european corporate governance institute

Regulating DeFi Platforms

Law Working Paper N° 937/2026
Revised November 2026

Gina-Gail S. Fletcher
Duke University School of Law and ECGI
Veronica Root Martinez
Duke University School of Law and ECGI
Steven L. Schwarcz
Duke University School of Law

© Gina-Gail S. Fletcher, Veronica Root Martinez and Steven L. Schwarcz 2026. All rights reserved. Short sections of text, not to exceed two paragraphs, may be quoted without explicit permission provided that full credit, including © notice, is given to the source.

This paper can be downloaded without charge from:
https://doi.org/10.67929/ecgi-law-937-2026

european corporate governance institute

ECGI Working Paper Series in Law

Regulating DeFi Platforms

Working Paper N° 937/2026
November 2026

Gina-Gail S. Fletcher
Veronica Root Martinez
Steven L. Schwarcz

© Gina-Gail S. Fletcher, Veronica Root Martinez and Steven L. Schwarcz 2026. All rights reserved. Short sections of text, not to exceed two paragraphs, may be quoted without explicit permission provided that full credit, including © notice, is given to the source.

Abstract

Traditional financial systems rely on a dense network of intermediaries - banks, brokers, exchanges, and clearinghouses - that not only facilitate transactions but also serve as compliance gatekeepers. These intermediaries protect the financial markets by implementing capital adequacy rules; disclosure requirements; and anti-money laundering and know-your-customer protocols. In doing so, these intermediaries constrain opportunism by actors within the financial markets, enable protocols that ensure reliable recordkeeping, and facilitate the information sources regulators need to monitor systemic risk. Decentralized finance (DeFi) disrupts this model by replacing traditional intermediaries with smart contracts: self-executing digital agreements that automatically perform transactions on blockchain or other encrypted computer code. While proponents tout DeFi as a more efficient and "purer" form of finance, its disintermediation eliminates the purposeful choke-points that historically enabled the oversight necessary to ensure the legitimacy of financial transactions, as well as to protect consumers from potential harms. This disintermediation creates opportunities for DeFi to magnify classic types of market and financial risks; risks that are quite similar to those that fueled the Great Depression and the 2008 Global Financial Crisis. DeFi is novel in that it layers upon those traditional risks a range of new vulnerabilities tied to new uses of computer code and cross-border anonymity. This Article argues that DeFi platforms' disaggregation of traditional intermediary functions requires the adoption of regulatory requirements that focus on (1) embedding compliance safeguards directly into platform design and (2) holding accountable the actors who build, operate, and maintain those platforms. Policymakers should prioritize the development of regulations that require DeFi platforms to incorporate technological and governance tools that replicate the critical compliance and risk-management functions historically supplied by intermediaries. The development of more robust safeguards is essential to preserve market integrity, mitigate systemic risk, and protect investors. Constructing such a regulatory regime will require substantial multijurisdictional coordination, both in harmonizing regulatory expectations and in building cross-border enforcement capacity. Fortunately, a range of existing international coordination mechanisms can be leveraged to facilitate this effort. DeFi - like many types of financial innovation - has both benefits and costs; it is time for governmental actors to constrain those costs through formal interventions.

Keywords: Decentralized Finance, DeFi Regulation, Smart Contracts, Financial Intermediaries, Compliance, Enforcement, Anti-money laundering, Investor Protection, Systemic Risk, Multijurisdictional Enforcement

Gina-Gail S. Fletcher

Duke University School of Law and ECGI

Veronica Root Martinez

Duke University School of Law and ECGI
ORCID 0009-0001-4592-6283

Steven L. Schwarcz

Duke University School of Law

Regulating DeFi Platforms

Gina-Gail S. Fletcher,† Veronica Root Martinez,†† and Steven L. Schwarcz†††

ABSTRACT

Traditional financial systems rely on a dense network of intermediaries—banks, brokers, exchanges, and clearinghouses—that not only facilitate transactions but also serve as compliance gatekeepers. These intermediaries protect the financial markets by implementing capital adequacy rules; disclosure requirements; and anti-money laundering and know-your-customer protocols. In doing so, these intermediaries constrain opportunism by actors within the financial markets, enable protocols that ensure reliable recordkeeping, and facilitate the information sources regulators need to monitor systemic risk.

Decentralized finance (DeFi) disrupts this model by replacing traditional intermediaries with smart contracts: self-executing digital agreements that automatically perform transactions on blockchain or other encrypted computer code. While proponents tout DeFi as a more efficient and "purer" form of finance, its disintermediation eliminates the purposeful chokepoints that historically enabled the oversight necessary to ensure the legitimacy of financial transactions, as well as to protect consumers from potential harms. This disintermediation creates opportunities for DeFi to magnify classic types of market and financial risks; risks that are quite similar to those that fueled the Great Depression and the 2008 Global Financial Crisis. DeFi is novel in that it layers upon those traditional risks a range of new vulnerabilities tied to new uses of computer code and cross-border anonymity.

This Article argues that DeFi platforms' disaggregation of traditional intermediary functions requires the adoption of regulatory requirements that focus on (1) embedding compliance safeguards directly into platform design and (2) holding accountable the actors who build, operate, and maintain those platforms. Policymakers should prioritize the development

† Professor of Law, Associate Dean for Intellectual Life, Duke University School of Law. Research Member, the European Corporate Governance Institute.

†† Simpson Thacher & Bartlett Distinguished Professor of Law, Duke University School of Law. Affiliate Faculty, Duke University Fuqua School of Business. Research Member, the European Corporate Governance Institute.

††† Stanley A. Star Distinguished Professor of Law & Business, Duke University School of Law. Senior Fellow, the Centre for International Governance Innovation.

We are grateful for comments from Ilya Beylin, Vanessa Villanueva Collao, Patrick Corrigan, Carole House, Kristin Johnson, Carla Reyes, Dirk A. Zetzsche, and participants in the 2026 Compliance Leadership Forum at Duke Law School. We benefited from research assistance from Emma Cline, Nick Hogan, Arianne Levine, Skylar McVicar, Isabelle Stewart, Jack Tiedemann, and Julie You.

of regulations that require DeFi platforms to incorporate technological and governance tools that replicate the critical compliance and risk-management functions historically supplied by intermediaries. The development of more robust safeguards is essential to preserve market integrity, mitigate systemic risk, and protect investors. Constructing such a regulatory regime will require substantial multijurisdictional coordination, both in harmonizing regulatory expectations and in building cross-border enforcement capacity. Fortunately, a range of existing international coordination mechanisms can be leveraged to facilitate this effort. DeFi—like many types of financial innovation—has both benefits and costs; it is time for governmental actors to constrain those costs through formal interventions.

TABLE OF CONTENTS

Introduction 2
I. The Rise of DeFi 12
A. Traditional Finance & Regulation Through Intermediaries.12
B. What Is DeFi? 15
C. The Benefits of DeFi 19
II. The Risk Architecture of Decentralized Finance 22
A. Traditional Risks. 22
B. New Risks 33
C. Overview of Regulatory Challenges 40
III. Targeted Compliance & Enforcement for DeFi Platforms 51
A. Ex Ante Architectural Constraints 52
B. Small vs. Large Firm Architecture 57
C. Ex Post Enforcement & Multijurisdictional Accountability62
IV. Additional Questions & Concerns 67
A. DeFi—A Public Good? 68
B. Collective Action and Public-Private Partnerships ... 70
C. Administrative Feasibility and Capacity Constraints 71
Conclusion 72
Appendix 73

INTRODUCTION

In February 2023, the Department of Justice indicted the founders of Forsage, a purported decentralized finance (DeFi) investment platform, for operating what prosecutors described as a $340 million "global Ponzi and pyramid scheme" that defrauded retail investors through self-executing smart contracts

on the Ethereum, Binance Smart Chain, and Tron blockchains.[1] Forsage's founders allegedly promised investors outsized returns "with zero risk."[2] But, in reality, participant funds were partly siphoned off to the company's founders and otherwise recycled to pay earlier investors.[3] The scheme succeeded precisely because of the technological opacity and legal fragmentation that characterize what has come to be known as DeFi. DeFi refers to financial products and services that use public, permissionless, decentralized technology to facilitate payments,[4] trading, lending, and other financial services[5] without the involvement of traditional financial intermediaries.[6]

1. Press Release, U.S. Dep't of Just., Forsage Founders Indicted in $340M DeFi Crypto Scheme (Feb. 22, 2023), https://www.justice.gov/archives/opa/pr/forsage-founders-indicted-340m-defi-crypto-scheme [https://perma.cc/BD5F-88CK].

2. *Id.*

3. *Id.*

4. Digital payment systems, using cryptocurrencies evidenced by blockchain technology, provide a well-known example of FinTech. *5 FinTech Examples Transforming Everyday Life*, WAKE FOREST UNIV. SCH. OF PRO. STUD. (Dec. 16, 2025), https://sps.wfu.edu/articles/fintech-examples-transforming-everyday-life [https://perma.cc/3FF7-X2JZ].

5. *See, e.g.*, *FinTech in Finance and Analytics: Advancements and Applications*, SANTA CLARA UNIV. LEAVEY SCH. OF BUS. (Oct. 18, 2023), https://onlinedegrees.scu.edu/media/blog/applications-of-financial-technology-in-finance-and-analytics [https://perma.cc/KA4S-67XK] (reporting that "[r]ecent technological advances have streamlined and reshaped traditional financial services" such as by incorporating robo-advising in investment platforms and enabling peer-to-peer digital lending platforms for small loans).

6. *See, e.g.*, *What is Decentralized Finance (DeFi)?*, FID. INVS. (May 18, 2026), https://www.fidelity.com/learning-center/trading-investing/crypto/decentralized-finance-defined [https://perma.cc/NE8L-FQU6] ("DeFi stands for decentralized finance, which means everything from simple transfers to complex financial functions are facilitated *without any third-party involvement*." (emphasis added)); Kevin Roose, *What is DeFi?*, N.Y. TIMES (Mar. 18, 2022), https://www.nytimes.com/interactive/2022/03/18/technology/what-is-defi-cryptocurrency.html [https://perma.cc/93ZN-R5YH] (defining DeFi as "an umbrella term for the part of the crypto universe that is geared toward building a new, internet-native financial system, using blockchains to replace traditional intermediaries and trust mechanisms" and later explaining that the traditional third-party intermediaries are replaced by software). *Cf.* Vanessa Villanueva Collao, *DeFi's Premise & Promise of Decentralization and Disintermediation*, NAT'L YANG MING CHIAO YUNG U. L. REV. (forthcoming 2026) (manuscript at 7) (stating that DeFi does not eliminate intermediaries, but it merely redistributes and reconfigures intermediaries).

The Forsage prosecution illustrates how DeFi's most celebrated innovation—disintermediation, meaning the removal of the need for those traditional intermediaries—can also be its most dangerous feature, especially when DeFi platforms actually have centrally managed governance processes. DeFi replaces traditional intermediaries with self-executing computer programs known as smart contracts.[7] These programs automatically execute algorithms on blockchain technology or other encrypted computer code that enables users to trade, lend, or borrow without relying on a centralized exchange or custodian.[8] Although banks and other financial intermediaries traditionally "have been the key nodes in the financial system that control the accuracy of customer accounts, perform bookkeeping functions, and ensure that unauthorized persons do not have access to an account,"[9] smart contracts arguably could perform those functions[10]—such as enabling investors and other parties to directly access financial services, including securities trading and borrowing.[11]

7. Ana Daily, Matthew Hanson & Thomas Spiegler, *Decentralized Finance—Risks, Regulation, and the Road Ahead,* KING & SPALDING (Sep. 1, 2021), https://www.jdsupra.com/legalnews/decentralized-finance-risks-regulation-9351911 [https://perma.cc/2L2B-L823].

8. David Gogel, *DeFi Beyond the Hype*, WHARTON BLOCKCHAIN & DIGIT. ASSET PROJECT 2 (May 2021), https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf [https://perma.cc/AFX8-VPFS]. *See, e.g.*, *id.* (arguing that financial intermediaries can create "inefficiencies, structural inequalities, and hidden risks"); *Illicit Finance Risk Assessment of Decentralized Finance*, U.S. DEP'T OF THE TREASURY 15 (Apr. 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf [https://perma.cc/4R42-W7XG] [hereinafter *Illicit Finance*] (noting that DeFi transactions, especially those that are blockchain-based, could speed up settlement and be more cost efficient).

9. Igor Makarov & Antoinette Schoar, *Cryptocurrencies and Decentralized Finance (DeFi)*, BROOKINGS PAPERS ON ECON. ACTIVITY 141, 145 (2022), https://www.brookings.edu/wp-content/uploads/2022/03/16265-BPEA-Sp22_MakarovSchoar_WEB-Appendix.pdf [https://perma.cc/Y3B9-33VJ].

10. *See, e.g.*, *What Are Smart Contracts on Blockchain?*, IBM, https://www.ibm.com/topics/smart-contracts [https://perma.cc/D5VU-YNTB] ("Smart contracts are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss.").

11. *See* Stuart D. Levi & Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, HARV. L. SCH. F. ON CORP. GOVERNANCE (May 26, 2018), https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations [https://perma.cc/L5MB-PA85] (stating that smart contracts also could "(1) ensur[e] the payment of funds upon certain triggering events and (2) impos[e] financial penalties if certain objective conditions are not satisfied").

In principle, disintermediation can reduce transaction costs and broaden market access, thereby expanding financial inclusion [12] and advancing FinTech's[13] oft-touted "democratization of the financial system."[14] The removal of intermediaries, however, also removes many of the internal controls—including recordkeeping requirements and anti-money laundering (AML) and know-your-customer (KYC) conventions—that firms have incorporated into their compliance systems as a core part of the financial regulatory framework.[15] Eliminating traditional intermediaries can create anonymity—at

12. *See, e.g.*, Carter Faust, Anthony Dukes & D. Daniel Sokol, *Fintech and Financial Inclusion: A Review of the Empirical Literature*, 95 S. CAL. L. REV. POSTSCRIPT 136, 136 (2022). In relevant part, those authors highlight the "important role that fintech can play in promoting *financial inclusion*—the availability and equality of opportunities to access financial services." *Id.* In the developing world, for example, "1.7 billion adults . . . are unbanked, meaning they lack an account with a financial institution or mobile money provider . . . ." *Id.* Access to financial services, however, "is a key enabler for financial inclusion and, on a broader scale, reducing worldwide poverty." *Id.*

13. FinTech generally refers to the use of technology to facilitate financial innovations. *See Fintech and How New Technologies Are Changing Finance*, AM. UNIV. OF ROME (Sep. 21, 2023), https://aur.edu/events/fintech-and-how
-new-technologies-are-changing-finance [https://perma.cc/T4B7-ZFZA] (stating that FinTech "is a catch-all term referring to software, mobile applications, and other technologies created to improve and automate traditional forms of finance"). Not being officially defined, the term FinTech is imprecise; it can also refer to financial innovations that are facilitated by technology. *See* Julia Kagan, *Understanding Fintech: Enhancing Financial Services and Everyday Life*, INVESTOPEDIA (May 23, 2026), https://www.investopedia.com/terms/f/fintech.asp [https://perma.cc/79PB-BU5W] ("Broadly, the term 'financial technology' can apply to any innovation in how people transact business, from the invention of digital money to double-entry bookkeeping."); *Fintech and the Future of Finance*, WORLD BANK GRP., https://www.worldbank.org/en/publication/fintech
-and-the-future-of-finance [https://perma.cc/NNT6-HZXD] ("Fintech [refers to] the application of digital technology to financial services . . . .").

14. Joe McKendrick, *The Coming Democratization of Financial Services, Thanks to Artificial Intelligence*, FORBES (Jan. 14, 2023), https://www.forbes.com/sites/joemckendrick/2023/01/14/the-coming-democratization-of-financial
-services-thanks-to-ai [https://perma.cc/2FUJ-UEKD] (interviewing FinTech venture capitalist Spiros Margaris on how FinTech is transforming the financial industry). *See also* Steven L. Schwarcz & Robert Bourret, *Fractionalizing Investment Securities: Using FinTech to Expand Financial Inclusion*, 84 OHIO ST. L.J. 773, 789–91 (2024) (examining how FinTech has led to the development of fractionalization which greatly expands financial inclusion by creating affordable securities).

