Law's Detrimental Reliance on Intermediaries

*Carla L. Reyes**

Abstract

Emerging technology is law's magic mirror. Even as law seeks to cabin the effects of emerging technology in society, when we hold emerging technology up to law, emerging technology often provides opportunity for reflection that reveals flaws or gaps in legal constructs. Of course, rather than recognizing those flaws or gaps, law retorts back "mirror, mirror, on the wall, who is the fairest of them all?," demanding that all other disciplines and constructs bow before law's mighty, near-perfect reach. Often, no matter how strongly emerging technology demands that law bend, legal evolution only occurs after regulatory failures harm individuals on a massive scale. One emerging technology—blockchain technology—serves as a magic mirror for financial and capital market regulation. Since 2009, blockchain technology has promised to disrupt centralized financial intermediaries—institutions acting as middlemen between parties to facilitate financial transactions. As the blockchain technology industry grows, such disruptions become more and more apparent.

Although some point to recent turmoil in the cryptocurrency industry as evidence of the technology's failure, this Article argues instead that the cycles of expansion and explosion prevalent in the blockchain ecosystem represent the magic mirror effect of emerging technology. Cycles of boom and bust in the cryptocurrency and blockchain industries reveal deep flaws in regulatory structures that depend on the compliance of centralized intermediaries. Indeed, this Article argues that if considered at this angle with a wide enough lens, blockchain technology reflects deep cracks in the lawmaking process itself.

Blockchain technology reduces the need for intermediaries in certain circumstances and can enable flatter governance structures. When considering law's responses to cryptocurrency and blockchain technology, recent regulatory proposals and enforcement actions seem to emphasize the need for centralized intermediaries more than ever, proposing an expanding definition of intermediary in an effort to combat specific harms in financial markets. However, recent rapid and significant failures in the cryptocurrency markets shine a light on law's potentially detrimental reliance on intermediaries and offers an opportune moment to consider—both as a matter of substantive financial regulation and as a matter of lawmaking itself—when deeper decentralization might improve legal and policy outcomes. To that end, this Article ignites a discussion about whether and how blockchain technology can unlock an avenue for mitigating law's practical

* Associate Professor of Law, Southern Methodist University Dedman School of Law; Affiliated Faculty, Indiana University Bloomington Ostrom Workshop Program on Cybersecurity and Internet Governance; Research Associate, University College London Centre for Blockchain Technology.

need for centralized intermediaries and sets up further research exploring the potential for disintermediating the lawmaking process itself. Ultimately, perhaps, the magic mirror reflects the power of disintermediation in the lawmaking process as a means to improve the legitimacy, effectiveness, and function of law.

Table of Contents

Introduction

Beginning in May 2022, a series of events involving cryptocurrency, blockchain technology, and businesses built around those technologies would ignite indignation and consternation among lawmakers and policy pundits nearly everywhere.[1] First, the Terra-Luna ecosystem

[1] *See, e.g.*, Ty Roush, *Here Are All the Crypto Firms Facing Charges from Regulators This Year*, Forbes (Nov. 22, 2023, 11:44 AM), https://www.forbes.com/sites/tylerroush/2023/11/22/

spectacularly crashed in a matter of days in early May 2022.[2] Ultimately the crash of the TerraUSD ("UST") stablecoin would lead to a $40 billion loss in value.[3] The very next month, Celsius halted withdrawals, signaling financial trouble that ultimately ended in Celsius's bankruptcy.[4] Just five days after Celsius began to crumble, Babel Finance, a Hong Kong based company, also halted withdrawals.[5] And by the end of June, Three Arrows Capital defaulted on payments to Voyager Digital[6] and entered liquidation proceedings in the British Virgin Islands.[7] The onslaught continued in July, when Voyager Digital filed for Chapter 11 bankruptcy.[8] By November, high profile exchange FTX's financial woes

---

here-are-all-the-crypto-firms-facing-charges-from-regulators-this-year/ [https://perma.cc/5JPK-3SSA]; Scott Chipolina, *Regulators Get Tough on Crypto Funds After FTX Collapse*, Fin. Times (Apr. 23, 2023), https://www.ft.com/content/0bb9180c-309d-445c-a054-62f15c9bd7d4 [https://perma.cc/NCW5-7YJE]; Tony Romm, *Congress Took Millions from FTX. Now Lawmakers Face a Crypto Reckoning*, Wash. Post (Nov. 17, 2022, 5:00 PM), https://www.washingtonpost.com/us-policy/2022/11/17/congress-crypto-ftx-regulations-law/ [https://perma.cc/U83C-VSCK]; Allyson Versprille & Lydia Beyoud, *How Crypto's Meltdown Changed the Regulatory Debate*, Bloomberg (Jan. 13, 2023, 5:15 PM), https://www.bloomberg.com/news/articles/2023-01-07/how-crypto-s-meltdown-changed-the-regulatory-debate [https://perma.cc/RHN6-RJ2J].

2 Jiageng Liu, Igor Makarov & Antoinette Schoar, *Anatomy of a Run: The Terra Luna Crash* 1 (Nat'l Bureau of Econ. Rsch., Working Paper No. 31160, 2023), https://www.nber.org/papers/w31160 [https://perma.cc/FMW9-Z5AE].

3 David Yaffe-Bellany & Erin Griffith, *How a Trash-Talking Crypto Founder Caused a $40 Billion Crash*, N.Y. Times (June 22, 2023, 5:00 PM), https://www.nytimes.com/2022/05/18/technology/terra-luna-cryptocurrency-do-kwon.html [https://perma.cc/MFV5-3APM].

4 Olga Kharif & Joanna Ossinger, *Crypto Lender Celsius Files for Bankruptcy After Cash Crunch*, Bloomberg (July 14, 2022, 3:21 PM), https://www.bloomberg.com/news/articles/2022-07-14/crypto-lender-celsius-files-for-bankruptcy-in-cash-crunch [https://perma.cc/2SJU-AB3Y].

5 Oliver Knight, *Babel Finance Suspends Withdrawals, Citing 'Unusual Liquidity Pressures*,' CoinDesk (May 11, 2023, 1:42 PM), https://www.coindesk.com/business/2022/06/17/babel-finance-suspends-withdrawals-citing-unusual-liquidity-pressures/ [https://perma.cc/C3P6-CRYM]; Oliver Knight & Nikhilesh De, *Nexo Proposes Celsius Buyout as Rival Lending Platform Halts Withdrawals*, CoinDesk (May 11, 2023, 2:54 PM), https://www.coindesk.com/business/2022/06/13/nexo-proposes-celsius-buyout-as-rival-halts-withdrawals/ [https://perma.cc/9CXQ-3YJ5]; Frances Yue, *Days After Celsius Paused Withdrawals, Another Crypto Lender Babel Finance Followed Suit*, MarketWatch (June 17, 2022, 10:26 AM), https://www.marketwatch.com/story/days-after-celsius-paused-withdrawals-another-crypto-lender-babel-finance-followed-suit-11655476000 [https://perma.cc/9CXQ-3YJ5].

6 MacKenzie Sigalos & Arjun Kharpal, *One of the Most Prominent Crypto Hedge Funds Just Defaulted on a $670 Million Loan*, CNBC Crypto World (June 28, 2022, 11:23 PM), https://www.cnbc.com/2022/06/27/three-arrows-capital-crypto-hedge-fund-defaults-on-voyager-loan.html [https://perma.cc/CHC6-QGNH].

7 Jamie Crawley, *Three Arrows Capital Liquidation Ordered in British Virgin Islands*, CoinDesk (May 11, 2023, 2:50 PM), https://www.coindesk.com/business/2022/06/29/three-arrows-capital-liquidation-ordered-in-british-virgin-isles-report/ [https://perma.cc/52XJ-BAUJ].

8 Nina Bambysheva, *Crypto Broker Voyager Digital Files for Chapter 11 Bankruptcy*, Forbes (July 8, 2022, 4:45 PM), https://www.forbes.com/sites/ninabambysheva/2022/07/06/crypto-broker-voyager-digital-files-for-chapter-11-bankruptcy/ [https://perma.cc/2AJ6-6XCY].

started to leak to the public,[9] and the firm filed for bankruptcy.[10] By the end of November, BlockFi became the fifth major cryptocurrency-related business to file for bankruptcy.[11] The eight-month cascade of cryptocurrency-related business failures ended 2022 with the arrest of FTX founder Sam Bankman-Fried.[12] Then, as though the failures would never end, in January 2023, Genesis filed for Chapter 11 bankruptcy.[13] This long series of business collapses led to approximately $2 trillion in value lost to consumers and investors[14] alike and sparked intense debate on a variety of issues.

In particular, in the wake of these implosions, various regulators, lawmakers, and commentators quickly declared that cryptocurrency itself was to blame,[15] lambasted the decentralization sought by those in

---

9 Ian Allison, *Divisions in Sam Bankman-Fried's Crypto Empire Blur on His Trading Titan Alameda's Balance Sheet*, CoinDesk (Aug. 16, 2023, 5:56 PM), https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet [https://perma.cc/LL8T-EFCH].

10 David Yaffe-Bellany, *Embattled Crypto Exchange FTX Files for Bankruptcy*, N.Y. Times (Nov. 11, 2022), https://www.nytimes.com/2022/11/11/business/ftx-bankruptcy.html [https://perma.cc/LA59-3AJ6].

11 Joshua Oliver, Nikou Asgari & Oliver Ralph, *Crypto Lender BlockFi Files for Chapter 11 Bankruptcy*, Fin. Times (Nov. 28, 2022), https://www.ft.com/content/36a6ec4e-15f8-4b15-8bfa-076b87004264 [https://perma.cc/7VZW-KYZ5]; Dietrich Knauth, *Crypto Companies Crash Into Bankruptcy*, Reuters (Dec. 1, 2022, 2:30 PM), https://www.reuters.com/technology/crypto-companies-crash-into-bankruptcy-2022-12-01/ [https://perma.cc/UY4L-F9R6] (explaining that after Terra-Luna the order of bankruptcies was as follows: (1) 3AC, (2) Voyager Digital, (3) Celsius Network, (4) FTX, and (5) BlockFi).

12 Joe Walsh, *Sam Bankman-Fried Arrested in Bahamas as U.S. Files Criminal Charges, Officials Say*, Forbes (Dec. 12, 2022, 7:38 PM), https://www.forbes.com/sites/joewalsh/2022/12/12/sam-bankman-fried-arrested-in-bahamas-as-us-files-criminal-charges-officials-say/ [https://perma.cc/W6RA-ULPT].

13 Robert Hart, *Crypto Giant Genesis Files for Bankruptcy as Casualties Mount After FTX Collapse*, Forbes (Jan. 20, 2023, 5:41 AM), https://www.forbes.com/sites/roberthart/2023/01/20/crypto-giant-genesis-files-for-bankruptcy-as-casualties-mount-after-ftx-collapse/ [https://perma.cc/6T73-XWK8].

14 Kharif & Ossinger, *supra* note 4.

15 *See*, *e.g.*, Jamie Redman, *Elizabeth Warren Blames 'Crypto Risk' for Silvergate Bank's Litigation, Critics Dismiss Senator's Claims as 'Terribly Misinformed*,*'* Bitcoin.com News (Mar. 9, 2023), https://news.bitcoin.com/elizabeth-warren-blames-crypto-risk-for-silvergate-banks-liquidation-critics-dismiss-senators-claims-as-terribly-misinformed/ [https://perma.cc/Q86H-UF6Z]; Allison Morrow, *Elizabeth Warren: Crypto Giants are 'Collapsing Under the Weight of Their Own Fraud*,*'* CNN Bus. (Jan. 25, 2023, 2:48 PM), https://edition.cnn.com/2023/01/25/investing/crypto-elizabeth-warren-ftx/index.html [https://perma.cc/P6F4-GJL5]; Press Release, Sen. Elizabeth Warren, Warren, Marshall, Kennedy, Call on Silvergate, Bank that Handled Bankrupt Crypto Firm FTX's Funds, to Release All Records on Improper Transfer (Dec. 6, 2022), https://www.warren.senate.gov/oversight/letters/warren-marshall-kennedy-call-on-silvergate-bank-that-handled-bankrupt-crypto-firm-ftxs-funds-to-release-all-records-on-improper-transfer [https://perma.cc/U9JL-ETVC].

the cryptocurrency ecosystem as a sham,[16] and called for further taming of the crypto "Wild West"[17] or to somehow "ban" crypto altogether.[18] Indeed, certain regulatory actions—such as listing various Tornado Cash smart contract addresses on the sanctions list—sought to achieve a ban on the use of at least certain privacy protecting software.[19] This Article argues that, despite these popular refrains and sound bites from crypto critics, these events do not reveal a failure of blockchain technology or cryptocurrency but rather point to deep and repetitive regulatory failures. The issue was not, as is often alleged, that the cryptocurrency and blockchain industry is not regulated[20] but rather that the law that already applied—and ostensibly should have prevented or mitigated the harms resulting from these business implosions—failed to achieve its aims. Viewed in that light, rather than condemning cryptocurrency and blockchain technology, the cascade of blockchain-related business

---

16 *See, e.g.*, Hilary J. Allen, *The Superficial Allure of Crypto: Cryptocurrencies Can't Deliver Their Claimed Benefits, and Instead Pose Grave Risks*, INT'L MONETARY FUND: FIN. & DEV. (Sept. 2022), https://www.imf.org/en/Publications/fandd/issues/2022/09/Point-of-View-the-superficial-allure-of-crypto-Hilary-Allen [https://perma.cc/CW2Z-SHZF]; *see also* Sirio Aramonte, Wenqian Huang & Andreas Schrimpf, *DeFi Risks and the Decentralisation Illusion*, BIS Q. REV., Dec. 2021, at 33 (discussing the full decentralization of crypto as an "illusion" and pointing out the need for regulatory safeguards before the system collapsed in 2022).

17 Dave Michaels, *Crypto Is Still the Wild West Almost a Year After FTX Collapse*, WALL ST. J. (Oct. 11, 2023, 5:30 AM), https://www.wsj.com/finance/currencies/whats-changed-for-crypto-after-ftx-not-much-17daba37 [https://perma.cc/QQ7L-8ERU].

18 *See e.g.*, Charlie Munger, *Why America Should Ban Crypto*, WALL ST. J. (Feb. 1, 2023, 6:16 PM), https://www.wsj.com/articles/why-america-should-ban-crypto-regulation-economy-finance-china-england-trading-currency-securities-commodity-gamble-11675287477 [https://perma.cc/8ZS7-FA3S]; Sabrina Toppa, *U.S. Senate Banking Chairman: 'Maybe' We Should Ban Crypto*, THESTREET (Dec. 19, 2022, 2:03 PM), https://www.thestreet.com/crypto/news/us-senate-banking-chairman-maybe-we-should-ban-crypto [https://perma.cc/VGE6-QH5E]; Billy Bambrough, '*Limit or Eliminate'—Biden Executive Order Triggers Shock U.S. Bitcoin Ban Proposal After Radical Ethereum Upgrade and Wild Crypto Price Swings*, FORBES (Sept. 8, 2022, 6:30 PM), https://www.forbes.com/sites/billybambrough/2022/09/08/limit-or-eliminate-biden-executive-order-triggers-shock-us-bitcoin-ban-proposal-after-radical-ethereum-upgrade-and-wild-crypto-price-swings/ [https://perma.cc/T6H9-JYNM]; *Stablecoins: How Do They Work, How are They Used, and What are Their Risks?: Hearing Before the S. Comm. on Banking, Hous. & Urb. Affs.*, 117th Cong. 12 (2021) [hereinafter Allen, *Testimony*] (statement of Prof. Hillary J. Allen, Am. Univ. Wash. Coll. of L.).

19 Press Release, Dep't of the 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/7UC3-GR8Q] (announcing sanctions against "the entity" Tornado Cash); Nizan Geslevich Packin & Hadar Yoana Jabotinsky, *Blocking as Regulating? Blacklisting Generative AI*, 73 AM. U. L. REV. 1467, 1473 (2024) (describing the action against Tornado Cash as blacklisting).

20 Indeed, activity conducted through blockchain technology is quite heavily regulated and has been for some time. For an early discussion of such regulation and its shortcomings, see Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191, 194 (2016).

failures since May 2022 invites revision of failed and outdated regulatory frameworks.

Emerging technology is law's magic mirror. Certainly, law applies to emerging technology, and sometimes no new legal rules are required to govern activity undertaken via technology.[21] However, emerging technology often reflects various flaws or gaps in existing legal regimes.[22] Regulatory failures occur in areas of emerging technology when law refuses to recognize functional equivalence,[23] or lack thereof, in the technical architecture that enables new forms of economically and socially productive activity. Specifically, this Article argues that the recent slate of crypto-intermediary failures reveals deep flaws in regulatory structures that depend on the compliance of centralized intermediaries. This detrimental reliance on intermediaries to serve as the object of regulation[24] sits so deeply at the heart of public law's approach to risk mitigation, that it fails to recognize the serious risks associated with infinite intermediation[25] itself. By demonstrating that the heart of the recent cryptocurrency-related business scandals lies with centralized actors rather than the technology, this Article aims to encourage

---

21 *See, e.g.*, Douglas S. Eakeley & Yuliya Guseva with Leo Choi & Katarina Gonzalez, *Crypto-Enforcement Around the World*, 94 S. CAL. L. REV. POSTSCRIPT 99, 100 (2021) (explaining that although the U.S. does not have a separate regulatory framework for cryptocurrency, its regulatory agencies "*assume*[] that the pre-crypto rules are appropriate for complex technological innovations"); Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 532–33 (2015) (arguing that the core insights and methods of cyberlaw will apply to emerging issues in the new technology of robotics); Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 208 (1996) (arguing that to understand property law in cyberspace, one must learn intellectual property law and then apply it to cyberspace).

