has formed the basis of some of the most important technological advances in computing that modern society currently enjoys.[31] For example, the Linux operating system (which currently powers the Android platform),[32] email, the World Wide Web, Internet Relay Chat, and many other programs that enable much of the activity undertaken via today's internet were developed as open-source software by communities of volunteer developers.[33] Many such communities create these software innovations through a governance structure that eschews the traditional hierarchy of most

28. Although often used interchangeably, the terms "open-source software" and "free software" reflect very different meanings to the communities that use those terms. Open-source software generally refers to software that is available without an economic cost, while free software refers to software imbued with certain ideals. *See* Yochai Benkler, *Coase's Penguin, or Linux and* The Nature of the Firm, 112 YALE L.J. 369, 371 n.2 (2002); Siva Vaidhyanathan, *Open Source as Culture—Culture as Open Source*, 2005 OPEN SOURCE JAHRBUCH 359, 359 n.1 (Ger.) (tracing the beginning of the open-source software movement to Richard Stallman's work in the late 20th century). Although many Layer-1 blockchain protocols and many Layer-2 smart contract protocols reflect libertarian and cypherpunk values, it is not possible to declare that every blockchain protocol does. As a result, we adopt the term open-source software in this Article to broadly encompass any blockchain protocol that is made available under an open-source software license, irrespective of any political ideals anyone may attribute to the community surrounding the open-source code.

29. *See* David McGowan, *Legal Implications of Open-Source Software*, 2001 U. ILL. L. REV. 241, 260 (2001) (dating the beginning of the free and open-source software movement to the 1970s); Eric von Hippel & Georg von Krogh, *Open-Source Software and the "Private-Collective" Innovation Model: Issues for Organizations Science*, 14 ORG. SCI. 209, 209 (2003) (dating the free and open-source software movement to the 1960s and 1970s).

30. *See* Vaidhyanathan, *supra* note 28, at 360; David Bretthauer, *Open-Source Software: A History*, 21 INFO. TECH. & LIBRS. 3, 4 (2002) (tracing the beginning of the open-source software movement to Richard Stallman's work on GNU in the 1970s).

31. *See* Vaidhyanathan, *supra* note 28, at 360.

32. *See* Colin Walls, *Android, Linux and Real-Time Development for Embedded Systems*, DESIGN & REUSE: INDUS. ARTICLES (June 16, 2011), https://www.design-reuse.com/articles/23806/android-linux-embedded-systems.html [https://perma.cc/58EE-SMHM] ("In practical terms, Android is an application framework on top of Linux, which facilitates its rapid deployment in many domains."). Notably, the Android kernel itself is open-source. *Id.* ("Android is open source and a majority of the source is licensed under Apache2, allowing adopters to add additional proprietary value in the Android source without source distribution requirements.").

33. Vaidhyanathan, *supra* note 28, at 362. Vaidhyanathan then goes further to claim "just about every other activity on the Internet all emerged from community-based project teams, often ad-hoc and amateur." *Id.*

organizations.[34] Although projects are often followed by a foundation, the structure of the community that contributes to the open-source code is not generally dictated by the foundation.[35] Further, although many commercial entities put open-source software to use in the products and services they offer to consumers, thereby profiting from the existence of the software, many of the contributors to open-source projects do not.[36] Irrespective of why open-source software developers contribute to specific projects, the reality is that open-source software powers core components of modern computing software such as HTML,[37] Apache,[38] Linux,[39] virtual private networks,[40] and email,[41] among others.

Notably, most of the key examples of open-source software that fuel the modern economy act as tools and platforms that enable others to further develop applications downstream. With a few notable exceptions, law has historically actively resisted direct regulation of such open-source software

34. *See* GEORGE DAFERMOS, GOVERNANCE STRUCTURES OF FREE/OPEN SOURCE SOFTWARE DEVELOPMENT 187 (2012).

35. *See* Jan-Felix Schrape, *Open-Source Projects as Incubators of Innovation: From Niche Phenomenon to Integral Part of the Industry*, 25 CONVERGENCE 410, 416–17, 422 tbl. 5 (2017) (listing key open-source projects operating under an umbrella foundation and explaining the role of the umbrella foundation, which, "while not directly in control of the development activities, nevertheless provide[s] the technical infrastructures [and] distribute[s] financial resources").

36. Benkler, *supra* note 28, at 372–73 ("Programmers do not generally participate in a[n open-source] project because someone who is their boss instructed them, though some do. They do not generally participate in a project because someone offers them a price, though some participants do focus on long-term appropriation through money-oriented activities, like consulting or service contracts. But the critical mass of participation in projects cannot be explained by the direct presence of a command, a price, or even a future monetary return, particularly in the all-important microlevel decisions regarding selection of project to which participants contribute.").

37. *See* TIM BERNERS LEE, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB BY ITS INVENTOR 40–44 (1999) (detailing, among other things, the open-source development of HTML as led by Tim Berners-Lee).

38. APACHE SOFTWARE FOUND., https://apache.org/ [https://perma.cc/UCV7-2LDP] (last visited Aug. 29, 2025).

39. *See* Bretthauer, *supra* note 30, at 5 (detailing the history of Linux's open-source development).

40. *See PGP*, *supra* note 4 (explaining that open-source software PGP forms a key component of many VPN software solutions); Miklos Zoltan, *The Evolution of VPN Technology: From Dial-Up to Modern Encryption*, PRIV. AFFS. (June 18, 2024), https://www.privacyaffairs.com/evolution-of-vpn-technology/ [https://perma.cc/V2UM-MA34] (discussing the importance of OpenVPN to making VPN technology available widely).

41. *See* Tom Van Vleck, *Electronic Mail and Text Messaging in CTSS, 1965–1973*, IEEE ANNALS HIST. COMPUTING, Jan.–Mar. 2012, at 4, 4–5 (explaining that Van Vleck's development of an email software in the 1960s laid the groundwork for modern email).

because it fulfills the function of infrastructure.[42] The plain meaning of the word "infrastructure," is, according to one source, "The underlying framework of a system; esp., public services and facilities (such as highways, schools, bridges, sewers, and water systems) needed to support commerce as well as economic and residential development."[43] Indentifying when open-source software acts as infrastructure in the digital environment requires determining when open-source software acts as "the underlying framework" for a networked system. Making that determination requires identifying which functions make some open-source software infrastructural in nature.

Infrastructure, broadly speaking, has long been included in the study of commons management.[44] Initially, industrial infrastructure featured prominently as the object of commons management discussion in both law and economics.[45] With the emergence of the internet, open-sourced software, and an increasingly networked economy, both legal scholars and economists began to explore the application of the law and economics of the commons to cyberspace.[46] In exploring the congruence between commons literature and the internet, Professor Yochai Benkler explained that the core element of a commons was "the absence of asymmetric power to determine disposition of

---

42. *See, e.g.*, Steve Winslow, Mike Dolan & Jason Perlow, *Understanding US Export Controls with Open Source Projects*, LINUX FOUND., https://www.linuxfoundation.org/resources/publications/understanding-us-export-controls-with-open-source-projects [https://perma.cc/7WLV-CW6W] (last visited Sep. 14, 2025) (explaining that open-source technologies are not subject to U.S. Export Administration Regulations); McGowan, *supra* note 29, at 241–42 (noting that the open-source community "seems to operate in the absence of traditional legal principles" and that while traditional legal principles like copyright do apply, they are "employed in creative ways not previously envisioned").

43. *Infrastructure*, BLACK LAW'S DICTIONARY (7th ed. 1999); *see also Infrastructure*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/infrastructure [https://perma.cc/8MYR-TUFT] (last visited July 23, 2025) ("1. The system of public works of a country, state, or region; *also*: the resources (such as personnel, buildings, or equipment) required for an activity; 2. The underlying foundation or basic framework (as of a system or organization) . . . .").

44. *See* Yochai Benkler, *Commons and Growth: The Essential Role of Open Commons in Market Economies*, 80 U. CHI. L. REV. 1499, 1499–50 (2013) (reviewing BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES (2012)). Commons management refers to the way that communities govern (or manage) a pool of shared finite resources (referred to as "the commons"). *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 1 (1990).

45. *See, e.g.*, Carol Rose, *The Comedy of the Commons: Custom, Commerce, and Inherently Public Property*, 53 U. CHI. L. REV. 711, 722 (1986).

46. *See, e.g.*, Brett M. Frischmann, *An Economic Theory of Infrastructure and Commons Management*, 89 MINN. L. REV. 917, 1008–09 (2005); BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES 317–57 (2012) [hereinafter FRISCHMANN, INFRASTRUCTURE]; Benkler, *supra* note 44, at 1517 ("In 2005, Frischmann first began to reconnect the work on the Internet and public domain to the kinds of physical commons with which Rose had begun the conversation.").

a resource."[47] Indeed, many scholars argued that the commons nature of the internet was the driving force behind the productivity and creativity exploding in cyberspace.[48] This analysis leads to a policy view that digital infrastructure, as commons, should be protected as open-access tools that can be used by everyone.[49]

To determine which open-source software to protect as commons because of their infrastructural nature, Professor Brett Frischmann proposed a paradigm for "identify[ing] and evaluat[ing] infrastructure resources functionally," through the following three criteria:

> (1) The resource may be consumed nonrivalrously for some appreciable range of demand. (2) Social demand for the resource is driven primarily by downstream productive activity that requires the resource as an input. (3) The resource may be used as an input into a wide range of goods and services, which may include private goods, public goods, and social goods.[50]

If a resource can be classified as infrastructure using these criteria, "then there are strong economic arguments that the resource should be managed in an openly accessible manner,"[51] leading to a legal approach to infrastructure resource technology that protects access to the open-source software and regulates individuals and entities conducting certain activity via the software.

By way of example, take the email protocol—the Simple Mail Transfer Protocol (SMTP).[52] The SMTP defines the rules by which one machine routes and sends a message to another machine.[53] SMTP can be used nonrivalrously

47. Benkler, *supra* note 44, at 1517.

48. *See, e.g.*, Yochai Benkler, *The Battle over the Institutional Ecosystem in the Digital Environment*, COMMC'NS ACM, Feb. 2001, at 84, 88 ("The capacity of thousands to scour a rich universe of existing information resources allows them to identify productive opportunities and the creative individuals who can best use these resources. That capacity is the primary source of increasing productivity gains that peer production offers our economy."); LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 147–76 (2001).

49. *See* Divya Siddarth & E. Glen Weyl, *The Case for the Digital Commons*, WORLD ECON. F. (June 2, 2021), https://www.weforum.org/stories/2021/06/the-case-for-the-digital-commons/ [https://perma.cc/DJL2-CGS3]. "Classic examples of infrastructure include roads and other transportation networks, telecommunications networks, the natural environment, ideas, and languages." James Grimmelmann & A. Jason Windawi, *Blockchains as Infrastructure and Semicommons*, 64 WM. & MARY L. REV. 1097, 1105 (2023).

50. FRISCHMANN, INFRASTRUCTURE, *supra* note 46, at xiv. The third criteria goes to the genericity of the infrastructure, meaning that "analysis of the resource cannot be assimilated to the analysis of its sole productive use." Grimmelmann & Windawi, *supra* note at 49.

51. FRISCHMANN, INFRASTRUCTURE, *supra* note 46, at 923.

52. *Beginner's SMTP Guide*, SOCKETLABS (Aug. 12, 2022), https://www.socketlabs.com/blog/beginners-smtp-guide/ [https://perma.cc/D5X6-Q75L].

53. *See id.*

by many people—nearly everyone sends email throughout the day, without any thought to whether others are also sending emails. Demand for use of SMTP is driven primarily by downstream commercial and personal activity[54]—we send emails to conduct business and to communicate with friends and family. As we do so, we very rarely consider the fact that our activity reflects a high level of demand for SMTP. Further, SMTP is used by actors as inputs into "a wide range of goods and services"[55] that includes the provision of corporate services (private goods), government services (public goods), and personal communication (social goods). Under Frischmann's functional framework for identifying infrastructure resources, SMTP is a digital infrastructure resource.

Now, imagine you operate a health care company that delivers medical supplies to remote regions by drone. You hold a long-term vendor contract with a local manufacturer of drones, and regularly place orders for parts and replacement drones as needed to ensure continued delivery of medical supplies to your rural health care provider clients. The vendor, in turn, emails you a monthly invoice for goods delivered. The order and invoice process has become so routinized over time that you barely read the email delivering the invoice anymore, you just forward it to accounting for payment. Last month, as it turns out, the invoice came via email in the usual manner, but from a slightly altered email address, and instructed payment be made to a bank account other than one to which you normally direct payment. But you didn't really notice these changes and you forwarded it to accounting as always, and accounting assumed that meant the payment was approved and sent a significant sum of your company's money to the new bank account contained in the invoice. Several weeks later, you receive what you believe is a duplicate invoice from the vendor, only to realize the mistake—your company has been the victim of a business email compromise—or a BEC scam—and you directed payment to a fraudster.

You immediately report these events to the police, who, luckily enough, track down the fraudster and charge the fraudster with theft and wire fraud, and begin a wider investigation into the fraudster's illegal activities. You deal with the recovery of funds through separate means, but you find the criminal action just and satisfying. The fraud that victimized you and your company, of course, was all perpetrated through the use of email, and email only works because of the digital resource infrastructure known as SMTP. The fraudster could not have stolen your money without SMTP enabling the operation of email. At no point, however, does it occur to you to try and prosecute the

54. *See* Bettina Specht, *Everything You Need to Know About SMTP (Simple Mail Transfer Protocol)*, POSTMARK (Sep. 13, 2022), https://postmarkapp.com/guides/everything-you-need-to-know-about-smtp [https://perma.cc/VCH5-FJRA].

55. FRISCHMANN, INFRASTRUCTURE, *supra* note 46, at xiv.

developers of the SMTP for building the tool used by the fraudster to perpetrate the scam, as they built a digital infrastructure resource and played no part in the use of that resource to commit fraud. Rather, the criminal law applies to the perpetrator of the BEC scam, not the digital tool—the digital infrastructure resource—that the perpetrator used as the medium for the scam.

Told as a story this way, the outcome makes intuitive sense. But the story also reflects the deeper theoretical point that digital infrastructure resources are traditionally regulated functionally—with the activity undertaken via the digital infrastructure serving as the object of regulation, and the infrastructure itself being preserved for open-access as a commons resource used by many people and entities for many different purposes.[56] Like their digital protocol predecessors, DLT protocols have been recognized as digital infrastructure resources,[57] and to understand why the application of financial regulation to such protocols makes so little sense, we first turn to the features and infrastructural functions of open-source Layer-1 DLT protocols and Layer-2 smart contract protocols.

B. Open-Source Layer-1 Distributed Ledger Technology Protocols and Layer-2 Smart Contract Protocols Represent a New Wave of Open-Source Infrastructure Development.

A lot of linguistic confusion surrounds the various components of DLT.[58] This linguistic confusion often leads to the use of metaphors—sometimes apt, sometimes not—which are predominately relied upon during legislative and

56. Admittedly, there are often intense policy debates about *how* to preserve access to commons infrastructure through law. For example, debates about the role of intellectual property in dividing and gatekeeping the internet. *See, e.g.*, Lawrence Lessig, *Intellectual Property and Code*, 11 J. CIV. RTS. & ECON. DEV. 635, 637 (1996); Paul Ganley, *Surviving* Grokster*: Innovation and the Future of Peer-to-Peer*, 28 EUR. INTELL. PROP. REV. 15, 23–25 (2006). The debate about net neutrality and whether it is appropriate for internet service providers to act as gatekeepers in terms of access to the internet offers a second example. *See, e.g.*, FRISCHMAN, INFRASTRUCTURE, *supra* note 46; John Blevins, *The Use and Abuse of 'Light-Touch' Internet Regulation*, 99 B.U. L. REV. 177, 212 (2019). More recently, to the extent the software is embedded in cyber-physical systems, some policy discussion has focused on the potential role of tort liability for physical harm suffered from a malfunctioning hybrid hardware-software product (e.g., an autonomous vehicle). *See* Bryan H. Choi, *Crashworthy Code*, 94 WASH. L. REV. 39, 62–65 (2019). This Article adds a new layer to that debate by addressing how to preserve access to decentralized digital commons infrastructure through law.