15. *See* Karen H.Y. Man, *Fintech and Financial Stability—Weighing the Interconnected Risks Technology Poses to Financial Systems*, GLOB. COMPLIANCE NEWS (Apr. 17, 2024) https://www.globalcompliancenews.com/
2024/04/17/https-www-bakermckenzie-com-en-insight-publications-resources

worst—or confusion—at best—over who should be regulated, creating a compliance conundrum.[16] It also can obscure the identity of the counterparties to financial transactions, preventing them from mutually resolving disagreements. Additionally, it encourages the shifting of financing away from regulated banks to unregulated funding sources.[17]

The DeFi platform Forsage exemplifies the structural conditions that can enable fraud to flourish. Forsage was a permissionless platform, meaning that anyone could invest in it even though its smart contracts were not subject to gatekeeping, audit, or compliance review.[18] Notwithstanding the open-source code on which Forsage operated, investors were unaware that Forsage's smart contracts were programmed to follow the fraudulent payout logic of a classic Ponzi scheme.[19] Without the oversight and monitoring of a centralized intermediary authorized to and capable of halting suspicious activity or conducting customer verification, Forsage's platform diverted funds from later investors to pay earlier participants and siphoned a portion of the funds into the pockets of Forsage's founders.[20] Additionally, despite not having a qualified

-fintech-and-financial-stability_042024 [https://perma.cc/DV48-39TB] ("For all the benefits that fintech has brought to consumers, businesses and societies, it has also introduced new sources of vulnerability to financial systems, raising questions about the latter's fragility."); Saule T. Omarova, *New Tech v. New Deal: Fintech as a Systemic Phenomenon*, 36 YALE J. ON REGUL. 735, 742 (2019) ("[R]ecent advances in computing power, cryptography, data analytics, and machine learning appear poised to amplify the long-lasting, systemically destabilizing trends in the financial markets.").

16. *See, e.g.*, Ian Talley, *Decentralized Cryptocurrency Markets Threaten U.S. Security, Treasury Says*, WALL ST. J. (Apr. 6, 2023), https://www.wsj.com/articles/decentralized-cryptocurrency-markets-threaten-u-s-national-security-treasury-says-d9dd324f [https://perma.cc/F8ET-C4VB] (reporting that the U.S. Department of the Treasury is concerned that DeFi platforms can enable cryptocurrency investors to "transact with each other through software running online, without a central intermediary overseeing transactions," thereby depriving regulators of insight into the transactions).

17. This shift is similar to, but different than, that of shadow banking. Both DeFi and shadow banking shift traditional banking functions towards unregulated non-bank entities. But whereas shadow banking turns towards hedge funds and structured investment vehicles, DeFi relies on the technology itself, rather than other financial institutions, to replicate credit creation and liquidity transformations outside of the banking system. *Cf. infra* Part II.A.3 (discussing parallels between shadow banking and DeFi).

18. *See* Amber Seira et al., *Governance of Permissionless Blockchain Networks*, FEDS NOTES (Feb. 9, 2024), https://www.federalreserve.gov/econres/notes/feds-notes/governance-of-permissionless-blockchain-networks-20240209.html [https://perma.cc/LNV5-3S44] (defining "permissionless blockchain network").

19. U.S. Dep't of Just., *supra* note 1.

20. *See supra* notes 1–6 and accompanying text.

intermediary, Forsage was not a true self-executing DeFi platform, as its founders colluded to tamper with the smart contracts, thereby misleading investors into thinking Forsage was decentralized when it had centralized components.[21] Moreover, DeFi firms and systems lack the embedded compliance safeguards traditionally supplied by financial intermediaries. As regulators have repeatedly emphasized,[22] DeFi transactions can generate severe information asymmetries, which may deprive investors of visibility into how funds move through the DeFi system and prevent regulators from deploying traditional monitoring and surveillance tools. In Forsage's case, hundreds of millions of dollars flowed through smart contracts without any mechanism to alert unsuspecting investors to the scheme's inherently unsustainable and unlawful structure.[23]

The upshot is that today's DeFi platforms exist in an ecosystem prone to anonymity, regulatory arbitrage, and jurisdictional evasion. These conditions allow fraudulent schemes like Forsage to flourish and, according to the U.S. Treasury, can potentially threaten national security by facilitating the financing of rogue states and other illicit actors.[24]

The contrast with traditional FinTech intermediaries is striking. Consider Robinhood Markets, Inc., a retail trading platform that, despite its digital veneer, remains a registered broker-dealer subject to the jurisdiction of the Financial Industry Regulatory Authority (FINRA) and the Securities and Exchange Commission (SEC).[25] In January 2025, the SEC sanctioned Robinhood for failing to "observe a broad array of significant regulatory requirements,

21. The Department of Justice refers to Forsage as "a purportedly decentralized finance (DeFi) cryptocurrency investment platform," U.S. Dep't of Just., *supra* note 1, but one could argue that it was not a DeFi company at all due to its centralized components. While this distinction matters, for purposes of this Article, the designation by enforcement authorities, the company, and the public of the firm as a DeFi firm helps to elucidate the challenges associated with applying standard regulatory requirements to emerging FinTech platforms.

22. *See, e.g.*, Caroline A. Crenshaw, *Statement on DeFi Risks, Regulations, and Opportunities*, U.S. SEC. & EXCH. COMM'N (Nov. 9, 2021), https://www.sec.gov/newsroom/speeches-statements/crenshaw-defi-20211109 [https://perma.cc/BSA8-DTL3] (discussing the information gap between retail investors and professional investors in DeFi transactions); *Illicit Finance*, *supra* note 8, at 29 (describing potential limits to the "collection of and access to information critical to supporting financial investigations").

23. *See* U.S. Dep't of Just., *supra* note 1.

24. *See, e.g.*, Talley, *supra* note 16 (reporting that the U.S. Department of the Treasury is also concerned that DeFi platforms can enable rogue states and other bad actors to "move money around the world without detection, facilitating the financing critical to their operations").

25. *About Us*, ROBINHOOD, https://robinhood.com/us/en/about-us [https://perma.cc/N7WG-8GJK].

including failing to accurately report trading activity, comply with short sale rules, submit timely suspicious activity reports, maintain books and records, and safeguard customer information."[26] Two months later, in March 2025, FINRA resolved claims with Robinhood for alleged supervisory failures which led to a failure to appropriately "respond to 'red flags' of potential misconduct."[27] Robinhood agreed to pay almost $30 million in penalties to FINRA and certified that it remediated the issues identified, including overhauling its internal controls and customer-support infrastructure.[28] When Robinhood allegedly violated their obligation to engage in certain supervisory and customer-protection activities, regulators were able to identify the responsible entity, investigate the misconduct, and impose meaningful sanctions.[29] Intermediation, though costly, can promote external accountability and ensure firms promote a strong compliance culture.

For example, DeFi platforms often distribute—or diffuse—governance responsibility across pseudonymous (that is, falsely named) developers, decentralized autonomous organizations (sometimes called DAOs), and token holders.[30] As former Commodity Futures Trading Commission (CFTC) Commissioner Kristin N. Johnson has emphasized, this "largely unregulated" structure deprives regulators of "foundational" safeguards such as the ability to review and monitor firms' customer identification programs, internal controls, and

26. Press Release, *Two Robinhood Broker-Dealers to Pay $45 Million in Combined Penalties for Violating More Than 10 Separate Securities Law Provisions*, U.S. SEC. & EXCH. COMM'N (Jan. 13, 2025), https://www.sec.gov/newsroom/press-releases/2025-5 [https://perma.cc/UP43-PBGM].

27. Jonathan Stempel, *Robinhood Paying $29.75 Million to End Financial Industry Regulatory Authority Probes*, USA TODAY (Mar. 7, 2025), https://www.usatoday.com/story/money/business/2025/03/07/robinhood-paying-fira/82012940007 [https://perma.cc/6AJV-SP2M].

28. *Id.*

29. Registered intermediaries like broker-dealers operate within a regulatory framework that allows misconduct to be traced to identifiable entities and individuals, provides restitution opportunities for injured customers, and subjects repeat offenders to escalating sets of sanctions—all features that decentralized systems have yet to replicate. *See Broker-Dealers*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/resources-small-businesses/capital-raising-building-blocks/broker-dealers [https://perma.cc/ZN4Q-WHV2] (defining broker-dealers and stating that those broker-dealers who fail to register "could be subject to legal repercussions").

30. Aina Turillazzi et al., Decentralised Finance (DeFi): A Critical Review of Related Risks and Regulation 6–7 (Oct. 5, 2023) (unpublished manuscript), https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4593242_code4303184.pdf [https://perma.cc/4KSN-73PZ].

conflict-of-interest mechanisms.[31] Importantly, recent enforcement actions confirm that even when DeFi platforms replicate traditional derivatives trading or lending, they often do so outside the regulatory and compliance frameworks that govern traditional financial intermediaries.[32]

This Article situates these developments within the broader evolution of financial technology with a particular focus on the platforms, like Forsage, that facilitate and exploit DeFi transactions. Advances in finance increasingly depend on FinTech, and DeFi represents FinTech's most radical extension: a financial ecosystem that purports to operate without traditional institutional intermediaries or human involvement.[33] While proponents claim that DeFi replaces potentially unreliable human discretion with "immutable code,"[34] thereby reducing the possibility of error, the absence of institutional oversight also eliminates the very mechanisms through which legal and regulatory requirements and industry standards are enforced. As a result, disintermediation in DeFi both enables innovation and magnifies risk.

At core, DeFi extends the FinTech revolution into financial innovations that redefine (or remove) who performs the critical gatekeeping, compliance, and risk-management functions that have historically served to stabilize financial markets. DeFi eliminates the ability to identify the actors who, in traditional markets, serve as the focal points of regulation and supervision. It also facilitates financial transactions through computer code rather than via accountable humans expected to exercise informed judgment. This shift raises a

31. Kristin N. Johnson, *Statement of Commissioner Kristin N. Johnson Regarding CFTC Resolving Charges Against Three Decentralized Finance Companies: The Need for Oversight*, CFTC (Sep. 7, 2023), https://www.cftc.gov/PressRoom/SpeechesTestimony/johnsonstatement090723b [https://perma.cc/QHB6-VJQF].

32. *See, e.g.*, *CFTC Wins Default Judgment Against Ooki DAO*, HUNTON: BLOCKCHAIN LEGAL RES. (June 20, 2023), https://www.hunton.com/blockchain-legal-resource/cftc-wins-default-judgment-against-ooki-dao [https://perma.cc/K7X8-U3GF] (discussing CFTC's successful enforcement against Ooki DAO for violations of the Commodity Exchange Act and KYC/AML failures); Elanit Snow & Jonathan Mollod, *CFTC Wades into DeFi Enforcement Again*, PROSKAUER: BLOCKCHAIN & THE LAW (Oct. 16, 2023), https://www.blockchainandthelaw.com/2023/10/cftc-wades-into-defi-enforcement-again [https://perma.cc/FV42-LMQZ] (describing settled charges against Opyn, Inc. and Deridex, Inc. for operating unregistered trading platforms and failing to implement customer-identification programs).

33. *But see* Villanueva Collao, *supra* note 6, at 25–32 (arguing that decentralization carries a "misconception" that it means "[an] absence of intermediaries/intermediation").

34. Erik Voorhees, A Response to SBF and Principled Crypto Regulation, Money & St. (Oct. 20, 2022), https://www.moneyandstate.com/blog/response-to-sbf [https://perma.cc/LK4R-5DFL].

number of questions about how to translate long-standing regulatory objectives—such as investor protection, financial integrity, and systemic stability—into a decentralized framework that lacks clear lines of responsibility to the actors or entities behind financial transactions. In short, DeFi puts the very legitimacy and integrity of the capital markets at risk.

Recent scholarship has rightly warned against the reflexive extension of existing intermediary-based regulation to DeFi and other forms of financial innovation.[35] Scholars caution that such an approach risks chilling innovation and misclassifying open-source protocols.[36] This Article does not dispute those concerns. Instead, it addresses a distinct problem: how core compliance and risk-mitigation functions—long supplied by intermediaries—can be preserved when those intermediaries (1) no longer exist, (2) are deliberately bypassed, or (3) lack the capacity to provide effective oversight of increasingly sophisticated financial technologies.

In response, this Article argues that effective regulation of DeFi platforms must focus on (1) embedding compliance safeguards directly into platform design and (2) holding accountable the actors who build, operate, and maintain those platforms. Because of the cross-border nature of DeFi, these regulatory and enforcement efforts will require multijurisdictional coordination to be effective. This Article proceeds in four parts.

Part I examines the evolution from traditional, institution-based finance to DeFi and explains how this shift transforms both market structure and regulatory challenges. Whereas banks, broker-dealers, and other intermediaries have historically served as purposeful points of oversight over financial transactions, DeFi reassigns these functions to algorithmic code, smart contracts, and decentralized governance mechanisms. This disintermediation may lower costs and expand access to financial transactions beyond traditional sophisticated parties, but it also displaces the institutional compliance infrastructure that has historically ensured transparency, accountability, and market stability.

35. *See generally* Carla L. Reyes, *Law's Detrimental Reliance on Intermediaries*, 92 GEO. WASH. L. REV. 1343 (2024) [hereinafter Reyes, *Detrimental Reliance*] (arguing that financial regulation's dependence on centralized intermediaries obscures both the causes of recent crypto failures and the potential benefits of deeper decentralization); Carla L. Reyes & Joseph P. Cutler, *Ready Layer One: Functional Regulation for Blockchain Infrastructure*, 77 S.C. L. REV. (forthcoming 2026) (warning that applying intermediary-based financial regulation directly to open-source blockchain infrastructure risks chilling innovation and misclassifying infrastructure as enterprise); Carla L. Reyes, *(Un)Corporate Crypto-Governance*, 88 FORDHAM L. REV. 1875 (2020) [hereinafter Reyes, *(Un)Corporate*] (cautioning against premature imposition of fiduciary and corporate governance frameworks on decentralized blockchain communities).

36. *See* sources cited *supra* note 35.

Part II analyzes the set of risks that follows from moving core intermediary functions overseen by accountable human beings and institutions into computer code. First, it shows that DeFi often revives—and in some cases amplifies—classic prudential and compliance failures: AML/KYC gaps, lending that rests on a single collateral pathway rather than two independent sources of repayment, and maturity and liquidity transformation analogous to shadow banking. Second, it assesses novel technological and governance risks arising from DeFi, which include (1) potentially irreversible smart-contract bugs and exploits, (2) misconduct facilitated by participants' concealed identities, and (3) governance models that are neither fully decentralized nor adequately accountable. Third, it outlines the regulatory implications of DeFi, examining how these layered risks are resistant to current enforcement levers, complicate consumer protection, and generate acute cross-border jurisdictional problems.

Parts I and II establish the foundation for the Article's broader argument, which is outlined in Part III—that because DeFi platforms disaggregate traditional intermediary functions, effective regulation must focus on embedding compliance safeguards directly into platform design and on holding accountable the actors who build, operate, and maintain those platforms. Part III explains why effective DeFi regulation must combine ex ante architectural constraints with ex post accountability for those who design, govern, and maintain decentralized systems. It shows how embedding compliance safeguards into platform design, paired with coordinated enforcement across jurisdictions, can reconstruct the stabilizing functions historically supplied by financial intermediaries without reinstating them. Our proposal to embed compliance safeguards builds on prior suggestions for embedded supervision[37] and embedded regulation,[38] which others have put forward as a means of addressing the supervisory and regulatory challenges of DeFi. We expand these insights and develop a framework that aims to reproduce traditional compliance and risk-monitoring functions through platform safeguards embedded into DeFi platforms, registration requirements for identifiable and accountable actors within the DeFi ecosystem, and robust, multijurisdictional enforcement.

Part IV considers a set of additional questions and objections that test the boundaries of the regulatory framework advanced in this Article.

37. Raphael Auer, *Embedded Supervision: How to Build Regulation into Decentralised Finance*, CESifo Working Paper No. 9771 (2022) http://dx.doi.org/10.2139/ssrn.4127658 (proposing embedded supervision to automate monitoring of DeFi markets through the ledger).

38. Dirk A. Zetzsche, Douglas W. Arner, & Ross P. Buckley, *Decentralized Finance*, 6 J. FIN. REG. 172, 173–75 (2020) (proposing embedded regulation for DeFi through a technology-based regulatory system).

I. THE RISE OF DEFI

This Part provides the foundation for understanding how decentralized finance challenges existing regulatory regimes established to oversee traditional financial markets. It begins by explaining how modern financial systems rely upon intermediaries—banks, broker-dealers, and other gatekeepers—to reduce transaction costs, manage risk, and provide oversight functions over financial transactions. It then contrasts this intermediary-based structure with the DeFi model, which replaces intermediaries with smart-contract–driven algorithms. Finally, it examines some benefits of DeFi, including its potential to accelerate financial innovation, reduce transaction costs, and broaden market access.