22 *See, e.g.*, Julie E. Cohen, *From Lex Informatica to the Control Revolution*, 36 BERKELEY TECH. L.J. 1017, 1027 (2021) ("The ultimate lesson of the control revolution for law is that networked information technologies are not simply new modes of knowledge production to be governed, but also powerful catalysts for organizational restructuring that change the enterprise of governance (and so, necessarily, also that of law) from the inside out." (footnote omitted)); Carla L. Reyes, *Autonomous Business Reality*, 21 NEV. L.J. 437, 442–43 (2021) (arguing that decentralized autonomous organizations reflect back the possibilities for corporate governance reform in more traditional corporations); Tom C.W. Lin, *The New Financial Industry*, 65 ALA. L. REV. 567, 590–95 (2014) (arguing that advances in financial technology revealed regulatory shortcomings).

23 For an early discussion of the importance of using the functional method to analyze activity conducted through blockchain technology, see Carla L. Reyes, *Conceptualizing Cryptolaw*, 96 NEB. L. REV. 384, 415–21 (2017).

24 In other words, the current regulatory paradigm uses centralized intermediaries as the archetypal "pathetic dot" from Professor Lawerence Lessig's influential pathetic dot theory of regulation. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 86–88 (1999).

25 *See generally* Tom C.W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643 (2015) (describing the inherently interconnected nature of finance as leading to infinite intermediation).

lawmakers to consider leaning into decentralization as an alternative path for the risk mitigation outcomes they seek. However, this Article argues that doing so requires fundamental changes in the process employed to create regulation. In particular, this Article argues that the disintermediated and participatory process that allows private law reform and harmonization projects to identify functional equivalents and use them to achieve policy aims should serve as a template for the development and enactment of public law.

To make these arguments, this Article first explains in Part I the historically increasing reliance of public law and regulation on intermediaries as an object of regulation. Part I explores the ways that regulation often reacts to the perceived threat posed by emerging technology through new and burdensome rules on entities designated, sometimes newly designated, as intermediaries. In Part II, the Article explores the history of cryptocurrency-intermediary failures, examining both earlier collapses and the events that have transpired since May 2022. In doing so, the Article examines the four most common narratives prevalent after the collapses in 2022 and 2023: (1) these bad things happened because cryptocurrency is not regulated, (2) the technology itself is to blame for these woes, (3) decentralization is a sham that resulted in these failures, and (4) cryptocurrency should simply be banned. Part II then demonstrates that although sensational, each of these blame narratives is demonstrably incorrect. Part II further argues that the damage done to consumers and the cryptocurrency ecosystem since May 2022 stemmed from traditional intermediary risks: bad behavior by those in charge of other people's money. The regulatory regime that relies on intermediaries to mitigate risk failed to prevent the crypto-intermediary failures of 2022 and 2023, reflecting deep flaws in the existing regime.

In Part III, the Article evaluates regulatory action since the collapses, which repeatedly insists on identifying and targeting an intermediary, even when doing so does not prevent the kinds of harms suffered when cryptocurrency intermediaries crashed in the summer and fall of 2022, and even when no intermediary functionally exists. This insistence on finding and targeting an intermediary ultimately impedes the adoption of workable rules and undermines the legitimacy of regulation and regulatory institutions. Indeed, the Article argues that the inflexibility of law in the face of disintermediated technology and business models stems, at least in part, from the deep layers of intermediaries used in the process of creating regulation. Enmeshed in their own systems and processes reliant on layers of intermediaries, lawmakers simply cannot imagine an approach where law applies to disintermediated activity. Ultimately, the Article concludes that cryptocurrency's ongoing regulatory battle acts as a magic mirror that reflects a poorly functioning public law and regulatory system. To remedy the regulatory gaps, the Article sets up further research into whether and how public lawmakers

and regulators can take a page from private law reform and harmonization efforts by employing a more participatory and truly functional approach to lawmaking.

I. U.S. Regulatory Regimes Increasingly Rely on Intermediaries but Nevertheless Fail to Prevent Harms Caused by Risky Intermediary Behavior

An exhaustive literature examines the use of regulatory tools that increasingly target intermediaries as the object of regulation.[26] In particular, finance and capital markets regulation rely heavily upon intermediaries.[27] This Part reviews the regulatory theory justifying reliance on intermediaries and the cyberlaw counternarrative that, when dealing with decentralized and emerging technologies, regulators may need to embrace additional tools to impact behavior.[28] This Part then examines the history of U.S. regulation of blockchain technology, highlighting that, despite the lessons of cyberlaw, U.S. regulatory regimes demand, and even encourage, centralization that the technology itself obviates. In so doing, this Part begins to uncover key inflection points for which blockchain technology acts as financial regulation's magic mirror.

---

26 *See, e.g.*, Gary Gorton & Andrew Winton, *Financial Intermediation*, *in* 1 Handbook of the Economics of Finance 433, 433 (G.M. Constantinides et al. eds., 2003) ("Financial intermediation is a pervasive feature of all of the world's economies."); Kenneth W. Abbott, David Levi-Faur & Duncan Snidal, *Introducing Regulatory Intermediaries*, 670 Annals Am. Acad. Pol. & Soc. Sci. 6, 7–8 (2017) (arguing that "[i]ntermediaries play diverse roles in regulation throughout the policy cycle" ranging from implementation of rules to compliance monitoring, enabling dialogue and feedback, and encouraging voluntary compliance); Sebastian Di Tella, *Optimal Regulation of Financial Intermediaries*, 109 Am. Econ. Rev. 271, 271 (2019) (exploring the best policy instruments for regulating financial intermediaries in recognition of "a large interest in the regulation of financial intermediaries, especially after the 2008 financial crisis"); Jai Massari & Christian Catalini, *DeFi, Disintermediation, and the Regulatory Path Ahead*, Reg. Rev. (May 10, 2021), https://www.theregreview.org/2021/05/10/massari-catalini-defi-disintermediation-regulatory-path-ahead/ [https://perma.cc/JN9K-EZNL] ("U.S. financial regulation assumes the presence of intermediaries, and it applies regulation to intermediaries as a way to regulate financial markets and related activities comprehensively."); Stephen J. Choi, *A Framework for the Regulation of Securities Market Intermediaries*, 1 Berkeley Bus. L.J. 45, 56–68 (2004) (exploring which regulatory approaches best fit which securities intermediary failures).

27 Lin, *supra* note 25, at 643 ("Intermediation is a fundamental fact of finance.").

28 Lessig, *supra* note 24, at 164–67 (arguing that four modalities impact (or regulate) behavior: the law, social norms, the market, and architecture, and that regulation of activity in cyberspace may need to rely more on the modalities other than law); Lawrence Lessig, Code: Version 2.0 123–24 (2006) (updating his discussion of the four modalities of regulation); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1387–91 (1996) (arguing that new rules will come to define cyberspace interactions, defined not by government-made law but rather by user interaction, social norms, and custom).

A. U.S. Regulatory Regimes Often Seek to Mitigate Negative Externalities by Targeting Intermediaries

Many critiques of the regulatory apparatus in the United States permeate public discourse, including that ill-fitting regulation kills innovation,[29] regulation fails to adequately understand risks associated with complex transactions,[30] businesses evade regulation in the name of progress,[31] and regulations requiring disclosure fail to achieve their goals,[32] among others. In the face of such critiques, which often resound quite loudly among actors in the blockchain technology industry, reviewing the basic theories justifying the regulatory apparatus is useful. Very broadly speaking, the traditional narrative anchors the need for regulation in the fact that rational actors will cause negative externalities in the pursuit of maximizing profit.[33] Regulatory regimes seek to influence relevant actors into undertaking desired behavior—namely, behavior that reduces risk of harm to others.[34] Specifically, regulation aims to mitigate the externalities that the actors would otherwise create if left to act entirely as they feel is most beneficial to their profit-seeking enterprise.[35]

Considering financial and capital market regulation more specifically, regulation generally targets negative externalities related to

---

29 *See, e.g.*, Joshua A.T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805, 830 (2015) (expressing concern that ill-fitting financial regulation may impede innovation in nonfinancial applications of blockchain technology).

30 Hilary J. Allen, *DeFi: Shadow Banking 2.0?*, 64 WM. & MARY L. REV. 919, 926 (2023) ("Complexity can make financial products—and their possible interactions with the broader financial system—harder to understand, increasing the chance that risks will go unanticipated."); Dan Awrey, *Complexity, Innovation, and the Regulation of Modern Financial Markets*, 2 HARV. BUS. L. REV. 235, 236–38 (2012) (arguing that the global financial crisis stemmed from "blind spots . . . emanating from within conventional financial theory"—namely, "fail[ure] to adequately account for both the complexity of modern financial markets and the nature and pace of financial innovation" (emphasis omitted)); Steven L. Schwarcz, *Disclosure's Failure in the Subprime Mortgage Crisis*, 2008 UTAH L. REV. 1109, 1109–10 (explaining that compliance with mandatory disclosures failed to adequately inform even sophisticated investors of the risks associated with subprime mortgage-backed securities because of the complexity of the transactions).

31 Elizabeth Pollman & Jordan M. Barry, *Regulatory Entrepreneurship*, 90 S. CAL. L. REV. 383, 415–16 (2017); Elizabeth Pollman, *The Rise of Regulatory Affairs in Innovative Startups*, *in* THE CAMBRIDGE HANDBOOK OF LAW AND ENTREPRENEURSHIP IN THE UNITED STATES 27, 32 (D. Gordon Smith et al. eds., 2018); Elizabeth Pollman, *Corporate Disobedience*, 68 DUKE L.J. 709, 731 (2019).

32 *See, e.g.*, OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 4 (2014) (cataloguing the evidence that regulatory disclosure regimes across a variety of sectors fail to produce the intended policy results); Schwarcz, *supra* note 30, at 1110 (arguing that the disclosure regime failed to prevent the harm of the subprime mortgage crisis even though disclosure compliance was common).

33 Brian Galle, *In Praise of Ex Ante Regulation*, 68 VAND. L. REV. 1715, 1722 (2015).

34 *Id.* at 1722–24.

35 *Id.*

transaction costs,[36] information asymmetries,[37] and risk complexity.[38] The financial system itself attempts to reduce the impact of these difficulties through a network of intermediaries that can "make core financial functions, like asset aggregation, market making, risk management, and information clearing, more efficient and less risky."[39] Traditionally, the financial intermediaries that performed these functions included "commercial banks, brokers, investment banks, and stock exchanges."[40] As financial intermediaries fulfilled these roles, technological and transactional innovations led to the emergence of new types of intermediaries and new types of markets.[41] Even as such entities resolve some of the traditional financial market risks, they also introduce risk of other negative externalities into the financial system and capital markets.[42]

Historically, in response to new risks posed by new technology or new forms of transactions, the U.S. regulatory system embraced the deployment of new technologies as what is commonly referred to now as Regulatory Technology, or "RegTech."[43] Indeed, between 1963 and 2008 the Securities and Exchange Commission ("SEC") and the Commodity Futures Trading Commission ("CFTC") actively adopted

---

36 *See* Franklin Allen & Anthony M. Santomero, *What Do Financial Intermediaries Do?*, 25 J. BANKING & FIN. 271, 272 (2001); Lin, *supra* note 25, at 646–48.

37 Allen & Santomero, *supra* note 36, at 272; *see* Lin, *supra* note 25, at 649.

38 *See* Lin, *supra* note 25, at 648.

39 *Id.* at 650 (citing Sudipto Bhattacharya & Anjan V. Thakor, *Contemporary Banking Theory*, 3 J. FIN. INTERMEDIATION 2, 3–7 (1993); Neal Galpin & Heungju Park, *The Roles of Financial Intermediaries in Raising Capital*, *in* CAPITAL STRUCTURE AND CORPORATE FINANCING DECISIONS: THEORY, EVIDENCE, AND PRACTICE 263, 265 (H. Kent Baker & Gerald S. Martin eds., 2011)).

40 *Id.*

41 Allen & Santomero, *supra* note 36, at 272 ("There has been a significant reduction in transaction costs and asymmetric information in recent decades. Over this same period, the importance of traditional banks that take deposits and make loans has, by some measures, been reduced. However, other forms of intermediaries such as pension funds and mutual funds have grown significantly. In addition, new financial markets such as financial futures and options have developed, as markets for intermediaries rather than for individuals."); Lin, *supra* note 25, at 652–54 ("While the core objectives of financial intermediation have remained the same, the methods and functionaries relating to those objectives have been changed by new technology and market developments.").

42 *See, e.g.*, Steven L. Schwarcz, *Regulating Shadow Banking*, 31 REV. BANKING & FIN. L. 619, 625, 638–41 (2012) (surveying the industry referred to as shadow banking and considering regulatory approaches to mitigate the new risks the industry introduces); Steven L. Schwarcz, *Systemic Risk*, 97 GEO. L.J. 193, 200 (2008) (arguing that the growth of disintermediation introduces new avenues for systemic risk to permeate a system); Stephen G. Cecchetti, *The Future of Financial Intermediation and Regulation: An Overview*, CURRENT ISSUES ECON. & FIN., May 1999, at 3–4 (arguing that regulation is warranted to address risks of consumer exploitation, systemic risk, and the moral hazard stemming from government guarantees).

43 *See* Eric W. Hess, *Bridging Policy and Practice: A Pragmatic Approach to Decentralized Finance, Risk, and Regulation*, 128 PENN ST. L. REV. 347, 348 (2024); Douglas W. Arner, Jànos Barberis & Ross P. Buckley, *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, 37 NW. J. INT'L L. & BUS. 371, 385–98 (2017); Phillip Treleaven, *Financial Regulation of FinTech*, J. FIN. PERSPECTIVES: FINTECH, Winter 2015, at 3, 9–10.

digital technologies to improve the structure and function of both the securities and commodities markets.[44] However, in the wake of the 2008 financial crisis, the flash crash of 2010, and a major algorithmic error that impacted the U.S. Treasury, the approach to technology in capital markets regulation changed drastically.[45] As one commentator explains:

> No longer was financial technology primarily viewed as a tool to disaggregate market functions or improve price discovery. Its role in facilitating transparency, capital markets efficiency, and investor protection would also be questioned. Instead, financial technology would be increasingly viewed as a threat that challenged the existing regulatory framework and raised hypothetical systemic risk concerns.[46]

Ultimately, this renewed skepticism reinforced traditional theories regarding the need for financial intermediaries and, as a result, modern regulatory approaches expect intermediation to feature prominently in functioning markets.[47] As a result, lawmakers increasingly, and nearly exclusively, craft regulations for financial services and capital markets participants that target intermediaries.[48]

Despite being predominately designed to apply to intermediaries, financial regulation represents one of the legal regimes most commonly applied to activity undertaken via blockchain technology—a technology created for the purpose of disintermediation.[49] The archetypal use for blockchain technologies that dominates public discourse revolves around payments.[50] Perhaps because of this seemingly widespread belief that blockchain technology achieves its greatest utility in financial applications, regulatory approaches to activity undertaken via blockchain technology tend to view everything through a financial services lens.[51] This nearly exclusive focus results in several problems. Namely, the analogy between blockchain technology and financial services is often extended in ways that cause misunderstandings of

---

44 *See* Hess, *supra* note 43, at 355–63.

45 *See id.* at 363–73.

46 *Id.* at 363.

47 Lin, *supra* note 25, at 643 ("Intermediation is a fundamental fact of finance."); Allen & Santomero, *supra* note 36, at 289 ("Financial markets and financial intermediaries then have a symbiotic relationship. Each is necessary to the other.").

48 Di Tella, *supra* note 26, at 271 ("[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.").

49 *See* Brett Hemenway Falk & Sarah Hammer, *A Comprehensive Approach to Crypto Regulation*, 25 U. PA. J. BUS. L. 415, 416 (2023) ("One unique challenge in policymaking related to cryptocurrency is the potential lack of a central entity or traditional intermediary that would be the subject of regulatory authority.").

50 *See* Reyes, *supra* note 20, at 196.

51 *See* Fairfield, *supra* note 29, at 830.

the actual activity undertaken through blockchain software.[52] Indeed, lawmakers tend to erroneously overfocus on applying various areas of financial regulation to the cryptocurrency industry, even when it creates negative externalities that impact other areas of innovation using the technology.[53] In particular, because of the ubiquitous intermediation expected as a feature of the modern financial system, constantly analogizing blockchain technology to financial and capital markets structures incorrectly imports an assumption that intermediaries exist. The whole point of blockchain technology is enabling the capacity to transact without intermediaries, and failure to account for that possibility lies at the heart of the ongoing regulatory battles between participants in the blockchain technology industry and lawmakers.

B. U.S. Regulatory Regimes Demand Centralization Even When Technology Enables Decentralization

Blockchain technology enables secure decentralized digital activity. To uncover how blockchain technology achieves this technological feat, and the importance of decentralization for cybersecurity in digital transactions, warrants a brief primer on blockchain technology. At the most general level, blockchain technology is one type of distributed database known broadly as distributed ledger technology ("DLT").[54] A distributed ledger "assumes the possible presence of malicious users (nodes)."[55] 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 cryptographic hashes.[56]

---

52 *See* Carla L. Reyes *Emerging Technology's Language Wars: Cryptocurrency*, 64 WM. & MARY L. REV. 1193, 1197–98 (2023).

53 Reyes, *supra* note 20, at 211.

54 GARRICK HILEMAN & MICHEL RAUCHS, GLOBAL BLOCKCHAIN BENCHMARKING STUDY 11 (2017) (defining blockchain technology as a "type of distributed ledger"). As explained at various times, the Author is aware of the continuing debate as to appropriate terminology. Indeed, the Author has written about the problems that misuse of words related to the cryptocurrency ecosystem can cause for the development of law. *See generally* Reyes, *supra* note 52; Carla L. Reyes, *Emerging Technology's Language Wars: Smart Contracts*, 2022 WIS. L. REV. FORWARD 85 (2023). Without taking a position on the winner in the debate about the precise meaning of the terms blockchain technology or DLT, in this Article, the term DLT is used as the broader, umbrella term to encompass both permissioned and permissionless blockchains, as well as protocols such as R3's Corda that do not strictly fit the definition of "linked 'blocks.'" HILEMAN & RAUCHS, *supra*, at 11. Meanwhile, the term "blockchain technology" is used to refer specifically to those distributed ledgers that use data structures composed of a cryptographically linked chain of blocked data, *see id.*, at least at Layer 1. Adopting these terms in this way is not a statement about the technical accuracy of this or any other terminology. As the Author has written elsewhere, however, it is imperative that law understand that variants of blockchain protocols exist, and blockchain technology is neither monolithic nor static.