57. *See* Grimmelmann & Windawi, *supra* note 49, at 1108–09.

58. *See* Carla L. Reyes, *Emerging Technology's Language Wars: Cryptocurrency*, 64 WM. & MARY L. REV. 1193, 1212–13 (2023); Carla L. Reyes, *Emerging Technology's Language Wars: Smart Contracts*, 2022 WIS. L. REV. FORWARD 85, 87 [hereinafter *Language Wars: Smart Contracts*]; Carla L. Reyes, *The Language Landmines of Blockchain Technology and Cryptocurrency*, *in* THE CAMBRIDGE HANDBOOK ON LAW & POLICY FOR NFTS 39–42 (Nizan Geslevich Packin ed., 2024).

regulatory discussions.[59] As a result, regulatory enforcement actions often apply ill-fitting legal paradigms to technology that, as a matter of technical reality, do not perform regulated activity. To help counter some of the confusion sewn by inapt metaphors for blockchain protocols, this Section offers a brief introduction to blockchain technology, with an emphasis on Layer-1 DLT protocols and certain open-source Layer-2 smart contract protocols. The Section then reorients the discussion of open-source Layer-1 DLT protocols and Layer-2 smart contract protocols to consider their roles as digital infrastructure resources.

Generally speaking, DLT protocols enable decentralized digital activity via demonstrably provable, secure means. Indeed, at the most general level, DLT is a broad term that covers various distributed databases, including a specific type of database referred to as a blockchain protocol.[60] DLT protocols "assume[] the possible presence of malicious users (nodes)" and structure data processing with the goal of thwarting those nodes.[61] "A blockchain protocol—one type of distributed ledger—structures its data in a literal chain of blocks by linking blocks of validated transactions together using one-way

59. *See* Reyes, *Language Wars: Smart Contracts*, *supra* note 58, at 95–96.

60. GARRICK HILEMAN & MICHEL RAUCHS, GLOBAL BLOCKCHAIN BENCHMARKING STUDY 11 (2017), https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-09-27-ccaf-globalbchain.pdf [https://perma.cc/2UVN-H9EZ]. The authors are aware of the continued scholarly and legal debate around appropriate terminology. Without weighing in on the merits of that debate, in this Article, the authors use the term DLT as the broader, umbrella term used to encompass both permissioned and permissionless blockchain protocols, *see id.*, as well as protocols such as R3's Corda and Hedera's hashgraph network, that do not strictly fit the blockchain protocol model of a chain of "linked blocks" that record transitions in state, *see* INDUS. INTERNET CONSORTIUM, DISTRIBUTED LEDGERS IN IIoT 4 (2020), https://www.iiconsortium.org/pdf/Distributed_Ledgers_in_IIoT_White_Paper_2020-07-22.pdf [https://perma.cc/ST5S-3AEG]. To specifically refer to permissionless DLT protocols, including blockchain protocols, the Authors use "open-source DLT protocols." Meanwhile, the Authors use "blockchain protocol" to refer specifically to those distributed protocols that use data structures composed of a cryptographically linked chain of blocked data, *see* HILEMAN & RAUCHS, *supra* note 11, at least at Layer-1. As one of the Authors has emphasized repeatedly elsewhere, it is important for the law to understand that variants of blockchain protocols exist, and blockchain technology is neither monolithic nor static. *See, e.g.*, Carla L. Reyes, *Conceptualizing Cryptolaw*, 96 NEB. L. REV. 384, 390–97 (2017) [hereinafter *Conceptualizing Cryptolaw*]; *Building Blockchain: Exploring Web 3 and Other Applications for Distributed Ledger Technologies: Hearing Before the Subcomm. on Innovation, Data, & Com. of the H. Comm. on Energy & Com.*, 118th Cong. 18 (2023) (statement of Carla L. Reyes, Assoc. Professor of L., SMU Dedman Sch. of L.). However, when considering policy decisions, it is important to take a wide view of whole scope of technology—DLT and blockchain protocols—that might be affected by policy choices. Since both open-source DLT protocols and open-source blockchain protocols can and do serve as digital infrastructure, this Article advances its argument as to the importance of functional regulation with regard to both variants of the technology—protocols that are a literal chain of blocks, and protocols that are not.

61. HILEMAN & RAUCHS, *supra* note 60, at 11, 23.

cryptographic hashes."[62] The architectural choices between using a DLT protocol broadly or a blockchain protocol specifically, along with choices among other specific features, vary widely among different protocols.[63] Although certain blockchain protocols are often held out as the archetypal protocols—Bitcoin and Ethereum—many other DLT protocols with very different features and goals exist.[64]

Nevertheless, DLT technology, as a general matter, is a protocol technology.[65] A protocol is "a set of instructions for the compilation and interaction of objects."[66] In particular, a network protocol simply sets the rules that allow networked computers—nodes—to communicate with each other[67] like the protocols that keep the internet running,[68] or SMTP, the protocol that enables email communication.[69] Similarly, a DLT protocol "sets the rules that enable networked computers to track transitions in the global state of recorded data without a centralized third-party intermediary."[70] DLT and blockchain protocols are commonly referred to as Layer-1 in what is conceptualized as a blockchain technology stack.[71] Conceptualizing DLT protocols as part of a stack of layered technologies is not a metaphor, but rather a technical reality

62. Reyes, *supra* note 23, at 1354 (citing HILEMAN & RAUCHS, *supra* note 60, at 11); *accord* HILEMAN & RAUCHS, *supra* note 60, at 11, 14).

63. Carla Reyes, *Creating Cryptolaw for the Uniform Commercial Code*, 78 WASH. & LEE. L. REV. 1521, 1537–38 (2021).

64. Reyes, *supra* note 23, at 1355.

65. *See id.*

66. ALEXANDER R. GALLOWAY, PROTOCOL: HOW CONTROL EXISTS AFTER DECENTRALIZATION 75 (2004).

67. *See* Will Warren, *The Difference Between App Coins and Protocol Tokens*, MEDIUM (Feb. 2, 2017), https://medium.com/@willwarren89/the-difference-between-app-coins-and-protocol-tokens-7281a428348c [https://perma.cc/8TQH-XUBF].

68. The Internet Protocol is a network protocol that defines the digital message formats and rules for communication among connected computers. *See* Mark de Wolf, *Internet Protocol (IP)*, TECHOPEDIA (Sep. 23, 2024), https://www.techopedia.com/definition/5366/internet-protocol-ip [https://perma.cc/M6A9-VTXQ].

69. Email is built on the SMTP protocol, which allows users to communicate with one another: "It's just a way for two computers to talk to one another." Ryan Shea, *When to Use Protocol Tokens*, MEDIUM (Nov. 13, 2017), https://medium.com/@ryanshea/protocol-tokens-1ed44fa89453 [https://perma.cc/7KDD-A4J8].

70. Reyes, *supra* note 23, at 1355 (citing Charles J. Delmotte, *Toward a Blockchain-Driven Tax System*, 43 VA. TAX REV. 37, 51–52 (2023)).

71. *See* Thibault Schrepel, *Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox*, 3 GEO. L. TECH. REV. 281, 306 (2019) (describing Layer-2 as the software layer that sits on top of a Layer-1 DLT protocol); Lewis Gudgeon et. al., *SoK: Layer-Two Blockchain Protocols*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 201, 204 (Joseph Bonneau & Nadia Heninger eds., 2020) (describing Layer 2 as software that scales blockchain transactions without changing the underlying crypto-economics of the Layer 1 protocol).

that mirrors the layered model of the internet stack.[72] Traditionally, the internet is conceptualized as existing in five, or sometimes seven, layers.[73] The five layer model consists of a physical hardware layer, a link layer, a network layer, a transport layer, and an application layer.[74] In the blockchain technology stack, Layer-1 is the DLT or blockchain protocol that serves as the network layer, and Layer-2 encompasses additional software that operates on or interacts with the network.[75] Meanwhile, applications and user interfaces exist at higher layers of the stack.[76]

Just as the protocols that enable the internet and email serve as open-source infrastructure for digital life, DLT and blockchain protocols represent the next wave in open-source digital infrastructure development.[77] In particular, DLT and blockchain protocols offer the infrastructure necessary for users to record transitions in the state of globally recorded data without the intervention of a third-party intermediary.[78] Layer-1 DLT and blockchain protocols fit Professor Brett Frischmann's definition of infrastructure.[79] Open-source DLT and blockchain protocols are nonrivalrous because anyone can record changes in state[80] to the protocol, and anyone—whether they have recorded a state change via the DLT protocol or not—can read the resulting data.[81] Most demand for open-source Layer-1 DLT protocols is for

72. *See* Lawerence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 816 (2004) ("The key innovation-enabling feature of Internet architecture is comprised of layers, narrowly understood as defined by code or broadly understood as functional components of a communication system.").

73. Grimmelmann & Windawi, *supra* note 49, at 1108–09.

74. *Id*. ("For example, the internet is commonly divided into a physical layer (hardware), a link layer (protocols designed for specific kinds of hardware), a network layer (internet protocol, which is universal across the internet, and from whence the 'IP' in 'IP address' derives), a transport layer (for example, protocols such as HTTP that are optimized for classes of applications), and an application layer (for example, Skype, Netflix, or Facebook).").

75. *See* Schrepel, *supra* note 71; Gudgeon et al., *supra* note 71.

76. *See* Reyes, *supra* note 23, at 1356 (citing *Layers of Blockchain Technology*, BLOCKCHAIN COUNCIL (Aug. 21, 2024), https://www.blockchain-council.org/blockchain/layers-of-blockchain-technology/ [https://perma.cc/5HRH-CQV7]).

77. *See* Grimmelmann & Windawi, *supra* note 49, at 1109 (explaining that blockchains are infrastructure and describing "the widespread interest in blockchains").

78. *Id*. at 1102.

79. *See id.* at 1109 ("Blockchains are ledgers, and as such they are infrastructure.").

80. "In computer science, the 'state' of a computer program refers to the content of program data stored in a computer's memory at any given point in the program's execution." Carla L. Reyes, *A Unified Theory of Code-Connected Contracts*, 46 J. CORP. L. 981, 992 (2021) (citing DICTIONARY OF COMPUTER SCIENCE, ENGINEERING, AND TECHNOLOGY 467 (Phillip A. Laplante ed., 2000)). The precise definition of "state" is "in any computation, the current set of values being operated upon." DICTIONARY OF COMPUTER SCIENCE, ENGINEERING, AND TECHNOLOGY 467 (Phillip A. Laplante ed., 2000).

81. *See* Grimmelmann & Windawi, *supra* note 49, at 1110.

downstream productive use—examples of which include, but are not limited to: building decentralized applications,[82] operating decentralized autonomous organizations,[83] creating privacy protecting software,[84] supply chain management,[85] carbon credit tracking,[86] and identity verification.[87] Further, open-source Layer-1 DLT protocols fulfil Frischmann's genericity requirement insofar as the downstream uses to which the protocols are put include private goods,[88] public goods,[89] and social goods.[90] Open-source

82. *See, e.g.*, Andrew Antar, *Hearo.fm to Build JAM Music Token on Hedera Hashgraph Public Distributed Ledger*, MEDIUM (Sep. 4, 2018), https://medium.com/hearo-fm/hearo-fm-to-build-jam-music-token-on-hedera-hashgraph-public-distributed-ledger-1fbdd9dfd89 [https://perma.cc/96S3-MPBZ] (describing a decentralized music streaming marketplace); CRYPTOTASK, https://www.cryptotask.org [https://perma.cc/95VY-9GZQ] (last visited July 28, 2025) (a decentralized task manager application for freelance task workers).

83. *See, e.g.*, MAKERDAO, https://makerdao.com [https://perma.cc/ACA5-EMKV] (last visited Aug. 26, 2025) (a decentralized autonomous organization that facilitates use of a stablecoin—DAI); METACARTEL VENTURE DAO, https://metacartel.xyz [https://perma.cc/P3ND-Y4B5] (last visited July 29, 2025) (a decentralized venture fund).

84. *See* Matthias Nadler & Fabian Schär, *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*, 105 FED. RSRV. BANK. ST. LOUIS REV. 122, 127 (2023).

85. *See, e.g.*, *Australian Agri Supply Chain Launches on Hedera Hashgraph*, HEDERA (Sep. 21, 2020) https://hedera.com/blog/australian-agri-supply-chain-launches-on-hedera-hashgraph [https://perma.cc/932L-MJ4N] (announcing Australia's "first full-service agricultural supply chain platform").

86. *See, e.g.*, *Envision Blockchain and Hedera Revolutionize Carbon Credit Management*, BLOCKNEWS (Dec. 5, 2023), https://blocknews.com/envision-blockchain-and-hedera-revolutionize-carbon-credit-management [https://perma.cc/WP65-2X84].

87. *See, e.g.*, Paul Madsen, *Decentralized Identity on the Hedera Consensus Service*, HEDERA (May 1, 2020), https://hedera.com/blog/decentralized-identity-on-hedera-consensus-service [https://perma.cc/H5MK-2X4Y]; SOVRIN FOUND., SOVRIN™: A PROTOCOL AND TOKEN FOR SELF-SOVEREIGN IDENTITY AND DECENTRALIZED TRUST 9–10 (2018), https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf [https://perma.cc/2H78-JWDM].

88. For an example of tracking transactions in private goods, see Pankaj Dutta et al., *Blockchain Technology in Supply Chain Operations: Applications, Challenges and Research Opportunities*, TRANSP. RSCH. PART E: LOGISTICS & TRANSP. REV., Oct. 2020, at 1, 6 [https://doi.org/10.1016/j.tre.2020.102067].

89. For an example of enabling carbon credit trades that encourage environmental protection, see Seong-Kyu Kim & Jun-Ho Huh, *Blockchain of Carbon Trading for UN Sustainable Development Goals*, SUSTAINABILITY, May (II) 2020, at 1, 9 https://www.mdpi.com/2071-1050/12/10/4021 [https://doi.org/10.3390/su12104021].

90. For an examples of digital art, decentralized social clubs, and decentralized online group games as social goods, see Edward Lee, *NFTs as Decentralized Intellectual Property*, 2023 U. ILL. L. REV. 1049, 1092–94 (2023); Tian Min et al., *Blockchain Games: A Survey*, 2019 IEEE CONF. ON GAMES, Sep. 26, 2019, at 1, 2 (decentralized blockchain-based games). *Cf.* Cédric Sueur, Jean-Louis Deneubourg & Odile Petit, *From Social Network (Centralized vs. Decentralized) to Collective Decision-Making (Unshared vs. Shared Consensus)*, PLOS ONE,

Layer-1 DLT protocols, like the internet and email protocols before them, should be regarded as digital infrastructure resources for which open-access should be protected, while activity undertaken through that access serves as the object of regulation.[91]

Open-source Layer 2 smart contract protocols, for their part, also functionally operate as digital infrastructure resources. A smart contract is one type of computer program commonly deployed on a Layer-1 blockchain protocol.[92] When smart contracts are so deployed, the term smart contract really just refers to computer software that takes some action after receiving some pre-defined data,[93] and then reflects the resulting state change in the history of the blockchain protocol.[94] As a very general matter then, "smart contracts are computer code that says, 'if data is received that X has occurred, Y will execute.'"[95] 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

---

Feb. 29, 2012, at 1, 8 https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0032566 [https://doi.org/10.1371/journal.pone.0032566] (finding an increase in shared consensus as social networks became more decentralized).