A. TRADITIONAL FINANCE & REGULATION THROUGH INTERMEDIARIES

"Intermediation is a fundamental fact of [traditional] finance."[39] In traditional finance markets, intermediaries such as banks, brokers, exchanges, and pension funds all play a crucial role in the flow of capital from those who have it to those who need it.[40] To take an everyday example, consider the role of banks in facilitating lending. In theory, a company could bypass banks or other intermediaries to raise necessary capital, but the transaction costs of doing so would be higher than going through an intermediary. Banks, however, take small-dollar deposits from savers and make loans to companies in need of capital to expand, develop, or otherwise support their businesses. Here, the bank as an intermediary serves several roles. It not only aggregates capital to be able to lend large loans more efficiently to a company in need of a loan, but it also acts as an aggregator of information.[41] In its position as lender, the bank can acquire information to determine to whom it should extend loans and on what terms.[42] The bank is also able to serve as a long-term monitor of the borrower's

39. Tom C.W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643, 643 (2015) (citing Gary Gorton & Andrew Winton, *Financial Intermediation*, *in* 1 Corporate Finance 433 (George M. Constantinides et al. eds., 2003)).

40. *See* Charles K. Whitehead, *Reframing Financial Regulation*, 90 B.U. L. REV. 1, 8 (2010) ("Financial intermediation helps bridge the gap between suppliers and consumers of capital, many of whom are located at a distance.").

41. Nina Boyarchenko, David O. Lucca & Laura Veldkamp, *Intermediaries as Information Aggregators: An Application to U.S. Treasury Auctions*, FED. RSRV. BANK OF BOS. 2–3 (Apr. 20, 2015) https://www.bostonfed.org/-/media/Documents/Macro-Financial-Society-2015/session2-boyarchenko-lucca-veldkamp.pdf [https://perma.cc/G4MM-XMJ3].

42. *Factors That Impact Loan Decisions (and How to Increase Your Approval Odds)*, BANK OF AM. (Apr. 4, 2025), https://business.bankofamerica.com/en/resources/factors-that-impact-loan-decisions-and-how-to-increase-your

condition, ensuring the return of the capital loaned and an increase in the value of the investment made.[43]

Although intermediation can be and often is much more complex, the simplified bank lending example above provides a useful framework for understanding the benefits of intermediation. The overall goal of financial intermediaries is to make transactions more efficient.[44] To accomplish this goal, intermediaries serve key roles in financial markets. First, intermediaries facilitate capital aggregation and reallocation, through deposit-taking, lending, and securitization, among other mechanisms.[45] In so doing, intermediaries improve market liquidity and "smooth the transfer of capital" within the markets.[46] Second, intermediaries collect, analyze, and disseminate information throughout the markets.[47] Exchanges, for example, facilitate the flow of information by allowing available information to be reflected in the price of assets through trading.[48] Other intermediaries, like underwriters and analysts, act as information brokers, reducing information asymmetries between companies

-approval-odds [https://perma.cc/2MCX-85W6] (listing the commonly requested information about the business and about the owners when applying for a loan).

43. *See generally* Matthew T. Gustafson, Ivan T. Ivanov & Ralf R. Meisenzahl, *Bank Monitoring: Evidence from Syndicated Loans*, 139 J. FIN. ECON. 452 (2021) (examining "how banks monitor syndicated loans, what factors determine banks' monitoring efforts, and how monitoring relates to other features of the loan contract and loan outcomes").

44. *See* Hans Genberg, *The Changing Nature of Financial Intermediation and Its Implications for Monetary Policy*, *in* Financial Market Developments and Their Implications for Monetary Policy, at 100, Bank for Int'l Settlements [BIS] Papers No. 39 (Apr. 2008), https://www.bis.org/publ/bppdf/bispap39f.pdf [https://perma.cc/CM8M-RKQF].

45. *See, e.g.*, Carol A. Corrado & Charles R. Hulten, *Financial Intermediation in the National Accounts: Asset Valuation, Intermediation, and Tobin's* q, *in* MEASURING WEALTH AND FINANCIAL INTERMEDIATION AND THEIR LINKS TO THE REAL ECONOMY 125, 128 (Charles R. Hulten & Marshall B. Reinsdorf eds., 2015) ("Financial intermediaries aggregate the savings of individual investors and transfer them through a variety of financial instruments to entrepreneurs and businesses, who then use the funds to acquire the capital necessary for their operations.").

46. Whitehead, *supra* note 40, at 9.

47. Ram T.S. Ramakrishnan & Anjan V. Thakor, *Information Reliability and a Theory of Financial Intermediation*, 51 REV. ECON. STUD. 415, 415–16 (1984) (describing financial intermediaries as diversified information brokers that acquire, process, and disseminate information to investors, thereby reducing duplication in screening and lowering information production costs in capital markets).

48. Will Kenton, *Understanding Exchanges: Types, Functions, and Real-World Examples*, INVESTOPEDIA (June 8, 2026), https://www.investopedia.com/terms/e/exchange.asp [https://perma.cc/N2PB-N2ES] (explaining that "an exchange ensures fair trading and spreads price information efficiently").

and investors.[49] Third, and related to their information functions, intermediaries are important to risk management. Owing to their positional advantage, intermediaries reduce and redistribute risk within financial transactions.[50] Underwriters in an initial public offering, for example, serve a risk management function both for the issuer (by helping with the pricing, marketing, and selling of the issuance) and the investors (by acting as a reputational agent and attesting to the worth of the issuance).[51]

Importantly, in addition to their benefits to the markets, the existence of financial intermediaries facilitates regulation. In the securities markets, regulations place obligations on investment advisors to ensure investment suitability for consumers;[52] on exchanges to provide equitable access to exchange pricing information;[53] and on underwriters to ensure reliable and complete issuer disclosures in an initial public offering.[54] With other intermediaries, like banks and insurers, regulations are concerned with protecting customers, both by ensuring that these intermediaries do not take on excessive risks, thereby jeopardizing their clients' money,[55] and by preventing fraud, discrimination, and other abusive practices.[56]

Given their importance and involvement in financial transactions, intermediaries are often the primary mechanism through which financial regulation occurs.[57] For regulators, financial intermediaries are clear, identifiable facilitators of transactions, which are fewer in number than market actors and therefore easier to regulate.[58] For their part, intermediaries are motivated to comply with and monitor applicable laws and regulations, as their profitability and

49. *See* Anita Indira Anand, *The Efficiency of Direct Public Offerings*, 7 J. SMALL & EMERGING BUS. L. 433, 438 (2003) (describing the informational role of underwriters).

50. Steven L. Schwarcz, *Intermediary Risk in a Global Economy*, 50 DUKE L.J. 1541, 1543 (2001) ("[M]arkets are diversifying investment risk by interposing intermediaries . . . .").

51. Lin, *supra* note 39, at 648–49.

52. Investment Advisers Act of 1940 § 206, 15 U.S.C. § 80b-6.

53. 17 C.F.R. § 242.603 (2023).

54. Securities Act of 1933 § 11, 15 U.S.C. § 77(k)(a)(5).

55. *See, e.g.*, Federal Deposit Insurance Act § 1, 12 U.S.C. § 1811 (delineating the responsibilities and impact of Comptroller General in risk evaluation); RISK-BASED CAPITAL (RBC) FOR INSURERS MODEL ACT §§ 2(b)–(d) (NAT'L ASS'N OF INS. COMM'RS 2012) (establishing factors considered in insurance risk analysis).

56. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act §§ 1031–1036, 12 U.S.C. §§ 5531–5536 (authorizing the Consumer Financial Protection Bureau to regulate unfair, deceptive, or abusive acts or practices in the consumer financial markets).

57. *See* Ilya Beylin, *How Portfolio Netting Deters Diversification and Competition in the Derivatives Industry*, 27 U. PA. J. BUS. L. 1, 20–21 (Fall 2024) (discussing how exchanges, clearinghouses, and other intermediaries are "conscripted into the regulatory project").

58. *Id.*

access to the markets are often tied to their reputation for reliability and legal compliance.[59]

Notwithstanding the benefits of intermediation, it has downsides. Most significantly, it is expensive. Intermediation adds a third party to the financial transaction, which invariably increases the cost of the transaction when compared to a frictionless scenario. Financial intermediaries constitute entire industries that must monitor risks, comply with regulations, and generate profits for their own shareholders. To facilitate their operations, intermediaries hire staff and, inevitably, generate their own bureaucracies. These expenses ultimately increase overall transaction costs, which may push some consumers out of the markets. For example, many low-income persons are unbanked or underbanked because of the fees associated with opening and maintaining a bank account.[60]

The problem of high transaction costs owing to intermediation is one that has been raised often. In a 2015 article, Professor Kathryn Judge argued that rather than lowering the overall transaction costs, intermediaries develop informational and positional advantages that allow them to promote and entrench high-fee arrangements that are not tied to any value added to the transaction.[61] Because of the high fees associated with intermediation, recent financial innovation has focused on removing intermediaries from transactions with the goal of lowering transaction costs. To its proponents, DeFi provides the best path towards true disintermediation, reduced costs and, ultimately, the democratization of the financial markets.

B. WHAT IS DEFI?

At the highest level of generality, DeFi refers to the range of financial services, products, and activities that rely on decentralized technology in lieu of traditional intermediaries.[62] DeFi uses decentralized, publicly accessible, and permissionless computerized blockchains, smart contracts, and distributed ledgers instead of the intermediaries—such as banks, exchanges, and

59. *Id.* at 36–37.

60. *See* Erin Bendig, *The Costs of Being Unbanked or Underbanked*, FORBES (Dec. 5, 2025), https://www.forbes.com/advisor/banking/costs-of-being-unbanked-or-underbanked [https://perma.cc/QS6K-9NHB] ("30.7% of households indicated that high monthly fees prevented them from opening a checking or savings account with a bank or credit union"). *See also* Nakita Q. Cuttino, *The Rise of "FringeTech": Regulatory Risks in Earned-Wage Access*, 115 NW. U. L. REV. 1505, 1525–26 (2021) (discussing low-income consumers' reliance on fringe financial services and distrust of mainstream financial institutions).

61. Kathryn Judge, *Intermediary Influence*, 82 U. CHI. L. REV. 573, 590–91 (2015).

62. PAUL TIERNO, CONG. RSCH. SERV., R48883, AN OVERVIEW OF DECENTRALIZED FINANCE (DEFI) 1 (2026).

brokers—and infrastructure central to traditional finance (TradFi).[63] DeFi thus aims to provide traditional financial activities through computer code, rather than relying on traditional intermediaries for trust.[64]

Structurally, DeFi operates through decentralized computerized record keeping. Among other things, it employs peer-to-peer settlement, whereby digital wallets connect directly, enabling value transfer without intermediaries.[65] DeFi utilizes programmable, composable infrastructure, that is, open-source smart contracts that can be combined to build new applications, along with community-driven governance.[66] Further, its design is non-custodial, meaning that users can hold custody over their own assets (self-custody) via digital wallets—unlike TradFi, where institutions hold custody.[67] Notably, unlike TradFi, DeFi operates without credit checks, identity verification, or underwriting standards; functions largely in a crypto-only closed loop; and eliminates institutional intermediaries.[68]

The term "DeFi" commonly refers to a computer-facilitated ecosystem of financial services, products, arrangements, and activities. This ecosystem may be viewed as having multiple layers. .[69] The foundation of DeFi is the underlying blockchain, known as the settlement layer, which stores and displays consistent transaction and ownership data.[70] The blockchain is a public, unalterable ledger that records all transactions and asset ownership that occur, thereby eschewing the need for a centralized authority.[71] To date, Ethereum is one of

63. *Id.* at 5.

64. *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, OECD 16 (2022), https://www.oecd.org/finance/Why-Decentralised-Finance
-DeFi-Matters-and-the-Policy-Implications.htm [https://perma.cc/D5PZ-3A2H].

65. Sandra Waliczek & Harry Yeung, *What Is 'Decentralized Finance' and What Can It Do in Practice?*, WORLD ECON. F. (Oct. 20, 2025), https://www.weforum.org/stories/2025/10/decentralized-finance-financial
-markets-in-practice [https://perma.cc/Z9Q3-SHW8].

66. OECD, *supra* note 64, at 18.

67. *Id.*

68. TIERNO, *supra* note 62, at 15–16.

69. BD. OF THE INT'L ORG. OF SEC. COMM'NS, PUB. REP. NO. OR01/2022, IOSCO DECENTRALIZED FINANCE REPORT 1 (2022) [hereinafter IOSCO], https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf [https://perma.cc/Q8CB-V9CW].

70. Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, 103 FED. RSRV. BANK OF ST. LOUIS REV. 153, 153 (2021) (proposing a multi-layered framework to analyze the implicit architecture and the various DeFi building blocks).

71. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-704SP, BLOCKCHAIN & DISTRIBUTED LEDGER TECHNOLOGIES (2019), https://www.gao.gov/assets/gao-19-704sp.pdf [https://perma.cc/6WRZ-MMTY] (noting that each time a transaction is added, it is verified via a consensus pool).

the most popular blockchains in use, but other notable blockchains include Binance Smart Chain, Polygon, and Solana.[72] The second layer is the asset layer, which holds the digital representation of value on the blockchain.[73] At the asset layer, there are a range of diverse assets and tokens, such as native tokens (e.g., Bitcoin and Ether), stablecoins (e.g., Tether and USD Coin), governance tokens, and utility tokens.[74]

The next two layers, which are the focus of this Article, are the protocol layer and the application layer.[75] The protocol layer, sometimes also referred to as the smart contract layer, sets the foundational, automated rules that enable decentralized financial activities—such as lending, borrowing, and trading—to occur without intermediaries.[76] Smart contracts are self-executing computer programs, often deployed on a blockchain, that are triggered automatically when predetermined criteria are satisfied.[77] Software engineers typically design, code, test, and deploy the smart contracts.[78] Importantly, the lack of licensing or auditing requirements means that any individual with the requisite skill can perform those functions.[79]

72. *See Top Blockchains by Total Value Locked (TVL)*, COINGECKO, https://www.coingecko.com/en/chains [https://perma.cc/7FCF-X5M6] (ranking Ethereum and other blockchains by total value locked).

73. Victor Budau & Herve Tourpe, *ASAP: A Conceptual Model for Digital Asset Platforms* 18 (IMF, Working Paper No. 24/14, 2024).

74. *See* Ray Chen, *Understanding the Differences: Tokenized Asset vs. Native On-Chain Assets*, KALEIDO (Apr. 18, 2023) https://www.kaleido.io/blockchain-blog/tokenized-assets-vs-native-on-chain-assets [https://perma.cc/AF7X-AV5P] (explaining the variety of tokenized assets and native on-chain assets).

75. *DeFi Stack: Getting a Grip on the DeFi Ecosystem*, HEDERA, https://hedera.com/learning/defi-stack [https://perma.cc/6SJ5-25NA].

76. *Id.*

77. *See supra* notes 7–9 and accompanying text (defining smart contracts).

78. *See, e.g.*, IOSCO, *supra* note 69, at 39 (noting that developers can "develop, deploy and engage with" smart contracts and "test and vet code"); Subcomm. on Digital Assets & Blockchain Tech., Tech. Advisory Comm., *Decentralized Finance*, CFTC 21 (Jan. 8, 2024), https://www.cftc.gov/media/10106/TAC_DeFiReport010824/download [https://perma.cc/J9XD-34N6] (describing how "software developers and engineers work[] to build, maintain, and update" DeFi projects).

79. *See* Eliza Mik, *Deconstructing Smart Contracts*, *in* THE CAMBRIDGE HANDBOOK OF EMERGING ISSUES AT THE INTERSECTION OF COMMERCIAL LAW AND TECHNOLOGY 375, 387 (Stacy-Ann Elvy & Nancy S. Kim eds., 2025) ("In the context of permissionless blockchains . . . anyone can create and deploy a smart contract, and anyone can use such smart contract.").

Smart contracts epitomize how DeFi can remove the need for a traditional financial intermediary.[80] Depending on their programming, smart contracts implement the rules that govern lending decisions, trade execution, collateral management, and other financial activities, all without (additional) human intervention once the code constituting the smart contract is deployed.[81] Smart contracts thus effectively perform the activities traditionally performed by exchanges, broker-dealers, banks, and other intermediaries.