55 HILEMAN & RAUCHS, *supra* note 54, at 11.

56 *Id.*

The combination and implementation of specific features vary across blockchain protocols.[57] Indeed, this point cannot be overemphasized: blockchain protocols are not monolithic. Although two blockchain protocols—Bitcoin and Ethereum—are often held out and used as archetypal blockchain protocols, many other protocols with significantly different features exist.[58] The differences in function enabled by those differences in features often impact the applicability and usefulness of regulatory regimes designed to apply to specific activities.[59]

That being said, generally speaking, blockchain technology is a protocol technology.[60] A protocol is "a set of instructions for the compilation and interaction of objects."[61] Generally, a "network protocol" simply sets the rules that allow networked computers—nodes—to communicate with each other.[62] A blockchain protocol, for its part, sets the rules that enable networked computers to track transitions in the global state of recorded data without a centralized third-party intermediary.[63] In the blockchain technology industry, a blockchain protocol may be referred to as Layer 1 in the blockchain technology stack.[64] Thinking of blockchain technology as existing in a stack of layered technologies stems from the layered model of the Internet stack.[65] In the blockchain

---

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

58 Reyes, *supra* note 52, at 1212–14.

59 *See infra* Section III.A.

60 Carla L. Reyes, *(Un)Corporate Crypto-Governance*, 88 FORDHAM L. REV. 1875, 1895 (2020).

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

62 *See* Will Warren, *The Difference Between App Coins and Protocol Tokens*, MEDIUM: OX BLOG (Feb. 2, 2017), https://blog.0xproject.com/the-difference-between-app-coins-and-protocol-tokens-7281a428348c?gi=20c71c10d4bf [https://perma.cc/GQC7-FS3E]. For example, the Internet Protocol is a network protocol that defines the digital message formats and rules for communication among connected computers. Mark De Wolf, *Internet Protocol (IP)*, TECHOPEDIA (Sept. 23, 2024), https://www.techopedia.com/definition/5366/internet-protocol-ip [https://perma.cc/VDD3-TLSY]. Email is also built on a protocol that 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/MXE7-W7Q6].

63 Charles J. Delmotte, *Toward a Blockchain-Driven Tax System*, 43 VA. TAX REV. 37, 51–52 (2023).

64 *See* Thibault Schrepel, *Is Blockchain the Death of Antitrust Law? The Blockchain Antitrust Paradox*, 3 GEO L. TECH. REV. 281, 306 (2018) (describing Layer 2 as the software layer that sits on top of a Layer 1 blockchain protocol); Lewis Gudgeon, Pedro Moreno-Sanchez, Stefanie Roos, Patrick McCorry & Arthur Gervais, *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).

65 *See* Lawrence 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

technology stack, if Layer 1 is the blockchain protocol—or network layer—Layer 2 refers to an additional software layer that operates on top of the Layer 1 protocol.[66] Stakeholders in the blockchain technology industry often think of the application layer in the blockchain technology stack as Layer 3.[67] Just as failure to understand nuanced differences between blockchain protocols can impact the useful application of law and regulation to activity undertaken via those protocols,[68] so too can failure to understand the layer at which a person or entity is undertaking regulatable activity.[69]

Layer 1 public, permissionless blockchain protocols are "transparent by design."[70] Although this design feature is necessary to achieve secure electronic peer-to-peer transactions, it causes a user's complete transaction history to be discoverable. To the extent a user relies on such Layer 1 protocols to conduct financial transactions, the public nature of the transactions poses problems for the user's financial privacy[71] and the user's ability to maintain the cybersecurity of their assets.[72] Indeed, the lack of privacy undermines the goal of using cryptocurrency as a payments mechanism—namely, transacting in an electronic equivalent to physical cash.[73] Why do users seek an electronic equivalent to physical cash? First, extensive research evidences the increasingly cashless

---

architecture is comprised of layers, narrowly understood as defined by code or broadly understood as functional components of a communications system.").

66 *See* Schrepel, *supra* note 64, at 295, 306; Gudgeon et al., *supra* note 64, at 204.

67 *Layers of Blockchain Technology*, Blockchain Council (Aug. 21, 2024), https://www.blockchain-council.org/blockchain/layers-of-blockchain-technology/ [https://perma.cc/5HRH-CQV7] (describing Layer 3 as the layer with which users will interact).

68 *See* Reyes, *supra* note 20, at 196 (observing even back then that "failure to appreciate these distinctions [between blockchain and a variety of similar technologies] constitutes a core element in the regulatory difficulty facing entrepreneurs integrating decentralized ledger technology into their products and services").

69 *See supra* notes 64–68 and accompanying text.

70 Vitalik Buterin, Jacob Illum, Matthias Nadler, Fabian Schär & Ameen Soleimani, *Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium* 1, 1 (Sept. 9, 2023) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563364 [https://perma.cc/YN62-A7UW].

71 *See infra* notes 278–82 and accompanying text.

72 *See, e.g.*, Lily Hay Newman, *How to Keep Your Bitcoin Safe and Secure*, Wired (Nov. 5, 2017, 7:00 AM), https://www.wired.com/story/how-to-keep-bitcoin-safe-and-secure/ [https://perma.cc/Q8C3-9VKM]; Gary Weinstein, *AI and Blockchain Analytics: The Urgent Need for Crypto Privacy Tools*, Forbes (Apr. 7, 2023, 9:44 AM), https://www.forbes.com/sites/digital-assets/2023/04/07/ai-and-blockchain-analytics-the-urgent-need-for-crypto-privacy-tools/ [https://perma.cc/ZPV3-7W3N]; Eli Tan, *Hacker Steals Bill Murray's Crypto After $185K NFT Charity Auction*, CoinDesk (May 11, 2023, 2:56 PM), https://www.coindesk.com/business/2022/09/02/hacker-steals-bill-murrays-crypto-after-185k-nft-charity-auction/ [https://perma.cc/P87B-ZMSF].

73 *See* Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 1 (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/3SKS-5XPK].

nature of commercial life.[74] Instead, electronic transactions dominate commerce. Electronic transactions in the modern financial system flow through a series of heavily regulated intermediaries, resulting in extensive government surveillance and monitoring of financial transactions.[75] In the absence of the capacity to undertake cash-based transactions, which by their very nature feature transactional privacy,[76] those who value privacy in the digital age seek an electronic equivalent to cash transactions.[77] In pursuit of digital cash-equivalent transactions and protection of a fundamental right to financial privacy,[78] software developers have created Layer 2 solutions for increasing privacy for transactions conducted via Layer 1 blockchain protocols. Many Layer 2 solutions implement such a high level of decentralization that no intermediary exists at all.[79] In the blockchain industry, such decentralized solutions are often referred to as decentralized finance—or "DeFi." DeFi, of course, directly challenges the financial regulatory regime that rests so heavily on the legal compliance of intermediaries.

And yet, regulatory responses to activity taken with this technology demand centralized intermediaries to whom the law may be applied.

---

74 *See, e.g.*, Emily Cubides & Shaun O'Brien, *2023 Findings from the Diary of Consumer Payment Choice*, Fed. Rsrv. Fin. Servs. 4–5 (2023), https://www.frbsf.org/cash/wp-content/uploads/sites/7/2023-Findings-from-the-Diary-of-Consumer-Payment-Choice.pdf [https://perma.cc/XQW8-XA8B]; Rodney J. Garratt & Maarten R.C. van Oordt, *Privacy as a Public Good: A Case for Electronic Cash*, 129 J. Pol. Econ. 2157, 2157–58 (2021); Tanai Khiaonarong & David Humphrey, *Cash Use Across Countries and the Demand for Central Bank Digital Currency* 29–30 (Int'l Monetary Fund Working Paper No. 19/46, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3367431 [https://perma.cc/DS3Y-2MNN].

75 *See* Ruth Plato-Shinar, *The Right to Financial Privacy in an Era of Mandatory Duties of Disclosure*, 38 Banking & Fin. L. Rev. 285, 286 (2022) ("Notwithstanding its importance, the right to financial privacy is not an absolute right. Financial entities are subject to a duty to disclose information about their customers, as part of an exception to the right to privacy. In recent years, the right to financial privacy has undergone a gradual process of constriction corresponding to the expansion of the obligation of disclosure."); Catherine M. Downey, Comment, *The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash?*, 14 UIC J. Marshall J. Computer. & Info. L. 303, 317 (1996).

76 Charles M. Kahn, James McAndrews & William Roberds, *Money Is Privacy*, 46 Int'l Econ. Rev. 377, 377 (2005); David Chaum, Amos Fiat & Moni Naor, *Untraceable Electronic Cash*, 1988 Advances in Cryptology 319, 319 ("Paper cash is considered to have a significant advantage over credit cards with respect to privacy, although the serial numbers on cash make it traceable in principle.").

77 *See* Jerry Brito, Coin Ctr., The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society 2–3 (2019), https://www.coincenter.org/app/uploads/2020/05/the-case-for-electronic-cash-coin-center.pdf [https://perma.cc/V282-DQCU]; Peter Van Valkenburgh, Coin Ctr., Electronic Cash, Decentralized Exchange, and the Constitution 12 (2019), https://www.coincenter.org/app/uploads/2020/05/e-cash-dex-constitution.pdf [https://perma.cc/MS5V-BUQX].

78 Brito, *supra* note 77; Van Valkenburgh, *supra* note 77.

79 *See* Blockchain Council, *supra* note 67 (describing the added nodes in Layer 2 as a means to further decentralize a blockchain).

This response can be explained, at least in part, by the historical regulatory issues raised by prior virtual currency models and the regulatory solutions adopted.[80] At the time that the first blockchain protocol—Bitcoin—became operational in 2009, key regulatory battles were unfolding in the context of centralized virtual currencies.[81] The largest virtual currency-related regulatory issue prior to the launch of Bitcoin centered around the prosecution of anti-money laundering violations by e-gold, Ltd.[82] The company e-gold, Ltd. operated a centralized virtual currency in which users could register using false names using only an email address[83] and deposit U.S. dollars or other fiat currency in exchange for a digital balance of e-gold—a virtual currency allegedly backed by gold reserves.[84] Between 2005 and 2008, e-gold faced regulatory and law enforcement actions for failure to comply with the anti-money laundering provisions of the Bank Secrecy Act[85] and enabling criminal activity.[86] These enforcement proceedings placed the regulatory approach to early virtual currencies squarely within the existing regime of financial intermediary regulation.

Indeed, the first regulatory actions against blockchain industry participants focused again on centralized intermediaries. On May 14, 2013, the Department of Homeland Security ("DHS") seized a Dwolla account belonging to Mt. Gox, a Japan-based Bitcoin exchange, in connection with allegations that Mt. Gox's U.S. subsidiary, Mutum Sigillum, LLC, operated an unlicensed money transmitting business in violation of 18 U.S.C. § 1960.[87] Mt. Gox and its U.S. subsidiaries operated in a traditional centralized finance manner by taking user assets and storing them on the user's behalf.[88] Just fourteen days later, Treasury's Financial Crimes Enforcement Network ("FinCEN") undertook an action under

---

80 *See* Reyes, *supra* note 20, at 203–05.

81 *Id.*

82 *Id.*

83 Catherine Martin Christopher, *Whack-a-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Money Laundering*, 18 LEWIS & CLARK L. REV. 1, 24 (2014). Notably, this meant that e-gold accounts existed under names like: "Mickey Mouse," "Anonymous Man," "bud wieser," and "No Name." *Id.*

84 *Id.*; Stephen T. Middlebrook & Sarah Jane Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM. MITCHELL L. REV. 813, 822 (2014).

85 Currency and Foreign Transactions Reporting Act, P.L. No. 91-508, 84 Stat. 1114-2 (1970) (codified as amended in scattered sections of 12 and 31 U.S.C.).

86 *See* Christopher, *supra* note 83, at 24. For details on the criminal charges and the guilty pleas entered, see *United States v. e-Gold, Ltd.*, 550 F. Supp. 2d 82, 85–86 (D.D.C. 2008).

87 Annunzio-Wylie Anti-Money Laundering Act of 1992, P.L. No. 102-550, 106 Stat. 3672 (codified as amended in 18 U.S.C.); Application and Affidavit for Seizure Warrant, In the Matter of the Seizure of the Contents of One Dwolla Account, No. 13-1162 SKG (D. Md. May 14, 2013) [hereinafter Warrant], https://cdn.arstechnica.net/wp-content/uploads/2013/05/Mt-Gox-Dwolla-Warrant-5-14-13.pdf [https://perma.cc/QJV9-U9D2].

88 Warrant, *supra* note 87, at 3.

section 311 of the USA PATRIOT Act[89] by designating Liberty Reserve, a Costa Rica-based centralized virtual currency platform, a financial institution of primary money laundering concern[90] and proposing that special measures be imposed against Liberty Reserve that would effectively cut the entity and its principals out of the U.S. financial system entirely.[91] In the wake of these early regulatory actions, regulators and law enforcement continued to focus on centralized actors in the virtual currency space, even as decentralized cryptocurrency and blockchain technology became more widely used.[92] For a long time, enforcement activity focused on traditional centralized structures, like corporations, that just happened to incorporate some element of blockchain technology or cryptocurrency into their products and services.[93] Enforcement activity in the early days also focused almost entirely on businesses that operated at a fairly large scale and on businesses whose product and services related to payments use cases of blockchain technology because those use cases most clearly mirrored traditionally regulated financial institutions and presumably did not require agencies to spend much time actually learning about the technology.[94] In an attempt to

---

89 31 USC § 5318A.

90 Notice of Finding that Liberty Reserve S.A. is a Financial Institution of Primary Money Laundering Concern, 78 Fed. Reg. 34,169 (June 6, 2013).

91 Imposition of Special Measure Against Liberty Reserve S.A. as a Financial Institution of Primary Money Laundering Concern, 78 Fed. Reg. 34,008 (June 6, 2013) (notice of proposed rulemaking); *see also* Jean-Jacques Cabou, J. Dax Hansen, Ashley Locke, Keith Miller & Carla Reyes, *Federal Government Crackdown on Virtual Currency Heats Up*, JD Supra (May 31, 2013), https://www.jdsupra.com/legalnews/federal-government-crackdown-on-virtual-09114/ [https://perma.cc/78GJ-GYA7].

92 Reyes, *supra* note 20, at 205.

93 *See id.*

94 *See id.* Various regulatory agencies undertook enforcement actions focused on centralized entities in addition to FinCEN. The Department of Justice went after Ripple Labs. *See* Settlement Agreement between U.S. Att'y N. Dist. of Cal. and Ripple Labs Inc. (May 2015), https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/05/05/settlement_agreement.pdf [https://perma.cc/8L5A-V4NS]. State banking regulators issued subpoenas and sent cease and desist letters. *See, e.g.*, Emily Spaven, *New York State Financial Regulator Issues Subpoenas to 22 Bitcoin Companies*, CoinDesk (Apr. 9, 2024, 10:51 PM), https://www.coindesk.com/markets/2013/08/12/new-york-state-financial-regulator-issues-subpoenas-to-22-bitcoin-companies/ [https://perma.cc/Y47E-5NNS]; Danny Bradbury, *California Issues Cease and Desist Letter to Bitcoin Foundation*, CoinDesk (Feb. 9, 2023, 8:18 AM), https://www.coindesk.com/markets/2013/06/23/california-issues-cease-and-desist-letter-to-bitcoin-foundation/ [https://perma.cc/3QBR-GEV6]. The CFTC enforced against Coinflip, Inc., and TerraExchange, LLC. *See* Press Release, Commodity Futures Trading Comm'n, CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering (Sept. 17, 2015), https://www.cftc.gov/PressRoom/PressReleases/7231-15 [https://perma.cc/5XHZ-Z24V]; Press Release, Commodity Futures Trading Comm'n, CFTC Settles with TeraExchange LLC for Failing to Enforce Prohibitions on Wash Trading and Prearranged Trading in Bitcoin Swap (Sept. 24, 2015), https://www.cftc.gov/PressRoom/PressReleases/7240-15 [https://perma.cc/Y69G-XCQ5]. The SEC enforced against a Ponzi scheme. SEC v. Shavers, No.

capture the technical and structural differences between these types of companies and the services they provide and DeFi solutions, the blockchain industry frequently refers to cryptocurrency-related businesses that mirror traditional financial services and institutions as centralized finance—or "CeFi."

While early enforcement actions focused on CeFi entities acting as crypto-payments intermediaries, regulatory intermediary targeting expanded to other sectors over the years. Anti-money laundering regulations continue to feature prominently in crypto-intermediary compliance discussions, of course.[95] But starting around 2017, the SEC entered the crypto-intermediary enforcement arena on a wide scale, insisting on finding "issuers" of cryptocurrencies and tokens that can comply with disclosure obligations and enforcing against exchange operators that list tokens and cryptocurrencies for which an issuer failed to register the offering and did not qualify for an exemption, or for which no true issuer exists.[96] The CFTC also jumped into the enforcement fray, seeking intermediaries that could be held liable for improperly traded leveraged derivatives and leveraged or margined retail commodity transactions.[97] The Internal Revenue Service and law enforcement sought to add entities and individuals to the ranks of intermediaries from which they require reporting.[98] This expanded enforcement activ-

---

4:13-CV-416, 2013 WL 4028182 (E.D. Tex. Aug. 6, 2013), adhered to on reconsideration, No. 4:13-CV-416, 2014 WL 12622292 (E.D. Tex. Aug. 26, 2014).