91. Others have made similar arguments about what the object of regulation should be in the DLT context—namely, activity taken through DLT, rather than the DLT protocol itself, including one of the authors. *See, e.g.*, Reyes, *supra* note 26, at 224–27 (2016) (proposing a form of co-regulation using the functional method); Reyes, *supra* note 23, *passim* (making the case that the existing and heavily intermediary reliant financial regulatory approach is fundamentally flawed); Miles Jennings, *Regulate Web3 Apps, Not Protocols*, A16ZCRYPTO (Sep. 29, 2022), https://a16zcrypto.com/posts/article/web3-regulation-apps-not-protocols [https://perma.cc/R2MH-H4E8].

92. *See* HENNING DIEDRICH, ETHEREUM: BLOCKCHAINS, DIGITAL ASSETS, SMART CONTRACTS, DECENTRALIZED AUTONOMOUS ORGANIZATIONS 176 (2016) ("In Ethereum, 'smart contract' often just means 'a Solidity script.'"); ANDREAS M. ANTONOPOULOS & GAVIN WOOD, MASTERING ETHEREUM: BUILDING SMART CONTRACTS AND DAPPS 127 (Rachel Roumeliotis et al. eds., 1st ed. 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.").

93. *See* DIEDRICH, *supra* note 92, at 167 ("Smart contracts are decentralized code that [executes] after a condition is fulfilled."); WILLIAM MOUGAYAR, THE BUSINESS BLOCKCHAIN: PROMISE, PRACTICE AND APPLICATION OF THE NEXT INTERNET TECHNOLOGY 42–43 (2016) ("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.").

94. *See* Reyes, *Language Wars: Smart Contracts*, *supra* note 58, at 92–93 (citing Gideon Greenspan, *Why Many Smart Contract Use Cases Are Simply Impossible*, COINDESK (Sep. 11, 2021, at 08:13 ET), https://www.coindesk.com/markets/2016/04/17/why-many-smart-contract-use-cases-are-simply-impossible [https://perma.cc/KF77-WSBC]).

95. Reyes, *supra* note 80, at 987 (citing Richard Gendal Brown, *A Simple Model for Smart Contracts* (Feb. 10, 2015), https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/ [https://perma.cc/2RLK-XE8P]).

conducted through blockchain protocols.[96] Indeed, many smart contracts are designed to be composable, meaning they solve a problem common to many developers and can be integrated into other smart contracts or applications.[97]

Open-source Layer-2 smart contract protocols represent only a subset of the technology often encompassed in a reference to "Layer-2." Broadly speaking, Layer-2 protocols operate on top of a Layer-1 distributed ledger or blockchain protocol, but operate under different parameters that enable a reduction in the processing load borne by the Layer-1 distributed ledger or blockchain protocol.[98] The goal of many Layer-2 solutions is to improve some aspect of the Layer-1 protocol: improve scalability, reduce transaction costs, and enhance privacy.[99] Some uses of the term "Layer-2" in the broader DLT industry actually refer to off-chain scaling solutions.[100] Sometimes, however, a network of smart contracts operates as a protocol at Layer-2. Such smart contract protocols are often built on an open-source basis, with no third-party intermediary to manage their operations.

An example of one such Layer-2 smart contract protocol that has received a lot of recent attention is the Tornado Cash software. "Tornado Cash" refers to a set of smart contracts that interact with one another in ways that allow anyone conducting transactions via the Ethereum blockchain protocol (and theoretically other protocols) to enhance the privacy of their transactions.[101] Why would anyone want to enhance the privacy of their transactions on Ethereum? When an Ethereum user conducts routine transactions on

96. *See 10 Real-World Smart Contract Use Cases*, HEDERA, https://hedera.com/learning/smart-contracts/smart-contract-use-cases [https://perma.cc/BYH2-WBU2] (last visited Sep. 25, 2025).

97. *See Smart Contract Composability*, ETHEREUM (Sep. 3, 2004) https://ethereum.org/en/developers/docs/smart-contracts/composability [https://perma.cc/KY6T-JNMW].

98. *See* Lipsa Das, *What Are Ethereum Layer 2 Blockchains and How Do They Work?*, LEDGER ACAD. (May 12, 2025), https://www.ledger.com/academy/topics/blockchain/what-are-ethereum-layer-2-blockchains-and-how-do-they-work [https://perma.cc/2MX8-JNJM].

99. *See What Is Layer 2?*, ETHEREUM, https://ethereum.org/en/layer-2/learn [https://perma.cc/QW75-R737] (last visited Feb. 14, 2025); *What Are Layer 2 Blockchains and How Do They Work? L1 Vs L2 Networks Explained*, TRANSAK (Sep. 28, 2024), https://transak.com/blog/what-are-layer-2-blockchains-and-how-do-they-work-l1-vs-l2-networks-explained [https://perma.cc/JCD6-NP2S].

100. *See, e.g.*, Scott Nevil, *Layer 1 Vs. Layer 2: The Difference Between Blockchain Scaling Solutions*, INVESTOPEDIA (Mar. 7, 2025), https://www.investopedia.com/what-are-layer-1-and-layer-2-blockchain-scaling-solutions-7104877 [https://perma.cc/483K-38LC].

101. *See* Alex Wade, Michael Lewellen & Peter Van Valkenburgh, *How Does Tornado Cash Work?*, COIN CTR. (Aug. 25, 2022), https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work [https://perma.cc/4VJC-UEY8]; Nadler & Schär, *supra* note 84 ("Tornado Cash is a smart contract-based crypto asset mixer that uses zkSNARKs to create a decentralized privacy-enhancing protocol. The code is open source and has been deployed on various blockchains, most notably Ethereum.").

Ethereum, those transactions are publicly recorded for anyone to see and data mine.[102] If an Ethereum user does not want what is the equivalent of masked versions of their bank account statements available for everyone to see, the user transacts funds to a Tornado Cash public key address that is operated by a pool and then withdraws them at a later time to a public key address different from depositing wallet's public key address.[103] The depositing wallet is given a private key, which acts like a passcode or receipt insofar as the user may present the private key to the smart contract operated Tornado Cash pool at a later date as proof of the right to withdraw the deposited funds at a later time.[104]

One drawback of the Tornado Cash deposit and later withdrawal process, however, is that because anyone who executes a transaction on the Ethereum protocol must pay a transaction fee, every deposit to and withdrawal from a Tornado Cash smart contract requires a fee payment.[105] Paying the fee at initial deposit, and again at withdrawal risks revealing the pseudonymous identity of the user, making the increased privacy to be obtained by using Tornado Cash difficult to achieve. To try and solve for this technical obstacle to transactional privacy, users may choose to use a "relayer."[106] Basically, the relayer uses its own pseudonymous identity to stand in for the Tornado Cash user in exchange for a fee by paying the Ethereum protocol transaction fee and transacting the funds the user originally deposited to whatever public key address the user designates.[107] In fulfilling this role, relayers merely pass on instructions to the Tornado Cash smart contracts; relayers never take custody or control over user deposits to the pools operated by smart contracts.[108] These technical features of the Tornado Cash software make it a digital infrastructure service. The Tornado Cash software is non-rivalrous in that anyone can use it to enhance the privacy of their transactions. User demand for the Tornado Cash software is not driven by the software itself, but by desires for

102. *See* Andrew R. Chow, *A New U.S. Crackdown Has Crypto Users Worried About Their Privacy*, TIME (Aug. 10, 2022, at 15:47 ET), https://time.com/6205143/tornado-cash-us-crypto-ban/ [https://perma.cc/ST3X-2EBN].

103. *See* Wade, Lewellen & Van Valkenburgh, *supra* note 104; Nadler & Schär, *supra* note 86, at 127–28.

104. *See* Wade, Lewellen & Van Valkenburgh, *supra* note 104; Nadler & Schär, *supra* note 86, at 127–28. Tornado Cash accepts transactions in increments, and mixes like denominations together. *See* ayefda, *Introduction to Tornado Cash*, GITHUB, https://github.com/tornadocash/docs[https://perma.cc/M343-WY9G] (last visited Sep. 21, 2025). The more users in the pool, the greater level of technical privacy provided to the transaction. Wade, Lewellen & Van Valkenburgh, *supra* note 104.

105. *Id.*

106. *See* Wade, Lewellen & Van Valkenburgh, *supra* note 101.

107. *Id.*

108. *Id*.

transactional privacy to enhance user cybersecurity and, sometimes, physical safety.[109] The Tornado Cash software can be, and was in fact, integrated into other software offered as private goods,[110] but also served as a public good when, for example, enabling donations to individuals affected by the war in Ukraine,[111] and served the social good of protecting the fundamental human right to privacy.[112]

But instead of protecting access to the Tornado Cash software as commons-based digital infrastructure, the software was placed on the Office of Foreign Assets Control (OFAC) sanctions list,[113] and its developers were prosecuted.[114] Other open-source Layer-2 smart contract protocols have been targeted by the Commodities Futures Trading Commission (CFTC).[115] These

109. *See* Matt Huang & Katie Biber, *Southern District, Stand Down: Prosecuting Code Is Not Justice*, PARADIGM (Apr. 21, 2025), https://www.paradigm.xyz/2025/04/southern-district-stand-down-prosecuting-code-is-not-justice [https://perma.cc/8W3W-J8J3].

110. *See, e.g.*, CWS Team, *What is Messier 87 (M87)? Complete Guide & Review About Messier 87*, COINWORLDSTORY: CRYPTOCURRENCIES (May 14, 2023), https://coinworldstory.com/messier-87 [https://perma.cc/3FG6-PJCP] (describing Messier 87 (M87) as "an improved fork of Tornado Cash"); *Introduction*, CYCLONE PROTOCOL, https://docs.cyclone.xyz [https://perma.cc/UV7B-PP8K] (last visited Sep. 21, 2025) (describing Cyclone as "a cross-chain, non-custodial, universal privacy-preserving protocol with the decentralized governance" and noting that in part it "is based on the attested implementation of tornado.cash").

111. André Beganski, *Ethereum Cofounder Says He Used Now-Blacklisted Tornado Cash to Donate to Ukraine*, DECRYPT (Aug. 9, 2022), https://decrypt.co/107075/ethereum-cofounder-used-blacklisted-tornado-cash-donate-ukraine [https://perma.cc/8MQ5-9Z5R].

112. *Cf.* PETER VAN VALKENBURGH, COIN CENTER, ELECTRONIC CASH, DECENTRALIZED EXCHANGE, AND THE CONSTITUTION 8 (2019), https://www.coincenter.org/app/uploads/2020/05/e-cash-dex-constitution.pdf [https://perma.cc/AU6T-2YWJ] (arguing that open-source software development of privacy enhancing digital finance software is an exercise of protected speech).

113. *See Cyber-Related Designation: Specially Designated Nationals List Update,* U.S. DEP'T OF THE TREASURY: OFF. OF FOREIGN ASSETS CONTROL (Aug. 8, 2022), https://ofac.treasury.gov/recent-actions/20220808 [https://perma.cc/W3FH-XUE8] (original designation); *Burma-Related Designations; North Korea Designations; Cyber-Related Designation, Cyber-Related Designation Removal; Publication of Cyber-Related Frequently Asked Questions*, U.S. DEP'T OF THE TREASURY: OFF. OF FOREIGN ASSETS CONTROL (Nov. 8, 2022), https://ofac.treasury.gov/recent-actions/20221108 [https://perma.cc/LB9V-B59B] (re-designation); *Cyber-Related Sanctions*, U.S. DEP'T OF THE TREASURY: OFF. OF FOREIGN ASSETS CONTROL (Nov. 8, 2022), https://ofac.treasury.gov/faqs/1095 [https://perma.cc/QG4Z-6336].

114. Press Release, U.S. Att'y's Off. for the S. Dist. of N.Y., Tornado Cash Founders Charged with Money Laundering and Sanctions Violations (Aug. 23, 2023), https://www.justice.gov/usao-sdny/pr/tornado-cash-founders-charged-money-laundering-and-sanctions-violations [https://perma.cc/6L4A-FN3U].

115. *See, e.g.*, *In re* ZeroEx, Inc., CFTC No. 23-41, 2023 WL 5937239, at 1 (Sep. 7, 2023) (charging ZeroEx with violations of the CEA for enabling transactions in leveraged retail commodity transactions with non-eligible contract participants); *In re* Deridex, Inc., CFTC No. 23-42, 2023 WL 5937236, at 1 (Sep. 7, 2023) (charging Deridex with violations of the CEA for

actions reflect a fundamental flaw in efforts to apply regulation to open-source Layer-1 DLT protocols and open-source Layer-2 smart contract protocols: ignoring the function of the protocols as disintermediated digital infrastructure. Ultimately, the U.S. Court of Appeals for the Fifth Circuit ruled that OFAC exceeded its authority in placing the Tornado Cash smart contracts on the sanctions list because the smart contracts were not property of a sanctionable entity.[116] The Fifth Circuit made this determination by carefully considering the technical reality of the Tornado Cash smart contracts and determining that in no way did they function as legally enforceable contracts that could fall within the regulatory definition of "property" relied upon by OFAC.[117]

Instead, considering the function of the Tornado Cash software as a Layer-2 smart contract protocol, the Fifth Circuit determined the software could not be characterized as property that could be placed on the sanctions list because they were not property of any one person or entity in particular,[118] but rather, the Tornado Cash software served as Layer-2 digital infrastructure.

---

enabling transactions in leveraged retail commodity transactions with non-eligible contract participants, failure to register as a swap execution facility or designated contract market, failure to register as a futures commission merchant for soliciting and accepting orders via the Deridex protocol, and failure to fulfil the duties of a futures commission merchant with regard to know-your-customer obligations).

116. In particular, the Fifth Circuit overturned the ruling by the U.S. District Court for the Western District of Texas that the Tornado Cash Smart Contracts were property under OFAC regulations because they constituted unilateral contracts that fell under the OFAC's definition that included "contracts of any nature whatsoever." Van Loon v. Dep't of the Treasury, 122 F.4th 549, 568–70 (5th Cir. 2024) (quoting 31 C.F.R. § 510.323 (2018)). The District Court made this determination because it relied on the Treasury's administrative characterization of smart contracts as legally enforceable contracts—a conclusion reached without considering the function of the Tornado Cash smart contracts at all. *See* Van Loon v. Dep't of the Treasury, 688 F. Supp. 3d 454, 467–68 (W.D. Tex. 2023)*, rev'd*, 122 F.4th 549 (5th Cir. 2024).

117. *See Van Loon*, 122 F.4th at 568–70.

118. *See id.* at 570. Indeed, the Fifth Circuit's analysis focused on the question of whether the smart contracts were property within the meaning of the regulations. *See id*. The Fifth Circuit could make that determination without considering OFAC's claim that the "Tornado Cash DAO"—which OFAC made up—constituted an entity capable of regulation. *Id.* at 571; *see also* Reyes*, supra* note 23, at 1382 ("In reality, . . . no 'entity known as Tornado Cash' exists; OFAC made it up."). Even in this respect, the Fifth Circuit's decision represents an example of the functional regulatory approach proposed in this Article—if considering the function of a protocol leads to a determination that it falls outside of regulation, there is no reason to consider whether a foundation, other entity, or other community of people connected to the protocol are an entity that can be regulated unless that foundation, other entity or other community of people are separately engaged in regulable activity. Focusing on the umbrella organization connected to open-source software leads regulators to attempt to find one where none actually exists. For example, one of the authors of this Article has argued in other work that the "Tornado Cash DAO" was not an entity, at least not of the kind that OFAC claimed: "an unincorporated association for profit"—also known as a general partnership. *See* Carla L. Reyes & Christine Hurt, *The Contractarian Joint Venture*, 76 ALA. L. REV. 741, 756–57 (2025).