The DeFi protocols of a smart contract might facilitate securities trading, for example, by providing that upon paying $100, an investor receives a one percent fractionalized interest in a specified security of a particular issuer. In this way, the protocols reproduce the functionalities of an exchange and enable users to submit orders to buy or sell securities while aggregating those orders, matching them, and executing matched transactions. Similarly, a DeFi lending platform might facilitate the borrowing of lender-deposited money by allowing parties to access funding using pre-specified forms of standardized collateral.[82] Loans can be disbursed nearly instantaneously, cutting lending costs.[83] In these ways, smart contracts allegedly can "eliminate the need for intermediaries in financial transactions—replacing exchanges, market-makers, asset managers, banks, and other lenders with software protocols."[84]

The final layer is the application layer, which facilitates the ability of users and investors to easily interact with the underlying protocols and assets.[85] For example, a user could trade cryptocurrencies by using the Uniswap Web App to swap its cryptocurrencies with cryptocurrencies held by other users.[86] In

80. *See supra* note 8 and accompanying text (discussing how smart contracts operate).

81. *See Glossary: Smart Contracts,* CHAINANALYSIS, https://www.chainalysis.com/glossary/smart-contracts [https://perma.cc/C8GE-H2MS] (describing how smart contracts automate financial agreements and proceedings without an intermediary and providing examples involving collateral).

82. *See* Sirio Aramonte et al., *DeFi Lending: Intermediation Without Information?*, at 1–2, Bank for Int'l Settlements [BIS] Bull. No. 57 (June 14, 2022), https://www.bis.org/publ/bisbull57.pdf [https://perma.cc/W9AP-TUVC] (describing how smart contracts administer loans through pre-specified rules). DeFi requires all loans to be collateralized due to the anonymity of the transactions. *Id.*

83. *See id.* (explaining how loan disbursement happens quickly and with low associated cost due to the automated nature of the process).

84. 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/H6JM-7RN3].

85. IOSCO, *supra* note 69, at 1, 3.

86. *Uniswap 101: What is Uniswap?*, UNISWAP LABS BLOG (May 31, 2023), https://blog.uniswap.org/what-is-uniswap [https://perma.cc/Q8RY-RWZE].

sum, DeFi is changing the ways users and investors access financial markets, all with limited reliance on traditional intermediaries. Smart contracts are key to this change and the many benefits that are expected as DeFi grows and is more widely integrated into TradFi.

C. THE BENEFITS OF DEFI

One widely cited benefit of DeFi is its potential to accelerate financial innovation.[87] At least in theory, DeFi developers can rapidly re-program smart contracts to build, modify, and combine financial applications without obtaining permission from traditional institutions. This ability to pivot and change without extensive oversight enables experimentation in lending, trading, insurance, and other financial functions to occur more quickly than in conventional markets.[88] Proponents of DeFi argue that this flexibility promotes competition and creativity, which facilitates the creation of innovative financial products and services.[89] Additionally, some believe the benefits DeFi provides are inherently welfare-enhancing, because it lowers certain transactions costs and has the potential to broaden financial opportunities to underserved and marginalized communities.[90] As discussed above, unlike TradFi, DeFi does not require underwriting or credit checks for lending or other financial services.[91] As such, persons excluded from TradFi may access financial services through DeFi with the internet and a smartphone, expanding financial inclusion among the unbanked.[92]

87. *See, e.g.*, Campbell R. Harvey & Daniel Rabetti, *International Business and Decentralized Finance*, 55 J. INT'L BUS. STUD. 840, 846 (2024) (describing how DeFi's transparency, in contrast to TradFi, does not rely on government regulators).

88. *Id.* at 846, 849.

89. *See id.* at 849 (referring to the "creative possibilities in the DeFi world" and the "seemingly endless" possibilities for innovation).

90. *See, e.g.*, Raluca Onufreiciuc & Lorena-Elena Stănescu, *Financial Inclusion through Decentralized Finance: A Citizen Perspective*, 10 EUR. J.L. & PUB. ADMIN. 117, 118 (2023)(arguing that DeFi improves welfare by reducing transaction costs and expanding financial access for underserved populations). The question of whether faster financial innovation and disintermediation necessarily improve social welfare—particularly when they externalize risk, undermine consumer protection, or exacerbate systemic fragility within the financial markets—is contested and addressed in Part IV.

91. TIERNO, *supra* note 62, at 1.

92. Ariyo Gracious Kazaara & Arinaitwe Julius, *The Role of Decentralized Finance (DeFi) in Enhancing Financial Inclusion: A Comparative Analysis*, 2 AVANCE INT'L J. BUS. & FIN. RSCH., Apr. 2026, at 3, https://www.researchgate.net/publication/404185521_The_Role_of_Decentralized_Finance_DeFi_in_Enhancing_Financial_Inclusion_A_Comparative_Analysis [https://perma.cc/93YR-6L4Q].

Another benefit commonly recited by DeFi proponents is that by allowing financial transactions to occur outside of the bank setting, and thereby outside of the monitoring and oversight of other financial intermediaries that charge for their services, DeFi reduces transaction costs.[93] Instead, proponents of DeFi argue that users may, in theory, be able to verify key information themselves—such as collateral levels, liquidity, and execution prices—without relying on a centralized intermediary to supply that data.[94] This purported transparency, combined with automated execution, arguably may have additional benefits, such as reducing opportunities for rent-seeking or discriminatory practices that can arise when human intermediaries make decisions about access to financial services.[95]

Furthermore, DeFi can help to democratize finance by broadening market access,[96] by making it accessible to anyone with an internet connection and a crypto wallet.[97] That would offer global access to borrowing, securities trading, and other investment opportunities without needing approval from traditional financial institutions,[98] thereby benefitting those who historically have found themselves financially excluded or underserved.

93. *See* Faust et al., *supra* note 12 and accompanying text (discussing benefits of DeFi further).

94. *See id.* at 138 (explaining that such "alternative information sources can address information asymmetries and thus benefit borrowers who would typically be classified as subprime by traditional lenders").

95. *See* Harvey & Rabetti, *supra* note 87, at 846 (noting that traditional finance relies on regulators to supervise financial activities which can fail at times, but "DeFi's transparency helps rectify this problem").

96. *See* discussion *supra* notes 12–14 and accompanying text.

97. A "crypto wallet" is a software- or hardware-based tool that enables users to manage digital assets by storing and controlling the cryptographic keys required to authorize transactions on a blockchain. Hyung-Jin Lim et al., *Comparative Analysis of Security Features and Risks in Digital Asset Wallets*, 14 ELECTRONICS 2436, 2437 (2025), https://doi.org/10.3390/electronics14122436. Importantly, cryptocurrency wallets do not store digital assets themselves; rather, they store private keys (or key shares) that allow users to access, transfer, and interact with assets recorded on a distributed ledger. *Id.* at 2439, 2446. Wallets vary significantly in structure and risk profile, including self-custody wallets—where users retain direct control over private keys—and custodial wallets, where key management is performed by a third party. *Id.* at 2447. Wallets are also commonly classified as "hot" or "cold" depending on their internet connectivity, reflecting tradeoffs between convenience and security. *Id.* at 2446. In decentralized finance, crypto wallets function as the primary technical interface through which users initiate transactions and interact with smart contracts, *id.*, while key loss, compromise, or misuse can result in irreversible asset loss. *Id.* at 2450–51.

98. Harvey & Rabetti, *supra* note 87, at 845–46.

DeFi's proponents further argue that by replacing human-managed intermediaries, smart contracts reduce the chance of human error.[99] Smart contracts also allow investors to retain direct control over their assets and automate financial activities according to pre-set rules, reducing opportunities for discretionary decision-making or operational missteps by institutional personnel.[100] In these ways, DeFi offers a level of speed, predictability, and user autonomy that conventional intermediaries struggle to match.[101]

The upshot, according to one industry leader, is that DeFi "operates through immutable code [e.g., smart contracts], and as such, represents 'an economy of laws and not of men.' It is this neutral, objective foundation for economic arrangements which future generations will look back upon and thank us for."[102]

* * *

While these features illustrate why DeFi has attracted significant enthusiasm, they also reveal how profoundly its architecture departs from the intermediary-based systems that have traditionally structured financial regulation. Part II examines the risks that arise when core financial functions are removed in total or delegated to decentralized technical infrastructures rather than to traditional institutional intermediaries. Importantly, the very qualities that DeFi's proponents argue promise efficiency, openness, and automation may also create significant hurdles to ensuring (1) the proper identification of actors within financial transactions, (2) appropriate compliance mechanisms are in place, and (3) the development of purposeful chokepoints upon which legal oversight has historically relied.

99. Vivek Jhunjhunwala, Sachin Shukla & Suryaksh Manot, *Artificial Intelligence and Smart Contracts*, LEXOLOGY (Dec. 27, 2023), https://www.lexology.com/library/detail.aspx?g=865220f0-e722-4c73-89ca-c58ce2120c64 [https://perma.cc/JN6Z-CLAG].

100. *See* Max Beinke et al., *Breaking the Chains of Traditional Finance: A Taxonomy of Decentralized Finance Business Models*, 34 ELEC. MKTS. 28, 31 (2024) ("DEX utilize smart contracts to tackle trust issues inherent in centralized exchanges by allowing users to retain control over their private keys.").

101. *See* Rakesh Sharma, *Understanding Decentralized Finance (DeFi): Basics and Functionality*, INVESTOPEDIA (last updated June 13, 2016), https://www.investopedia.com/decentralized-finance-defi-5113835 [https://perma.cc/P29K-U7W4] (explaining that Internet connectivity, low fees, and high autonomy help facilitate a global network).

102. Voorhees, *supra* note 34.

II. THE RISK ARCHITECTURE OF DECENTRALIZED FINANCE

This Part begins by surveying the traditional financial risks that DeFi reintroduces, including money-laundering vulnerabilities, one-way-out lending, and shadow-banking–style maturity and liquidity risks. It then examines the new risks created by DeFi's technical architecture, such as smart-contract failures, pseudonymity, and fragile or opaque governance systems. Finally, it identifies some of the regulatory and enforcement challenges these risks generate, including potential challenges in assigning responsibility for problematic transactions or systems, protecting consumers, and applying jurisdiction-bound regulatory regimes to DeFi transactions that routinely cross borders.

A. TRADITIONAL RISKS

This Section examines how DeFi revives the same prudential and compliance risks that have long challenged financial regulators. Though marketed as an innovation that increases efficiency and eliminates—or at the very least reconfigures—intermediaries, DeFi reproduces familiar dangers under a new technological guise. The first subsection explores how disintermediation undermines the AML and KYC safeguards[103] that anchor the domestic Bank Secrecy Act's and international Financial Action Task Force's regulatory regime. The second subsection focuses on how lending occurs on DeFi platforms and explains how smart-contract–based credit markets violate the traditional "two-ways-out" principle that once constrained excessive risk-taking by banks. The third subsection situates DeFi within the broader history of shadow banking, comparing the liquidity and maturity-transformation risks that fueled the 2008 Global Financial Crisis with those now emerging in digital-asset markets. Taken together, these subsections show that DeFi systems and transactions may amplify many of the risks that financial regulation was designed to address.

1. Money Laundering: DeFi's Compliance & Enforcement Challenge

A long-standing risk is that financial market participants might engage in money laundering, which would threaten monetary integrity,[104] or that they

103. Recall that AML refers to anti-money laundering safeguards and KYC refers to know-your-customer safeguards. *See supra* note 15 and accompanying text.

104. Money laundering and terrorist financing threaten the integrity of domestic payments. *See National Money Laundering Risk Assessment*, U.S. DEP'T OF THE TREASURY 6 (2015), https://home.treasury.gov/system/files/246/National-Money-Laundering-Risk-Assessment-06-12-2015.pdf [https://perma.cc/UK6E-QKSK] (explaining the risk money laundering poses to the financial system and national security); *National Terrorist Financing Risk Assessment*, U.S. DEP'T OF THE TREASURY 4 (2015), https://home.treasury.gov/system/files/246/National-Terrorist-Financing-Risk-Assessment-06-12-2015.pdf [https://

might even finance terrorists, jeopardizing national security.[105] The decentralization of finance would make it much more difficult to enforce the laws against money laundering and terrorist financing.[106] Enforcement difficulties would arise for at least two reasons. First, other things being equal, it would be harder to identify decentralized, rather than centralized, financial market participants. Second, enforcement costs would increase because there likely would be more such participants to monitor and bring enforcement proceedings against (plus, the benefit-to-cost ratio would decrease if each decentralized participant on average has a smaller financial stake than an intermediary in a traditional market).

In traditional intermediated markets, firms such as broker-dealers, banks, and payment processors often serve as the first line of defense against money laundering and related financial crimes. Under the Bank Secrecy Act and its implementing regulations, financial institutions must establish risk-based AML programs that include (1) KYC protections to identify and verify customer identity, (2) ongoing monitoring, and (3) the filing of Suspicious Activity Reports.[107] Broker-dealers, who are regulated by both the SEC and FINRA, are further subject to FINRA Rule 3310, which requires them to maintain written AML compliance programs reasonably designed to detect and report suspicious transactions.[108]

The obligation to ensure financial transactions are legitimate transactions that are not hiding nefarious purposes is not merely aspirational; it is routinely enforced and violators are sanctioned. In 2025, for example, Robinhood

perma.cc/UUB6-WMLM] (explaining how Terrorist Financing risk assessment complements the National Money Laundering Risk Assessment to find domestic monetary vulnerabilities).

105. Talley, *supra* note 16.

106. These laws are proposed by the Financial Action Task Force (FATF), an intergovernmental body established by the G7 nations, for countries to consider enacting into their national law. *See What Do We Do*, THE FINANCIAL ACTION TASK FORCE, https://www.fatf-gafi.org/about/whatwedo [https://perma.cc/ZWH8-8E39] (stating that the FATF seeks "to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system").

107. *See* Bank Secrecy Act of 1970, 31 U.S.C. §§ 5311–5332 (describing the goal and framework for financial institutions with the purpose of preventing money laundering); 31 C.F.R. §§ 1023.210, .320 (2024) (requiring broker-dealers to maintain AML programs and file Suspicious Activity Reports (SARs)).

108. FINRA MANUAL § 3310 (FINRA 2024). FINRA is a self-regulatory organization that oversees both broker-dealers individually and broker-dealer firms. *About FINRA*, FINRA, https://www.finra.org/about [https://perma.cc/S8UG-KMGY]. One author of this Article is a prior member of FINRA's National Adjudicatory Council (NAC), and one author is a current member of FINRA's NAC.

Markets, Inc. and its affiliated broker-dealers agreed to pay nearly $75 million in combined penalties to resolve investigations by both the SEC and FINRA into systemic supervisory and AML failures.[109] The SEC found that Robinhood Securities LLC and Robinhood Financial LLC "failed to timely investigate suspicious transactions" and to "file suspicious activity reports" in violation of their Bank Secrecy Act obligations.[110] FINRA also independently concluded that Robinhood lacked "reasonable anti-money laundering programs" and failed to respond to "'red flags' of potential misconduct."[111] These enforcement actions underscore how regulators may identify responsible parties, compel remediation efforts, and verify compliance through the firm's centralized recordkeeping systems—demonstrating that the presence of an intermediary provides the infrastructure and accountability required for effective AML oversight.

Recent enforcement actions against cryptocurrency intermediaries also illustrate how the presence of a centralized, legally accountable entity enables effective AML oversight even in digital-asset markets. In December 2025, the Department of Justice announced a guilty plea by a peer-to-peer convertible virtual currency, known as the CVC Exchange, for conspiring to violate the Bank Secrecy Act, operating an unlicensed money transmitting business, and promoting unlawful activity in violation of the Travel Act.[112] In parallel, the Financial Crimes Enforcement Network (FinCEN) entered into a consent order finding that the exchange willfully failed to implement an effective AML program, lacked meaningful KYC procedures for several years, failed to detect geographic spoofing that enabled transactions with comprehensively sanctioned jurisdictions, and did not file a single suspicious activity report despite facilitating hundreds of millions of dollars in suspicious transactions tied to fraud, prostitution, and state-sponsored cybercrime.[113]

The guilty plea of CVC Exchange and the underlying alleged conduct underscore a critical point for decentralized finance: AML enforcement is possible in crypto markets when an identifiable actor exists that governmental

109. *See supra* notes 25–27 and accompanying text (describing Robinhood's alleged violations and penalties).