95 *See, e.g.*, Press Release, Sen Elizabeth Warren, Warren, Marshall Introduce Bipartisan Legislation to Crack Down on Cryptocurrency Money Laundering, Financing of Terrorists and Rogue Nations (Dec. 14, 2022), https://www.warren.senate.gov/newsroom/press-releases/warren-marshall-introduce-bipartisan-legislation-to-crack-down-on-cryptocurrency-money-laundering-financing-of-terrorists-and-rogue-nations [https://perma.cc/BBM9-5QCC] (discussing the Digital Asset Anti-Money Laundering Act proposal).

96 *See, e.g.*, Sec. & Exch. Comm'n, Exchange Act Release No. 81207, Report of Investigation: The DAO (July 25, 2017) (explaining the SEC's view of its legal justification for treating certain tokens as securities); *Framework for Investment Contract Analysis of Digital Assets*, Sec. & Exch. Comm'n (July 5, 2024), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets [https://perma.cc/VS2F-3BQH]; Eakeley et al., *supra* note 21, at 99–100 ("We find that the United States Securities and Exchange Commission . . . brings more enforcement actions against digital-asset issuers, broker-dealers, exchanges, and other crypto-market participants than any other major crypto-jurisdiction.").

97 *See, e.g.*, Order Instituting Proceedings, *In re* Opyn, Inc., CFTC No. 23-40 (Sept. 7, 2023); Order Instituting Proceedings, *In re* ZeroEx, Inc., CFTC No. 23-41 (Sept. 7, 2023); Order Instituting Proceedings, *In re* Deridex, Inc., CFTC No. 23-42 (Sept. 7, 2023).

98 Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions, 88 Fed. Reg. 59,576 (Aug. 29, 2023) (notice of proposed rulemaking). The proposed rules were met with a flurry of backlash. *See, e.g.*, Caleb Harshberger, *ABA Pushes for Changes to Proposed IRS Crypto Broker Rules*, Bloomberg Tax (Dec. 19, 2023, 3:15 PM), https://news.bloomberglaw.com/daily-tax-report/aba-pushes-for-changes-to-proposed-irs-crypto-broker-rules [https://perma.cc/UEY5-PHNH]; Jesse Hamilton, *IRS 'Raided' by Crypto Investors as Industry Puts Up Fight Against U.S. Tax Proposal*, CoinDesk (Nov. 15, 2023, 11:20 AM), https://www.coindesk.com/policy/2023/11/13/

ity against intermediaries pushed some projects to explore deeper decentralization.[99] Or, put another way, many CeFi entities considered how they might undertake technological transformations to become DeFi protocols. Decried as a form of purposeful evasion of law, such moves to increase decentralization serve both a traditional start-up purpose of regulatory entrepreneurship[100] and a technical imperative for heightened cybersecurity and privacy.[101] Rather than allow the blockchain industry to explore the benefits of increased decentralization, regulatory agencies and lawmakers appear to seek increased centralization to facilitate enforcement activity, particularly in the wake of the recent crypto-intermediary failures of 2022 and 2023.

II. Recent Scandals in Cryptoland Expose the Extent of Risk Caused by a Legal Regime that Over Relies on Intermediaries

This Part explores the failure of various cryptocurrency and blockchain related firms—both historical and more recent—and reveals where law and regulation applied but failed to intercept bad activity or prevent the resulting harms. In doing so, this Part makes apparent that, far from the popular refrains espoused by regulators, lawmakers, and legal academics in the wake of these events that the technology itself, lack of regulation, or sham decentralization was to blame, the losses suffered in 2022 and 2023 generally stemmed from garden variety failure of intermediaries to adequately protect their customers. In fact, the events that sparked renewed calls to tame the "Wild West" of cryptocurrency evidence instead that the cryptocurrency ecosystem—and particularly CeFi—is not a Wild West at all. Indeed, the cryptocurrency and blockchain industry is, and has been for a decade, highly regulated. As unveiled in detail below, the stories of Terra, Celsius, 3AC, Voyager, FTX, BlockFi, and others are not stories of sham decentralization, but rather, stories of failed regulation.

A. A Brief History of Cryptocurrency-Intermediary Failures

Although the current environment invites us to focus on the cryptocurrency intermediary failures beginning in May 2022, considering several historical events helps illustrate the risks of centralization and

irs-raided-by-crypto-investors-as-industry-puts-up-fight-against-us-tax-proposal/ [https://perma.cc/9PLH-VGTY].

99 *See, e.g.*, Jai Massari & Christian Catalini, *DeFi, Disintermediation, and the Regulatory Path Ahead*, Regul. Rev. (May 10, 2021), https://www.theregreview.org/2021/05/10/massari-catalini-defi-disintermediation-regulatory-path-ahead/ [https://perma.cc/UMX8-YHLQ].

100 Pollman & Barry, *supra* note 31, at 392.

101 *See supra* notes 70–78 and accompanying text.

intermediation in the cryptocurrency and blockchain technology industry. Mt. Gox represents an early cryptocurrency exchange failure that caused significant consumer losses and attracted significant attention. Jed McCaleb founded Mt. Gox in 2010, but as Mt. Gox's volume of transactions grew, McCaleb sold it to Mark Karpelès.[102] By 2014, nearly 70 percent of all Bitcoin transactions flowed through Mt. Gox.[103] In the early months of that year, Mt. Gox customers began experiencing difficulties withdrawing their funds, and on February 7, 2014, Mt. Gox froze all customer withdrawals.[104] Eventually, Karpelès would reveal that Mt. Gox's online (or "hot") wallet had been the target of long-term theft, with an unknown person or persons stealing cryptocurrency by changing transaction identifiers.[105] The U.S. Attorney's Office for the Southern District of New York only recently indicted two individuals in June 2023, alleging they orchestrated the Mt. Gox theft of approximately 647,000 Bitcoins between September 2011 and May 2014.[106] The Mt. Gox theft highlighted the importance of strong financial and technical management by the intermediary—financial mismanagement and failure to deploy strong technical infrastructure made Mt. Gox more vulnerable and hastened its downfall.[107]

Several years after the Mt. Gox debacle, another exchange spectacularly failed as a result of intermediary mismanagement. In 2018, after a decline in the price of Bitcoin, users seeking to liquidate their positions on the QuadrigaCX exchange found their transaction requests denied.[108] In a bizarre tale that would later become the subject of a Netflix documentary,[109] Canadian regulators and journalists uncovered

---

102 Adrianne Jeffries, *Inside the Bizarre Upside-Down Bankruptcy of Mt. Gox*, THE VERGE (Mar. 22, 2018, 10:30 AM), https://www.theverge.com/2018/3/22/17151430/bankruptcy-mt-gox-liabilities-bitcoin [https://perma.cc/NUC9-YK54].

103 *Id.*

104 Nathaniel Popper, *How Mt. Gox Imploded*, VICE (May 19, 2015, 9:00 AM), https://www.vice.com/en/article/ae38qb/how-mt-gox-imploded [https://perma.cc/K4FE-ZL3Z].

105 *Id.*

106 Press Release, United States Att'ys Off. S. Dist. N.Y., Russian Nationals Charged with Hacking One Cryptocurrency Exchange & Illicitly Operating Another (June 9, 2023), https://www.justice.gov/usao-sdny/pr/russian-nationals-charged-hacking-one-cryptocurrency-exchange-and-illicitly-operating [https://perma.cc/ER97-KG77].

107 Jose Pagliery, *How Mt. Gox Went Down*, CNN BUS. (Feb. 26, 2014, 10:43 AM), https://money.cnn.com/2014/02/25/technology/security/bitcoin-mtgox/index.html [https://perma.cc/AK7A-YLLK] ("Mt.Gox is blaming a costly computer hack for its current troubles. But in reality, the company was in dire financial straits long before that. Cash flow issues are to blame, as the exchange balanced a tiny revenue stream with a giant burning hole in its pocket.").

108 *See* Tim Copeland, *The Complete Story of the QuadrigaCX $190 Million Scandal*, DECRYPT (Dec. 16, 2019), https://decrypt.co/5853/complete-story-quadrigacx-190-million [https://perma.cc/LV7Q-DA52].

109 Peter A. Berry, *This 'Trust No One' Trailer Will Make You Clutch Your Bitcoin*, TUDUM BY NETFLIX (Mar. 9, 2022), https://www.netflix.com/tudum/articles/trust-no-one-the-hunt-for-the-crypto-king-trailer [https://perma.cc/956Y-ML7Q].

evidence that the founder and chief operator of the QuadrigaCX, Gerry Cotten, ran the platform like a Ponzi scheme.[110] Customers would transfer their cryptocurrency or money to QuadrigaCX, and then Cotten would use those transfers to fund trades in his own name or in the name of aliases.[111] Unfortunately, Cotten turned out to lack skill at day trading and lost more money than he made, so when the price of Bitcoin dipped, he could not cover all customer withdrawal requests.[112] Before regulators could ascertain exactly what happened at QuadrigaCX, and before customers could be made whole, Cotten died in India, and allegedly took the private keys to the wallets holding over 190 million dollars of customer funds with him.[113] Ultimately, the QuadrigaCX debacle stemmed from a failure of an intermediary, not from failure of blockchain technology. As the Ontario Securities Commission put it, "[w]hat happened at Quadriga was an old-fashioned fraud wrapped in modern technology. There is nothing new about Ponzi schemes, unauthorized trading with client funds, and misappropriation of assets."[114]

Some commentators consider the 2022 and 2023 cryptocurrency-related business failure to be distinct from these early exchange failures, arguing that the later failures resulted from flaws in the technology itself or the sham decentralization inherent in blockchain technology and related services.[115] The collapse of the Terra Luna cryptocurrency ecosystem in May 2022 features as a prominent example for these critiques.[116] The company TerraForm Labs developed the Terra blockchain protocol and its native cryptocurrency, Luna.[117] The Terra blockchain protocol also supported a stablecoin called UST.[118] TerraForm Labs designed UST to hold a value of one dollar by pegging one UST to $1 worth of Luna.[119] The crypto-economics behind this type of peg relied upon traders to keep UST at $1 through rational trading behavior.[120]

---

110 Ontario Sec. Comm'n, Quadriga CX: A Review by Staff of the Ontario Securities Commission 3–4 (Apr. 14, 2020), https://www.osc.ca/quadrigacxreport/web/files/QuadrigaCX-A-Review-by-Staff-of-the-Ontario-Securities-Commission.pdf [https://perma.cc/RH5K-KFYR].

111 Cassie Williams, *QuadrigaCX Founder Used Aliases, Moved Assets into Personal Accounts: Report*, CBC (June 20, 2019, 1:29 PM), https://www.cbc.ca/news/canada/nova-scotia/quadrigacx-founder-used-aliases-moved-assets-into-personal-accounts-ernst-and-young-1.5182984 [https://perma.cc/8P57-PHTT].

112 Ontario Sec. Commi'n, *supra* note 110, at 21–22.

113 Copeland, *supra* note 108.

114 Ontario Sec. Comm'n, *supra* note 110, at 4.

115 *See infra* notes 190–95 and accompanying text.

116 *See, e.g.*, Hilary J. Allen, *The Superficial Allure of Crypto*, IMF Fin. & Dev., Sept. 2022, at 28.

117 Liu et al., *supra* note 2, at 2.

118 *Id.* at 1–2.

119 *Id.* at 2–3.

120 *Id.* at 3 ("The pegging mechanism relied on traders taking advantage of an arbitrage opportunity that would present itself every time UST lost its peg in either direction. For example, if the price of UST falls below $1, arbitrageurs could buy UST at a price below $1 and convert it

Meanwhile, to try and increase its user base, TerraForm Labs created the Anchor savings and lending protocol, in which users could deposit UST and receive a 19.5 percent yield on their savings and borrow at a favorable rate compared with other market prices.[121] To provide these types of benefits to users, TerraForm Labs paid out of their own pocket.[122] In fact, by April 2022, TerraForm Labs was paying out $6 million daily to make good on the interest rates promised by the Anchor protocol.[123] Following a May 1, 2022 decrease in the deposit interest rate on Anchor, several Anchor depositors withdrew their large holdings from the protocol on May 7, 2022, and the UST price began to falter.[124] Between May 7 and May 13, 2022, the value of UST dropped from $1 to $0.20.[125] Essentially, during those six days, "users swapped UST worth $4.65 billion. As users swapped UST for LUNA, the price of LUNA precipitously fell, leading to increasing dilution, which further depressed the price of LUNA, and led to a dramatic 'death spiral.'"[126]

Although this discussion of the technical aspects of UST's depegging and ultimate demise makes it easy to see why some believe the technology shoulders the blame for consumer losses, a closer look demonstrates the key role that intermediaries played in causing the disaster. First, TerraForm Labs propped up unsustainable products and services in an attempt to market the Terra ecosystem.[127] Such activity injected instability into the system that did not exist as a result of the technology alone. Second, in response to market expressions of concern regarding Terra's stability, TerraForm Labs created the Luna Foundation Guard—a type of insurance fund promised for use in shoring up the UST-Luna peg if market conditions became volatile.[128] The Luna Foundation Guard mimicked the role of deposit insurance and propped up market confidence that may have dissipated earlier and mitigated

---

into $1 worth of LUNA, and in the process, reduce the supply of UST and drive up its price. And vice versa if the UST price is above $1.").

121 *Id.* at 3, 11.

122 *Id.* at 3.

123 *Id.*

124 *Id.* at 3–4.

125 *Id.* at 4.

126 *Id.* at 5.

127 *See id.* at 11 (describing the subsidized Anchor 19.5 percent yield and allegedly fake transactions via the Chai payments application).

> Anchor was never self-sustaining but relied from significant subsidies from [TerraForm Labs]. This imbalance was primarily driven by the deposit rate on Anchor having been set exogenously and artificially high. Early on, the high deposit rate might have been intended as a marketing tool to attract users to the Terra ecosystem. But our analysis suggests that these users did not start generating more fees over time to support the high deposit rate.

Id. at 20.

128 *Id.* at 11–12.

the ultimate amount of losses suffered.[129] Third, TerraForm Labs and several partners silently prevented a prior depegging event by manipulating the market, falsely signaling financial stability of a system that rested on unsustainable subsidies to consumers.[130] Finally, TerraForm Labs itself contributed to the crash of Luna and UST by engaging in large swaps of UST for Luna during the crisis.[131] Ultimately, TerraForm Labs's attempts to provide overly attractive products with unsustainable returns, offer an insurance-like safety net to prop up user confidence, its own trading activity, and "aggressively underplaying the risks building up in the system on social media and other outlets" all combined to manufacture the collapse of the Terra ecosystem and the loss of over $50 billion in valuation.[132]

A month later, in June 2022, an investment fund named Three Arrows Capital would also collapse.[133] Founded in 2012 with $1 million as a foreign exchange derivative trading company, Three Arrows Capital's initial business model quickly failed.[134] By 2018, the fund shifted its focus to cryptocurrency markets, arbitraging trades across international markets.[135] To fund its trading activity, Three Arrows Capital borrowed significant sums of money from a variety of key cryptocurrency industry players, including Voyager Digital and Genesis Global Trading.[136] The fund suffered significant losses starting in January 2022,[137] but still made a $200 million investment into Luna in February 2022.[138] When Luna collapsed in March 2022, Three Arrows Capital's stake went from about $500 million to about $604.[139] The fund nevertheless represented to concerned lenders that it did not have much of its portfolio tied up in Luna, and all would be well.[140] Nevertheless, when Three Arrows Capital

---

129 *See id.*

130 *See id.* at 6.

131 *Id.* at 30 (describing how TerraForm Labs conducted swaps in order to maintain its governance position in the ecosystem).

132 *Id.* at 37, 1; *see supra* notes 121–23, 127–29.

133 Jen Wieczner, *The Crypto Geniuses Who Vaporized a Trillion Dollars*, N.Y. Mag. (Aug. 15, 2022), https://nymag.com/intelligencer/article/three-arrows-capital-kyle-davies-su-zhu-crash.html [https://perma.cc/KLA4-X5JL].

134 *See id.* ("By 2017, the banks began cutting [Three Arrows] off" when the company needed a price to conduct a foreign exchange trade).

135 *Id.*

136 *Id.*

137 Three Arrows Capital suffered from bad positions in Lido-staked ether and the Grayscale Bitcoin Trust, which caused significant losses and a liquidity crunch. Danny Nelson & David Z. Morris, *Behind Voyager's Fall: Crypto Broker Acted Like a Bank, Went Bankrupt*, CoinDesk (May 11, 2023, 1:22 PM), https://www.coindesk.com/layer2/2022/07/12/behind-voyagers-fall-crypto-broker-acted-like-a-bank-went-bankrupt/ [https://perma.cc/S4U5-JMZV].