The Fifth Circuit's analysis represents a clear use of the functional approach that has characterized law's interaction with open-source software up to this point, adapting it to the DLT context. But protocol developers and communities should not be forced to rely on *ex-post* correction of faulty regulatory actions. If regulators and lawmakers approached DLT through a functional method, the law could provide *ex-ante* clarity that would ultimately benefit both industry and consumers. Unfortunately, to date, regulators have largely taken the opposite approach—without assessing the function of the tools, regulators have insisted on applying a regulatory system designed to apply to entities that act as intermediaries to digital infrastructure that lacks any intermediary at all.[119] This fundamental mismatch does not serve stated policy aims and instead harms the legitimacy of legal and regulatory institutions.[120]

III. OPEN-SOURCE DISTRIBUTED LEDGER TECHNOLOGY'S INHERENT MISMATCH WITH FINANCIAL REGULATION BUILT FOR INTERMEDIATED FINANCE.

The fundamental nature of open-source Layer-1 DLT and blockchain protocols and open-source Layer-2 smart contract protocols rests in digital infrastructure for an emerging peer-to-peer digital economy—that is, a way for individuals to own, sell, and transfer property analogously to the way they do in most of the physical world, without requiring some sort of institutional oversight. Despite this fact, the use of inapt metaphors has led to the inappropriate application of financial regulation designed for intermediaries to computer code that has no intermediary. Frequently analogized to a ledger, many lawmakers and regulators conjure an image of a payments network when they think of DLT protocols,[121] when instead they should be thinking of sending an email or data over the internet.[122] Indeed, popular references to "blockchain transactions" often harken to financial transactions,[123] when, in

119. *See* Reyes, *supra* note 23, at 1383–84.

120. *Id*.

121. *Cf.* Reyes, *supra* note 26, at 201–02 (explaining that "regulatory efforts predominantly center on payment applications of" DLT, despite its many other potential applications).

122. *Cf. What is a Protocol?*, COINBASE, https://www.coinbase.com/en-gb/learn/crypto-basics/what-is-a-protocol [https://perma.cc/9RYM-LYHG] (last visited July 29, 2025) (explaining that "protocols aren't exclusive to cryptocurrency[: t]hey're fundamental to how the internet works, governing the transmission of data from one computer to the other").

123. *See, e.g.*, Ella Vincent, *Blockchain Is 'A Completely Different Animal' in Personal Finance*, Yahoo! Fin. (Mar. 12, 2023), https://finance.yahoo.com/news/blockchain-is-a-completely-different-animal-in-personal-finance-181320033.html [https://perma.cc/7M4M-

fact, the computing activity undertaken by Layer-1 DLT protocols and Layer-2 smart contract protocols are more accurately "software operations."[124] The constant analogies drawn between open-source Layer-1 DLT protocols and traditional financial systems wreak havoc on regulatory and legal policy discussions because the analogies ignore the differences in infrastructure and function between the two systems. Specifically, modern-day payment networks operate within a highly intermediated financial system.[125] Financial regulation, for its part, assumes the presence of intermediaries to serve as the object of regulation.[126] By investigating these dualling realities, this Part argues that when the existing regulatory paradigm is applied to open-source Layer-1 DLT protocols and open-source Layer-2 smart contract protocols, the results are suboptimal.

A. Existing Financial Regulation Assumes an Intermediated Financial System.

The modern regulatory apparatus aims to mitigate negative externalities caused by private actors pursuing their own benefit.[127] Financial regulation is no different. The traditional modern day financial system operates almost entirely through intermediaries[128] which operate to provide, allocate, and deploy capital.[129] Even as intermediaries fulfill these generalized capital funding functions, they also participate in "core financial functions, like asset aggregation, market making, risk management, and information

M3KV]; Roomy Khan, *Blockchain: The Operating System For Global Finance*, Forbes (Apr. 10, 2025, at 07:43 ET), https://www.forbes.com/sites/roomykhan/2025/04/10/blockchain-the-operating-system-for-global-finance [https://perma.cc/XL94-FZEV].

124. *Cf. Software*, TECHCAREER.NET, https://www.techcareer.net/en/dictionary/software [https://perma.cc/D5JP-5645] (last visited July 29, 2025) ("Typically written in a programming language, software executes various operations on a computer's hardware.").

125. *See* Tom C.W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643, 656–57 (2015) (discussing Apple Pay as a modern example of payment networks with "layers of intermediation" that "create the illusion of disintermediation").

126. *See id.* at 667; Schwarcz, *supra* note 27, at 1443–44 (explaining that "the pre-crisis financial regulatory framework . . . assumed the dominance of bank-intermediated funding"); Reyes, *supra* note 23, at 1350 (citing Lin, *supra* note 129, at 643).

127. *See* Reyes, *supra* note 23, at 1351 (citing Brian Galle, *In Praise of Ex Ante Regulation*, 68 VAND. L. REV. 1715, 1722–24 (2015)).

128. *See* Lin, *supra* note 125, at 650–51.

129. *See* Schwarcz, *supra* note 27, at 1450 ("Financial firms and markets have several key economic functions. The principal function is capital provision, allocation and deployment (hereinafter, funding): the process of aggregating funds from multiple investors and then transferring the funds to firms that can productively use it.").

clearing . . . ."[130] Financial intermediaries aggregate assets from multiple investors and make markets in order to make capital available to entities that can put it to productive use.[131] In terms of risk management, financial intermediaries, in a well-functioning market, will diversify their risk profile, thereby hedging against risk and improving their overall investment.[132] In properly functioning markets, financial intermediaries act as information clearinghouses, reducing information asymmetries between investors and issuers.[133] Properly fulfilling each of these functions, of course, assumes a properly functioning market. But financial intermediaries, as profit-seeking entities themselves, may engage in behavior that introduces new risk to the market, or causes market failures. Financial regulation aims to reduce the likelihood that financial intermediaries engage in activity that might contribute to such market risks and failures.[134]

Specifically, financial regulation targets negative externalities related to transaction costs,[135] information asymmetries,[136] risk complexity,[137]

130. Lin, *supra* note 125, at 650; *see* Schwarcz, *supra* note 27, at 1450–51 ("Economists also identify a range of other functions related to funding. These related functions involve risk management, behavior monitoring, and information processing. The risk management function goes to diversifying investment risk in order to maximize the amount of investment. . . . The behavior monitoring function goes to reducing agency costs. . . . The information-processing function goes to reducing information asymmetry between investors and issuers of securities."); Steven L. Schwarcz, *Keynote Address: Towards More Sustainable and Less Crisis-Driven Financial Regulation*, 11 U. ST. THOMAS L.J. 427, 429–30 (2014) [hereinafter Schwarcz, *Sustainable Financial Regulation*].

131. *See* Schwarcz, *supra* note 27, at 1452.

132. *See id*. at 1450–51.

133. *See id*. at 1451.

134. *See id*.

135. *See* Franklin Allen & Anthony M. Santomero, *What Do Financial Intermediaries Do?*, 25 J. BANKING & FIN. 271, 272 (2011); Lin, *supra* note 125, at 646–47.

136. *See* Allen & Santomero, *supra* note 135; Lin, *supra* note 125, at 649 ("Intermediaries mitigate the negative implications of information asymmetries that may lead to gridlocks and misallocations in the marketplace.").

137. *See* Lin, *supra* note 125, at 648–49.

consumer exploitation,[138] systemic risk[139] and moral hazard.[140] Each of these risks is inherent to intermediaries. For example, markets rely on financial intermediaries to properly assess the risk of financial products, but as financial transactions and products become more complex, financial intermediaries themselves begin to rely on short-hand indicators of risk to make risk assessments.[141] If the indicator becomes faulty in some respect, but financial intermediaries fail to take notice or ignore the problem in pursuit of short-term gains, they can introduce deeper risk to the markets.[142] Indeed, many acknowledge the role of complexity risk in the events that led to the 2008 financial crisis.[143] In order to mitigate intermediary-related risks—and, ostensibly, avoid another 2008-like financial crisis—lawmakers increasingly, and nearly exclusively, craft regulations for financial services and capital markets participants that target intermediaries.[144]

Targeting financial regulation at intermediaries that aggregate capital and clear information related to transactions on a global scale also allows governmental surveillance of transactions in an attempt to prevent or

138. *See* Stephen G. Cecchetti, *The Future of Financial Intermediation and Regulation: An Overview*, CURRENT ISSUES IN ECON. & FIN., May 1999, at 1, 3.

139. *See id*.; Schwarcz, *supra* note 27, at 1446 ("The other function of the financial system is to serve as a network within which the underlying economic functions can be conducted. . . . Economists use the term 'systemic risk' to refer to the risk that the financial system could fail to so function."); Steven L. Schwarcz, *Systemic Risk*, 97 GEO. L.J. 193, 204 (2008) (defining systemic risk as "the risk that (i) an economic shock such as market or institutional failure triggers (through a panic or otherwise) either (X) the failure of a chain of markets or institutions or (Y) a chain of significant losses to financial institutions, (ii) resulting in increases in the cost of capital or decreases in its availability, often evidenced by substantial financial-market price volatility.").

140. *See* Cecchetti, *supra* note 138.

141. *See* Schwarcz, *supra* note 27, at 1453 (first citing Christopher L. Culp, Merton H. Miller & Andrea M.P. Neves, *Value at Risk: Uses and Abuses*, 10 J. APPLIED CORP. FIN. 26, 27 (1998); and then citing Steven L. Schwarcz, *Private Ordering of Public Markets: The Rating Agency Paradox*, 2002 U. ILL. L. REV. 1, 1–3 (2002)).

142. *See id*. at 1454.

143. *See, e.g*., Steven L. Schwarcz, *Disclosure's Failure in the Subprime Mortgage Crisis*, 2008 UTAH L. REV. 1109, 1110 (2008); Hilary J. Allen, *Defi: Shadow Banking 2.0?*, 64 WM. & MARY L. REV. 919, 922–23 (2023); Hilary J. Allen, *Driverless Finance*, 10 HARV. BUS. L. REV. 157, 174 (2020); Saule T. Omarova, *License to Deal: Mandatory Approval of Complex Financial Products*, 90 WASH. U. L. REV. 63, 65 (2012); Dan Awrey, *Complexity, Innovation, and the Regulation of Modern Financial Markets*, 2 HARV. BUS. L. REV. 235, 236–38 (2012); Saule T. Omarova, *The New Crisis for the New Century: Some Observations on the "Big Picture" Lessons of the Global Financial Crisis of 2008*, 13 N.C. BANKING INST. 157, 160–61 (2009).

144. *See* Sebastian Di Tella, *Optimal Regulation of Financial Intermediaries*, 109 AM. ECON. REV. 271, 271 (2019) ("[E]xcessive risk taking by financial intermediaries can create macro-instability and lead to financial crises. This has created a large interest in the regulation of financial intermediaries, especially after the 2008 financial crisis.").

otherwise detect and prosecute illicit financial transactions, including money laundering and terrorist financing.[145] The United States enacted the Bank Secrecy Act (BSA) in 1970[146] to "require institutions to maintain certain records the government could use to support criminal and tax evasion investigations."[147] Congress would later amend the BSA to address white collar financial crimes, to better detect money laundering by identifying "suspicious activity," and to account for new threats and new schemes as they arose.[148] To achieve these ends, the BSA requires financial institutions (a defined term that covers a variety of financial intermediaries) to file various reports about transactions they facilitate and the customers that undertake those transactions.[149] Because the BSA and its implementing regulations require reporting on the vast majority of transactions,[150] the BSA regime has come under fire for eroding privacy rights and acting as a financial surveillance dragnet that captures even law-abiding citizens.[151] Essentially, the BSA turns all financial institutions into financial intermediaries that double as surveillance tools.

Targeting financial regulation at intermediaries suffers from a fundamental flaw—namely, by tying regulation to a specific archetype of intermediated financial institution, the law fails to achieve its policy aims when the financial system undergoes periods of transformation and innovation.[152] To facilitate legal change that keeps pace with industry

145. *Cf.* Daniel Barabander, Amanda Tuminelli & Jake Chervinsky, *Through the Looking Glass: Conceptualizing Control and Analyzing Criminal Liability for Unlicensed Money Transmitting Businesses Under Section 1960*, at 7 (Int'l Acad. of Fin. Crime Litigators, Working Paper No. 3, 2024) ("Law enforcement has increasingly relied on financial intermediaries . . . to report information about allegedly suspicious financial activity.").

146. Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114, 1114–1118 (1970) (codified as amended at 12 U.S.C. §§ 1829b, 1951–1959; 31 U.S.C. §§ 5311–5314, 5316–5322).

147. Natalie Noyes, *The Bank Secrecy Act: A Supervisory Update*, SUPERVISORY INSIGHTS, Summer 2021, at 21, 21–22.

148. *See* Rebecca Rettig, Michael Mosier & Katja Gilman, *Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance*, 11 J. FIN. REGUL. 215, 218–19 (2025).

149. *See id*. at 222–23 ("Under the BSA, financial institutions' AML/CFT programs focus on detection, documentation, and deterrence of illicit financial activity.").

150. *See* Heather Trew, *Ten Large Isn't What It Used to Be*, WALL ST. J. (May 15, 2024, at 17:25 ET), https://www.wsj.com/opinion/ten-large-isnt-what-it-used-to-be-regulation-banking-suspicious-transaction-1412e30d [https://perma.cc/PZD5-KCRK].

151. *See* Barabander, Tuminelli & Chervinsky, *supra* note 145.

152. *See* Schwarcz*, Sustainable Financial Regulation*, *supra* note 130, at 427 ("Indeed, because the financial system is constantly changing, future financial crises are unlikely to resemble, and may have very different causes than, past crises. . . . We need to develop a financial regulatory framework that can anticipate, or at least respond to, future financial crises and a dynamically changing financial system.").

transformation, Professor Steven Schwarcz has argued for policymakers to consider functional financial regulation.[153] Functional regulation, for its part, requires "examining the functionality of a process or application without worrying about the details of its internal structure."[154] Then, using the policy goals of financial regulation—namely, to prevent market failures that would interrupt the functions of the intermediated financial system—functional financial regulation would ask what market failures would impede the functions of the financial system.[155] For example, if regulators worry that the complexity of an emerging financial product might result in information asymmetry and rationality failure that will impede the function of a financial institution in aggregating funds for redistribution to firms that can put the funds to use, then regulation might require less use of benchmark data to assess the financial products.[156] Ultimately, functional regulation requires consideration of the function of the law and of the object of regulation. Only by considering them together can regulation be crafted effectively. The result, of course, is a regulatory system that eschews a one-size-fits all approach to law making and instead enacts fit for purpose regulation tailored to the function.

Fascinatingly, regulators initially took a functional approach to applying existing law to DLT protocols and smart contract protocols. For example, in 2019, the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) issued guidance that functionally applied the BSA and its implementing regulations.[157] Under the 2019 FinCEN Guidance, FinCEN used four functional criteria to determine whether a cryptocurrency wallet provided money transmission services: "(a) who owns the value; (b) where the value is stored; (c) whether the owner interacts directly with the payment system where the [cryptocurrency] runs; and, (d) whether the person acting as intermediary has total independent control over the value."[158] Under those criteria, FinCEN instructed that hosted wallet providers acted as "account-based money transmitters that receive, store, and transmit [cryptocurrencies] on behalf of their accountholders," while "[u]nhosted wallets are software hosted on a person's computer, phone, or other device that . . . do not require an additional third party to conduct transactions," and therefore were deemed

153. *See* Schwarcz, *supra* note 27, at 1452; Schwarcz, *Sustainable Financial Regulation, supra* note 130, at 430–34.