110. U.S. SEC. & EXCH. COMM'N, *supra* note 26.

111. Stempel, *supra* note 27.

112. Brad A. Resnikoff et al., *Virtual Currency Exchange Pleads Guilty to Criminal Charges Related to Anti-Money Laundering Violations and Pays Multi-Million Dollar Fine to FinCEN*, MAYER BROWN (Dec. 23, 2025), https://www.mayerbrown.com/en/insights/publications/2025/12/virtual-currency-exchange-pleads-guilty-to-criminal-charges-related-to-anti-money-laundering-violations-and-pays-multi-million-dollar-fine-to-fincen [https://perma.cc/PHP7-YMF8].

113. *Id.*

authorities can identify and monitor. Because CVC Exchange operated as a money services business with centralized control over functions like customer onboarding, transaction monitoring, and recordkeeping, regulators were able to successfully bring an action that resulted in the imposition of criminal penalties.[114] By obtaining a guilty plea, the government was able to ensure that the firm would engage in appropriate remediation efforts, which included ongoing compliance reporting.[115] The government was able to achieve this outcome even though the underlying assets were pseudonymous and blockchain based.[116] In contrast, DeFi platforms that eliminate traditional features such as centralized operators, compliance personnel, or the ability to identify the legal entities participating in financial transactions remove the institutional hooks that made enforcement against the CVC Exchange feasible.

In DeFi, the structural features that enable disintermediation—anonymity, self-custody, and automated execution through smart contracts—may frustrate compliance with even the most basic requirements of the Bank Secrecy Act.[117] DeFi platforms typically have no physical headquarters, no compliance officers, and no practical mechanism for conducting customer identification or monitoring transactions in real time.[118] The absence of centralized control over customers or transactions makes it difficult to implement KYC and AML programs, both of which serve as foundational tools for preventing illicit finance.[119] Although some DeFi platforms claim to employ geofencing—

114. *Id.*

115. *Id.*

116. *Id.*

117. Bank Secrecy Act of 1970, 31 U.S.C. §§ 5311–5332; 31 C.F.R. §§ 1023.210, .320 (2024) (requiring broker-dealers and other covered entities to maintain AML programs and file suspicious activity reports).

118. *See* Zetzsche, Arner, & Buckley, *supra* note 38, at 187 (noting that without traditional "headquarters to which financial regulation will apply . . . regulatory agencies are likely to struggle to exert control").

119. Know Your Customer (KYC) requirements require financial institutions to verify information such as customer identity, beneficial ownership, and risk profile to detect and prevent misconduct such as money laundering or terrorist financing. *See generally* Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398 (May 11, 2016) (to be codified at 31 C.F.R. pts. 1010, 1020, 1023, 1024, 1026). These measures enable effective AML programs and enforcement efforts by linking transactions to identifiable actors and ensuring accountability within the financial system. While certain AML and KYC functions can be partially automated through transaction monitoring, wallet screening, sanctions filtering, and other technological tools, effective compliance systems require more. AML compliance systems must be updated, monitored, and audited as illicit actors adapt their techniques, otherwise the systems will become outdated and ineffective. DeFi platforms frequently lack identifiable employees or actors responsible for ensuring that these compliance activities are implemented,

blocking internet protocol (IP) addresses associated with sanctioned jurisdictions[120]—or crypto-wallet-screening software to exclude addresses flagged by the Office of Foreign Assets Control (OFAC), such measures are easily circumvented through the use of virtual private networks or newly created crypto wallets.[121]

Public details about enforcement actions confirm the regulatory and compliance challenges currently arising across DeFi transactions. For example, in 2023, the CFTC brought actions against DeFi platforms Opyn, Inc., Deridex, Inc., and ZeroEx, Inc., finding that each offered leveraged or margined digital asset transactions without registering as required under the Commodity Exchange Act.[122] Opyn and Deridex failed to adopt KYC and AML programs consistent with the obligations imposed on registered futures commission merchants under 17 C.F.R. § 42.2.[123] The absence of a legal entity capable of performing—or being compelled to perform—KYC and AML requirements may exacerbate the occurrence of illegitimate financial transactions.[124] Compliance activities conducted by private firms are an important component of larger efforts to ensure the legitimacy of financial transactions.[125] In part, this is because the government does not have the resources to engage in direct

operate effectively, and evolve in response to emerging risks. The result is the absence of reliable controls to ensure that compliance functions are implemented and maintained.

120. *Implementing a Sanctions Compliance Program for Digital Assets*, TRM LABS (Nov. 8, 2022), https://www.trmlabs.com/resources/trm-talks/implementing-a-sanctions-compliance-program-for-digital-assets [https://perma.cc/KV9V-RC3Z].

121. *See* Off. of Foreign Assets Control, *Sanctions Compliance Guidance for the Virtual Currency Industry*, U.S. DEP'T OF THE TREASURY 14 (Oct. 2021), https://ofac.treasury.gov/media/913571/download [https://perma.cc/9V9P-6YB5] (discussing crypto-wallet-address screening and sanctions exposure in the virtual currency sector); *Illicit Finance*, *supra* note 8, at 35 (noting DeFi services' use of crypto-wallet screening, and other sanctions-compliance measures).

122. Press Release No. 8774-23, CFTC, CFTC Issues Orders Against Operators of Three DeFi Protocols for Offering Illegal Digital Asset Derivatives Trading (Sep. 7, 2023), https://www.cftc.gov/PressRoom/PressReleases/8774-23 [https://perma.cc/KY7S-PC9V]. *See also CFTC v. Ooki DAO*, No. 3:22-CV-05416-WHO, 2023 WL 5321527, at *1 (N.D. Cal. June 8, 2023) (describing that CFTC asserted Ooki DAO's individual platform functioned as a trading platform and did not meet the CEA requirements for registration).

123. Press Release No. 8774-23, CFTC, *supra* note 122; Snow & Mollod, *supra* note 32.

124. *See, e.g.*, *Illicit Finance*, *supra* note 8, at 1 (discussing DeFi services' regulatory non-compliance as a key factor in facilitating illicit transactions).

125. *See* Veronica Root Martinez, *The Government's Prioritization of Information over Sanction: Implications for Compliance*, 83 L. & CONTEMP. PROBS. 85, 88 (2020) (arguing that "the transfer of information from the corporation to the government is integral to any federal enforcement model").

monitoring of all activities within firms, and because of this the government has traditionally relied on firms to monitor their customers and agents directly.[126]

Importantly, DeFi makes the efforts of government enforcement authorities more challenging. DeFi operates across pseudonymous networks and self-executing code leaving agencies such as the CFTC and the SEC struggling to fit round pegs of decentralized misconduct into the square holes of traditional enforcement activity.[127] The CFTC's 2023 enforcement action against Ooki DAO exemplifies this mismatch. The CFTC was unable to identify a single responsible entity, so the agency brought suit against the decentralized autonomous organization itself, characterizing it as an "unincorporated association" under the Commodity Exchange Act—a novel application of the well-established statutory framework.[128] In granting default judgment, the U.S. District Court for the Northern District of California permanently enjoined Ooki DAO and imposed civil penalties for operating an unregistered trading platform and failing to implement required KYC and AML procedures.[129] It is worth noting that this case was not actively litigated, and the CFTC's authority to bring the case was therefore not questioned by a litigant.[130] The CFTC's need to engage in this sort of creative enforcement effort underscores another set of challenges presented by DeFi; disintermediation obscures accountability of particular actors or entities and it also erodes the mechanisms through which the U.S. government safeguards monetary integrity and combats financial crime.[131]

Importantly, the risks of DeFi extend beyond AML and KYC to other areas of law. As the next subsection explains, the automatic execution of smart

126. *See id.* at 88–90 (explaining that government enforcers rely on corporations for information concerning misconduct and that firms are expected to monitor and police their own agents because internal misconduct is difficult for outsiders to detect).

127. *See, e.g.*, Zetzsche, Arner, & Buckley, *supra* note 38 and accompanying text.

128. CFTC v. Ooki DAO, No. 3:22-CV-05416, 2023 WL 5321527, at *5 (N.D. Cal. June 8, 2023); *see also* Press Release No. 8715-23, CFTC, Statement of CFTC Division of Enforcement Director Ian McGinley on the Ooki DAO Litigation Victory (June 9, 2023), https://www.cftc.gov/PressRoom/PressReleases/
8715-23 [https://perma.cc/R7SY-ZHQ7] (reporting that "in a precedent-setting decision, the court held that the Ooki DAO is a 'person' under the Commodity Exchange Act and thus can be held liable for violations of the law").

129. *Ooki DAO*, 2023 WL 5321527, at *8–9.

130. *Id.* at *2; *see also id.* at *6 (finding Ooki DAO in violation of 17 C.F.R. § 42.2 (2023) for failing to implement a customer-identification program and AML procedures).

131. *See* Zetzsche, Arner, & Buckley, *supra* note 38, at 184–88 (discussing a wide variety of enforcement, regulatory, and jurisdictional problems posed by DeFi's decentralized and disintermediated nature).

contracts can amplify instability in ways that parallel historical financial crises—particularly when DeFi platforms lack "two-ways-out" lending, a long-recognized structure in TradFi characterized by two independent sources of repayment—cash flow and asset value.

2. One-Way-Out Lending: DeFi's Failure to Meet Prudential Standards

DeFi lending is growing rapidly.[132] However, the smart contracts that underpin DeFi's functions could exacerbate old risks by undermining the prudent banking doctrine that a loan should always have at least "two ways out"—not only through collateral or asset-liquidation value but also through borrower cash flow.[133] The DeFi lending model has only one way out: collateral. DeFi lending allows parties to access funding simply by providing pre-specified forms of standardized collateral.[134] The rationale is to enable loans to be disbursed nearly instantaneously, cutting lending costs.[135]

Violations of the two-ways-out lending rule can have serious consequences, being causal factors in both the Great Depression and the Global Financial Crisis. Lending that depends only on collateral or asset-liquidation value invites disaster if the value declines. As Iman Anabtawi and author Steven L. Schwarcz have previously explained:

> Prior to the Great Depression, many banks engaged in margin lending to risky borrowers, securing the loans by shares of stock that the borrowers purchased with the loan proceeds. The value of the stock collateral started out being at least equal to the amount of the loan, and banks assumed that the stock market, which had been continuously rising in value for some years, would continue to rise, or at least not decline, in value.
>
> At the time, that assumption was viewed as reasonable. In August 1929, however, a (relatively) modest decline in stock prices, causing some of these margin loans to become under-collateralized.[136]

132. *Compare* Aramonte et al., *supra* note 82, at 1 (reporting that DeFi lending has risen from virtually zero in 2020 to more than $50 billion by early 2022), *with* Giulio Cornelli et al., *Why DeFi Lending? Evidence from Aave V2*, 63 J. FIN. INTERMEDIATION 1, 2 (2025) (reporting that the IMF estimated the overall DeFi lending debt outstanding to be around $25 billion in 2022).

133. *See, e.g.*, Steven L. Schwarcz, *Next-Generation Securitization: NFTs, Tokenization, and the Monetization of "Things"*, 103 B.U. L. REV. 967, 971–72 (2023) (explaining "two ways out" as the money generated from the investments and the ability to resell these interests).

134. *See supra* note 82 and accompanying text (explaining how smart contracts administer loans through collateral).

135. *See supra* note 83 and accompanying text (discussing the speed and low costs of loan disbursement in DeFi).

136. Iman Anabtawi & Steven L. Schwarcz, *Regulating Systemic Risk: Towards an Analytical Framework*, 86 NOTRE DAME L. REV. 1349, 1356–57 (2011) (footnotes omitted).

Banks began to lose money on those loans, and many became unable to pay their debts, contributing to the series of bank failures that triggered the Great Depression.[137]

Similarly, one-way-out lending almost certainly caused, or at least exacerbated, the Global Financial Crisis. In the years prior to the Global Financial Crisis, "many mortgage lenders made loans to risky borrowers secured by the homes that the borrowers purchased with the loan proceeds."[138] Those "'subprime mortgage loans' were then bundled together as collateral to partially support the payment of complex asset-backed securities that were sold to banks and other institutional investors worldwide."[139] These securities—which were highly rated by credit-rating agencies such as Standard & Poor's and Moody's—"maintained their value so long as home prices appreciated, as they had been doing for decades and as most market observers assumed would continue."[140] Home prices began falling, however, causing some of these asset-backed securities to default and "requiring financial institutions heavily invested in these securities to write down their value . . . ."[141] That, in turn, caused these institutions to appear, if not become, financially risky, contributing to the loss of confidence in banks and credit ratings that triggered the Global Financial Crisis.[142]

DeFi's one-way-out lending model invites these same risks. The problem is that any type of asset used as collateral can unexpectedly decline in value, causing loans secured by such assets to become undercollateralized. Thus, a $100,000 loan that is initially secured, for example, by $110,000 of a certain type of cryptocurrency[143] will become significantly undercollateralized if the value of that cryptocurrency declines, say, by 20 percent (reducing the collateral value to $88,000). The borrower's cash flow may be insufficient, indeed vastly insufficient, to repay the loan because DeFi lending does not take income into account.[144] If multiple loans secured by the same type of collateral

137. *Id.* at 1357.

138. *Id.* at 1359.

139. *Id.*

140. *Id.* at 1359–60.

141. *Id.* at 1360.

142. *Id.*

143. *See, e.g.*, Cornelli et al., *supra* note 132, at 1 ("Anonymity and crypto assets volatility leads to reliance on overcollateralisation as a risk management tool, as there is no other way to assess the borrower's ability to repay . . . . DeFi's reliance on crypto assets as collateral also makes it largely self-referential and limits its interaction with the real economy.").

144. *See supra* note 82 and accompanying text (discussing that DeFi lending allows parties to access funding simply by providing pre-specified forms of standardized collateral); *see also* Cornelli et al., *supra* note 132, at 1 ("Unlike traditional banks that rely on extensive credit

become undercollateralized, the DeFi lending platform will appear, if not become, financially risky. That in turn can create a loss of confidence in DeFi lending and also potentially trigger a systemic collapse of interconnected DeFi platforms.[145]

3. Shadow Banking & the DeFi Parallel

DeFi's decentralization of finance also could pose risks similar to those caused by the advent of shadow banking. Shadow banking refers broadly to the movement of financial intermediation away from traditional, regulated banks into markets and nonbank financial entities such as hedge funds, money market funds, and structured investment vehicles.[146] Although these entities perform bank-like functions—taking in short-term funds and making longer-term loans or investments—they operate outside of the prudential and supervisory framework that applies to banks.[147]

By encouraging regulatory arbitrage, this shift caused a significant portion of the financial system to become unregulated.[148] Without deposit insurance,

assessments and personal identification, DeFi operates on the principles of anonymity. Borrowers and lenders interact without revealing their identities, *making traditional creditworthiness assessment methods unfeasible*." (emphasis added)). DeFi lending's failure to take income into account might also be viewed as a new risk insofar as such lending "lacks the relationship-building and trust elements inherent in traditional banking, which can play a role in risk assessment and loan recovery." *Id.*

145. *See* Aramonte et al., *supra* note 82, at 4 (noting that "[t]he interconnectedness of the various components of DeFi lending can exacerbate procyclicality, as it implies that shocks to part of the DeFi ecosystem can affect the system as a whole").

146. Michael Bromberg, *Understanding Shadow Banking: Definition, Examples, and Function*, INVESTOPEDIA (last updated July 21, 2026), https://www.investopedia.com/terms/s/shadow-banking-system.asp [https://perma.cc/6KCT-53H2].

147. *Id.*; *see also* Victor Fleischer, *Regulatory Arbitrage*, 89 TEX. L. REV. 227, 275 (2010) ("[W]hen new forms are chosen because they reduce regulatory costs and increase transaction costs compared to the old structure, we lose twice: [E]fficiency is reduced by the increase in transaction costs, and the regulatory burden is shifted onto those who cannot engage in arbitrage.").