138 Wieczner, *supra* note 133.

139 *Id.*

140 *Id.*

lenders called their loans, the fund defaulted, its founders disappeared, and reports would later reveal that the founders had purchased lavish homes and other luxury items before the fund's ultimate demise.[141]

Quickly following the downfall of Three Arrows Capital, Voyager Digital, a publicly traded digital asset brokerage, froze customer funds and filed for bankruptcy in July 2022.[142] Voyager Digital made a $650 million unsecured loan to Three Arrows Capital, a loan that went unpaid after that fund collapsed.[143] A default on such a large loan would represent a significant problem for any lender, but for Voyager Digital, the default raised several red flags about the operations of this centralized intermediary. First, lending at such a high amount on an unsecured basis without sufficient due diligence represented shocking business mismanagement.[144] Second, Voyager Digital used customer deposits of cryptocurrency to make such loans.[145] The play worked well when borrowers repaid loans in full at high interest rates so that Voyager Digital could pass some of the earnings back to its customers, but when a very risky unsecured $650 million loan went unpaid,[146] many retail customers were left holding the bag.[147]

Two other cryptocurrency companies that employed similar business models also filed for bankruptcy in the summer and fall of 2022—Celsius[148]

---

141 *Id.*

142 Nelson & Morris, *supra* note 137. Voyager Digital was "one of the few digital asset brokerages listed on stock markets anywhere in the world"; however, it was listed in Canada—not the United States. *Id.*

143 *Id.* The value of the loan to Three Arrows Capital varies depending on how the assets lent are valued. The loan was made in cryptocurrency—$350 million worth of USD Coin and 15,250 Bitcoin. Dietrich Knauth, *Crypto Lender Voyager Settles with Executives Who Approved Risky Loan*, Reuters (Oct. 18, 2022, 5:51 PM), https://www.reuters.com/legal/litigation/crypto-lender-voyager-settles-with-executives-who-approved-risky-loan-2022-10-18/ [https://perma.cc/5AH6-QCFM]. In April 2022, certain court filings pegged the value of that cryptocurrency at around $935 million, but by October 2022, the value had fallen to around $650 million. *Id.*

144 Indeed, Voyager Digital's chief executive officer and chief operating officer settled potential claims related to the risky loan to Three Arrows Capital as part of the entity's bankruptcy plan. *See In re:* Voyager Digital Holdings, Inc., Case No. 22-10943, Notice of Filing of First Amended Disclosure Statement Relating to the Second Amended Joint Plan of Voyager Digital Holdings, Inc. and its Debtor Affiliates Pursuant to Chapter 11 of the Bankruptcy Code, at 21–34, 37–38 (Bankr. S.D.N.Y. Oct. 17, 2022), https://fingfx.thomsonreuters.com/gfx/legaldocs/lbvgnqqrwpq/voyager%20amended%20disclosure%20statement.pdf [https://perma.cc/3TJK-RDUG].

145 Nelson & Morris, *supra* note 137.

146 For reasons that will become apparent in the discussion of FTX below, Voyager made another large unsecured loan of about $500 million to Alameda Research Ltd. *Id.*

147 *Id.*

148 Kadhim Shubber & Joshua Oliver, *Inside Celsius: How One of Crypto's Biggest Lenders Ground to a Halt*, Fin. Times (July 13, 2022), https://www.ft.com/content/4fa06516-119b-4722-946b-944e38b02f45 [https://perma.cc/68V7-QJHB] ("Celsius relied on a stream of deposits from retail investors that it lent to large crypto companies and used for risky bets on untested ventures. It promised exceptionally high interest rates while also claiming the risks were small. In 2021, as

and BlockFi.[149] In Celsius's case, "[t]he company's own compliance department warned of poor oversight, weak internal systems and the possible misrepresentation of financial information."[150] Indeed, Celsius founder, Alex Mashinsky, would later face federal charges for allegedly manipulating the market into believing the platform's financial performance was stronger than in reality.[151] In BlockFi's case, like Voyager Digital, the company suffered significant losses when Three Arrows Capital failed.[152] The cryptocurrency exchange FTX promised to bail out BlockFi with a $400 million revolving credit facility in exchange for, among other things, an option to purchase BlockFi at maximum price of $240 million.[153] However, FTX's backstop proved hollow, BlockFi's exposure to FTX's sister-company, Alameda Research, proved fatal, and BlockFi filed for bankruptcy in November 2022.[154]

Between 2019 and 2023, FTX operated a seemingly successful international digital assets trading platform and exchange, FTX.com, and a U.S.-based digital asset spot-trading exchange, FTX.US, which boasted approximately seven million users worldwide and over 1 million U.S. users, respectively, by November 2022.[155] FTX worked

---

demand for loans from institutional investors waned, Celsius began taking greater risks to generate yield.").

Celsius filed for Chapter 11 bankruptcy in July 2022, and the bankruptcy proceedings ended in November 2023. *See* Neil Khilwani, *Settling Scores: Celsius' Chapter 11 Debt Resolution*, FORDHAM J. CORP. & FIN. L. (Apr. 5, 2024), https://news.law.fordham.edu/jcfl/2024/04/05/settling-scores-celsius-chapter-11-debt-resolution/ [https://perma.cc/7BVD-EALY].

149 Thomas Meyer, *Does BlockFi's Risk Justify the Reward?*, COINDESK (Sept. 14, 2021, 8:33 AM), https://www.coindesk.com/markets/2021/03/29/does-blockfis-risk-justify-the-reward/ [https://perma.cc/WC9U-Y9JE] ("BlockFi is essentially a modern-day crypto bank (without insurance) that pays account holders significantly higher interest than traditional banks. It is able to pay such high levels of interest because it's charging even higher rates on the lending side."). BlockFi filed for bankruptcy in November 2022. Hannah Lang, Niket Nishant & Manya Saini, *Crypto Lender BlockFi Files for Bankruptcy, Cites FTX Exposure*, REUTERS (Nov. 29, 2022, 1:59 AM), https://www.reuters.com/technology/crypto-lender-blockfi-files-bankruptcy-protection-2022-11-28/ [https://perma.cc/9VQT-7AU9].

150 Shubber & Oliver, *supra* note 148.

151 Evan Ochsner, *Crypto Collapses Force Bankruptcy Judges to Act Like Regulators*, BLOOMBERG L. (Dec. 27, 2023, 5:00 AM), https://news.bloomberglaw.com/bankruptcy-law/crypto-collapses-leave-bankruptcy-judges-making-sense-of-rubble [https://perma.cc/S4ZM-6KVH].

152 Frances Yue, *FTX Signs Deal to Bail Out Lender BlockFi with Option to Buy it for up to $240 Million*, MARKETWATCH (July 1, 2022, 2:55 PM), https://www.marketwatch.com/story/ftx-signs-deal-to-bail-out-crypto-lender-blockfi-with-option-to-buy-it-for-up-to-240-million-2022-07-01 [https://perma.cc/674Y-XG7W].

153 *Id.*

154 Lang et al., *supra* note 149.

155 First Interim Report of John J. Ray III to the Independent Directors on Control Failures at the FTX Exchanges at 4, *In re* FTX Trading LTD, No. 22-11068 (Bankr. D. Del. Apr. 9, 2023) [hereinafter First Interim Report of John J. Ray]. "At its peak, the FTX Group operated in 250 jurisdictions, controlled tens of billions of dollars of assets across its various companies, engaged in as many as 26 million transactions per day, and had millions of users." *Id.* at 10.

closely with a loosely affiliated cryptocurrency hedge fund called Alameda Research.[156] In his first declaration in support of the bankruptcy proceedings, John J. Ray III, newly appointed chief executive officer ("CEO") of FTX Trading LTD and its affiliated entities named in the Chapter 11 case and the expert brought in to restructure Enron after its fraud was discovered, declared "[n]ever in my career have I seen such a complete failure of corporate controls and such a complete absence of trustworthy financial information as occurred [at FTX]."[157] Ray undertook an internal investigation, which determined that a small group of individual actors controlled both FTX and Alameda Research, and that "[t]hese individuals stifled dissent, comingled and misused corporate and customer funds, lied to third parties about their business, joked internally about their tendency to lose track of millions of dollars in assets" and caused FTX to spectacularly collapse at an unprecedented scale through entirely routine intermediary risks of "hubris, incompetence, and greed."[158] Moreover, attempts to improve regulatory compliance "were not welcome and resulted in backlash."[159]

Although FTX companies and Alameda Research formally operated as separate entities, the finances of both companies intertwined so heavily that Alameda funds frequently paid for FTX operations, and Alameda and FTX funds were often transferred directly to employees and executives "to fund personal investments, political contributions, and other expenditures," including real estate purchases, only some of which were half-documented as "loans."[160] Alameda also received special access to FTX trading platforms, which allowed it "an effectively limitless ability to trade and withdraw assets from the exchange regardless of the size of Alameda's account balance, and to exempt Alameda from the auto-liquidation process that applied to other customers."[161] As alarming as these failures of compliance and corporate governance are,

---

156 Matthew Goldstein, Alexandra Stevenson, Maureen Farrell & David Yaffe-Bellany, *How FTX's Sister Firm Brought the Crypto Exchange Down*, N.Y. Times (Nov. 18, 2022), https://www.nytimes.com/2022/11/18/business/ftx-alameda-ties.html [https://perma.cc/6QVZ-URM4]. Alameda predated FTX, having been founded in 2017. *Id.* Much like Three Arrows Capital's early business model, Alameda's business model was such that "[i]t bought Bitcoin and other cryptocurrencies in one part of the world and sold them in another, pocketing the difference." *Id.* When more traditional sources of capital dried up, FTX emerged as a solution to Alameda's liquidity crisis. *See id.*

157 Declaration of John J. Ray III in Support of Chapter 11 Petitions and First Day Pleadings ¶ 5, *In re* FTX Trading LTD, No. 22-11068 (Bankr. D. Del. Nov. 17, 2022).

158 First Interim Report of John J. Ray, *supra* note 155, at 3. "As a general matter, policies and procedures relating to accounting, financial reporting, treasury management, and risk management did not exist, were incomplete, or were highly generic and not appropriate for a firm handling substantial financial assets." *Id.* at 11.

159 *Id.* at 8.

160 *Id.* at 17.

161 *Id.* at 18.

they only scratch the surface of the wrongdoing undertaken by FTX. Notably, FTX was a centralized intermediary to which existing laws applied but nevertheless failed to prevent customer harm.[162] Ultimately, the founder and CEO of FTX, Sam Bankman-Fried, received a guilty verdict on seven counts of fraud.[163] Bankman-Fried was sentenced to 25 years in prison on March 28, 2024, less than the maximum sentence of 110 years.[164]

Despite the internal mess that was FTX and Alameda operations,[165] FTX and its founder, Sam Bankman-Fried, for a long time enjoyed regulatory deference and near-celebrity status.[166] For example, at the time

---

162 For example, FTX also allegedly perpetrated market manipulation through various avenues, including the use of its own exchange token FTT. Goldstein et al., *supra* note 156. The management teams of both entities also allegedly actively avoided the creation of audited financial statements and created financial records out of whole cloth. *See* First Interim Report of John J. Ray, *supra* note 155, at 7, 11, 14.

163 Allison Morrow, *Sam Bankman-Fried Found Guilty of Seven Counts of Fraud in Stunning Fall for Former Crypto Billionaire*, CNN Bus. (Nov. 3, 2023, 7:04 AM), https://www.cnn.com/2023/11/02/business/ftx-sbf-fraud-trial-verdict/index.html [https://perma.cc/QRA4-T46M].

164 David Yaffe-Bellany & J. Edward Moreno, *Sam Bankman-Fried Sentenced to 25 Years in Prison*, N.Y. Times (Mar. 28, 2024), https://www.nytimes.com/2024/03/28/technology/sam-bankman-fried-sentenced.html [https://perma.cc/FFW4-WPWM].

165 The full scale of the problems within the FTX corporate entity family, which included FTX, Alameda and 134 other corporate entities, are simply too much to document here and are beyond the scope of this Article. Daniela Ešnerová, *FTX Alameda Contagion: Full List of Entities with Exposure to SBF's Firms Including Voyager, Stargate, Tom Brady Seed Investments*, Capital.com (Nov. 18, 2022, 10:52 AM), https://capital.com/ftx-alameda-contagion-list-entities-exposure-sbf-miami-voyager-tom-brady [https://perma.cc/3AQL-2CCT]. Indeed, complete books have been written documenting the saga. To that end, for further reading about the FTX collapse, see, for example, Zeke Faux, Number Go Up: Inside Crypto's Wild Rise and Staggering Fall (2023); Michael Lewis, Going Infinite: The Rise and Fall of a New Tycoon (2023); Ben Armstrong, Catching Up to FTX: Lessons Learned in My Crusade Against Corruption, Fraud, and Bad Hair (2023); Brady Dale, SGF: How the FTX Bankruptcy Unwound Crypto's Very Bad Good Guy (2023).

166 Indeed, in May 2022, Sam Bankman-Fried appeared in the *Time Magazine* list of 100 Most Influential People of 2022. Andrew R. Chow, *Sam Bankman-Fried—The 100 Most Influential People of 2022*, Time Mag. (May 23, 2022, 6:06 AM), https://time.com/collection/100-most-influential-people-2022/6177770/sam-bankman-fried/ [https://perma.cc/E3NJ-288Z]. The profile reads, in part:

> The 30-year-old founder of the exchange platform FTX has become a key public face of crypto, using every tool imaginable to convince the public of its strengths, whether that's hiring Larry David for a Super Bowl commercial, renaming the Miami Heat's arena after his company, donating millions to political campaigns, or testifying in front of Congress.
>
> Bankman-Fried is working to reshape the way the world sees crypto because he believes in its transformative power for good. . . . In a crypto landscape ridden with scams, hedonism, and greed, Bankman-Fried offers a kinder and more impactful vision brought forth by the nascent technology.

Id.

Nearly one year later, Time ran a piece alleging that various people tried to raise warnings "that Sam Bankman-Fried was unethical, duplicitous, and negligent in his role as CEO of Alameda

of FTX's collapse, the CFTC was considering a proposal to "permit[] FTX to self-clear non-intermediated crypto derivatives traded on margin by retail investors."[167] FTX and Bankman-Fried also purportedly lobbied for proposed legislation under consideration by the Senate at the time of FTX's collapse, which sought to "create a new federally recognized asset class called digital commodities and give oversight of digital commodities markets to the CFTC."[168] Representatives from FTX and IEX, a broker-dealer in which FTX invested, including Bankman-Fried, met with SEC staff and discussed a no-action letter in March 2022, prior to FTX's collapse months later.[169] Although the SEC would later claim it had been investigating FTX for months and charge Bankman-Fried with defrauding equity investors in FTX Trading Ltd., such enforcement action came far too late to avoid customer harm.[170] The SEC regulatory action and FTX's engagement with the CFTC and with federal and other lawmakers does, however, highlight the fact that FTX entities acted as intermediaries subject to many of the core regulatory compliance obligations that the financial system relies upon to protect financial markets and that FTX imploded after years of undetected fraud despite such rules.[171]

Readily apparent from even this brief review of the cryptocurrency-related business failures[172] that underlie recent calls for greater

---

Research." Charlotte Alter, *Exclusive: Effective Altruist Leaders Were Repeatedly Warned About Sam Bankman-Fried Years Before FTX Collapsed*, Time Mag. (Mar. 15, 2023, 7:00 AM), https://time.com/6262810/sam-bankman-fried-effective-altruism-alameda-ftx/ [https://perma.cc/3N5Z-255Q].

167 Lee Reiners & Sangita Gazi, *Wanted: A Prudential Framework for Crypto-Assets*, 76 Ark. L. Rev. 311, 312 (2023).

168 *Id.*

169 Colin Wilhelm & Kollen Post, *FTX Asked About, but Did Not Receive Special Exemption from SEC*, The Block (Nov. 14, 2022, 9:17 PM), https://www.theblock.co/post/186908/ftx-asked-about-but-did-not-receive-special-exemption-from-sec [https://perma.cc/A3GD-8JUK]; SEC File No. S7-25-20, Re: Meeting with IEX/FTX (Apr. 29, 2022), https://www.sec.gov/comments/s7-25-20/s72520-20127575-288804.pdf [https://perma.cc/FE3T-GVCX].

170 Complaint at 1, 24, SEC v. Samuel Bankman-Fried, No. 22-cv-10501 (S.D.N.Y. Dec. 13, 2022); Lydia Beyoud & Olga Kharif, *FTX's Sam Bankman-Fried Faces SEC Probe as His Empire Crumbles*, Bloomberg (Nov. 10, 2022, 7:32 PM), https://www.bloomberg.com/news/articles/2022-11-11/ftx-s-sam-bankman-fried-faces-sec-probe-as-his-empire-crumbles [https://perma.cc/K6NL-2URC]. The CFTC also filed fraud charges against Bankman-Fried and FTX in December 2022, long after the implosion already caused unprecedented damage. Complaint at 2-3, CFTC v. Samuel Bankman-Fried, No. 1:22-cv-10503 (S.D.N.Y. Dec. 13, 2022).

171 *See* Peter Whoriskey & Tory Newmyer, *FTX Crypto Implosion Focuses Scrutiny on SEC Chief Gensler*, Wash. Post (Dec. 14, 2022, 2:22 PM), https://www.washingtonpost.com/technology/2022/12/14/sec-gensler-crypto-ftx/ [https://perma.cc/4X2D-W7FN].

172 Notably not mentioned in this brief history of cryptocurrency-intermediary failures are the Genesis bankruptcy of January 2023, the JPEX exchange collapse of 2023, and major cyber-security hacks such as those that occurred at LCX or HTX. *See* Jack Denton, *Crypto Lender Genesis Files for Bankruptcy. It Could be Far Worse for Bitcoin.*, Barron's (Jan. 20, 2023, 10:34 AM), https://www.barrons.com/articles/genesis-bankruptcy-crypto-bitcoin-51674206942 [https://perma.cc/4TXQ-T4XQ]; Suvashree Ghosh & Kiuyan Wong, *Crypto Platform JPEX Shuts Down Trading*

intermediary regulation in the blockchain industry is that (1) each of these failures were failures of CeFi institutions—entities that used blockchain technology but mirrored traditional finance in their structure and service model, and (2) the failures of 2022 and 2023 resulted from choices made by the CeFi intermediaries themselves as part of extensively regulated financial activity. Ponzi schemes, theft, financial mismanagement, and market manipulation all represent intermediary risks that financial regulation attempts to mitigate. Such risks also represent some of the very risks Layer 1 blockchain protocols and Layer 2 DeFi solutions were developed to mitigate through technology. That such activity nevertheless takes place through services related to cryptocurrency has led policy makers and commentators to direct four common, but demonstrably incorrect, policy critiques at cryptocurrency and blockchain technology as a whole.