154. Schwarcz, *supra* note 27.

155. *See id*. at 1451.

156. *Id*. at 1453–55.

157. *See* FIN. CRIMES ENF'T NETWORK, DEP'T OF THE TREASURY, FIN-2019-G001, APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES 1 (2019).

158. *Id*. at 15.

outside the scope of the BSA and its implementing regulations.[159] Using similarly functional criteria, FinCEN also instructed that an "anonymizing services provider"—a "person[] that accept[s cryptocurrencies] and retransmit[s] them in a manner designed to prevent others from tracing the transmission back to its source"—acted as a money transmitter subject to the BSA regulations while "[a]n anonymizing software provider is not a money transmitter" because "FinCEN regulations exempt from the definition of money transmitter those persons providing 'the delivery, communication, or network access services used by a money transmitter to support money transmission services" and open-source software—even if it anonymizes DLT activity—is digital infrastructure, not an intermediary with independent control over the value.[160]

However, a tendency to conflate centralized actors like the ill-fated FTX exchange and the related counterparty risk that led to fraud, theft and a string of cryptocurrency failures in the summer of 2022 with the DLT industry as a whole,[161] increasingly led to calls for stricter adherence to existing law—even when existing law did not fit the function undertaken by the technology.[162] As a result, the last several years saw the functional approach to regulating DLT protocols give way to an approach that forces laws designed for intermediaries—namely, financial regulation—onto systems in which no intermediaries exist—and which perform operations different in kind from financial transactions.[163] Even in an industry somewhat used to regulation by enforcement, the public outcry in response to this perceived overreach was swift and significant. Users of smart contract protocols sued the U.S. Department of Treasury for exceeding its authority by attempting to list software code on the economic sanctions list,[164] a cryptocurrency user sued the Internal Revenue Service alleging illegal collection of data related to cryptocurrency users,[165] artists sued the Securities and Exchange Commission to prove non-fungible tokens and digital art do not constitute securities,[166] two

159. *Id*. at 15–16.

160. *Id*. at 19–20.

161. *See* Reyes, *supra* note 23, at 1346–47.

162. *See id.*

163. *See id.* at 1353–54.

164. *See* Van Loon v. Dep't of the Treasury, 688 F. Supp. 3d 454, 458, 471 (W.D. Tex. 2023)*, rev'd*, 122 F.4th 549 (5th Cir. 2024); Van Loon v. Dep't of the Treasury, 122 F.4th 549, 553–54 (5th Cir. 2024).

165. *See* Complaint ¶¶ 18, 106, Harper v. Werfel, 118 F.4th 100 (1st Cir. 2023) (No. 23-1565).

166. *See* Complaint ¶¶ 18–19, Mann v. SEC, No. 24-cv-01881 (E.D. La. July 29, 2024); Cheyenne Ligon, *Does the SEC Really Have Jurisdiction Over NFT Art? Two Artists Sue SEC to Get an Answer*, COINDESK (July 31, 2024, at 13:22 ET), https://www.coindesk.com/policy/

industry associations and a non-profit advocacy group sued the IRS alleging regulatory overreach by unduly broadening the definition of broker,[167] and a developer of an open-source and decentralized crowdfunding platform sued the Department of Justice for regulatory overreach.[168] A variety of companies,[169] academics,[170] and non-profit associations[171] filed amicus briefs[172] in support of these attempts by the public to reign in the regulatory insistence on intermediaries run amok.

Why would regulators so uniformly embrace an approach that undermines their own legitimacy[173] to such an extent that companies and individuals alike feel compelled to file lawsuits to vindicate individual rights? Perhaps the persistent regulatory adherence to finding an intermediary where none exists relates to the realization that the lack of intermediaries in open-source Layer-1 DLT protocols and open-source Layer 2 smart contract protocols "means that the traditional approach to [anti-money

2024/07/31/does-the-sec-really-have-jurisdiction-over-nft-art-two-artists-sue-sec-to-get-an-answer. [https://perma.cc/4X8V-SRZN].

167. *See* Complaint for Declaratory and Injunctive Relief ¶¶ 1–5, 20–22, Blockchain Ass'n v. IRS, No. 24-cv-03259-X (N.D. Tex. Dec. 27, 2024) ("[T]he IRS adopted a [regulation] requiring DeFi industry participants that are not brokers to act as brokers." (citation omitted)).

168. *See* Complaint, *supra* note 1, ¶¶ 5, 33, 36; Vismaya V, *Crypto Developer Michael Lewellen Sues DOJ for Regulatory Overreach*, DECRYPT (Jan. 17, 2025), https://decrypt.co/301494/crypto-developer-michael-lewellen-sues-doj-for-regulatory-overreach [https://perma.cc/6W37-NBX8] ("Lewellen contends that the DOJ's interpretation of 18 U.S.C. §1960 (Prohibition of illegal money transmitting businesses) improperly classified non-custodial software developers as unlicensed money transmitter. The DOJ's stance 'betray[s] its own representations to the public by criminally prosecuting people who publish non-custodial cryptocurrency software,' reads the lawsuit." (alteration in original)).

169. *See, e.g.*, Brief of Amicus Paradigm Operations LP at 1, Mann v. SEC, No. 24-cv-01881 (E.D. La. Dec. 18, 2024).

170. *See, e.g.*, Brief of Law Professors Carla L. Reyes et al. as Amici Curiae in Support of Plaintiffs-Appellants & Reversal at 3–5, Van Loon v. Dep't of Treasury, 112 F.4th 549 (5th Cir. 2023) (No. 23-50669).

171. *See, e.g.*, Brief for DeFi Education Fund as Amicus Curiae Supporting Appellant & Urging Reversal, at i, Harper v. Werfel, 118 F.4d 100 (1st Cir. 2023) (No. 23-1565) (arguing that the IRS data collection practices violate Fourth Amendment rights in light of the way blockchain records function compared to the way traditional records function); Brief for the DeFi Education Fund as Amicus Curiae in Support of Appellants & Reversal, at 24, *Van Loon*, 122 F.4d 549 (No. 23-50669); Brief of Amicus Curiae Electronic Frontier Foundation in Support of Plaintiffs' Motion for Partial Summary Judgment, at 1, Van Loon v. Dep't of Treasury, 688 F. Supp. 3d 454 (W.D. Tex. Apr. 27, 2023) (No. 23-cv-00312).

172. *See, e.g.*, Brief of Paradigm Operations LP et al. as Amici Curiae in Support of Plaintiff's Opposition to the Motion to Dismiss, at 4, Michael Lewellen v. Pamela Bondi, No. 25-cv-00030-O (N.D. Tex. July 7, 2025) (arguing that software developers of non-custodial cryptocurrency software do not transmit money within the meaning of 18 U.S.C. § 1960 because they do not take control of assets).

173. For a detailed explanation of the how regulators have undermined their legal legitimacy by over-relying on intermediaries, see Reyes, *supra* note 23, at 1375–90.

laundering/countering the financing of terrorism (AML/CFT)] regulation in which AML/CFT requirements are imposed on a private sector entity and compliance is monitored by supervisors, cannot be applied."[174] Indeed, perhaps just as worries over clandestine Russian communications made PGP a target in the 1990s, worries about illicit finance made all disintermediated protocols a current target of regulatory wrath. Whatever the reason for the deep shift in regulatory approach, the attempt to crack-down on bad actors in the DLT ecosystem only really highlighted the many ways that applying existing intermediated financial regulation to open-source digital infrastructure characterized by open access, disintermediation, and genericity utterly fails to reduce the types of risks that financial regulation is designed to mitigate.

B. Applying Existing Financial Regulation to Open-Source Digital Infrastructure Fails to Achieve Stated Policy Goals and Undermines Broader Technology Development.

This Section explores the outcomes achieved by applying existing financial regulation to open-source Layer-1 DLT protocols and open-source Layer-2 smart contract protocols. Through the use of several case studies, this Section makes clear the mismatch inherent in applying regulation meant for financial intermediaries to digital infrastructure. In particular, this Section argues that the enforcement actions taken to date with respect to Layer-1 DLT protocols and Layer-2 smart contract protocols serve none of the regulatory policy aims the regulation was designed to address.

For our first case study, we turn to a decentralized exchange. In its purest form, no intermediary operates in the middle of decentralized exchange.[175]

---

174. IMF & FIN. STABILITY BD., *Policies for Crypto-Assets*, IMF-FSB Synthesis Paper 14 (Sep. 7, 2023), https://www.fsb.org/uploads/R070923-1.pdf [https://perma.cc/S6FY-SYML]; *see also* U.S. DEP'T TREAS., ILLICIT FINANCE RISK ASSESSMENT OF DECENTRALIZED FINANCE 36 (2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [https://perma.cc/V7LD-ABWY] ("DeFi services that lack an entity with sufficient control or influence over the service may not be explicitly subject to AML/CFT obligations.").

175. *See* Peter Van Valkenburgh, *There's No Such Thing as a Decentralized Exchange*, THE BLOCK (Oct. 3, 2020, at 12:01 ET), https://www.theblock.co/post/79768/theres-no-such-thing-as-a-decentralized-exchange [https://perma.cc/EJ72-KB2W].

> First, if a decentralized exchange is truly decentralized . . . then grammatically it's an action not a thing, a verb and not a noun: *I make a decentralized exchange*; not, *I use a decentralized exchange*. When I use free software and an open blockchain network to trade one token for another directly with another trader, then I am engaged in decentralized exchange — an action, just as I might engage in running or paying.
>
> *Id.*

When the software that we often refer to as "a DEX" is truly decentralized, there is no intermediary called a DEX—"just software and an internet connection."[176] One such protocol was called the 0x Protocol, and was a software tool enabling the decentralized exchange of cryptocurrencies.[177] Although a company called ZeroEx, Inc. developed the Layer-2 0x Protocol, the software itself "was a collection of smart contracts on the Ethereum blockchain" which the company "developed and deployed" but did not further control in any meaningful technical or business sense of control.[178] Indeed, the company ZeroEx, Inc. gave up its control over the software when it transitioned management over the protocol to the 0x protocol community of users.[179]

ZeroEx, Inc. did, however, create a website, "Matcha," through which users could access the 0x Protocol.[180] ZeroEx, Inc. similarly exercised no measure of technical or business control over Matcha—the company did not interact with users, did not intermediate transactions for users, did not charge for the use of the website, and did not charge trading fees on transactions.[181] Yet, the Commodity Futures Trading Commission (CFTC) became concerned that "certain leveraged digital assets" traded via the 0x Protocol without complying with the relevant Commodities Exchange Act (CEA) requirements.[182] The difficulty for the CFTC in addressing its concern, of course, lies in the fact the CEA requirements are intended to apply to intermediaries that facilitate such trades in a centralized manner.[183] No such entity exists in the 0x Protocol.[184] This conflict of the old regime designed for intermediaries and the new disintermediated technology reflects the broader

176. *Id*. ("We have this habit of saying that a DEX is a thing rather than an action because we are stuck in a centralized services frame of mind. Coinbase is a thing, a business, a corporation. . . . There are no DEXs; there is just decentralized exchange, the action, taking place using software tools, open blockchains, and the internet.").

177. *See In re* ZeroEx, Inc., CFTC No. 23-41, 2023 WL 5937239, at *1 (Sep. 7, 2023) ("0x users trade [digital assets] on a peer-to-peer basis, meaning, according to 0x, that users 'trade directly from [their] Ethereum wallet and retain complete custody of [their] tokens throughout the entire process.'" (second and third alterations in original)).

178. *Id.* at 2.

179. *See* Eric Wong, *0x Protocol Governance Roadmap—Making 0x Protocol an Unstoppable Force*, 0X PROTOCOL (Feb. 2023), https://forum.0xprotocol.org/t/0x-protocol-governance-roadmap-making-0x-protocol-an-unstoppable-force/3506 [https://perma.cc/PLL6-TCKX].

180. *In re ZeroEx*, CFTC No. 23-41, at 1.

181. *See id.* at 1–2.

182. *Id.* at 2.

183. *See* Joshua Durham, *Regulatory Sandboxes Enable Pragmatic Blockchain Regulation*, 18 WASH. J.L. TECH. & ARTS 27, 38–39 (2023).

184. *See In re ZeroEx*, CFTC No. 23-41, at 1.

problem facing U.S. financial regulators—namely, that financial regulation applies to intermediaries.

Rather than attempt to adapt capital markets regulations to a disintermediated financial platform, regulators applied existing law—designed to apply to an intermediary—to the developer of the decentralized protocol. In an order dated September 7, 2023, the CFTC and ZeroEx entered into a settlement arrangement, ostensibly because ZeroEx created the website, Matcha.[185] The CFTC maintained the settlement was warranted because ZeroEx violated the CEA.[186] And yet, the ZeroEx action represented a stark departure from other capital markets enforcement activity in so far as the 0x Protocol was not specifically designed to support transactions that fall under CFTC jurisdiction, and was not specifically marketed as a way to avoid regulation by the CFTC.[187] Further, ZeroEx did not issue the offending tokens, did not approve or facilitate the listing of the offending tokens, did not make any profit from the trading of the offending tokens via the open-source protocol, and remained powerless to take the offending tokens out of circulation.[188] Further still, it could not prevent the actual creator of the offending tokens from recreating and relisting the tokens via another decentralized exchange tool or on a centralized exchange, nor prevent anyone else from creating an identical user interface, like Matcha, that would provide users the exact same access to the 0x Protocol.[189] Given that reality, the CFTC appears to have achieved little through its action against ZeroEx that advances its regulatory mandate.

In contrast, what could the CFTC have achieved if it had taken a functional approach to ZeroEx? The 0x Protocol community described 0x as "an open-source public good that serves as the underlying settlement layer for the global exchange of value."[190] Further, the 0x community believed that eventually "the 0x Protocol [would] serve as a fundamental building block to a system that will provide individuals with greater sovereignty."[191] To assess these claims, and whether they should have impacted the CFTC's approach to the enforcement action, we first consider whether the 0x Protocol fits Frischmann's three criteria for digital infrastructure. As an initial matter, the

185. *See id.* at 1–3.

186. *See id.* at 3–4.

187. *See* John Servidio, *The CFTC's DeFi Trifecta: Lessons and Implications for DeFi Participants Inside and Outside the US*, GOODWIN (Sep. 18, 2023), https://www.goodwinlaw.com/en/insights/publications/2023/09/alerts-finance-ftec-cftc-decentralized-finance-defi-lessons-implications [https://perma.cc/C26A-G8BW].

188. *See In re ZeroEx*, CFTC No. 23-41, at 2.

189. *Id.* at 3.

190. Wong, *supra* note 179.

191. *Id*.

Layer-2 0x Protocol is nonrivalrous[192] in two important ways: first, as open-source software, the source code for the protocol was and is available for anyone to use in launching another similar protocol, and second, any specific instantiation of the 0x software launched on a DLT protocol can be used by anyone to execute software operations.[193] Further, the demand for the 0x Protocol is primarily driven by downstream productive activity—the creation and use of other tokens and applications.[194] Finally, the 0x Protocol, whether as source code or as a specific instantiation of the software, can be incorporated into other software and put to use for private, public and social purposes.[195]

Because the 0x Protocol functionally meets Frischmann's criteria for digital infrastructure, the first policy priority should have been to preserve open access to the infrastructure. With that in mind, the CFTC could have taken different steps to maintain market integrity and transparency other than requiring that Matcha—which provided access to the 0x Protocol—be shuttered. For example, the CFTC could have required ZeroEx to require that issuers make disclosure statements on Matcha to explain new tokens listed on 0x using Matcha. The disclosures could serve as both an information tool for prospective purchasers of tokens listed on Matcha and as an information tool for the CFTC, to enable the CFTC to pursue the issuer of the tokens rather than the creator of the digital infrastructural resource. Alternatively, and more appropriately, the CFTC could have pursued enforcement actions against the issuers themselves. Such enforcement activity, of course, would be more expensive and time-intensive than pursuing ZeroEx, the obviously identifiable entity. That, however, is what financial regulation more appropriately required, and what would have actually achieved the policy aims of the CEA.