148. *See* Erik Feyen et al., *Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy*, at 13, Bank for Int'l Settlements [BIS] Papers No. 117 (July 2021), https://www.bis.org/publ/bppdf/bispap117.pdf [https://perma.cc/KKV8-BZGA] (comparing the growth of the shadow banking sector before the global financial crisis); *cf.* Ben Protess, *Shadow Banking Makes a Comeback*, N.Y. TIMES: DEALBOOK (May 27, 2011), https://archive.nytimes.com/dealbook.nytimes.com/2011/05/27/shadow-banking-makes-a-comeback [https://perma.cc/6RV4-7XSX] (explaining that the Dodd-Frank Act does not subject shadow banks to many of the regulations that the Act put into place).

capital requirements, or direct oversight, shadow banking transactions expose financial markets to maturity and credit transformation risks.[149] The lack of regulatory protection allowed excessive "maturity and credit transformation . . . [in] the shadow banking system,"[150] which arguably "contributed significantly to asset price bubbles in real estate markets" prior to the Global Financial Crisis.[151] The shift also was thought to increase transaction costs, motivating parties to use higher-cost deal structures that offer a net gain because they can avoid regulation.[152]

Decentralized finance replicates many of these same vulnerabilities, albeit primarily through the technology itself. For example, researchers argue that the digital asset ecosystem reproduces many of the vulnerabilities associated with traditional financial intermediation, including "runs," high leverage, and maturity transformation, across centralized lenders, stablecoin issuers, and DeFi protocols, often without comparable regulatory safeguards.[153] In both shadow banking and DeFi transactions, credit creation and liquidity transformation occur outside of the banking system, exposing markets to destabilizing feedback loops when prices fall or liquidity dries up.[154] For example, DeFi lending protocols allow parties to borrow by posting volatile digital collateral,[155] creating a danger of "large, sudden withdrawals of funds" and fire sales during adverse shocks.[156] Because DeFi credit and liquidity provisions typically rely on crypto-native assets—including volatile cryptocurrencies and

149. FED. RSRV. BANK OF N.Y., STAFF REPORT NO. 458, SHADOW BANKING 2 (2010), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr458_July_2010_version.pdf [https://perma.cc/W2EQ-DGJ6]. Maturity transformation, for example, involves borrowing short and lending long, which can destabilize credit markets in a downturn. *Id.* at 8.

150. *Id.* at 51.

151. *Id.* at 3.

152. Fleischer, *supra* note 147, at 275; *see also* Frank Partnoy, *Financial Derivatives and the Costs of Regulatory Arbitrage*, 22 J. CORP. L. 211, 240–42 (1997) (describing increased transaction costs resulting from financial market participants seeking to avoid regulations). On the other hand, to the extent shadow banking is not driven by regulatory arbitrage, it could constitute a public good by helping to achieve efficiencies. FED. RSRV. BANK OF N.Y., *supra* note 149, at 3.

153. Pablo D. Azar et al., *The Financial Stability Implications of Digital Assets*, 30 FED. RSRV. BANK N.Y. ECON. POL'Y REV., Nov. 2024, at 1, 3 (identifying "runs" on centralized lenders, stablecoins, and DeFi protocols as evidence of systemic fragility).

154. *Id.*

155. *See supra* notes 143–144 and accompanying text (discussing DeFi lending's reliance on crypto assets as collateral).

156. Azar et al., *supra* note 153, at 2.

stablecoins that reference fiat currency[157] but lack sovereign guarantees—changes in crypto-asset prices directly impact collateral values, leverage ratios, and the solvency of lending protocols.[158] When crypto prices decline, these protocols automatically liquidate collateral positions, potentially exacerbating downward price spirals—a dynamic strikingly similar to the "runs" and forced liquidations that destabilized shadow banking during the Global Financial Crisis.[159]

From a financial-stability perspective, some commentators argue that DeFi amounts to "shadow banking 2.0," pointing to the network of algorithmic protocols performing credit, liquidity, and maturity transformation without prudential supervision.[160] Yet unlike the pre-2008 shadow-banking system, DeFi's risk propagation is accelerated by technological innovations that have increased the capacity of both automation and global pseudonymity. Researchers warn that "[t]he lack of a strong and cohesive regulatory framework for digital assets"—combined with high leverage, liquidity mismatches, and cross-platform interconnections—renders the DeFi system "very fragile against the occurrence of adverse shocks."[161] Just as policymakers after 2008 sought to bring shadow banking within the ambit of legal and regulatory requirements through capital and liquidity standards,[162] regulators today face the challenge

157. Fiat currency is government-issued money—such as U.S. dollars or euros—that has value because the government declares it legal tender, not because it is backed by a physical commodity like gold or silver. *Glossary: Fiat Currency*, CHAINANALYSIS, https://www.chainalysis.com/glossary/fiat-currency [https://perma.cc/7C6Y-PWLP]. Congress has recently sought to reduce some of the risks associated with payment stablecoins through the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act. *See generally* GENIUS Act, 12 U.S.C. §§ 5901–5916. The Act generally requires permitted payment stablecoin issuers to maintain one-to-one reserves in highly liquid assets, including cash and short-term U.S. Treasury obligations, and imposes disclosure, redemption, and supervisory requirements on issuers. *Id.* These requirements may reduce the likelihood that regulated payment stablecoins themselves become a source of instability. At the same time, they further tie significant portions of the DeFi ecosystem to regulated financial institutions and traditional reserve assets, illustrating the extent to which even ostensibly decentralized markets continue to rely on centralized financial infrastructure.

158. *See* Azar et al., *supra* note 153, at 3 (arguing that "the use of leverage by crypto investors appears widespread, amplifying investors' exposure to shocks to crypto-asset prices and the feedback loop between leverage and crypto-asset prices").

159. *Id.* at 25–26 (describing automated liquidations and cascading price effects across DeFi platforms).

160. Hilary J. Allen, *DeFi: Shadow Banking 2.0?*, 64 WM. & MARY L. REV. 919, 924 (2023).

161. Azar et al., *supra* note 153, at 3.

162. *See, e.g.*, Allen, *supra* note 160, at 928–29 (describing steps taken by Congress and regulators in response to the 2008 financial crisis).

of applying those same prudential concepts to DeFi systems that often lack identifiable legal entities or centralized control.

* * *

The upshot is that these "old" risks—compliance failures, imprudent lending, and unregulated intermediation—underscore how DeFi, despite its technological novelty, replicates the structural vulnerabilities that are present but well addressed in centralized, traditional finance.[163] What distinguishes DeFi, however, is not the type of risk it generates but the way those risks manifest in a permissionless, computer-code-driven environment. The next Section turns to these "new" risks and examines how the mechanics of DeFi create fresh challenges for regulation and enforcement.

B. NEW RISKS

In moving financial transactions away from intermediaries, DeFi poses new risks that arise from the technology's architecture and operation. These risks may impose significant costs on DeFi investors and DeFi platforms. Further, given DeFi's increased interconnectedness with TradFi, these risks may spill over into the broader financial markets, especially as DeFi continues to grow at an accelerated pace.[164] This Part focuses on three risks associated with DeFi, raising questions about the inherent costs of DeFi for consumers, the markets, and the DeFi platforms themselves.

1. Technological Vulnerabilities

One of the primary risks that DeFi faces relates to its very foundation—smart contracts. The computer code that enables smart contracts to operate is susceptible to attack. Errors or bugs in the code, whether intentional or not, may render smart contracts vulnerable to exploitation.[165] This could be a

163. *See, e.g.*, *id.* at 938 (emphasizing that while "regulations relating to reserve, capital, margin, and netting requirements are all used to limit leverage in the established financial system," these controls are absent on decentralized exchanges).

164. Joseph Abadi, *Making Sense of Decentralized Finance*, 9 FED. RSRV. BANK OF PHIL.: ECON. INSIGHTS, First Quarter 2024, at 18, 19, https://www.philadelphiafed.org/-/media/FRBP/Assets/Economy/Articles/economic-insights/2024/q1/eiq124-making-sense-of-decentralized-finance.pdf [https://perma.cc/N2RL-4YJE] (providing data showing a ten-fold increase in the amount invested in DeFi platforms from 2020 to 2023).

165. Alexandra Born et al., *Decentralised Finance—A New Unregulated Non-Bank System?*, EUR. CENT. BANK: MACROPRUDENTIAL BULL. (July 2022), https://www.ecb.europa.eu/press/financial-stability-publications/macroprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html [https://perma.cc/2DN5-G5PS].

particular problem given the irreversibility and finality of transactions executed on a blockchain.[166] Further compounding the issue is the absence of any centralized authority, which could leave victims without recourse in the event of theft or fraud or other loss.[167] For example, in 2016, programming flaws in the recently launched Decentralized Autonomous Organization smart contract on the Ethereum platform were exploited, leading to the theft of $50 million in virtual currency.[168] As DeFi has grown, so too have the attacks on DeFi platforms, with billions of dollars of value being lost each year.[169]

Another risk that arises from DeFi's technological underpinning relates to the composability of smart contracts. Composability refers to the ability of smart contracts to build on the functionalities of other smart contracts to create new, more complex products.[170] With composability, smart contracts can interoperate to provide novel, highly sophisticated products and services not available from a single smart contract.[171]

A paradigmatic illustration of composability risk is the use of "flash loans," which permit users to borrow large quantities of cryptocurrency without posting collateral, so long as the loan is borrowed and repaid within a single blockchain transaction.[172] Flash loans involve the interaction of multiple DeFi protocols, including a lending protocol to originate the loan, an exchange to execute trades, and a pricing oracle to supply asset values—each operating through separate smart contracts.[173] Because these steps occur within a single

166. *Id.*; *see also The Financial Stability Risks of Decentralised Finance*, FIN. STABILITY BD. 18 (Feb. 16, 2023), https://www.fsb.org/uploads/P160223.pdf [https://perma.cc/JV4U-Y2CB] (stating that smart contracts "may be impossible to stop, modify, or reverse").

167. Born et al., *supra* note 165.

168. Klint Finley, *A $50 Million Hack Just Showed That the DAO Was All Too Human*, WIRED (June 18, 2016), https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human [https://perma.cc/UL7S-Q9PR].

169. Jonathan Greig, *Cybercriminals Stole $1.7 Billion from Crypto Funds in 2023 as Attacks Proliferated*, RECORD (Jan. 24, 2024), https://therecord.media/cybercriminals-stole-over-1-billion-from-crypto-funds-2023 [https://perma.cc/4VV4-6T7U].

170. Francesca Carapella et al., *Decentralized Finance (DeFi): Transformative Potential & Associated Risks* 5 (Fed. Rsrv. Bank of Bos., Supervisory Research and Analysis Working Paper 22-02, 2022), https://www.bostonfed.org/-/media/Documents/Workingpapers/PDF/2022/sra2202.pdf [https://perma.cc/8KQM-8MF5].

171. *Id. See also* FIN. STABILITY BD., *supra* note 166, at 9 (explaining that "components of the DeFi space" can be "pieced together by developers to create new and potentially highly sophisticated products").

172. *What Are Flash Loans?*, CHAINLINK (May 24, 2023), https://chain.link/education-hub/flash-loans [https://perma.cc/379Y-92EK].

173. *Id.*

transaction, the flash loan either executes in full or is automatically reversed, flash loans enable users to carry out rapid, multi-step strategies that are difficult to replicate in TradFi settings.[174]

Although flash loans may facilitate legitimate financial activities, they may also introduce significant systemic vulnerabilities into financial transactions. In a number of documented incidents, attackers have used flash loans to exploit weaknesses in one protocol's pricing or governance logic, temporarily distorting market conditions and triggering losses across interconnected platforms.[175] These events demonstrate how composability may magnify the consequences of a single design flaw in even one step of the transaction. A vulnerability in one smart contract may be leveraged instantaneously across several protocols, allowing losses to occur throughout a DeFi system before any human actor can intervene.[176]

Imagine two DeFi platforms that are linked together. The first platform is a trading venue that sets prices for digital assets. The second platform is a lending service that allows users to borrow money if they post those digital assets as collateral, relying on the prices set by the first platform. Using a flash loan, an attacker briefly borrows a large amount of cryptocurrency from the lending platform and uses it to push up the price of a particular asset on the trading platform. Importantly, the lending platform automatically relies on that price, therefore causing the lending platform to treat the asset as more valuable than it really is, which allows the attacker to borrow more funds than should be possible. The attacker immediately repays the flash loan—so the transaction is technically valid—but keeps the excess funds borrowed from the lending platform. Once the transaction ends, prices return to normal, leaving the lending platform undercollateralized and its users bearing the loss. This example illustrates how DeFi's composability can allow a temporary distortion in one protocol to generate losses across another.[177] Because smart contracts generally cannot observe market conditions directly, they rely on oracles and other mechanisms for external information.[178] Those dependencies can become

174. *See, e.g.*, *What Are Flash Loans in DeFi?*, BINANCE ACAD. (last updated Apr. 29, 2026), https://www.binance.com/en/academy/articles/what-are-flash-loans-in-defi [https://perma.cc/VL25-QY89] (discussing the mechanics and financially innovative applications of flash loans).

175. *Id.*

176. *Id.*

177. *See id.* (describing a similar kind of flash loan attack).

178. *See* FIN. STABILITY BD., *supra* note 166, at 18–19 (explaining "oracle risk" and noting that errors or attacks may trigger liquidations and propagate shocks); *see also* Chanelle Duley et al., *The Oracle Problem and the Future of DeFi*, at 3, Bank for Int'l Settlements [BIS] Bull. No. 76 (Sep. 7, 2023), https://

vulnerabilities when the available information is limited or susceptible to manipulation.[179]

As shown in this example, a web of inter-operational smart contracts could magnify vulnerabilities because a vulnerability in any one contract could impact the remaining contracts, and the failure of a web of such contracts could more easily spread throughout the DeFi ecosystem.[180] Further, composability increases complexity as smart contracts build on and interact with one another; that in turn makes it harder to identify interdependencies that may allow losses or disruptions to spread across protocols.[181] Finally, composability also can create asset-based interconnections that are a source of risk. For example, assets created for one DeFi protocol may be used as collateral on another protocol, creating linkages among DeFi platforms.[182] Thus, the failure of a single protocol could impact multiple DeFi platforms, potentially creating a cascading effect.[183]

2. Transparent Yet Anonymous

As discussed above, DeFi is often built on public blockchains and, as such, anyone can see the transactions being executed, purportedly limiting the need for verification by intermediaries.[184] However, this transparency only extends so far. Users of the blockchain are distinguished through an identifier that displays the blockchain address of the counterparty but not their identity.[185] To many, the pseudonymity of blockchain and DeFi transactions is "a feature, not a bug," viewed as one of the primary improvements of DeFi over traditional,

www.bis.org/publ/bisbull76.pdf [https://perma.cc/C3CD-MVFG] (describing oracle manipulation triggering liquidations).

179. *See, e.g.*, FIN. STABILITY BD., *supra* note 166, at 18–19 (describing intrinsic issues related to oracle reliance).

180. *Defi's Composability: More Possibility, More Risk*, QUANTSTAMP (July 15, 2021), https://quantstamp.com/blog/defis-composability-more-possibility
-more-risk [https://perma.cc/6X2B-GBJ9].

181. FIN. STABILITY BD., *supra* note 166, at 21.

182. Lewis Gudgeon et al., *The Decentralized Financial Crisis*, ARXIV 2–3 (last updated June 27, 2020) https://arxiv.org/pdf/2002.08099 [https://perma.cc/CFW3-5HML].

183. *Id.* at 3.

184. *See supra* Part I.B.

185. Matteo Aquilina et al., *Cryptocurrencies and Decentralised Finance: Functions and Financial Stability Implications*, at 16, Bank for Int'l Settlements [BIS] Papers No. 156 (Apr. 2025), https://www.bis.org/publ/bppdf/
bispap156.pdf [https://perma.cc/Z92X-S52W] (stating that crypto-wallets are "anonymous and cannot be linked to physical or legal entities" or persons).

centralized financial markets.[186] Indeed, according to one study, some traders prefer decentralized exchanges over centralized ones because of their greater anonymity despite the fact that these exchanges can sometimes be relatively costlier (due to execution costs) for small transactions.[187] The inherent pseudonymity of DeFi, however, has its own set of challenges.

To start, the innate anonymity of DeFi effectively eliminates most reputational risks, incentivizing misconduct.[188] Because smart contract activities are not linked to legal identities, actors have an incentive to take advantage of counterparties, whether through excessive risk taking or fraudulent behavior.[189] A prime example is the "rug pull" scam, in which DeFi developers disappear with funds raised after a token issuance, leaving investors with a worthless asset.[190] While such fraudulent activity is possible in TradFi, victims generally have clearer avenues for recovery because misconduct can often be traced to identifiable entities operating within regulatory and remedial frameworks.[191] With DeFi, however, victims of a rug pull scam may not know whom to sue if identities are unknown.[192]

Additionally, pseudonymity makes it difficult for investors to differentiate between legitimate assets or transactions and illegitimate or manipulative ones. In a pseudonymous market, one cannot easily tell if transactions or asset prices reflect legitimate transactions between unaffiliated counterparties or collusive trading or even bots trading at the behest of a single person.[193] Such malicious or manipulative behavior therefore cannot always feasibly be detected or punished.[194] As such, notwithstanding the transparency of smart contracts, DeFi

186. Igor Makarov & Antoinette Schoar, *Cryptocurrencies and Decentralized Finance* 26–27 (Bank for Int'l Settlements [BIS], Working Paper No. 1061, 2022), https://www.bis.org/publ/work1061.pdf [https://perma.cc/JK55-M59P].