B. The Four Most Common, and Incorrect, Policy Responses to Cryptocurrency-Intermediary Failures

In the wake of the cryptocurrency-intermediary turmoil of 2022 and 2023, the tendency among policymakers, lawmakers, regulators, and other commentators was to direct one of four common critiques at cryptocurrency and blockchain technology: (1) cryptocurrency is not regulated, and the cryptocurrency-intermediary failures of 2022 and 2023 reflect that lack of regulation,[173] (2) cryptocurrency technology itself shoulders the blame for the cryptocurrency-intermediary failures of 2022 and 2023,[174] (3) decentralization is a sham and its false promise caused the consumer harm experienced since 2022,[175] or (4) cryptocurrency should be banned altogether.[176] The difficulty with each of these policy narratives lies either in their inaccuracy—not as a matter of opinion, but as a matter of technical fact—or in the fact that enacting rules based on these narratives will not achieve the stated policy aims that motivate them. Indeed, the history of cryptocurrency-intermediary

---

Amid Hong Kong Probe, BLOOMBERG (Sept. 18, 2023, 7:40 AM), https://www.bloomberg.com/news/articles/2023-09-18/crypto-platform-jpex-shuts-down-trading-amid-hong-kong-probe [https://perma.cc/H344-XVAR]; *LCX Hack Update*, LCX (June 7, 2022), https://www.lcx.com/lcx-hack-update/ [https://perma.cc/BV7U-2Z84]; Tom Mitchelhill, *Crypto Exchange HTX Sees Outflows Top $258M Following Exploit*, COINTELEGAPH (Dec. 11, 2023), https://cointelegraph.com/news/crypto-exchange-htx-outflow-258-million-hack-november [https://perma.cc/HCS6-YJUK]. The point here is that reliance on intermediaries in the cryptocurrency ecosystem injects risk at Layer 2, which Layer 1 blockchain protocols are designed to mitigate.

173 *See* Redman, *supra* note 15; Morrow, *supra* note 15.

174 *See* Allen, *supra* note 16; Aramonte et al., *supra* note 16.

175 *See* Michaels, *supra* note 17; Aramonte et al., *supra* note 16.

176 *See* Munger, *supra* note 18; Toppa, *supra* note 18; Bambrough, *supra* note 18; Allen, *Testimony*, *supra* note 18.

failures as far back as Mt. Gox shines a light on the core problem underlying each of these policy responses and their corresponding narratives.[177]

First, CeFi intermediaries providing cryptocurrency-related services often face heavy regulatory burdens, and they have faced such regulation since at least March 2013, when FinCEN issued its initial virtual currency guidance.[178] Regulation covers certain statutorily defined activity, and if an entity undertakes regulated activity, the entity shoulders regulatory compliance obligations irrespective of the medium through which that activity is accomplished.[179] As a result, cryptocurrency intermediaries must comply with state money transmission license requirements,[180] state asset custody and consumer protection obligations,[181] federal money transmission registration and related compliance obligations,[182] securities and commodities regulatory requirements,[183] data privacy protection rules,[184] and tax reporting obligations,[185] among other regulatory regimes. Far from operating in a "Wild West" that lacks any regulation at all, cryptocurrency intermediaries face so many potentially applicable, and sometimes conflicting, regulatory regimes that many industry representatives and researchers

---

177 *See infra* notes 178–91.

178 Reyes, *supra* note 20, at 204; Middlebrook & Hughes, *supra* note 84, at 828–31; Stephen T. Middlebrook & Sarah Jane Hughes, *Virtual Uncertainty: Developments in the Law of Electronic Payments and Financial Services*, 69 BUS. LAW. 263, 264 (2013).

179 Hess, *supra* note 43, at 356–63.

180 *See* Middlebrook & Hughes, *supra* note 84, at 833–34; Joseph Jasperse, *50-State Review of Cryptocurrency and Blockchain Regulation*, STEVENS CTR. INNOVATION FIN., https://stevenscenter.wharton.upenn.edu/publications-2te-review/ [https://perma.cc/9BU8-K4W2].

181 *See* Ronald David Smith & Mike Keeley, *Texas Department of Banking Allows State Banks to Provide Virtual Currency Custody Services*, NORTON ROSE FULBRIGHT (June 22, 2021), https://www.nortonrosefulbright.com/en/knowledge/publications/2b7ca476/texas-department-of-banking-allows-state-banks-to-provide-virtual-currency-custody-services [https://perma.cc/7XYP-N6CF].

182 *See* DEP'T TREASURY FIN. CRIMES ENF'T NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES, FIN-2019-G001 (May 9, 2019), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models [https://perma.cc/55Y2-73DQ].

183 *See* Brian Elzweig & Lawrence J. Trautman, *When Does a Nonfungible Token (NFT) Become a Security?*, 39 GA. ST. U. L. REV. 295, 310 (2023); Yuliya Guseva, *When the Means Undermine the End: The Leviathan of Securities Law and Enforcement in Digital-Asset Markets*, 5 STAN. J. BLOCKCHAIN L. & POL'Y 1, 3 (2022); Carol R. Goforth, *Regulation of Crypto: Who is the Securities and Exchange Commission Protecting?*, 58 AM. BUS. L.J. 643, 647 (2021); Andrew Verstein, *Crypto Assets and Insider Trading Law's Domain*, 105 IOWA L. REV. 1, 58 (2019).

184 Raffi Teperdjian, *The Puzzle of Squaring Blockchain with the General Data Protection Regulation*, 60 JURIMETRICS 253, 254–55 (2020).

185 Joshua Durham, *Regulatory Sandboxes Enable Pragmatic Blockchain Regulation*, 18 WASH. J.L. TECH. & ARTS 28, 39 (2023).

repeatedly call for increased regulatory clarity.[186] Rather than take such calls for clarity seriously, many policymakers and other commentators cling to the narrative—one irreconcilable with reality—that cryptocurrency-related businesses are unregulated and the enactment of sweeping, strict, and universally applicable new and technology-specific regulation will reduce the number of cryptocurrency intermediary failures and mitigate related consumer harms.[187] To date, however, the existing and clearly applicable regulatory regimes failed to prevent the massive cryptocurrency-intermediary failures of 2022 and 2023, all of which were caused by common financial fraud which regulatory intervention already allegedly addresses.[188]

The second and third critiques suffer from a failure to distinguish between the different layers of the blockchain technology stack and the different technical structures and business models that exist across the industry. When critics point to the cryptocurrency intermediary failures of 2022 and 2023 and allege that the technology itself caused the massive consumer losses, they often point to the complexity of the technology and argue that consumers and investors could not properly hedge against such complex risk.[189] With the potential exception of the Terra-Luna collapse, the risks that caused consumer harm in 2022 and 2023 were all fairly straightforward counterparty risks: making risky loans on bad terms and stealing customer funds.[190] That the blockchain protocols upon which cryptocurrencies can be transacted are themselves technically complex has nothing to do with risky loans or theft of funds. The technical complexity of Layer 1 blockchain protocols does not prevent customers and investors from understanding the risks of CeFi entities that act as intermediaries and operate at Layer 2 or Layer 3.

Similarly, critiques alleging that consumer harm stems from "sham decentralization" in blockchain technology fail to appreciate that actors operating at each layer of the blockchain technology stack can operate at a different level of decentralization. A Layer 1 protocol might be characterized by significant levels of decentralization, while a service provided at Layer 2 is offered by a corporation on a highly centralized basis.[191] In CeFi, a centralized exchange like FTX, for example, often conducts trades between users off chain, recording trades executed through a website like FTX.com (Layer 3) throughout a single day in

---

186 *See, e.g.*, *id.* at 40–42; Lewis R. Cohen, Greg Strong, Freeman Lewin & Sarah Chen, The Ineluctable Modality of Securities Law: Why Fungible Crypto Assets are not Securities 10–11 (Nov. 10, 2022) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4282385 [https://perma.cc/W83P-6NHM]; Michaels, *supra* note 17.

187 *See supra* notes 178–85.

188 *See supra* Section II.A.

189 Allen, *supra* note 30, at 926.

190 *See supra* Section II.A.

191 *See supra* notes 70–79 and accompanying text.

an internal record (Layer 2) and only recording the day's end positions on the public blockchain protocol (Layer 1).[192] Alternatively, in DeFi, a decentralized exchange might enable peer-to-peer trades through smart contracts (Layer 2) that automatically record transactions to the underlying blockchain protocol (Layer 1) at regular intervals. In both cases—centralized or decentralized exchange—the level of decentralization at the blockchain protocol layer remains unaffected by whether trading activity occurs through a more centralized or more decentralized mechanism at the higher levels in the blockchain technology stack. Accusations that the mere existence of cryptocurrency intermediaries prove that decentralization of Layer 1 blockchain protocols are a sham[193] reflect a lack of technical nuance that can derail attempts to create effective legal and policy attempts to reduce risky cryptocurrency-intermediary behavior and mitigate future consumer harm. Critics lump CeFi and DeFi together, ignoring the very real differences in the risks their technical and business structures pose to consumers and markets, and then claim the technology itself is to blame.[194] Doing so does very little to actually reduce risks in CeFi and impedes efforts to explore the benefits of DeFi.

Finally, although blockchain technology bans and blacklists are possible,[195] such regulatory responses will ultimately fail to achieve the policy aims of investor protection and systemic risk reduction that such proposals seek. Instead of actually eliminating the existence of blockchain technology or the use of cryptocurrency, it is more likely that a ban on blockchain technology would simply push technical architecture designs toward deeper decentralization.[196] In other words, because bans and blacklists are easier to implement in CeFi, such regulatory responses will likely push projects toward DeFi. This type of deeper decentralization would make regulatory intervention by a system over reliant on intermediaries extremely difficult to undertake.

Ultimately, none of the activity that resulted in the cryptocurrency-intermediary implosions of 2022 and 2023 was unique to cryptocurrency or inherently required by blockchain technology.[197]

---

192 *See* Kristin N. Johnson, *Regulating Cryptocurrency Secondary Market Trading Platforms*, U. CHI. L. REV. ONLINE (2020), https://lawreviewblog.uchicago.edu/2020/01/07/298/ [https://perma.cc/3DGX-VCEN].

193 *See, e.g.*, Allen, *supra* note 16.

194 *See* Johnson, *supra* note 192.

195 Packin & Jabotinsky, *supra* note 19, at 4.

196 *See* Massari & Catalini, *supra* note 99.

197 Indeed, prior commentary has recognized that the activity undertaken by certain cryptocurrency intermediary firms at Layer 2 involve activity that existing regulation is designed to address. *See* Kristin N. Johnson, *Decentralized Finance: Regulating Cryptocurrency Exchanges*, 62 WM. & MARY L. REV. 1911, 1920 (2021).

The technology itself is not to blame for the customer harm and loss of value suffered because of those corporate failures. Rather, traditional fraud, outright refusal to comply with regulatory requirements, and bad business judgment—the same type of activity that fueled the Enron and London Interbank Offered Rate ("LIBOR") scandals and the subprime mortgage crisis—featured prominently as causes of lost value in the cryptocurrency market. Notably, in the wake of the Enron, LIBOR, and subprime mortgage crises, lawmakers enacted new regulations to allegedly address precisely these types of harms.[198] If those laws work so well, why did they not catch the impending cryptocurrency implosions before they happened? Perhaps the regulatory regime failed to prevent these intermediary failures not because cryptocurrency is unique or unregulated, or because the fraud was particularly complex. Perhaps, instead, the cryptocurrency industry is acting as a magic mirror for financial intermediary regulation and warning of cracks in the existing approach to financial regulation.

III. Overreliance on Intermediaries Undermines Public Law's Effectiveness and Legitimacy

The summer and fall of 2023 saw the cryptocurrency and blockchain community in shock as the CFTC, Office of Financial Asset Control ("OFAC"), the Department of Justice, and several courts labeled various actors in the blockchain ecosystem as intermediaries and expected them to shoulder certain corresponding regulatory responsibility and liability.[199] Even Congress considered adopting legislation that would impose obligations on intermediaries that, in view of the technical reality of many blockchain systems and DeFi projects, simply do not exist. As regulators and lawmakers identified actors in the blockchain technology ecosystem that could serve as the targets of intermediary-centered regulation, the process by which such decisions were made lacked transparency, deliberation, and technical nuance.[200] Instead, the legal and regulatory process remained inflexible, as though it simply could not adapt to a world where certain activities could be achieved without any intermediary other than technology. This inflexibility undermines the effectiveness and legitimacy of the applicable legal and regulatory regimes and reflects a highly centralized approach

198 *See, e.g.*, Regulations Implementing the Adjustable Interest Rate (LIBOR) Act, 88 Fed. Reg. 5204 (Jan. 26, 2023) (to be codified at 12 C.F.R. pt. 253); Pamela H. Bucy, *"Carrots and Sticks": Post-Enron Regulatory Initiatives*, 8 Buff. Crim. L. Rev. 277 (2004).

199 *See, e.g.*, David Kappos, Evan Norris & Daniel Barabander, *More than Just the Ooki DAO: Lessons for Web3 Companies About Control After bZx*, CoinDesk (June 14, 2024, 2:26 PM), https://www.coindesk.com/opinion/2022/10/31/more-than-just-the-ooki-dao-lessons-for-web3-companies-about-control-after-bzx/ [https://perma.cc/Q56D-RYB4]; *infra* Section III.A.

200 *See infra* Section III.A.

to lawmaking that itself relies upon a massive, layered tower of intermediated decision makers.

A. Law's Overreliance on Intermediaries Impedes Adoption of Workable Rules

To mitigate the risk that people can take customer money and run, software developers in the blockchain ecosystem began experimenting with code that could perform the functions that intermediaries traditionally perform—DeFi protocols. Blockchain technology itself sought to absolve the need for an intermediary for a one-way transfer of electronic value from one person to another.[201] Building on that idea, developers began experimenting with software tools that enable decentralized exchange—truly peer-to-peer trades that eliminate centralized exchange services such as those provided by Coinbase.[202] The blockchain community often refers to such tools as a decentralized exchange, or "DEX."[203] Like most software, products, and services in the blockchain technology ecosystem, not all things often referred to as DEXs use the same technical architecture. One of the many variables that may differentiate one decentralized exchange tool from another lies in the level of technical control and business control retained by founders, software developers, and token holders.[204] Regulatory agencies seem to view even a very low level of technical and business control as sufficient centralization to warrant treatment as an intermediary.[205]

One type of technical and business control regulators have targeted centers on the use of governance tokens to approve updates to the software that enables decentralized exchange.[206] When governance tokens are employed this way by a decentralized exchange software development project, users of the decentralized exchange software

---

201 *See, e.g.*, Brad Bourque, *The Crypto Wars and the Future of Financial Privacy*, FORDHAM J. CORP. & FIN. L.: BLOG (Mar. 31, 2023), https://news.law.fordham.edu/jcfl/2023/03/31/the-crypto-wars-and-the-future-of-financial-privacy/ [https://perma.cc/W8JV-B9CV] ("Bitcoin's revolutionary promise was to offer a method for exchanging value online without sharing personal, private information with financial intermediaries that are subject to the Bank Secrecy Act ('BSA')—information that the government can readily access without a warrant under the Supreme Court's Third-Party Doctrine.").

202 *E.g.*, Will Warren, *Decentralized Exchange*, COIN CTR. (Oct. 10, 2018), https://www.coincenter.org/education/key-concepts/decentralized-exchange/ [https://perma.cc/7SJG-DTRE].

203 *Id.* A DEX is one type of DeFi protocol.

204 Kappos et al., *supra* note 199 ("The bZx enforcement action demonstrates how at least one key regulator is thinking about control of Web3 protocols in order to hold operators accountable: by examining both technical and business control to draw the line between identifiable persons and autonomously run protocols.").

205 *See id.*

206 Reyes, *supra* note 52, at 1217–18 (explaining the concept of governance tokens).

that hold a specific token manage updates to the software code.[207] For example, the Ooki protocol[208] enables decentralized margin trading and lending.[209] Ooki styles itself as "a community-run project, governed by the community vote for all major changes to the protocol."[210] Discussion on proposed changes occurs in the Ooki Forum,[211] and anyone who holds OOKI tokens can vote on proposals.[212]

In October 2022, the CFTC sued the Ooki decentralized autonomous organization ("DAO"), alleging that the DAO operated an unregistered designated contract market and an unregistered futures commission merchant in violation of the Commodity Exchange Act ("CEA").[213] The provisions of the CEA related to future commission merchants apply to individuals, associations, partnerships, corporations, or trusts that conduct certain enumerated activities.[214] As a result, the CFTC argued that "[t]he Ooki DAO is an unincorporated association comprised of Ooki Token holders who have voted those tokens to govern the Ooki Protocol."[215] The CFTC variously stated that the Ooki DAO constitutes an unincorporated association under the federal definition of that entity,[216] and that, more specifically, Ooki DAO operated as a for-profit partnership under state general partnership law principles[217] even while recognizing that "the Ooki DAO does not explicitly define its own membership."[218] The idea that an open-source software

---

207 Kappos et al., *supra* note 199.

> Technical control refers to technical mechanisms protocol developers use to control their protocol on the smart contract level, often by defining 'admin-only' functions that can be called solely by specific parties . . . [T]he CFTC focuses on four levers of control—admin-only functionalities retained by bZeroX and the co-founders, and subsequently, the DAO: (1) upgrading protocol smart contracts; (2) pausing or suspending trading; (3) pausing or suspending contributions or withdrawals of assets and redemptions; and (4) directing disposition of the funds held on protocol smart contracts.

Id.

208 The Ooki protocol was formerly the bZx Protocol. *See* Complaint ¶ 2, CFTC v. Ooki DAO, No. 3:22-cv-5416 (N.D. Cal. Sept. 22, 2022).

209 *Introduction to Ooki*, GitBook, https://ooki.gitbook.io/ooki/ [https://perma.cc/4TCU-SC87].