The CFTC also settled potential charges with the Deridex Protocol for similar violations of the CEA.[196] Notably, the Deridex Protocol was a Layer-2 smart contracts protocol operating on the Algorand blockchain.[197] Anyone

192. *See* FRISCHMANN, INFRASTRUCTURE, *supra* note 46, at 26–27, 32.

193. *See id.*

194. *See id.* at 61–66.

195. *See id.*

196. *Compare In re ZeroEx, Inc*., CFTC No. 23-41, 2023 WL 5937239, at 1 (Sep. 7, 2023) (charging ZeroEx with violations of § 4(a) of the CEA for enabling transactions in leveraged retail commodity transactions with non-eligible contract participants), *with In re Deridex, Inc.*, CFTC No. 23-42, 2023 WL 5937236, at 1 (Sep. 7, 2023) (charging Deridex with violations of § 4(a) of the CEA for enabling transactions in leveraged retail commodity transactions with non-eligible contract participants, failure to register as a swap execution facility or designated contract market, failure to register as a futures commission merchant for soliciting and accepting orders via the Deridex protocol, and failure to fulfil the duties of a futures commission merchant with regard to know-your-customer obligations).

197. *In re Deridex, Inc.*, CFTC No. 23-42, at 2.

could use the smart contracts to contribute margin or trade on a leveraged basis, and they could do so either through Deridex's website or through direct interaction with the smart contracts.[198] Ultimately, the CFTC reasoned that because Deridex retained the capacity to update the smart contract code, it retained sufficient control over the Deridex Protocol to be treated as an intermediary to which the CEA requirements applied.[199] This conclusion is problematic as a matter of simple software development best practices, insofar as it discourages open source software developers from making smart contract software code upgradeable. The best interest of the software's users demands a path for updating software code in the event that a software bug is identified. Ultimately, as with ZeroEx, it remains unclear how the settlement with Deridex furthers the policy goals of the CEA. Indeed, it appears to put open-source DeFi software developers in a bind: retain the capacity to upgrade code and face potential commodities regulation enforcement or intentionally make it impossible to upgrade software code, still face enforcement regulation (like ZeroEx), *and* face potential consumer protection or other liability if a software bug causes user losses. By insisting on finding an intermediary so that it could apply the CEA to the Deridex Protocol, the CFTC created a terrible double bind for developers while claiming that it had the authority to impose liability whether you could not upgrade the code (ZeroEx) or you could upgrade the code (Deridex).

If the CFTC had instead considered a functional regulatory approach, would the outcome have been different for Deridex? Deridex can be "consumed nonrivalrously for some appreciable range of demand"[200] because anyone who wanted to use the Deridex Protocol could bypass Deridex's website and interact with it directly.[201] Further, users of the Deridex Protocol used it as a transaction management software for downstream productive activity—to help minimize risks and simplify operations[202] by providing cross-chain functionality for network flexibility, heightened data robustness, and enhanced efficiency.[203] Finally, Deridex smart contracts, as open-source software, could be used as component parts of other software—meaning that

198. *See id*. at 1.

199. *See id.* at 2–4.

200. FRISCHMANN, INFRASTRUCTURE, *supra* note 46, at xiv.

201. *See* Deridex, *Introducing Deridex—A New Decentralized Derivatives Management Protocol*, MEDIUM (Dec. 2, 2021), https://medium.com/@Deridex_io/introducing-deridex-a-new-decentralized-derivatives-management-protocol-b80f37130f3c [https://perma.cc/48V5-SBTU] ("Our protocol is open, and anyone can freely connect and use our services.").

202. *See id.*

203. *See* 0XA2LPHA ET AL., DERI V4: A CROSS CHAIN DECENTRALIZED PROTOCOL OF DERIVATIVES 2 (2023), https://github.com/deri-protocol/whitepaper/blob/master/deri_v4_whitepaper.pdf [https://perma.cc/WT2Q-NTLB] (describing Deri V4, the protocol utilized in Deridex Protocol).

the Deridex Protocol also satisfies the genericity criteria for digital infrastructural resources. Indeed, perhaps the fact that the Deridex Protocol served as digital infrastructure made Deridex's decision to retain the ability to upgrade smart contracts an important exercise in developer responsibility. In the traditional infrastructure and commons management literature, the question of who and how to maintain the commons infrastructure relied upon by many for public, private, and social goods represents one of the key issues of inquiry. If the CFTC had taken a functional approach to the application of the CEA to the Deridex Protocol, it would have recognized the protocol as digital infrastructure for which Deridex had volunteered to be one of the potentially many actors who contributed to the maintenance of the commons.[204]

As with ZeroEx, under a functional regulatory approach, Deridex should have been preserved as digital infrastructure, while issuers that violated the CEA by offering leveraged and margin-imbued tokens were more appropriately the true enforcement targets for undertaking noncompliant activity. Moreover, the "control" attributed to Deridex merely because they retained the software development capacity to upgrade the software and mend bugs would not have served as a regulatory enforcement trigger. Rather, maintaining the capacity to upgrade software in an open-source context would be encouraged by a functional regulatory approach that recognizes Layer-1 DLT protocols and Layer-2 smart contract protocols as digital infrastructure. Indeed, analyzing the CFTC's action against the Deridex Protocol through a functional regulatory lens reveals that the functional regulatory approach can help regulatory agencies align their policy priorities. For example, by charting a path where retaining the capacity to upgrade software is not considered a CEA regulatory trigger, the functional regulatory approach helps align CFTC enforcement activity with broader policies of investor and consumer protection in the context of complex software. The ZeroEx and Deridex case studies demonstrate the power of a functional regulatory approach over current efforts to identify intermediaries in disintermediated systems where intermediaries do not exist. The next section considers how legislatures and regulators can operationalize functional regulation in practice.

204. Admittedly, if the CFTC could thereafter prove that Deridex offered retail commodity transactions directly through the Deridex website, undertaking such activity on an unregistered basis might indeed be a violation of the CEA. Merely creating and maintaining the software, however, not so much. *See* Alexander C. Drylewski et al., *Skadden Discusses CFTC Charges that DeFi Developers Facilitated Off-Exchange Trading*, CLS BLUE SKY BLOG (Sep. 26, 2023), https://clsbluesky.law.columbia.edu/2023/09/26/skadden-discusses-cftc-charges-that-defi-developers-facilitated-off-exchange-trading/ [https://perma.cc/SNQ8-HGW8].

IV. THE EMERGING DECENTRALIZED ERA REQUIRES A RETURN TO FUNCTIONAL REGULATION.

The current architecture of financial regulation targets intermediaries and aims to change their behavior to mitigate risks posed by information asymmetry, customer exploitation, risk complexity, and moral hazard.[205] Attempting to apply those rules to disintermediated open-source protocols ignores the fact that such protocols serve as disintermediated digital infrastructure. Indeed, modern financial regulation's focus on intermediaries fails to recognize that certain technical attributes of the code fulfill the risk mitigation function that the law plays in the U.S. financial market. This approach, unfortunately, inhibits innovation in financial and capital markets.[206] If the U.S. shifted to a functional regulatory approach—"examining the functionality of a process or application without worrying about the details of its internal structure" [207]—the regulatory apparatus could more nimbly respond to market risk while allowing for technological and other innovation.[208] This Section explores the contours of the traditional functional method in both the arena of financial regulation and in other contexts, and uses Layer 1 protocols as a case study through which to argue for a return to functional regulation of the DLT industry.[209] Recognizing the limitations of applying any single functional method developed in a different context, this Section proposes a framework of key principles reflected across three functional approaches to law for use by regulators and law makers as they make policy choices for new and emerging digital infrastructure resources.

205. *See supra* Section III.A.

206. *See* Schwarcz, *supra* note 27, at 1443; Schwarcz, *Sustainable Financial Regulation*, *supra* note 134, at 433.

207. Schwarcz, *supra* note 27 (explaining that the functional approach "facilitates the analysis of a highly complex or unknown structure. It also facilitates the analysis of a rapidly changing structure.").

208. *See id*. at 1444 ("In thinking about regulating a dynamically changing financial system it may be more effective—or at least instructive—to focus on the system's underlying, and thus less time-dependent, economic functions than to tie regulation to any specific financial architecture.").

209. For a discussion of FinCEN's previously functional approach to the DLT industry, see *supra* notes 157–160 and accompanying text.

A. Functional Regulation of Layer-1 DLT Protocols and Layer-2 Smart Contract Protocols can be Developed Through Existing Functional Methodologies in Law.

Technological developments in the financial and capital markets have pushed the boundaries of regulation since as early as 1963.[210] Initially, financial and capital markets regulators embraced technology to make their own regulatory approaches nimbler and more sophisticated.[211] In the wake of the 2008 financial crisis and the 2010 flash crash, however, financial and capital market regulators became more skeptical of technological innovation.[212] The resulting regulatory structure has been criticized by economists and financial regulatory scholars as being too stagnant.[213] Financial regulation is stuck, and will fail to adequately address market failures, they argue, because the law is mapped to existing financial intermediaries.[214] Law could be more responsive to innovation in the market, and indeed, could enable greater innovation in the market without expecting greater risk, if financial regulation was instead tied to the *functions* performed by financial intermediaries.[215] The emergence of Layer-1 DLT protocols and the failure of traditional financial regulation with respect to those protocols represents further evidence that tying regulation to the existence of intermediaries undermines the efficacy of the legal system.

Layer-1 DLT protocols and decentralized Layer-2 smart contract protocols provide digital infrastructure for facilitating transactions but do not actually shoulder any of the policy, consumer protection, and illicit finance risks that financial regulation tries to mitigate. Such protocols do not generally aggregate capital in order to independently decide which firms can best put it to productive use.[216] Layer-1 DLT protocols and Layer-2 smart contract protocols also do not issue signals as to the merits of complex financial

---

210. *See* Eric W. Hess, *Bridging Policy and Practice: A Pragmatic Approach to Decentralized Finance, Risk, and Regulation*, 128 PENN. ST. L. REV. 347, 355–63 (2024).

211. *See* Reyes, *supra* note 23, at 1352–53.

212. *See* Hess, *supra* note 210, at 363–65.

213. *See* Schwarcz, *supra* note 27, at 1443; Schwarcz, *Sustainable Financial Regulation*, *supra* note 130, at 428.

214. *See* Schwarcz, *supra* note 27, at 1441–42.

215. *See id*. at 1444–46.

216. *See generally* ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION (2016) (explaining the data operation and validation process, which does not involve aggregating funds and directing them in a discretionary manner to firms deemed worthy by a centralized decisionmaker. There is no centralized decision maker).

instruments—they do not serve as an information clearinghouse.[217] Because such protocols do not perform traditional financial intermediary market functions, they should not be regulated in the same way as financial intermediaries—the protocols do not pose the same risk, so they should not be subject to the same regulation and should not be expected to produce the same regulatory outcome.[218] Instead, to the extent law "regulates" open-source Layer-1 DLT protocols and Layer-2 smart contract protocols at all, it should be in accordance with the functions the protocols perform as digital infrastructure resources, leaving regulation to intervene with respect to individual actors using the protocol, as it does with any other form of digital infrastructure resource. Lawmakers, however, struggle to craft appropriate regulatory frameworks for DLT protocols for the same reason they struggle to keep pace with the ever-changing and increasingly complex financial marketplace: taking a functional approach sounds great, but it remains unclear how to operationalize the theory in every context.

By way of example, consider the issue of prosecuting the developers of non-custodial software as money transmitters. Recognizing that as a matter of technical reality, non-custodial software does not give control over customer assets to the person who crafted the software's code, lawmakers introduced the Blockchain Regulatory Certainty Act (BRCA) on May 21, 2025,[219] and again on January 12, 2026.[220] The BRCA aims to provide a safe harbor for developers of non-custodial blockchain software from prosecution as money transmitters under 18 U.S.C. 1960.[221] The BRCA reaches a result that flows from a functional analysis—by considering the function performed by money transmitters and comparing it to the function of non-custodial software

217. Rather than keep data internally, open-source public Layer-1 DLT protocols "like Bitcoin and Ethereum are designed to be transparent—so that anyone can view transactions and wallet balances." Dhiraj Nallapaneni, *Blockchain Explorers: A Beginners Guide 2025*, COINLEDGER, https://coinledger.io/learn/blockchain-explorers [https://perma.cc/BT3R-A7GQ] (last visited July 30, 2025). Entities external to the protocols interact with the publicly available data on Layer-1 DLT protocols and make it searchable and more easily accessible to the public. *See id*. Even this function is very different than the function of information clearinghouse and signal provider served by financial intermediaries.

218. *See* Hess, *supra* note 210, at 394 (documenting the claims made by regulatory agencies that they are simply pursuing an enforcement strategy of "same activities, same risk, same rules" or "same activities, same risks, same regulatory outcome[s]").

219. H.R. 3533, 119th Cong. (2025). Indeed, the law had been introduced in the House in both 2023 and 2024 as well.

220. S. 3611, 119th Cong. (2025); *see* Press Release, Cynthia Lummis, Lummis, Wyden Introduce Bipartisan Legislation to Protect Blockchain Developers from Money Transmitter Requirements (Jan. 12, 2026), https://www.lummis.senate.gov/press-releases/lummis-wyden-introduce-bipartisan-legislation-to-protect-blockchain-developers-from-money-transmitter-requirements/ [https://perma.cc/867H-5PH3].

221. *See* Lummis, *supra* note 220.

developers—and concludes that such developers do not undertake money transmission services because they serve different functions. However, the law itself is not an example of functional regulation. As originally written, instead of using functional language to describe the activity covered by the safe harbor, the BRCA used technology-specific terminology that arguably described activity and software the does not exist.[222] Even if such an error did not invalidate the safe harbor that the BRCA intended to provide, the problem with enacting a law that reflects the result of a functional analysis without actually enacting functional regulation is that the safe harbor is limited to the one very specific context of money transmission but would not come to the aid of open source developers that create protocols like 0x and Deredex. Eventually, new drafts of the BRCA resolved the issue of technical neutrality, and the BRCA does in fact represent a step in the right direction. However, the development of the BRCA make clear that even with all the recent attention on the fact that Layer-1 DLT protocols and Layer-2 smart contract protocols do not serve the same functions as financial intermediaries, well-meaning lawmakers and regulators struggle to adopt a methodology that would enable a new, functional form of regulation.

A variety of disciplines have, however, successfully deployed different methodologies that they might refer to as a "functional method." Professor Frischmann, for example, built his functional definition of infrastructure on an economic approach to function.[223] Professor Schwartz similarly grounds his functional financial regulatory framework in the economic functions performed by financial intermediaries.[224] In law, the functional method is operationalized most successfully in two arenas: commercial law and comparative law. In commercial law, the Uniform Law Commission (ULC) and the American Law Institute (ALI) jointly undertake a functional approach

222. The BRCA's core provision provided a safe harbor from money transmission prosecution so long as the developer does not have "control over digital assets" through the software. The term "digital assets," for its part was defined as "any form of intangible personal property that can be exclusively possessed and transferred person to person without necessary reliance on an intermediary." Blockchain Regulatory Certainty Act, H.R. 3533, 119th Cong. § 2(c)(5) (2025). As a matter of property and commercial law, it is impossible to "possess" intangible property because possession is a physical concept that assumes the tangibility of the property possessed. *See* João Marinotti, *Possessing Intangibles*, 116 NW. L. REV. 1227, 1228–30 (2022). Had the BRCA been enacted using this language, the law would have provided protection to no one because it covered activity related to a type of property that does not exist as a legal and factual matter. This kind of error highlights the importance of using technology-neutral language rather than technology-specific language when crafting regulation for blockchain infrastructure, as further discussed below.