187. Sirio Aramonte et al., *DeFi Risks and the Decentralisation Illusion*, BIS Q. REV., Dec. 2021, at 21, 26, https://www.bis.org/publications/defi-risks-and-decentralisation-illusion_0.pdf [https://perma.cc/ADJ9-356M].

188. Aquilina et al., *supra* note 185, at 16.

189. *Id.* at 17.

190. *Id.* (defining a rug pull scam); *see also* Jared Ronis, *DeFi 101: The Good, the Bad, and the Regulatory*, WILSON CTR.: ACROSS KARMAN (Sep. 29, 2023), https://acrosskarman.wilsoncenter.org/article/defi-101-good-bad-and-regulatory [https://perma.cc/P3YQ-W952] (describing rug pulls as one of "several risk factors to be aware of" in the DeFi space).

191. *See* Stempel, *supra* note 27 and accompanying text (discussing Robinhood example).

192. *See* Aquilina et al., *supra* note 188, at 17 (detailing how it is much more difficult for consumers to pursue potential perpetrators of fraud through the court system in the DeFi context than it is in traditional finance).

193. Crenshaw, *supra* note 22.

194. *Id.*

investors still can fall prey to scams and frauds because they lack the information, time, and expertise needed to ferret out illegitimate transactions in a pseudonymous marketplace.[195] Thus, pseudonymity can benefit malicious actors who conceal their bad behavior, thereby evading consequences for their misdeeds.

Although smart contracts technically make individual transactions publicly observable on the blockchain, they do not reliably reveal the real-world identities or economic relationships of the parties involved. Pseudonymity makes it difficult to determine who controls DeFi platforms, how risks are distributed across transactions, and if or how different DeFi protocols are interconnected.[196] A single developer, for example, may operate multiple wallets across several DeFi protocols under different pseudonyms, making it difficult for investors and regulators to assess the extent of that developer's activity or influence.[197] As DeFi becomes increasingly interconnected both internally and with traditional financial markets,[198] this inability to map who controls or is participating in transactions complicates risk assessment efforts and increases the possibility that losses or disruptions will spread across markets.[199]

3. Governance Risks

Although a central promise of DeFi is decentralization, the actual level of decentralization varies, especially with respect to DeFi governance.[200] DeFi governance refers primarily to the process by which decisions are made for a

195. Vincent Gramlich et al., *Decentralized Finance (DeFi): Foundations, Applications, Potentials, and Challenges*, FRAUNHOFER FIT 44 (2022), http://dx.doi.org/10.2139/ssrn.4535868.

196. FIN. STABILITY BD., *supra* note 166, at 9, 32.

197. *See, e.g.*, *id.* at 17 (explaining that developers' "economic incentives are not always clear and almost always poorly disclosed").

198. *See, e.g.*, Logan Hitchcock, *Bermuda Plots 'Fully On-Chain National Economy' with Help from Coinbase and Circle*, YAHOO FIN.: DECRYPT (Jan. 19, 2026) https://finance.yahoo.com/news/bermuda-plots-fully-chain-national
-204255639.html [https://perma.cc/S8KG-Q8CQ] (highlighting Bermuda's efforts to create "the world's first fully on-chain national economy"); Jona Jaupi, *J.P. Morgan Launches Tokenized Money Market Fund on Ethereum*, DEFIANT (Dec. 15, 2025), https://thedefiant.io/news/defi/j-p-morgan-launches-tokenized
-money-market-fund-on-ethereum [https://perma.cc/DDN4-3NSN] (discussing "how large financial institutions are increasingly using blockchain infrastructure to deliver traditional products").

199. Makarov & Schoar, *supra* note 186, at 3–4.

200. Carapella et al., *supra* note 170, at 21 ("In practice, the extent to which the governance of a blockchain is decentralized is better thought of as a spectrum rather than a discrete choice between two opposites."); FIN. STABILITY BD., *supra* note 166, at 36 ("[T]he actual degree of decentralization among underlying DeFi organisational structures varies broadly . . . .").

platform.[201] So, for example, when there is a bug or other error in a smart contract's computer code, the governance framework is the mechanism by which decisions about correcting the errors are made.[202] Similar considerations are at play when any amendments need to be made to smart contracts—who gets to decide and by what process? Early on in their existence, DeFi platforms are often highly centralized to better ensure their viability and stability.[203] Later, as a DeFi platform gains popularity and grows its investor base, its governance may become more dispersed among developers and other stakeholders, resulting in greater decentralization. However, even when governance is dispersed, two interrelated claims are true of DeFi governance. First, full decentralization is unlikely.[204] And, second, governance authority is typically concentrated in the hands of a few.[205]

To participate in DeFi governance, developers and investors often must acquire a governance, or voting, token.[206] These tokens are explicitly assigned specific governance rights and do not have independent monetary value outside the ability to vote on future governance measures.[207] Insiders, such as developers, founders, and early funders of a DeFi platform, are often granted a substantial number of governance tokens, concentrating power in their hands.[208] Additionally, insiders can aggregate governance tokens, increasing their concentration of power.[209] This concentration of governance authority means that a small group can exert outsized influence over

201. Iwa Salami, *Challenges and Approaches to Regulating Decentralized Finance*, 115 AJIL UNBOUND 425, 427 (2021).

202. *See* Carapella et al., *supra* note 170, at 21 ("This ability to change the protocol, however, raises a governance question: [W]hat process does someone follow to make changes to the protocol? This question includes not only who makes the final decision on changes, but who is authorized to draft changes to the protocol and who decides which draft changes are considered for adoption." (footnote omitted)).

203. *Id.*

204. *See* Aramonte et al., *supra* note 187, at 27 (calling full decentralization of DeFi "illusory" since all DeFi platforms have an element of centralization around governance).

205. *See id.* at 28 (explaining that "all DeFi platforms have an element of centralization").

206. Gogel, *supra* note 8, at 3.

207. *See id.* at 13 (explaining that "the value of the token reflects investor expectations about the success of the protocol").

208. *See* Aramonte et al., *supra* note 187, at 28 (explaining that "[m]any blockchains also allocate a substantial part of their initial coins to insiders").

209. *See* Turillazzi et al., *supra* note 30, at 7 (explaining how the voting mechanism is "criticised for enabling . . . disproportionate voting power that early investors or the original team can have on the votes").

the platform's operation, rather than the decentralized and democratized governance that is often touted with respect to DeFi.[210]

Governance concentration has implications and risks beyond perceived unfairness. Concentration may facilitate collusion among large governance-token holders, allowing a small group of insiders to manipulate or exploit a platform for their own gain.[211] Further, if governance tokens are tradable, malicious actors could acquire enough power to alter the platform for their own financial gain.[212] For example, in April 2023, the RookDAO experienced a coordinated attack from insiders who gained enough governance authority to pass a proposal to dissolve the DAO, liquidate its $44 million treasury, and distribute $25 million of the treasury to themselves.[213]

In addition to governance being concentrated, it is also opaque. For instance, by granting veto rights only to particular governance-token holders, some DeFi platforms fully embrace the concept that while all governance votes are equal, some are more equal than others. The problem is not necessarily that different governance models exist, but rather that these governance features are not fully transparent to investors.[214] Potential investors, therefore, may believe that they are able to contribute to the mechanisms of DeFi governance but, in reality, their ability to do so may be limited or curtailed in ways that are unknown to them.

C. OVERVIEW OF REGULATORY CHALLENGES

The traditional and novel risks discussed above expose gaps in the regulatory and supervisory tools currently available to address DeFi. More specifically, DeFi complicates both systemic-risk regulation and investor protection efforts, calling into question how prudential regulation should be structured in the absence of institutional intermediaries. In addition to the macro- and micro-prudential concerns, DeFi raises significant cross-border enforcement challenges, as the elimination of identifiable intermediaries deprives regulators of the jurisdictional hooks on which traditional oversight depends.

1. Macroprudential & Microprudential Concerns

DeFi poses challenges both to the stability of the financial system and to the individual integrity of parties acting in that system. "Macroprudential" regulation may be needed to protect the financial system's stability, and "microprudential" regulation may be needed to protect the integrity—that is, the

210. *See id.* (referring to this as "governance capture").
211. Aramonte et al., *supra* note 187, at 28.
212. OECD, *supra* note 64, at 34.
213. Turillazzi et al., *supra* note 30, at 7.
214. FIN. STABILITY BD., *supra* note 166, at 12.

safety and soundness—of those parties. This Article considers how such regulation should be designed to regulate DeFi platforms.

a. Macroprudential Regulation

Regulation designed to protect financial stability by identifying and reducing systemic risks is referred to as "macroprudential."[215] At least five types of market failures could cause shocks that could impair financial stability: complexity, conflicts, behavioral limitations, change, and a type of tragedy of the commons (where individually rational behavior leads market participants to overuse or degrade shared resources).[216] Also, maturity transformation—a firm using short-term financing to make long-term investments, creating the liquidity risk that its cash flow may become insufficient to repay maturing debt—could cause a maturity gap, which in turn could lead to a default that triggers a systemic shock.[217] Macroprudential regulation of DeFi platforms should be designed to protect against these failures if and when they may become applicable.

Macroprudential regulation typically proceeds by identifying structural market failures that can amplify localized shocks into system-wide instability.[218] In the DeFi context, the most acute macroprudential risks appear to stem from technological and organizational complexity, which may obscure the extent of risk in a market and magnify information asymmetries in ways that traditional regulatory frameworks are ill-equipped to monitor and detect.

As one of us has explained, complexity represents a market failure insofar as it can distort the understanding of information and impair disclosure, thereby increasing asymmetric information.[219] In the DeFi context, complexity comes not only from the sophisticated financial products themselves, but also from the way smart contracts and protocols interact. Governance mechanisms, composability across protocols, and opaque control rights can make it difficult for investors and regulators to identify who bears particular risks or how losses in one protocol may affect others. Complexity can also result in mutual

215. *See* Kadija Yilla & Nellie Liang, *What Are Macroprudential Tools?*, BROOKINGS INST. (Feb. 11, 2020), https://www.brookings.edu/articles/what-are -macroprudential-tools [https://perma.cc/ZWZ6-UX5G] (describing macroprudential policies).

216. Steven L. Schwarcz, *Systematic Regulation of Systemic Risk*, 2019 WIS. L. REV. 1, 26.

217. *Id.*

218. Yilla & Liang, *supra* note 215.

219. *See, e.g.*, Steven L. Schwarcz, *Disclosure's Failure in the Subprime Mortgage Crisis*, 2008 UTAH L. REV. 1109, 1110–11 (observing that even sophisticated institutional investors did not fully understand certain complex financings).

misinformation.[220] As discussed below, the macroprudential regulation of DeFi platforms will need to focus on this market failure.

Conflicts of interest represent a distinct but closely related source of macroprudential risk. More specifically, conflicts can refer to internal management conflicts or to conflicts between managers and third parties. DeFi platforms typically concentrate control in their developers, particularly in early stages.[221] Therefore, they are unlikely to have significant internal management or management-owner conflicts. DeFi platforms, however, may be subject to management-investor conflicts, as shown by the reported investor frauds.[222] These conflicts, though, are exacerbated by complexity, which greatly increases the information asymmetry between DeFi-platform managers and investors.[223] The regulation of conflicts should therefore focus on the reduction of information asymmetry caused by DeFi's complexity.

The remaining market failures—behavioral limitations, change, tragedy of the commons, and maturity transformation—do not appear to apply to DeFi platforms any differently than they apply to other financial business organizations.[224] Accordingly, the existing macroprudential regulation that applies to those market failures should already help to protect against DeFi financial instability. For example, DeFi platforms that become significant enough to be designated as systemically important financial institutions (SIFI) would be subjected to SIFI-related macroprudential regulation. Such regulation is designed to protect against liquidity failures as well as against financial contagion—the

220. *See* Steven L. Schwarcz, *Regulating Complexity in Financial Markets*, 87 WASH. U. L. REV. 211, 241–42 (2009) (discussing the mutual misinformation problem caused by re-securitization's complexity because neither the sponsor of the re-securitization, nor the investors, fully understood the risks).

221. *See* Gogel, *supra* note 8, at 6 (explaining that DeFi developers initially retain substantial control over protocol decisions, with full DAO-based decentralization as a later objective).

222. *See supra* notes 1-3, 168–169, and 190 and accompanying text (discussing various fraud cases involving DeFi).

223. *See supra* notes 219–220 and accompanying text (explaining how lack of information or misinformation can lead to asymmetry between investors and DeFi-platform managers).

224. There is nothing about DeFi platforms that uniquely involves behavioral limitations. Change pertains to financial change, which this Article's discussion of DeFi already addresses. The tragedy of the commons refers to a firm's risk-taking to increase profitability for its owners and managers, without full regard for third parties and the public. That, however, is a possible market failure that is common to all financial firms, and it is already addressed by SIFI designation and regulation. *Cf. supra* note 187 and accompanying text (discussing how such designation and regulation should apply to DeFi platforms). Maturity transformation refers to a firm using short-term financing to make long-term investments, creating the liquidity risk that its cash flow may become insufficient to repay maturing debt. That again is addressed by the SIFI regulation that governs liquidity risk. *See id.*

risk of debt defaults being transmitted through the interconnectedness of SIFIs.[225]

For these reasons, any new macroprudential regulation of DeFi platforms should focus on reducing the information asymmetry between developers of DeFi platforms, on the one hand, and investors and users of the platforms, on the other hand, that stems from DeFi's complexity. A blunt way to reduce DeFi's complexity would be to prohibit decentralized finance. That, however, would stifle innovation.[226] It also would likely be costly and futile because DeFi platforms outside the United States could develop DeFi products and services, which would infiltrate U.S. markets.[227] Reducing DeFi's complexity by requiring the standardization of DeFi products and services would also fail. It would not only be subject to the preceding problems but also could potentially increase systemic risk by correlating investments.[228]

Incentive-based approaches to try to control DeFi's complexity would have greater flexibility and less downside risk. For example, the European Union has been creating a regulatory framework favoring simple, transparent, and standardized (STS) securitization transactions.[229] This framework incentivizes,

225. *See, e.g.*, IMF, Bank for Int'l Settlements & Fin. Stability Bd., *Guidance to Assess the Systemic Importance of Financial Institutions, Markets and Instruments: Initial Considerations*, IMF 13 (Oct. 28, 2009), https://www.imf.org/external/np/g20/pdf/100109.pdf [https://perma.cc/8C8E-CKKZ]; Basel Comm. on Banking Supervision, *Global Systemically Important Banks: Assessment Methodology and the Additional Loss Absorbency Requirement*, BANK FOR INT'L SETTLEMENTS 1 (July 2011) https://www.bis.org/publ/bcbs201.pdf [https://perma.cc/9VR2-HP7U].

226. Steven L. Schwarcz, *Controlling Financial Chaos: The Power and Limits of Law*, 2012 WIS. L. REV. 815, 820.

227. *See* Letter from Miller Whitehouse-Levine, DeFi Educ. Fund, to Vanessa A. Countryman, Sec'y of Sec. & Exch. Comm'n 11–12 (Apr. 18, 2022), https://www.sec.gov/comments/s7-02-22/s70222-20123960-280119.pdf [https://perma.cc/SGD3-TH6X] (stating that "the Commission cannot impede decentralization in other jurisdictions, which are taking affirmative steps to attract the disintermediated market industry" and "[i]f the United States is to reap the benefits of the industry and help determine the ultimate regime that regulates it, the Commission must not adopt regulations that could regulate its development out of existence within the United States' borders").

228. *See, e.g.*, Charles K. Whitehead, *Destructive Coordination*, 96 CORNELL L. REV. 323, 326–27 (2011) (discussing how standardization could exacerbate systemic risk). *But see* Saule T. Omarova, *License to Deal: Mandatory Approval of Complex Financial Products*, 90 WASH. U. L. REV. 63, 84 (2012) (arguing for requiring approval of complex financial products by "adopting and operationalizing the general *concept of precaution* in the context of post-crisis financial systemic risk regulation may be a worthwhile, and even necessary, exercise").