210 *Id.*

211 *Ooki DAO*, GitBook, https://ooki.gitbook.io/ooki/governance/dao-governance [https://perma.cc/2H9N-X7PH].

212 *Id.*

213 7 U.S.C. §§ 1–26; Complaint ¶ 1, CFTC v. Ooki DAO, No: 3:22-cv-05416 (N.D. Cal. Sept. 22, 2022).

214 Complaint, *supra* note 213, ¶¶ 56–62.

215 *Id.* ¶ 47; *see also* Order Instituting Proceedings, bZeroX, LLC, CFTC No. 22-31, at 11 (Sept. 22, 2022) [hereinafter *bZeroX CFTC Order*] ("The Ooki DAO is a for-profit unincorporated association.").

216 *bZeroX CFTC Order*, *supra* note 215, at 10.

217 *Id.* at 11.

218 *Id.* at 10.

community constituted a general partnership shocked many.[219] Indeed, the CFTC's insistence on enforcing against the Ooki Protocol by proposing a DAO membership and purpose that the "Ooki DAO" did not ascribe to itself undermines the general purpose and effectiveness of general partnership law[220] and makes it incredibly difficult for open-source projects to effectively draw lines around software development activities.[221]

In other technical architectures, even a loosely affiliated group of token holders cannot be said to meaningfully "control" the software enabling decentralized exchange. In its purest form, no intermediary operates in the middle of decentralized exchange.[222] 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."[223] For example, the 0x Protocol is a software tool enabling the

---

219 *See* Reply Brief of Amicus Curiae DeFi Education Fund Regarding Plaintiff's Motion for Alternative Services at 9, CFTC v. Ooki DAO, No. 3:22-cv-05416 (N.D. Cal. Nov. 21, 2022) ("[T]he Commission is asking the Court to adopt a novel theory that rests solely on token-voting, even though that theory is a clear departure from the cases on which the Commission relies."); Reply Brief of Amicus Curiae LexPunk in Opposition to Commodity Futures Trading Commission's Consolidated Opposition to Amicus Curiae Motions for Reconsideration of Order Granting Plaintiff's Motion for Alternative Service at 6, *Ooki DAO* (N.D. Cal. Nov. 21, 2022); Reply Amicus Curiae Brief of Andreesen Horowitz Regarding Plaintiff's Motion for Alternative Service at 11–12, *Ooki DAO* (N.D. Cal. Oct. 31, 2022).

220 For more on the potential conflict between the purpose of general partnership law and government agency determinations that open-source software development communities operate general partnerships, see Carla L. Reyes & Christine Hurt, *The Contractarian Joint Venture*, 76 Ala. L. Rev. (forthcoming 2025) (on file with author).

221 "The legal treatment of DAOs whose members vote through governance tokens has been the subject of considerable debate among those in the Web3 space." Alexander C. Drylewski, Stuart D. Levi, Daniel Michael & Ian C. Lerman, *CFTC Settles Claims Against Founders of a Decentralized Protocol and Sues its Successor DAO and its Members, Pressing a Novel Theory of Liability*, Skadden (Oct. 5, 2022), https://www.skadden.com/insights/publications/2022/10/cftc-settles-claims [https://perma.cc/3URZ-6SYH]. Indeed, the Author has been warning that this type of mismatch would occur since 2019. *See* Carla L. Reyes, *If Rockefeller Were a Coder*, 87 Geo. Wash. L. Rev. 373 (2019).

222 Peter Van Valkenburgh, *There's No Such Thing as a Decentralized Exchange*, The Block (Oct. 3, 2020, 12:01 PM), https://www.theblock.co/post/79768/theres-no-such-thing-as-a-decentralized-exchange [https://perma.cc/C2B2-29TU].

> 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.

223 *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.").

decentralized exchange of cryptocurrencies.[224] Although a company called ZeroEx, Inc. developed the software known as the 0x Protocol, the software "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.[225] ZeroEx, Inc. did, however, create a website, "Matcha," through which users could access the 0x Protocol.[226] 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.[227] Yet the CFTC became concerned that "certain leveraged digital assets" traded via the 0x Protocol without complying with the relevant CEA requirements.[228] The difficulty for the CFTC in addressing its concern, of course, lies in the fact the CEA requirements governing leveraged or margined retail commodity transactions, like the ones that took place via 0x, are intended to apply to intermediaries that facilitate such trades in a centralized manner.[229] No such entity exists in the 0x Protocol.[230]

In this way, the ZeroEx order is emblematic of the broader problem facing U.S. financial regulators—namely, that financial and capital markets regulations apply to intermediaries. Regulators rely upon centralized entities to combat money laundering via financial surveillance of customers and to reduce market information asymmetries through disclosure of certain required and material information.[231] In the face of DeFi technology such as that developed by the software engineers at ZeroEx, how could such regulations apply? Without an intermediary to serve as the object of financial and capital markets regulation, the legal interventions on the books simply do not function.[232]

Rather than attempt to adapt capital markets regulations to a disintermediated financial platform, regulators decided to pretend that an intermediary existed anyway. In an order dated September 7, 2023, the

---

224 Order Instituting Proceedings at 2, *In re* ZeroEx, Inc., CFTC No. 23-41 (Sept. 7, 2023) [hereinafter ZeroEx Order] ("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)).

225 *Id.* at 3.

226 *Id.*

227 *See id.* at 3–4.

228 *Id.*

229 Durham, *supra* note 185, at 38–39.

230 *See* ZeroEx Order, *supra* note 224, at 2.

231 *See* Van Valkenburgh, *supra* note 222.

232 *See, e.g.*, *id.* (arguing that regulations designed for intermediaries simply do not apply to decentralized exchange software and that attempts to enforce against such software may face constitutional challenges related to free speech and privacy).

CFTC and ZeroEx entered into a settlement arrangement in anticipation of the CFTC pursuing an enforcement proceeding against ZeroEx for creating Matcha.[233] The CFTC maintained the settlement was warranted because ZeroEx "conduct[ed] an office or business in the United States for the purpose of soliciting or accepting orders for, or otherwise dealing in, off-exchange leveraged or margined retail commodity transactions with customers who were not eligible contract participants or eligible commercial entities."[234] It remains unclear how the enforcement action achieved the goals of the CEA. 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. Further, 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.[235] Given that reality, what did the CFTC achieve in its action against ZeroEx?

The same day as the ZeroEx Order, the CFTC entered an Order in relation to the Deridex Protocol for similar violations of the CEA.[236] Notably, the Deridex Protocol was comprised of smart contracts on the Algorand blockchain.[237] Anyone 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.[238] 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.[239] 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

---

233 ZeroEx Order, *supra* note 224, at 5–8.

234 *Id.* at 2.

235 *See id.* at 3.

236 Order Instituting Proceedings, *In re* Deridex, Inc., CFTC No. 23-42 (Sept. 7, 2023).

237 *Id.* at 3.

238 *Id.*

239 *See id.* at 3–4.

upgrade software code and face potential consumer protection or other liability if a software bug causes user losses.

In another area of law altogether, OFAC took a page from the CFTC's playbook and created an "entity" out of thin air in order to sanction a specific instance of computer code and place it on the Specially Designated National List. The cryptocurrency ecosystem uses the term "Tornado Cash" to refer to a set of smart contracts that together form privacy-enhancing software that anyone can use to protect themselves when conducting transactions via, primarily, the Ethereum blockchain protocol.[240] When an Ethereum user wants to increase the privacy of their financial transactions—recall, routine transactions are publicly recorded for anyone to see and data mine[241]—the user transacts funds to a Tornado Cash pool and then withdraws them at a later time to a different public key address.[242] The depositing wallet is given a private key—like a receipt—which enables any public key that presents that private key for redemption to withdraw the funds from the Tornado Cash smart contracts at a later time.[243] Tornado Cash accepts transactions in increments, and mixes like denominations together; the larger the amount of transacted cryptocurrency in the pool, the greater level of technical privacy provided to the transaction.[244]

Moreover, users may choose to use a "relayer" for additional privacy.[245] Anyone who executes a transaction on the Ethereum protocol must pay a transaction fee, including any transaction to or withdrawal from the Tornado Cash smart contracts.[246] One way to pay the transaction fee would be to preload funds for the relayer as part of the initial transaction to Tornado Cash; however, doing so would impede the Tornado Cash software from providing the privacy the user seeks to achieve in the first place.[247] To ensure the privacy enhancing purpose of the software can be achieved, users can choose a third-party relayer from Tornado Cash's Relayer Registry.[248] The relayer pays the Ethereum

---

240 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/8A9D-TJQ4]; 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) ("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.").

241 See *infra* notes 278–82 and accompanying text for a more complete discussion as to why such radical transparency is problematic for everyday financial privacy.

242 Wade et al., *supra* note 240; *see also* Nadler & Schär, *supra* note 240, at 127–28.

243 Nadler & Schär, *supra* note 240, at 127–28.

244 Wade et al., *supra* note 240.

245 *See id.*

246 *Id.*

247 *Id.*

248 *Id.*

protocol transaction fee and sends the user's funds to whatever public key address the user designates in return for a fee.[249] At no point, however, do relayers have custody or control over user assets.[250]

Amidst concerns that the Tornado Cash smart contracts had been used to facilitate money laundering and that certain transactions that flowed through the smart contracts could be connected to certain terrorist groups, the OFAC designated a number of the Tornado Cash smart contracts as Specially Designated Nationals in August 2022.[251] In November 2022, OFAC redesignated various Tornado Cash smart contracts as property belonging to "the entity known as Tornado Cash," claiming Tornado Cash was an organization consisting of (1) "its founders and other associated developers," and (2) "the Tornado Cash DAO."[252] OFAC specifically asserted that it had not designated "Tornado Cash's individual founders, developers, members of the DAO, or users, or other persons involved in supporting Tornado Cash at this time."[253] In reality, however, no "entity known as Tornado Cash" exists; OFAC made it up.

Why would OFAC make up an entity out of thin air? Because OFAC only enjoys the authority to sanction specific intermediaries and their property—namely, a foreign country or national under the International Emergency Powers Act ("IEEPA"),[254] or a person under the North Korea Sanctions & Policy Enhancement Act ("North Korea Act").[255] OFAC regulations interpret the term person to include "an individual or entity,"[256] and defines an entity as a "a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization."[257] In *Van Loon v. Department of Treasury*[258] the U.S. District Court for the District of West Texas upheld OFAC's determination that Tornado Cash is an association composed of its founders, developers, and DAO.[259] If Tornado Cash is a

---

249 *Id.*

250 *Id.*

251 *Specially Designated Nationals List Update*, Off. Foreign Assets Control (Aug. 8, 2022), https://ofac.treasury.gov/recent-actions/20220808 [https://perma.cc/UUD4-TDHH] (original designation).

252 *See Burma-related Designations; North Korea Designations; Cyber-related Designation, Cyber-related Designation Removal; Publication of Cyber-related Frequently Asked Questions*, Off. Foreign Assets Control (Nov. 8, 2022) [hereinafter "FAQ No. 1095"], https://ofac.treasury.gov/recent-actions/20221108 [https://perma.cc/GLM7-VFST] (redesignation); *Frequently Asked Questions*, Off. Foreign Assets Control (Nov. 8, 2022), https://ofac.treasury.gov/faqs/1095 [https://perma.cc/Q54L-BY53].

253 FAQ No. 1095, *supra* note 252.

254 50 U.S.C. § 1702(a)(1)(B).

255 22 U.S.C. § 9214(c)(1).

256 31 C.F.R. § 578.313.

257 31 C.F.R. § 510.305.

258 688 F. Supp. 3d 454 (W.D. Tex. Aug. 17, 2023).

259 *Id.* at 466–67 ("Based on the plain meaning of 'association,' OFAC need only show: (1) that Tornado Cash consists of a body of individuals, and (2) that this body furthers a common

properly designated entity, then transactions involving the Tornado Cash smart contracts could be blocked under OFAC's sanctions authority if they are "property in which any foreign country or a national thereof has any interest" under IEEPA,[260] or are "property and interests in property of a person designated under [the North Korea Act]."[261] OFAC concluded, and the district court upheld, that the Tornado Cash entity held property interests in the smart contracts because the phrase "property and property interest" includes "contracts of any nature whatsoever,"[262] and the court believed that smart contracts are "merely a code-enabled species of unilateral contracts," a "type of contract and, thus, a type of property within the meaning of the regulation."[263] Smart contracts, of course, are not legally enforceable contracts by default, but rather simply if-then computer software programs.[264]

Ultimately, then, for OFAC to achieve this result, and for the District Court in *Van Loon* to uphold it, both either plainly misunderstood the technology or understood it but blatantly ignored the decentralized reality of the technical artifacts that make up the Tornado Cash software.[265] Notably, none of this is required as a technical matter in order to prove that certain funds are free of the taint from illegal transactions. The Tornado Cash software offers a built-in compliance tool that allows a user to selectively deprivatize a transaction that used Tornado Cash to enhance privacy.[266] A user can share a cryptographic proof that links their deposit to their withdrawal address, allowing whomever the user shares the proof with to analyze the blockchain protocol as though the user had never transacted through the Tornado Cash software.[267]

Each case study examined in this Section reveals a regulatory regime that overly relies on intermediaries to achieve their policy aims. In the face of radical disintermediation made possible in DeFi, such as decentralized exchange, the regulatory regime does not apply. Under pressure from the four predominant, even if demonstrably incorrect,

---

purpose. OFAC has done so.").

260 50 U.S.C. § 1702(a)(1)(B).

261 22 U.S.C. § 9214(c)(1).

262 31 C.F.R. § 510.323.

263 *Van Loon*, 688 F. Supp. 3d at 468 (citing 31 C.F.R. § 510.305).

264 *See* Reyes, *supra* note 57, at 1541–42.

265 Unfortunately, however, making up intermediaries that do not exist as a matter of technical fact is not limited to regulatory agency action or isolated court decisions. Rather, Congress itself sought to create new intermediaries in blockchain protocols. Durham, *supra* note 185, at 39–40 (discussing the proposed expansion of tax reporting obligations intended to be achieved by expanding the definition of broker to encompass cryptocurrency miners and developers, concluding that "a lack of care and expertise in drafting this bill made compliance with it impossible and created perverse and unintended policy outcomes").

266 Buterin et al., *supra* note 70, at 1; Nadler & Schär, *supra* note 240, at 132 & n.11.

267 Nadler & Schär, *supra* note 240, at 132 & n.11.

policy responses to the crypto-intermediary failures of 2022 and 2023, regulatory agencies decided to force existing rules to work by identifying intermediaries that do not actually exist in technical reality.

Although useful in producing an object of regulation that can be enforced against, the problem with creating intermediaries that do not exist is threefold. First, enforcement actions and legislative proposals that seem to push an agenda instead of addressing technological facts directly develop mistrust in the law and the lawmaking process. Second, court decisions that evidence a misunderstanding of the technology and seemingly approve of sloppy agency work develop disdain for the judicial process. Third, attempts to force centralization on activity and technology developed to encourage decentralization will only push the industry toward deeper decentralization rather than less. Such deeper decentralization may have good effects in some respects, such as encouraging the use of privacy protecting tools that many believe to be the backbone of simple, good cyber hygiene in the blockchain ecosystem. On the other hand, deeper decentralization will also mean that addressing negative externalities of decentralized behavior when it arises—and it will arise—may be next to impossible. Ultimately, law's overreliance on intermediaries results in a lack of workable rules and undermines law's legitimacy.

B. Even the Lawmaking Process Over Relies on Intermediaries, Undermining Institutional Legitimacy

For many, an approach to regulatory enforcement that targets nonexistent or made-up intermediaries reflects either deep incompetence inside regulatory agencies[268] or intentional overreach that threatens broader democratic values and systems,[269] or both. Setting accusations of agency technical incompetence aside, law's failure to create workable rules that acknowledge the usefulness of decentralization in certain circumstances imbues worry about threats to the broader open-source software

---

268 *See, e.g.*, Durham, *supra* note 185, at 39 ("Fundamentally, legislators and regulators currently lack the expertise required to adapt regulatory approaches to blockchain. Without this expertise, regulators cannot draft rules that enable technical compliance."); *DeFi Education Fund CEO Slams U.S. Treasury's 'Confusing and Self-Refuting' Draft Regulations on Crypto*, CryptoGlobe (Aug. 26, 2023), https://www.cryptoglobe.com/latest/2023/08/defi-education-fund-ceo-slams-u-s-treasurys-confusing-and-self-refuting-draft-regulations-on-crypto/ [https://perma.cc/5GM5-S3G2].

269 *See* Andrew R. Chow, *A New U.S. Crackdown Has Crypto Users Worried About Their Privacy*, Time Mag. (Aug. 10, 2022, 3:47 PM), https://time.com/6205143/tornado-cash-us-crypto-ban/ [https://perma.cc/46P4-XRRK]; Ciaran Lyons, *Coinbase Refutes Senator Warren's Government Insider Allegations*, CoinTelegraph (Dec. 24, 2023), https://cointelegraph.com/news/coinbase-senator-warren-allegations [https://perma.cc/2CVE-WQSM].

development system,[270] privacy,[271] and free speech.[272] Open-source software has played a significant role in U.S. economic productive activity for some time.[273] Indeed, as far back as September 2000, "[t]he President's Information Technology Advisory Committee recommended that the federal government support open source software as a strategic national choice to sustain the U.S. lead in critical software development."[274] Since that time, open-source software has come to form the basis for the internet, public cloud computing platforms, and the cryptography that powers virtual private networks and email encryption, among other key technologies individuals use every day.[275] Open-source software is also thought to democratize technology, allowing customers to inspect the code and encouraging innovation by pointedly allowing other developers to copy and modify source code.[276] Even if regulatory approaches to disintermediated activity via blockchain technology and related software only

---

270 *See* Jack Solowey, *Financial Regulators' Open-Source Crackdown Sets Bad Precedent for AI, DeFi, and Innovation*, CATO AT LIBERTY (Sept. 1, 2023, 12:12 PM), https://www.cato.org/blog/financial-regulators-shouldnt-treat-open-source-software-enemy [https://perma.cc/QF57-7KUK] ("Unfortunately, financial regulators have led the way in cracking down on novel, open-source technologies. In doing so, they risk creating dangerous precedents for the use of open-source software—AI-based and otherwise—in both financial applications and in tech innovation more broadly.").