223. FRISCHMANN, INFRASTRUCTURE, *supra* note 46, at xiii.

224. Schwarcz, *supra* note 27, at 1445.

when drafting and maintaining the Uniform Commercial Code (UCC).[225] Because the UCC provides the framework for commercial contracting, the ULC and the ALI map the rules it contains to the economic realities of transactions as they are undertaken in commerce.[226] They achieve this feat by engaging an exceptional number of stakeholders during any process that might result in UCC revisions, and by engaging in a detailed and instructive discourse about the factual realities facing actors in commerce.[227] While the process is diligent, thorough, and as inclusive as possible, the functional method used to craft and maintain the UCC does not move very quickly.[228] The measured pace of the commercial law approach to the functional method may pose certain disadvantages for addressing the fast pace of federal regulatory developments in the DLT space;[229] however, the principles underlying the commercial law functional method can be adapted to improve the regulatory enterprise.

In a separate context, the comparative law functional method considers elements of a legal system in light of the function that they serve in responding to a societal problem.[230] Importantly, comparative law starts by identifying the societal problem and then looks broadly for ways that the society in question has addressed this problem, recognizing that not all functional equivalents will be laws; rather, there may be "other institutions, legal or non-legal, that perform the same function."[231] Comparative law also recognizes that when two societies address the same problem with law, they may do so through different areas of law altogether, and therefore comparative law views the functional method as a methodological tool for identifying when "different

225. *See* John L. Gedid, *U.C.C. Methodology: Taking a Realistic Look at the Code*, 29 WM. & MARY L. REV. 341, 369–70 (1988) (discussing the functional method as "situation-sense" as a key role in the drafting and interpretation of the UCC).

226. *See id.* at 343.

227. *See* UNIFORM LAW COMMISSION, A SUMMARY OF THE 2022 AMENDMENTS TO THE UNIFORM COMMERCIAL CODE 1 (2022), https://flabizlaw.org/wp-content/uploads/2022/08/UCC-Art-12-Summary-Amendments-2022_Summary.pdf [https://perma.cc/G6KD-XGZW] (explaining that between 2019 and 2022, the ALI and the ULC worked with "approximately 350 observers from academia, trade groups, government agencies, law firms, private technology companies, and foreign participants from multinational law reform organizations or who are active in technology-related law reform efforts in their own countries").

228. *See id.*

229. *Cf.* Schwarcz, *supra* note 27, at 1443 (explaining how the Uniform Commercial Code approach to regulation may not function well in areas governed by federal law).

230. Ralf Michaels, *The Functionalism of Legal Origins*, *in* DOES LAW MATTER? ON LAW AND ECONOMIC GROWTH 1, 3 (Michael Faure & Jan Smits eds., 2011).

231. Ralf Michaels, *Comparative Law by Numbers? Legal Origins Thesis,* Doing Business *Reports, and the Silence of Traditional Comparative Law*, 57 AM. J. COMPAR. L. 765, 778 (2009).

legal rules can play similar functions."[232] "Functionalist comparative law compares systems by focusing on facts, such as the effects of rules, events, and judicial responses or decisions in response to real life situations."[233] Functionalist comparative law then applies "the theory that [comparative law's] objects must be understood in the light of their functional relation to society" to the facts present in the society or system being studied.[234] Together, this process of functional analysis allows the identification of doctrinally or institutionally different responses to the same problem that fulfill similar functions.[235] As with the commercial law approach to developing legal rules that reflect the function of transactions in commerce, the comparative law functional method grounds itself in the factual and social reality that affects different legal systems. This, in turn, resonates with the approach that internet scholars have taken in identifying digital infrastructure resources.

Indeed, more broadly, scholars also often use a functional frame when considering what law applies to issues at the intersection of law and emerging technology. For example, when scholars consider the intersection of artificial intelligence systems and law, they first recognize that artificial intelligence systems do not stand on their own as mere technical artifacts, but rather, such systems are built for and deployed in a specific social context.[236] Only by considering their socio-technical nature does the true function of an algorithmic system become clear.[237] And only by understanding the true function of an algorithmic system can the law anticipate how to mitigate any

232. Tom Ginsburg, *Lawrence M. Friedman's Comparative Law, with Notes on Japan*, 5 J. COMPAR. L. 92, 102 (2010) (citing R. ZWEIGERT & H. KOTZ, AN INTRODUCTION TO COMPARATIVE LAW (TONY WHITE trans., 3rd ed. 1983)).

233. Reyes, *Conceptualizing Cryptolaw*, *supra* note 63, at 415 (citing Ralf Michaels, *The Functional Method of Comparative Law*, *in* THE OXFORD HANDBOOK OF COMPARATIVE LAW 339, 342 (Mathias Reimann & Reinhard Zimmermann eds., 2d ed. 2019)).

234. Michaels, *supra* note 236, at 342.

235. *Id.*

236. *See* Carla L. Reyes & Jeff Ward, *Digging into Algorithms: Legal Ethics and Legal Access*, 21 NEV. L.J. 325, 354–55 (2020); Paul M. Leonardi, *Materiality, Sociomateriality, and Socio-Technical Systems: What Do These Terms Mean? How Are They Different? Do We Need Them?*, *in* MATERIALITY AND ORGANIZING: SOCIAL INTERACTION IN A TECHNOLOGICAL WORLD 25, 38 (Paul M. Leonardi, Bonnie A. Nardi & Jannis Kallinikos eds., 2012) (citing Jos Benders et al., *First Organise, Then Automate: A Modern Socio-Technical View on ERP Systems and Teamworking*, 21 NEW TCH., WORK & EMP. 242 (2006); Robert P. Bostrom & J. Stephen Heinen, *MIS Problems and Failures: A Socio-Technical Perspective Part II: The Application of Socio-Technical Theory*, 1 MGMT. INFO. SYS. Q. 11, 14–15 (1977)); LUCY SUCHMAN, HUMAN-MACHINE RECONFIGURATIONS 42–43 (2d ed. 2007) (explaining that "we are more likely to view ourselves as engaging in interaction with [a machine] than as just performing operations on it or using it as a tool to perform operations upon the world").

237. *See* Reyes & Ward, *supra* note 236, at 355.

related risk.[238] This approach systematizes and crystalizes the two core inquiries that each of the other three disciplines (financial regulation, commercial law, and comparative law) ask in different ways when engaging in the functional method: (1) as a matter of technical reality, what function does the technological system serve, and (2) as a matter of policy and social values, what function does society need it to serve? Only when both the technical function of the system and the societal demands on how the technology should function are clearly identified can legislatures and regulators determine what function law can and should serve in relation to the technology. It is the failure of legislatures and regulators to engage in this inquiry that has led to the law's failure to recognize Layer-1 DLT protocols and Layer-2 smart contract protocols as a foundational new wave of digital infrastructure and instead mistakenly apply regulation for intermediaries to systems where no intermediaries exist. Rectifying this policy mistake moving forward requires internalizing core principles of the functional approach that inform all the disciplines that use it when adopting regulation for Layer-1 DLT protocols and Layer-2 smart contract protocols.

B. Five Key Principles of Functional Regulation Lawmakers Should Internalize as they Continue to Confront Policy Choices in an Increasingly Disintermediated Society.

Professor Schwarcz's proposal for functional financial regulation revolves around the four micro-prudential functions of the financial intermediaries and concerns about preventing systemic risk at the macroprudential level.[239] The commercial law approach to drafting law from a functional perspective requires constant monitoring and updating that may prove difficult to achieve at the federal level.[240] The comparative law functional method, for its part, was created for work involving comparisons

238. As a result, there is no generalized "regulation" of artificial intelligence systems at the source code level. Rather, lawmakers and scholars address legal issues that arise within a specific context to which artificial intelligence systems are applied. *See, e.g.*, Nathan Cortez, *A Black Box for Patient Safety?*, 68 DEPAUL L. REV. 239, 244–50 (2019) (exploring health care regulation in an age of experimental AI); Harry Surden, *Artificial Intelligence and Law: An Overview*, 35 GA. ST. U. L. REV. 1305, 1326–37 (2019) (exploring existing AI tools and their relationship to law and law practice); Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1346–53 (2018) (exploring the role of trade secret law in preventing defendants from confronting evidence against them produced by AI and other emerging technologies); Jason R. Bent, *Is Algorithmic Affirmative Action Legal?*, 108 GEO L.J. 803, 805–09 (2020) (exploring the intersection of algorithms and employment law).

239. *See* Schwarcz, *Sustainable Financial Regulation*, *supra* note 130, at 430–34.

240. *Id*. at 428; Schwartz, *supra* note 27, at 1443.

across legal systems,[241] making it an approach that may not map wholesale to designing functional regulation of DLT.[242] The broader questions asked about the technical function of the system and the functional needs of society with relation to the technical system help systematize the inquiries across each of the other three disciplines when considering how to regulate activity undertaken through Layer-1 DLT protocols and Layer-2 smart contract protocols. As a result of that process of systemization, this Section extrapolates from the functional method several policy principles that cross each of the disciplines in which the functional method is used that lawmakers can use to identify public digital infrastructure and then focus regulation on activity undertaken through such infrastructure. These principles should serve as policy guideposts for the new era of emerging technology that lawmakers now face.

1. The functional method should apply to the substance of regulation rather than the form of regulation.[243]

Undertaking a functional regulatory approach requires fact-intensive inquiries that investigate the function of the object to be regulated,[244] the societal context in which the regulated object achieves that function,[245] the societal demands upon and values associated with that function,[246] and the risks that might prevent the regulated object from fulfilling its function and meeting the necessary societal demands placed on it while nevertheless upholding important related societal values.[247] When innovative and emerging technology disrupts functions traditionally fulfilled by long-standing institutional actors, policy makers can be tempted to view the changed function as more of a change in form rather than substance.

---

241. *See* Michaels, *supra* note 236, at 341–42.

242. For a proposal of how the comparative functional method might be used to construct both regulatory structures and private law solutions for DLT, see Reyes, *supra* note 26, at 224–27; Reyes, *Conceptualizing Cryptolaw*, *supra* note 63, at 389; Carla L. Reyes, *Enforcing International Law in an Era of Decentralized Entities*, 65 HARV. INT'L L.J. ONLINE (Dec. 20, 2024), https://journals.law.harvard.edu/ilj/2024/12/enforcing-international-law-in-an-era-of-decentralized-entities/ [https://perma.cc/5MFL-8PYU].

243. *See* Schwarcz, *supra* note 27, at 1449–50.

244. *See* Reyes, *Conceptualizing Cryptolaw*, *supra* note 63, at 416–17; Schwarcz, *supra* note 27, at 1451–52.

245. *See* Reyes & Ward, *supra* note 236.

246. *See id.* at 355.

247. *Cf.* Schwarcz, *supra* note 27, at 1451–52 (discussing how market failure and risk should inform regulation design to ensure it aligns with "the interests of principals and their agents").

This has been the crux of the financial regulatory approach to the Layer-1 DLT protocols and Layer-2 smart contract protocols: an assumption, even after recognizing that they function differently than intermediaries at a purely technical level, that the protocols perform the same activity as traditional intermediaries, just in a different form.[248] So, for example, based on a belief that non-custodial wallet software performs the same functions as brokers, just through a different form, the Internal Revenue Service revised the definition of broker in its regulations so that anyone who provides a "trading front-end service" or "other effectuating services" must collect and report data even if done for free and even if done without actually taking custody of assets of any kind.[249] Doing so ignores the substantive differences between the functions served by non-custodial wallet software as opposed to those functions performed by custodial brokers.[250] Ultimately, ignoring these core difference creates a rule with which most non-custodial wallet software simply cannot comply as a matter of technical and functional reality.[251]

If regulators consider that the technical system might change the substance of activity in legally consequential ways rather than merely change the form through which the same function is achieved, they will also move beyond merely changing the form of regulation rather than the substance. As a matter of technical reality and societal demand, non-custodial wallet software serves the same function as a physical wallet that holds a person's cash, debit, and credit cards.[252] The only person or entity capable of reporting data related to the use of the items held within the wallet is the person or entity in control of the wallet—in this case the person using the items within the wallet to conduct software operations on distributed ledger technology.[253] If the IRS wants individuals to report on every software operation conducted with the technical artifacts held in their non-custodial software wallets, the substance of the regulation must change to reflect the same approach the IRS uses to require reporting of barter and cash transactions. Failure to do so jeopardizes the future of important digital infrastructure resources including

248. *See* Hess, *supra* note 210, at 394.

249. Treas. Reg. § 1.6045-(a)(21)(iii)(B) (2024).

250. *See* Complaint for Declaratory & Injunctive Relief ¶ 15, Blockchain Ass'n v. Internal Revenue Serv., No. 24-cv-03259-X (N.D. Tex. Dec. 27, 2024) (alleging that DeFi protocols "remove the very bank-like intermediaries that might be in a position to report on transactions").

251. *See id.* ¶¶ 13–15 ("[C]ompliance is impossible . . . given how DeFi and blockchain technology works").

252. *See id.* ¶ 9 ("[D]ecentralized protocols allow users to transact with their digital assets while maintaining custody over them using 'self-custodial' or 'non-custodial' wallet applications, so named because no institution or entity takes or maintains custody of the assets in the wallet applications, similar to keeping cash in a physical wallet.").

253. *See id.* ¶¶ 8–9.

open-source non-custodial wallet software, Layer-1 DLT protocols, and Layer-2 smart contract protocols.[254]

A truly functional approach to DLT regulation applies the functional method to the substance of the regulation rather than the form. Doing so allows legislatures and regulators to craft rules that both address the functional risks associated with the actual function of new technology like non-custodial software wallets, while also preserving the important policy of open access for related digital infrastructure resources. Focusing on the substance of regulation rather than the form of regulation enables a holistic functional regulatory approach that can preserve multiple policy aims at once: preserving transactional autonomy, enhancing consumer protection, preventing illicit finance, enforcing tax obligations, and preserving open access to digital infrastructure resources.

2. Functional regulation should be technology neutral.

Functional regulation should craft legal rules that are technology neutral and focus instead on regulatable activity.[255] Frischmann's definition of infrastructural resources is technology neutral. It applies with equal force to describe industrial infrastructure as it does to describe digital infrastructure.[256] Similarly, the UCC drafters examine the functions of commercial practices and then craft rules that address those practices in technology neutral terms.[257] The benefit of taking a technology neutral approach is two-fold: (1) a technology-neutral approach forces lawmakers to truly understand the functional activity for which it seeks to craft legal rules; and (2) technology neutral rules enable a sort of legal future-proofing—the law will apply to any activity that performs the function irrespective of the tool used to aid in the activity.

---

254. Indeed, many commentators go much further than that, suggesting that the IRS broker rule is so broad as to cover software operations undertaken through Internet Service Providers—like AT&T or Verizon. *Id.* ¶ 98.

255. Technology neutral drafting lies at the heart of the functional method. It requires drafting laws that describe the function of what should be regulated, rather than calling out a specific activity. For example, the Uniform Electronic Transactions Act is a technology neutral approach to providing for the legal sufficiency of digital signatures—regardless of the specific technology used to create the digital signature. The technological neutrality of the law enables the law to be future proof in so far as it already encompasses signatures via blockchain protocols or smart contracts. Indeed, attempts by states to amend their version of UETA by adding technology-specific provisions to accommodate smart contracts actually achieved the opposite. *See* Reyes, *Language Wars: Smart Contracts*, *supra* note 58, at 87–88, 109–12.

256. FRISCHMANN, INFRASTRUCTURE, *supra* note 46, at 923–29.

257. *See* Marek Dubovec, *Toward Decentralized Commercial Law for Digital Assets*, 19 NW. J. TECH. & INTELL. PROP. 239, 242–43 (2022).

The difficulty of the technology neutral approach is also two-fold, however. First, the technology-neutral approach to legal drafting has been criticized as leading to the use of overly abstract or archaic language in drafting statutory text. The UCC, for example, is often criticized for seemingly having been written in a different language—a technology neutral one.[258] The second difficulty of the technology neutral approach is that it requires a time intensive and demanding fact gathering process. The technology neutral approach only works if what the law describes in technology neutral language is an accurate description of the function achieved by the activity subject to the law. Despite these drawbacks, a technology neutral approach ensures strict adherence to the principle of reflecting the function of an activity in the substance of regulation rather than the form of regulation. One cannot be achieved well without the other.

3. Functional regulation should be grounded in the factual and technical realities of Layer-1 DLT protocols and Layer-2 smart contract protocols.

The innovative nature of the technology and the industry will require lawmakers to consider whether and how new tools serve which functions. As lawmakers and regulators consider the function of Layer-1 DLT protocols and Layer-2 smart contract protocols, they will inevitably come to the determination that such protocols operate entirely in the background, enabling system functionality that: is available to anyone who wants to access it (e.g., available on a nonrivalrous basis), is used as a tool in achieving downstream productive activity, and supports a variety of public, private and social goods.[259] And yet, even when it has been confirmed that a given Layer-1 DLT protocol or a specific smart contract protocol serves as a digital infrastructural resource, the next step is to understand the societal demands placed on the infrastructure. Only at that point is it possible to determine the scope and content of relevant rules needed to mitigate any negative externalities that might prevent the technology from fulfilling the demands placed on it by social contexts.

---

258. *See* Gedid, *supra* note 225, at 341 (noting complaints that the UCC text is ambiguous or inconsistent). Another such example is the Uniform Electronic Transactions Act, which smart contract advocates believed not to apply to signatures implemented via smart contracts because smart contracts were not specifically mentioned in the act. Smart contract advocates therefore convinced a variety of states to alter their uniform statutes to "accommodate" smart contracts, only to actually achieve the opposite by ultimately excluding them from technology neutral language that previously covered smart contracts without any problem. *See* Reyes, *supra* note 80, at 999 n.88.

259. *See* FRISCHMANN, INFRASTRUCTURE, *supra* note 46, at 61–62 (describing the three criteria infrastructural resources satisfy).

When considered from this light, one of the challenges to implementing functional regulation is that the type of investigations required to take a deep-dive into both the technology and its uses requires a collaborative stakeholder-rich approach. Perhaps anticipating this and recognizing the usefulness of the functional approach, regulators and lawmakers are currently working to create spaces for stakeholder engagement and technology education.[260] These efforts signal the importance of increased innovation within regulators themselves to develop adequate technical expertise to achieve functional regulation. As Congress hears testimony about the efficacy of private-public partnership in creating regulatory technology (RegTech) solutions to address legal compliance in decentralized applications,[261] and as lawmakers both within the United States and overseas implement regulatory sandboxes,[262] it becomes clear that lawmakers and regulators are being pro-active in building their capacity to test functional regulation. Such innovative and collaborative stakeholder building efforts should be encouraged.

4. Functional regulation should embrace public review and comment of proposed regulations to ensure broad stakeholder participation.

A key challenge to the functional regulatory approach is that it requires a certain level of expertise of lawmakers and their policy teams that may exceed their realistic time commitment capacity. First, the functional regulatory approach requires understanding Layer-1 DLT protocols and Layer-2 smart

260. For example, the U.S. Securities and Exchange Commission recently launched a Crypto Task Force to study digital assets markets and craft a clear path for the application of federal securities laws when warranted. *Crypto Task Force*, SEC, https://www.sec.gov/about/crypto-task-force [https://perma.cc/2Q9E-BH4A] (last visited July 31, 2025). The House Digital Assets, Financial Technology, and Artificial Intelligence Subcommittee held a hearing entitled "A Golden Age of Digital Assets: Charting a Path Forward" in February 2025. Memorandum from Comm. Majority Staff, Comm. on Fin. Serv. to Members of the Comm. on Fin. Serv. (Feb. 6, 2025) (announcing that the Subcommittee on Digital Asset, Financial Technology, and Artificial Intelligence would hold a hearing titled "A Golden Age of Digital Assets: Charting a Path Forward" and announcing expected witnesses) https://docs.house.gov/meetings/BA/BA21/20250211/117872/HHRG-119-BA21-20250211-SD002.pdf [https://perma.cc/ VXX2-7EMM].

261. *See* GOPFinancialServices, *Hearing Entitled: Decoding DeFi: Breaking Down the Future of Decentralized Finance*, at 30:56–56:08 (YouTube, Sep. 10, 2024), https://www.youtube.com/watch?v=YEz4TgWNj-U [https://perma.cc/9SBC-YCF6] (discussing how to address DeFi regulation).

262. Durham, *supra* note 183, at 48–49; Patrick Gleason, *Regulatory Sandboxes Give States an Edge Attracting Innovation and Investment*, FORBES (Apr. 21, 2022, at 09:32 ET), https://www.forbes.com/sites/patrickgleason/2021/12/31/regulatory-sandboxes-give-states-an-edge-attracting-innovation-and-investment/ [https://perma.cc/TLF2-BAJC]; Hilary J. Allen, *Regulatory Sandboxes*, 87 GEO. WASH. L. REV. 579, 592 (2019).

contract protocols at a sufficiently sophisticated level so as to be able to identify whether the demand for the protocol rests in characteristics internal to the protocol or rests in downstream applications being built on or with the protocol. Second, even if lawmakers can internally source this level of technical expertise, functionally regulating Layer-1 DLT protocols and Layer-2 smart contract protocols requires understanding the social context in which the protocols will be put to use. "Identifying the social context requires more than merely naming a context. A social context is composed of a variety of stakeholders, processes, rules, and other institutional forces (such as roles, statuses, hierarchies, power relations, and communication networks)."[263] Understanding the social context and its impact on the function of an emerging technology "requires understanding each of these components of the social system and the linkages between them."[264] Practically speaking, however, how can lawmakers implement the functional regulatory approach given their time and resource constraints?

In order to achieve a truly functional analysis of both the technology and its social context, functional regulation should be undertaken through a legislative approach that appropriately empowers an existing regulator to promulgate rules in accordance with the Administrative Procedure Act.[265] More than mere rule-making, however, a functional regulatory approach would require broad stakeholder coalition building in order to foster relationships that enable trust. Trust building through coalition building is an important element for functional regulation because regulators are heavily dependent upon stakeholders for education in the technology realm and insight into the relevant social contexts. Further, regulators will only listen to comments submitted during the request for comments if they can ascribe a measure of trust to the person or entity submitting the comment.[266] Indeed,

263. Reyes & Ward, *supra* note 236, at 355.

264. *Id*.

265. *See* 5 U.S.C. § 553.

266. The broker IRS rules were noticed and put up for public comment. Many commented. The IRS did not listen. The IRS failed to fully understand the technology about which it sought to make new rules, and failed to understand the social context in which the technology operates, so no trustful stakeholder coalition had been built sufficiently to encourage the IRS to listen to and alter the final rule to reflect the comments submitted. *See Industry Groups Sue Over Finalized IRS "Broker" Rulemaking*, DEFI EDUC. FUND (Dec. 27, 2024), https://www.defieducationfund.org/post/industry-groups-sue-over-finalized-irs-broker-rulemaking [https://perma.cc/ 7RPC-WR3N] ("During the rule's comment period, the public warned the IRS and Treasury that moving forward with the rule would cripple the digital asset industry. But the government ignored this feedback, leaving the digital asset sector with a rule that puts unlawful compliance burdens on software developers who build so-called "trading front-end services.").

CFTC Commissioner Summer Mersinger, in dissenting from the orders on ZeroEx DAO and Deridex, "questioned whether enforcement actions were suitable…suggesting that rulemaking and stakeholder engagement might provide a more comprehensive approach."[267] Specifically, Commissioner Mersinger "emphasized the need to balance regulatory oversight with fostering responsible innovation and stakeholder engagement."[268]

The importance of building a coalition of stakeholders that can provide insight into the factual realities of how the technology functions in a given social context is reflected in one of the most active contexts that applies the functional method to legal rule drafting: the Uniform Commercial Code.[269] Whenever the Uniform Law Commission and American Law Institute begin an amendments project for the UCC, the meetings are open to the public, and members of the public can register to serve as "observers"—active participants in the uniform drafting process that provide key insight into how to structure new rules functionally.[270] These drafting coalitions work best when the observers and committee members trust each other. For example, the committee process that led to the adoption of the 2022 Amendments to the UCC involved a formal committee that worked alongside approximately 350 industry participants and lawyers serving as observers.[271] To replicate this kind of atmosphere at the federal level, regulations should be promulgated through an open notice and public comment period alongside open listening and dialogue sessions that allow stakeholders to elaborate on their policy recommendations, explain the technology in detail, and highlight how the social context in which the technology is put to use helps mold the function the technology serves when deployed.

5. Open access to digital infrastructure resources should be protected.

Because digital infrastructure resources are open to, and depended upon by, everyone, when lawmakers and regulators identify open-source Layer-1

267. Alexandra C. Scheibe, Rachel Rosen & Ethan M. Heller, *CFTC Crackdown: Three DeFi Platforms Face Enforcement Actions*, MCDERMOTT WILL & EMERY (Sept. 20, 2023), https://www.mwe.com/insights/cftc-crackdown-three-defi-platforms-face-enforcement-actions/ [https://perma.cc/UD69-TPJ9].

268. *Id*.

269. *See, e.g.*, UNIFORM LAW COMMISSION, *supra* note 227.

270. *Observer's Manual: 2020 Edition*, UNIF. L. COMM'N 3 (Mar. 30, 2020), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=60335478-d340-2e88-2e90-88ced3902cb3 [https://perma.cc/SE8F-8EY2].

271. *See* UNIFORM LAW COMMISSION, *supra* note 227.

DLT protocols and Layer-2 smart contract protocols that serve the function of digital infrastructure, one of the societal demands placed on those protocols should be considered a highly important value worth protecting: open access to the infrastructure resource. Preserving open access to the infrastructure will also require a regulatory refusal to turn software development best practices (like retaining the ability to upgrade the software's smart contracts) into regulatory jurisdictional hooks. Indeed, embracing functional regulation requires recognizing that the developers of the new wave of digital infrastructure resources are not intermediaries for regulatory purposes merely by writing and publishing code.[272] At least some courts are already adopting a functional method that leads them to effectively treat open-source Layer-1 DLT protocols and Layer-2 protocols as digital infrastructure. In *Risley v. Universal Navigation, Inc*, Judge Failla, siting in the Southern District of New York, determined that the "it defies logic that a drafter of computer code underlying a particular software platform could be liable under § 29(b) for a third-party's misuse of that platform."[273] But the DLT industry should not have to wait for the resolution of *ex post* disputes to confirm the principles of protecting blockchain digital infrastructure and confirmation that the engineers who built it are not imprisoned or otherwise held liable for creation of the infrastructure. Instead, lawmakers and regulators should adopt these five principles to help provide *ex ante* clarity in ways that go beyond one specific context like money transmission, but rather offer *ex ante* clarity for a large variety of activity that might be conducted using open-source public digital infrastructure.

---

272. Lawmakers are already beginning to internalize this principle, at least in part. On June 24, 2025, the U.S. Senate Committee on Banking, Housing & Urban Affairs released the Senate Banking Committee Crypto Market Structure Principles, which outlined several principles that reflect a functional approach and carry echoes of the principles outlined in this Article. *See* STAFF OF S. COMM. ON BANKING, HOUS. & URB. AFFS., 119TH CONG., SENATE BANKING COMMITTEE CRYPTO MARKET STRUCTURE PRINCIPLES (Comm. Print 2025) https://www.banking.senate.gov/imo/media/doc/6-24-25_market_structure_principles.pdf [https://perma.cc/N84 E-PA99] (noting that individual authors are Senators Tim Scott, Cynthia Lummis, Thom Tillis, and Bill Hagerty). For example, the principles recognize that "not all distributed ledger technology should be regulated equally." *Id.* In particular, "[l]egislation should recognize the different risks and benefits between centralized firms, decentralized finance protocols, and non-custodial software platforms." *Id.* The principles also specifically state that "self-custody of digital assets should be explicitly preserved," and that using DLT and smart contract protocols for "non-financial purposes, such as to manage health data, should not be regulated like financial products." *Id.* Finally, and perhaps most closely reflecting the principles outlined in this paper: "Legislation should not apply principles designed for centralized firms to decentralized protocols." *Id.* The authors of this Article could not agree more with that final sentiment: Decentralized protocols should instead be treated as public digital infrastructure to which access must remain available to all.

273. 690 F. Supp. 3d 195, 215 (S.D.N.Y. 2023).

V. CONCLUSION

Because open-source Layer-1 DLT protocols and open-source Layer-2 smart contract protocols represent the next wave of open-source digital infrastructure development, it is not at all surprising that they have been the subject of intense policy debates. Policy debates around the proper approach to road and bridge maintenance, intellectual property law reform, energy policy, network neutrality, and the internet have always sounded loudly in the halls of state and federal legislatures.[274] As Frischmann explained, the debates are loud, contentious, and prolonged because they are ultimately "a battle to control infrastructure resources, set the terms and conditions under which the public gets access, and determine how the infrastructure and various infrastructure-dependent systems will evolve over time."[275] The stakes are just as high in the debate over what regulatory approach should be used for the DLT industry. The discussions over whether and how to regulate Layer-1 DLT protocols and Layer-2 smart contract protocols touch on important questions of fundamental rights, personal autonomy, national economic resiliency, and the future of U.S. innovation.

This Article argues that because open-source Layer-1 DLT protocols and open-source Layer-2 smart contract protocols are nonrivalrous, support demand from downstream productive uses, and exhibit genericity—the ability to be the foundation upon which other private, public and social goods are built—regulation should approach such protocols functionally and recognize their role in the new era of decentralized commerce as digital infrastructure. A functional regulatory regime that characterizes such protocols as digital infrastructural resources would protect public access to the protocols while targeting activity-based regulation toward those that use the protocols to conduct regulable behavior. While this Article's proposal that a functional regulatory approach be applied to open-source Layer-1 DLT protocols and open-source Layer-2 smart contract protocols to achieve this outcome is novel, functional regulation of open-source protocols represents the historical norm. The United States has long taken a functional regulatory approach that recognizes open-source protocols as digital infrastructure while targeting regulation at specific behavior conducted through those protocols. The proposal in this Article merely suggests an extension of these policy priorities to the next wave of public digital infrastructure and develops a framework for doing so that recognizes the unique context of Layer-1 DLT protocols and Layer-2 smart contract protocols.

274. FRISCHMANN, INFRASTRUCTURE, *supra* note 46, at xi.
275. *Id*. at xi–xii.

Importantly, developing this framework may have important consequences for other emerging digital architecture currently developing at a rapid pace. Specifically, developing a working functional regulatory approach for emerging and complex technologies has implications for other applications of emerging technology in commerce, including artificial intelligence. Applying the framework proposed in this Article to other emerging technologies, particularly those that, like digital asset technology, stand as a national strategic priority for economic resiliency and innovation, will enable regulatory clarity for the development of other foundational decentralized technical architectures beyond DLT protocols. The importance of identifying which elements of emerging technology serve as digital infrastructural resources and protecting access to them as such by using the functional method proposed in this Article to craft new law cannot be overstated. Correctly calibrating regulation to emerging technologies will help pave the way for such technologies as they become the backbone of new and strengthened commercial life in the United States, just as PGP formed the backbone of new and strengthened expectations for privacy in the internet age.