271 *See, e.g.*, Bourque, *supra* note 201 ("Governments around the world, including the United States' government, have set their sights on the 'shadowy super coders' pioneering new frontiers in cryptography and encryption-based technologies in order to prevent bad actors from using digital assets to facilitate crime. Proponents of the technology, however, tout the potential for encryption-based technologies to preserve individual autonomy in a digital age. At the heart of this battle lies the idea of encryption as a tool for maintaining privacy—'the power to selectively reveal oneself to the world.'"); MILLER WHITEHOUSE-LEVINE & LINDSEY KELLEHER, SELF-HOSTED WALLETS AND THE FUTURE OF FREE SOCIETIES: A GUIDE FOR POLICYMAKERS 29 (2020), https://docslib.org/doc/2680399/self-hosted-wallets-and-the-future-of-free-societies [https://perma.cc/9V29-SB27] ("If cash usage continues to be substituted for digital transaction options and peer-to-peer transactions using self-hosted wallets are restricted, only non-private payment options will be available to individuals. This lack of transactional privacy will not only threaten fundamental civil liberties but also hasten the creation of all-knowing surveillance systems."); BRITO, *supra* note 77, at 2–3 ("In a world without cash (a bearer and peer-to-peer form of money) all transactions must be necessarily intermediated by financial institutions. Intermediate transactions are by their nature subject to surveillance and control. . . . [W]e must . . . develop and foster *electronic cash* that is as privacy-preserving and permissionless as physical cash.").

272 *See* VAN VALKENBURGH, *supra* note 77, at 2.

273 *See* Yochai Benkler, *Coase's Penguin, or, Linux and* The Nature of the Firm, 112 YALE L.J. 369, 371 (2002).

274 *Id.* (citing PRESIDENT'S INFO. TECH. ADVISORY COMM., DEVELOPING OPEN SOURCE SOFTWARE TO ADVANCE HIGH END COMPUTING (2000)).

275 Amanda Brock, *What is Open Source, and Why Does it Matter Today?*, OPEN ACCESS GOV'T (Feb. 8, 2022), https://www.openaccessgovernment.org/open-source-technology/129261/ [https://perma.cc/CH67-GTB6]; Hila Lifshitz-Assaf & Frank Nagle, *The Digital Economy Runs on Open Source. Here's How to Protect it*, HARV. BUS. REV. (Sept. 2, 2021), https://hbr.org/2021/09/the-digital-economy-runs-on-open-source-heres-how-to-protect-it [https://perma.cc/VYC4-FGY5].

276 *See* Brock, *supra* note 275.

unintentionally threaten the open-source community or inadvertently chill open-source development activity, regulators and lawmakers should carefully consider whether the marginal regulatory enforcement benefit is worth the cost.

Concerning privacy, the reality is that transactions on a permissionless blockchain protocol may be pseudonymous, but they remain far from private and even farther from anonymous.[277] With just a little technical sleuthing, linking pseudonymous public key addresses with real identities routinely occurs.[278] Once determined, the public nature of the blockchain protocol makes a person's entire financial transaction history via the protocol knowable to the public.[279] In recognition of this fact, the Fifth Circuit recently ruled that no expectation of privacy exists for users of permissionless public blockchains who take no additional action to privacy-protect their transactions.[280] Moreover, scholars have long examined the potential incompatibility of blockchain protocols and compliance with strict privacy regulations in the European Union.[281]

To overcome this drawback of blockchain protocols, open-source software developers built new privacy-enhancing technologies—including decentralized exchanges like Ooki,[282] decentralized mixers like Tornado Cash,[283] privacy-enhancing noncustodial wallets,[284] privacy pools,[285] and

---

277 *See* Chow, *supra* note 269.

278 *See id.* ("Investigators or eagle-eyed sleuths can then use this public information to follow money flows and learn about a person or company's financial activity.").

279 *See id.*

280 *See* United States v. Gratkowski, 964 F.3d 307, 310–12 (5th Cir. 2020); Mark Rasmussen & Margaret I. Lyle, *No Search Warrant Required for Records of Bitcoin Transactions, the Fifth Circuit Holds*, Jones Day: Insights (July 2020), https://www.jonesday.com/en/insights/2020/07/no-search-warrant-required-for-records-of-bitcoin-transactions-the-fifth-circuit-holds [https://perma.cc/Z9ES-BV6V] ("The Fifth Circuit ruled that no search warrant is required to obtain records of Bitcoin transactions under the well-established doctrine that 'a person generally has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'").

281 *See generally* Michèle Finck, Blockchain Regulation and Governance in Europe (2019); Michèle Finck, *Blockchains and Data Protection in the European Union*, 4 Eur. Data Prot. L. Rev. 17 (2018); Michèle Finck, *Smart Contracts as a Form of Solely Automated Processing Under the GDPR*, 9 Int'l Data Priv. L. 78 (2019); Noah Walters, *Privacy Law Issues in Blockchains: An Analysis of PIPEDA, the GDPR, and Proposals for Compliance*, 17 Canadian J.L. & Tech. 276 (2019); W. Gregory Voss, *Data Protection Issues for Smart Contracts*, *in* Smart Contracts: Technological, Business and Legal Perspectives 79 (Marcelo Corrales Compagnucci et al. eds., 2021).

282 *See supra* notes 208–13 and accompanying text.

283 *See generally* Nadler & Schär, *supra* note 240, at 122.

284 *See* Ian Allison, *Self-Hosted Bitcoin Wallets Become Front Line in Fight Over Crypto Regulations*, CoinDesk (Apr. 9, 2024, 10:38 PM), https://www.coindesk.com/policy/2020/12/18/self-hosted-bitcoin-wallets-become-front-line-in-fight-over-crypto-regulations/ [https://perma.cc/QPF9-XTU8].

285 *See generally* Buterin et al., *supra* note 70 (discussing other types of privacy-preserving cryptocurrencies).

other privacy-by-design cryptocurrencies,[286] among others.[287] Many view the increased targeting of such privacy-enhancing tools with exceptional skepticism and decry the apparent attempts to recentralize activity in the blockchain ecosystem.[288] Indeed, many view regulatory and lawmaker activity to eliminate decentralized applications of blockchain technology as part of a long history of government overreach attempting to limit privacy enhancing technologies for the digital era.[289] A digital era, in which everything can be traced[290] and monetized,[291] calls for technology that enables individuals with the autonomy to choose financial privacy.

Some view regulatory and lawmaker overreach as encroachment upon constitutionally protected rights of free speech. The Supreme Court has determined that some computer programs constitute protected speech.[292] Although debate exists as to what characteristics lift certain computer software to the level of protected speech but not others,[293] some commentators argue that the computer code that powers

---

286 *See* Andrea O'Sullivan, *What Are Mixers and "Privacy Coins"?*, Coin Ctr. (July 7, 2020), https://www.coincenter.org/education/advanced-topics/what-are-mixers-and-privacy-coins/ [https://perma.cc/SM85-5UMY].

287 *See, e.g.*, Fabrice Benhamouda, Shai Halevi & Tzipora Halevi, *Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation*, 63 IBM J. Rsch. & Dev. 1 (2019) (discussing secure multiparty computation as a privacy-enhancing technology); OpenDime, https://opendime.com/ [https://perma.cc/G7GX-AR7D] (offering a hardware wallet optimized for secure in-person cryptocurrency transactions).

288 *See* Van Valkenburgh, *supra* note 77, at 8; Brito, *supra* note 77, at 12–13.

289 *See, e.g.*, Bourque, *supra* note 201 ("The present attack on privacy-enhancing technologies is not a new phenomenon, but rather a continuation of the U.S. government's decades-long effort to limit and criminalize the use and distribution of such technologies by its citizens. This campaign, commonly known as the 'Crypto Wars,' involved unsuccessful government attempts to constrain technologies facilitating privacy in personal communications." (quoting Daniel Oberhaus, *How the Government is Waging Crypto War 2.0*, Vice (Aug. 10, 2016, 11:40 AM), https://www.vice.com/en/article/jpgvy3/encryption-debate-the-end-of-end-to-end [https://perma.cc/QAT4-C4WM])); *see also* Steven Levy, *Why Are We Fighting the Crypto Wars Again?*, Wired (Mar. 11, 2016, 12:00 AM), https://www.wired.com/2016/03/why-are-we-fighting-the-crypto-wars-again/ [https://perma.cc/9D6V-V7YP] (placing the "iPhone Crisis" in the timeline of the Crypto War, and demonstrating the on-going battle for privacy in the digital age).

290 Kashmir Hill, *The House That Spied on Me*, Gizmodo (Feb. 7, 2018), https://gizmodo.com/the-house-that-spied-on-me-1822429852 [https://perma.cc/28WE-NQYE] (describing invasive digital tracing in the form of a "smart home").

291 *See generally* Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (2019) (discussing the rise of "surveillance capitalism" in the digital age).

292 Van Valkenburgh, *supra* note 77, at 37 (citing Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 788 (2011); Sorrell v. IMS Health Inc., 564 U.S. 552 (2011)).

293 *See, e.g.*, Andrew Tutt, *Software Speech*, 65 Stan. L. Rev. Online 73, 77 (2012) (discussing whether software is a means to convey ideas or to gather, manipulate, and convey data in a manner similar to speech).

cryptocurrency and decentralized exchange systems should constitute protected speech.[294] Indeed, at least one commentator expects regulations that interfere with such protected speech to be subject to strict scrutiny review.[295] In its amicus brief in the *Van Loon* case, the Electronic Frontier Foundation argued that OFAC's designation of Tornado Cash software violated the First Amendment.[296] Ultimately, irrespective of whether constitutional challenges to cryptocurrency-related regulatory interventions succeed or not, the mere widespread belief that such regulatory action violates the constitutional rights of the open source software community will undermine the legitimacy of the law in this arena and the institutions that promulgate it.

Although traditionally, the blockchain technology community believes in participation in the democratic process as a way to educate lawmakers and policymakers about the technology, its development processes, and its myriad uses,[297] policy debates increasingly exhibit discouraging characteristics of political polarization.[298] All too often, in the midst of such polarization, those governed by the laws made on Capitol Hill and in State capitals feel unheard and disenfranchised.[299] Evidence of this sentiment amongst members of the blockchain technology

---

294 *See, e.g.*, VAN VALKENBURGH, *supra* note 77, at 38–39 (arguing that cryptocurrency and decentralized exchange systems are "heavily laden with facts that advance human knowledge and allow us to conduct human affairs" and therefore meet the Supreme Court's standard for protected speech); Universal City Studios, Inc. v. Corley, 273 F.3d 429, 445 (2d Cir. 2001) ("Communication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code. Mathematical formulae and musical scores are written in 'code,' *i.e.*, symbolic notations not comprehensible to the uninitiated, and yet both are covered by the First Amendment."); Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000) ("Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment.").

295 *See, e.g.*, VAN VALKENBURGH, *supra* note 77, at 45, 47.

296 Brief for Electronic Frontier Foundation as Amicus Curiae Supporting Plaintiffs at 7–14, Van Loon v. Dep't of the Treasury, 688 F. Supp. 3d 454 (W.D. Tex. 2023, May 8, 2023) (No. 1:23-cv-00312).

297 For example, the DeFi Education Fund was created to explain DeFi to policymakers and lawmakers. *DeFi Education Fund CEO Slams U.S. Treasury's "Confusing and Self-Refuting" Draft Regulations on Crypto*, CRYPTOGLOBE (Aug. 26, 2023), https://www.cryptoglobe.com/latest/2023/08/defi-education-fund-ceo-slams-u-s-treasurys-confusing-and-self-refuting-draft-regulations-on-crypto/ [https://perma.cc/R2V8-JF7R].

298 Zachary Warmbrodt, *Elizabeth Warren Is Building an Anti-Crypto Army. Some Conservatives Are on Board*, POLITICO (Feb. 14, 2023, 4:30 AM), https://www.politico.com/news/2023/02/14/elizabeth-warren-anti-crypto-ftx-00082624 [https://perma.cc/5SY6-QUKF]; Emily Crane, *Ted Cruz Says Senate Can't Regulate Crypto Without Knowing 'What in the Hell' It Is*, N.Y. POST (Aug. 10, 2021, 12:16 PM), https://nypost.com/2021/08/10/ted-cruz-says-senate-will-harm-cryptocurrency-industry-with-regulations/ [https://perma.cc/5K6W-2NXW].

299 *See, e.g.*, Pamela Foohey & Christopher K. Odinet, *Silencing Litigation Through Bankruptcy*, 109 VA. L. REV. 1261, 1262 (2023); Charlotte S. Alexander & Nicole G. Iannarone, *Winning, Defined? Text-Mining Arbitration Decisions*, 42 CARDOZO L. REV. 1695, 1698 (2021); Pamela Foohey, *Access to Consumer Bankruptcy*, 34 EMORY BANKR. DEVS. J. 341, 341 (2018); Pamela Foohey, Robert

community can be found amidst "most influential" people lists that name SEC Commissioners[300] and in the community's public statements related to ongoing litigation against regulatory agencies, which allege overreach and demand formal rulemaking processes that allow for public notice and comment.[301] In other words, many view the government threats to the open source development process, privacy, and free speech as evidence of the decaying legitimacy of lawmaking institutions and regulatory agencies. Unfortunately, the lawmaking process—the point at which public input can be incorporated—does nothing to increase constituent satisfaction or institutional legitimacy. Rather, like the regulations they craft, Congress and state legislatures rely on layers upon layers of intermediaries to make policy and draft new legal rules. Perhaps previously thought to be the only way to get things done, political polarization on nearly every issue suggests that the current lawmaking process no longer works well. At this point, blockchain technology is no longer functioning as a magic mirror merely for the substance of law but also for the lawmaking process itself—highlighting deep and long-engrained flaws in the creation and enforcement of regulation that overly rely upon intermediaries to law's greater detriment.

Conclusion

The ongoing crypto-intermediary controversy acts as a mirror that reflects a poorly functioning regulatory system. Regulators and lawmakers often repeat the refrain "same activities, same risk, same rules" or "same activities, same risks, same regulatory outcome[s]" to justify their approach to enforcement in the cryptocurrency and blockchain technology industry without new rulemaking.[302] Commentators have lamented this approach as failing to internalize key differences in certain decentralized activities enabled by blockchain technology.[303] Yet this phrase reflects a time-tested methodology—the functional method, even if not labeled as such. And in another context altogether, private law reform and harmonization efforts prove that an activities-based

M. Lawless, Katherine Porter & Deborah Thorne, *"No Money Down" Bankruptcy*, 90 S. Cal. L. Rev. 1055, 1057 (2017).

300 *CoinDesk's Most Influential 2023*, CoinDesk (Nov. 30, 2023, 1:29 PM), https://www.coindesk.com/most-influential-2023/ [https://perma.cc/3T6Q-2AY6].

301 *See, e.g.*, Sam Reynolds, *U.S. Court Tells SEC to Respond to Coinbase's Rulemaking Petition Within a Week*, CoinDesk (June 7, 2023, 3:34 PM), https://www.coindesk.com/policy/2023/06/07/us-court-tells-sec-to-respond-to-coinbases-rulemaking-petition-within-a-week/ [https://perma.cc/9RFQ-B2Y2].

302 Hess, *supra* note 43, at 394.

303 *Id.*

legal approach can succeed as a basis for workable legal rules applicable to cryptocurrency and blockchain technology.[304]

The difference between the two efforts? The private law reform and harmonization approach employs the functional method well; the feat is possible, at least in part, by the way that private law reform and harmonization projects unfold—through a distributed process that relies on input from a variety of viewpoints, including technical experts and industry representatives. Perhaps the regulatory gaps caused by an unrelenting insistence on centralization and intermediation can be closed and further harms avoided if regulators and lawmakers took a page from their private law counterparts and their processes used to develop recommended reforms and harmonization products.

To truly learn the lessons reflected in blockchain technology's magic mirror for regulation, further research should explore the potential for state and federal legislatures to better adhere to their stated goal of functional regulation. At present, state and federal legislators and regulators fail to achieve their stated goal of "same activities, same risk, same rules" because they only badly approximate the functional method. Indeed, an actual method exists,[305] and the intermediated process of public law making does not provide the time or incentives to employ that method. Instead, the functional mantra "same activity, same risks, same rules" becomes a lightning rod for finding an intermediary even if one does not exist, making it impossible to adopt workable rules and heightening rather than diminishing negative externalities.

Ultimately, this Article examines the recent history of cryptocurrency-intermediary failures and uses them to debunk common policy refrains seeking to justify regulatory action that targets intermediaries to the exclusion of all other options. The Article argues that instead of revealing deep flaws in blockchain technology, the recent regulatory turmoil reflects an improperly functioning financial regulatory regime more broadly. Ultimately, if law and regulation fail to course correct, government insistence on infinite financial intermediation and related regulation will threaten the legitimacy of the law and lawmaking institutions. Law's detrimental reliance on intermediaries not only results in poorly functioning rules but also in distrust of and reduced esteem for legal and lawmaking institutions.

---

304 *See* Carla L. Reyes, *Emerging Technology's Unfamiliarity with Commercial Law*, 119 Nw. U. L. Rev. Online 31, 31 (2024) (discussing the collaborative "project to revise the Uniform Commercial Code (UCC) to account for the impact of emerging technologies on commercial transactions" and, in particular, the inclusion of a separate asset class for cryptocurrency).

305 Reyes, *supra* note 23, at 415–21.