229. *See generally* Proposal for a Regulation of the European Parliament and of the Council Laying Down Common Rules on Securitisation and Creating a European Framework for

rather than mandates, STS transactions by reducing regulatory capital requirements for investors therein, thereby allowing for potential innovation.[230] That potential, plus the framework's flexible definition of what could qualify as an STS transaction, could help to reduce complexity without unnecessarily stifling innovation.

Creating such an incentive-based framework for DeFi platforms at this time, however, puts the cart before the horse. In contrast to the STS framework, which built on years of experience with securitization transactions, we do not yet know enough about DeFi and DeFi platforms to determine what would work. To that end, and also to further reduce DeFi's complexity, we will need to better understand DeFi.

For that purpose, regulators may wish to monitor and collect data about DeFi's uses and their consequences. By analogy, in order to better understand systemic risk, the Dodd-Frank Act created a nonpartisan Office of Financial Research (OFR)[231] as well as a Financial Stability Oversight Council (FSOC)[232] to monitor and identify potential systemic threats. The Bank of England similarly established a Financial Policy Committee (FPC) to identify, monitor, and reduce systemic risk.[233] In the European Union, a "European Systemic Risk Board (ESRB) was established to monitor and assess potential threats to financial stability," including providing early warning of system-wide risks that may be building up and issuing recommendations for dealing with the risks.[234]

Until we more fully understand DeFi and its risks, ex ante preventative regulation almost certainly will be insufficient standing alone. The difficulty is that financial innovators often develop products and organizational structures that do not fit neatly within existing regulatory categories or that take advantage of gaps in the current framework. Regulators are therefore often forced to respond to risks only after they emerge, which, of course, means the development of ex ante rules is sometimes not fully possible. Regulators

Simple, Transparent and Standardised Securitisation and Amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU and Regulations (EC) No 1060/2009 and (EU) No 648/2012, COM (2015) 472 final (Sep. 30, 2015).

230. *Id.*

231. Dodd-Frank Wall Street Reform and Consumer Protection Act § 152, 12 U.S.C. § 5342.

232. § 111.

233. Robert Peston, *The FPC: Running the Financial Economy?*, BBC NEWS (Feb. 17, 2011), http://www.bbc.co.uk/blogs/thereporters/robertpeston/2011/02/the_fpc_running_the_financial.html [https://perma.cc/Z8NM-E465].

234. European Commission Press Release MEMO/14/244, A Comprehensive EU Response to the Financial Crisis: Substantial Progress Toward a Strong Financial Framework for Europe and a Banking Union for the Eurozone, at 3 (Mar. 28, 2014), http://europa.eu/rapid/press-release_MEMO-14-244_en.htm [https://perma.cc/2J2C-F3F3].

therefore may wish also to examine potential ex post regulation—measures designed to contain or remediate harm after a DeFi platform fails—in an effort to mitigate any harmful consequences caused by the collapse of DeFi platforms.[235] In connection with the COVID pandemic, for example, the Federal Reserve provided such ex post regulation by creating the Commercial Paper Funding Facility to support "the flow of credit to households and businesses" that was lost when the private commercial paper market collapsed.[236] Regulators could learn from that by monitoring the growth of DeFi products and services. If any such DeFi market sector becomes large enough for its collapse to destabilize the financial system, they should consider what ex post regulation may be needed to mitigate the harmful consequences of that collapse.

Finally, it is essential that any macroprudential regulation of DeFi platforms be coordinated globally. Such coordination is discussed below.[237] Although global coordination is important, regulators should be cautious to avoid excessively correlating macroprudential rules. Such correlation would exacerbate systemic risk by decreasing the flexibility and resilience of the financial system. In our "rapidly changing financial system," there also is "a very real danger that the wrong rules will be" coordinated.[238] Some argue, for example, that the Basel II capital requirements, which set international standards for the minimum capital a bank must hold based on risk, contributed to the 2008 financial crisis by globally correlating faulty rules.[239] Regulatory harmonization also, paradoxically, can invalidate existing risk-management strategies that are premised on randomness and independent action.[240] For example, the value-

235. *See* Iman Anabtawi & Steven L. Schwarcz, *Regulating* Ex Post*: How Law Can Address the Inevitability of Financial Failure*, 92 TEX. L. REV. 75, 91–93, 102–06 (2013) (discussing the importance and providing examples of ex post macroprudential financial regulation).

236. *See Commercial Paper Funding Facility*, BD. OF GOVERNORS OF THE FED. RES. SYS.: POL'Y TOOLS (last updated June 11, 2021), https://www.federalreserve.gov/monetarypolicy/cpff.htm [https://perma.cc/F9W9-3876] (explaining that "[t]he Federal Reserve Board established a Commercial Paper Funding Facility (CPFF) on March 17, 2020, to support the flow of credit to households and businesses," in response to the collapse of private commercial paper markets).

237. *See infra* Part III.C.2 and accompanying text (describing how to implement coordinated and multijurisdictional enforcement for DeFi platforms).

238. RICHARD J. HERRING & ROBERT E. LITAN, FINANCIAL REGULATION IN THE GLOBAL ECONOMY 134–35 (1995) (alteration omitted); *see also* Roberta Romano, *For Diversity in the International Regulation of Financial Institutions: Critiquing and Recalibrating the Basel Architecture*, 31 YALE J. ON REGUL. 1, 5–7 (2014) (advocating for "international regulatory harmonization").

239. *See* Romano, *supra* note 238, at 13–20 (comparing Basel-compliant institutions with institutions that operate outside of Basel regulation).

240. Whitehead, *supra* note 228, at 347.

at-risk (VaR) model presumed that portfolio managers act independently of each other.[241] Incorporating VaR into regulation, however, can incentivize managers to act more uniformly, thereby undermining VaR's utility as a risk-management tool.[242]

b. Microprudential Regulation

Regulation designed to protect the individual safety and soundness of parties acting in the financial system is referred to as "microprudential."[243] The purpose is to reduce the chance that any given party fails, thereby harming its investors and counterparties.[244] Traditional bank regulation epitomizes such regulation, requiring each bank to act with prudence.[245]

So long as DeFi platforms remain small and bespoke in their nature, microprudential regulation may be relatively unimportant. The investors in a DeFi platform are typically its insider developers and non-developer third parties.[246] Insiders should be deemed to take the risk that their project could fail. Non-developer investors are typically sophisticated third parties in private offerings of securities. Microprudential regulation is not intended—and would not normally be efficient—to protect small firms that have sophisticated private investors.[247] Accordingly, this Article does not currently recommend microprudential regulation to protect the safety and soundness of DeFi platforms individually. Regulators nonetheless should consider monitoring the ongoing growth of DeFi markets and platforms for purposes of determining whether, at some point, microprudential regulation may be needed.

241. *Id.* at 341.

242. *Id.* at 347–51; *see also* World Econ. & Fin. Surveys, *Global Financial Stability Report: Financial Market Turbulence: Causes, Consequences, and Policies*, IMF 62 (Oct. 2007), https://www.imf.org/-/media/websites/imf/imported-flagship-issues/external/pubs/ft/gfsr/2007/02/pdf/_textpdf.pdf [https://perma.cc/J7UF-BK7G] (finding that having institutions employ the same risk model has destabilizing effects).

243. *E.g.*, Lucrezia Cipriani & Andrea Minto, *Microprudential Regulation*, *in* COMPARATIVE FINANCIAL REGULATION 155 (Alessio M. Pacces, Edoardo D. Martino & Hossein Nabilou eds., 2025).

244. *Id.*

245. *See id.* (observing that microprudential regulation is concerned with the ability of banks and other financial intermediaries individually to perform their functions).

246. *See supra* notes 206–210 and accompanying text (discussing governance distribution among early developers and founders of a given DeFi platform).

247. *See* JOHN ARMOUR ET AL., PRINCIPLES OF FINANCIAL REGULATION 167–69 (2016) (explaining how regulations such as mandatory disclosure requirements are generally unnecessary for sophisticated investors who can contract for any necessary information).

Readers may question why, if DeFi platforms individually remain small and bespoke in their nature, this Article recommends macroprudential but not microprudential regulation. The answer is that the correlated failure of multiple small financial providers can still have a destabilizing systemic impact on the financial system.[248]

2. Consumer Protection Difficulties

One of the most important aspects of intermediation is that it provides ways for various actors within the financial markets to protect consumers. Intermediaries—including actors like broker-dealers and financial advisers—are required to disclose risks, maintain accurate records, refrain from deceptive practices, and provide redress if and when fraud occurs that causes harm to investors.[249]

Forsage illustrates the acute consumer-protection challenges posed by disintermediated financial systems. As is explained above, although Forsage was marketed as a legitimate "decentralized matrix project [that is, platform]," it in fact encoded the mechanics of a classic Ponzi and pyramid scheme directly into its smart contracts, diverting funds from new investors to earlier participants as soon as each "slot" was purchased.[250] Because there was no intermediary responsible for normal consumer protection activities, like vetting financial disclosures or supervising sales practices, approximately $340 million was extracted from retail investors worldwide, with over 80% of those investors receiving fewer ETH back than they invested and more than half never receiving any payout at all.[251] By relying on self-executing smart contracts, the platform was able to carry out the fraud across jurisdictions without many of the protections that traditional financial intermediaries ordinarily provide.

The Department of Justice was able to identify and indict Forsage's founders—Russian nationals who aggressively promoted the scheme online[252]—but this case is more of an exception than the rule in DeFi, where pseudonymous developers and globally dispersed operators often render meaningful, governmental enforcement functionally impossible. As was noted above, the individuals who develop, deploy, or control DeFi platforms are

248. *See, e.g.*, Jeremy C. Kress & Matthew C. Turk, *Too Many to Fail: Against Community Bank Deregulation*, 115 NW. U. L. REV. 647, 655–68 (2020) (discussing the risks of perpetuating "too-many-to-fail" theory).

249. *See supra* notes 107–108 and accompanying text (explaining the regulations intermediaries must follow).

250. U.S. Dep't of Just., *supra* note 1.

251. *Id.*

252. *Id.*

often pseudonymous or geographically dispersed, and they may have intentionally structured their operations in a manner to purposefully frustrate formal mechanisms of accountability.[253] The CFTC's action against Ooki DAO illustrates the potential consumer protection problem. Because the agency could not identify a conventional legal entity or a clear management structure, it proceeded against the DAO itself as an unincorporated association under the Commodity Exchange Act.[254] The case ultimately resulted in a default judgment because no one appeared to defend the DAO.[255] Despite winning the suit against Ooki DAO, to date it does not appear that the CFTC has collected on its judgment because of the decentralized nature of the entity and the inability to identify *who* is responsible for paying the judgment.[256] Thus, even in cases where regulators succeed in obtaining a judgment from an adjudicator, the remedy may arrive years after consumer harm has occurred and sometimes provides little to no meaningful redress to victims.

In short, DeFi raises practical challenges for protecting retail investors in ways that traditional financial markets have long provided. The intermediaries who traditionally bear legal duties to disclose risks, monitor misconduct, and compensate harmed investors have been intentionally removed from the system in the name of potential benefits like "democratization." And these accountability gaps for retail investors are only magnified by DeFi's global reach, which triggers a range of complex, cross-border enforcement challenges.

253. Alexandre Birry et al., *Regulating Crypto: The Bid to Frame, Tame, or Game the Ecosystem*, S&P GLOB.: RATINGS 16 (July 13, 2022), https://www.spglobal.com/content/dam/spglobal/corporate/en/images/articles/regulating-crypto-final.pdf [https://perma.cc/XQ8B-VGX8] (discussing the difficulty in identifying those who can be held accountable).

254. Complaint ¶¶ 2–3, CFTC v. Ooki DAO, No. 3:22-CV-05416, 2023 WL 5321527 (N.D. Cal. June 8, 2023); *see also* Order Granting Motion for Default Judgment at 7–8, *Ooki DAO*, No. 3:22-CV-05416-WHO, 2023 WL 5321527 (explaining the court's decision to treat the DAO as an unincorporated association because no identifiable entity could otherwise be served).

255. Order Granting Motion for Default Judgment at 12–13, *Ooki DAO*, No. 3:22-CV-05416-WHO, 2023 WL 5321527.

256. *Ooki DAO Default Judgment: Regulators Still Face Many Technical and Legal Challenges in Regulating Smart Contracts*, HERBERT SMITH FREEHILLS KRAMER: INSIGHTS (June 20, 2023), https://www.hsfkramer.com/insights/2023-06/ooki-dao-default-judgment-regulators-still-face-many-technical-and-legal-challenges-in-regulating-smart-contracts [https://perma.cc/V58Y-Y6GB].

3. Cross-Border Challenges

The ease with which DeFi operations cross national borders raises national and international security concerns. DeFi can provide loopholes for sanctions evasion, terrorist financing, and ransomware attacks with little-to-no commensurate guardrails to hold bad actors accountable.[257] For example, in March 2022, a North Korean sponsored cyber hacking group stole virtual assets worth approximately $620 million from a blockchain project.[258] A few months later, in June 2022, the same group stole another $100 million from Horizon, a DeFi cross-chain bridge.[259] North Korea is also allegedly behind numerous ransomware attacks and has allegedly dispatched thousands of hackers worldwide to steal and launder virtual assets.[260] The stolen virtual assets and revenue generated therefrom may have been used for North Korea's nuclear weapons and ballistic missile programs, in addition to providing a source of revenue for the heavily-sanctioned nation.[261]

The cross-border regulatory and enforcement difficulties are underscored by the jurisdictional challenges that are inherent to DeFi. DeFi operates globally, providing services and products to investors worldwide. [262] The

257. *See generally Illicit Finance*, *supra* note 8 (explaining the ways bad actors can take advantage of the pseudonymous nature of DeFi).

258. Press Release, Fed. Bur. of Invest., *FBI Statement on Attribution of Malicious Cyber Activity Posed by the Democratic People's Republic of Korea* (Apr. 14, 2022), https://www.fbi.gov/news/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea [https://perma.cc/ENS4-HP73].

259. Press Release, Fed. Bur. of Invest., FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft (last updated Feb. 6, 2023), https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft [https://perma.cc/FN88-FC3B]. As Chainalysis explains:

> Cross-chain bridges are the connective tissue that allow different blockchains to securely share data and assets. At their core, these bridges employ a messaging system that permits blockchains to pass information to each other in a verifiable way. Instead of relying on a centralized intermediary, trustless bridges use automated software on each blockchain to exchange and verify messages independently.

Introduction to Cross-Chain Bridges, CHAINALYSIS: BLOG (Dec. 5, 2024), https://www.chainalysis.com/blog/introduction-to-cross-chain-bridges [https://perma.cc/3GG3-PLEX].

260. *Illicit Finance*, *supra* note 8, at 24–25.

261. *Id.*

262. *Project Atlas: Mapping the World of Decentralised Finance*, BANK FOR INT'L SETTLEMENTS: INNOVATION HUB 6 (Oct. 2023), https://www.bis.org/

multinational nature of DeFi's operations complicates the application of laws and, in some instances, makes it difficult to determine which laws apply in certain transactions or instances.[263] For example, a DeFi platform registered in the Cayman Islands may facilitate transactions between U.S.-based and India-based customers.[264] In such a scenario, there are legitimate questions about which laws apply to a transaction that is illicit or fraudulent.

Even when the applicable laws are otherwise clear, DeFi platforms may try to limit compliance requirements by registering in a jurisdiction with less stringent laws.[265] A 2023 enforcement order against Binance provides a salient example.[266] The CFTC, Department of Justice, and Treasury Department settled with Binance and its founder for violating U.S. anti-money laundering and sanctions laws and failing to report suspicious transactions involving terrorist groups and child abusers.[267] Binance—which was registered in the Cayman Islands—solicited and executed transactions for U.S.-based customers, while purposefully refusing to comply with U.S. laws.[268] Further, DeFi platforms often seek to exploit or create regulatory gaps that may arise because of decentralization. For example, some DeFi platforms that otherwise have Bank Secrecy Act obligations or that operate as futures commission merchants try to avoid their regulatory obligations by transitioning to a decentralized autonomous organization, claiming that it insulates them from compliance with U.S. laws.[269]

Similarly, criminal actors may seek out jurisdictions with relaxed or non-existent regulations to carry out their illicit activity to further avoid

publications/project-atlas-mapping-world-decentralised-finance.pdf [https://perma.cc/R39J-8BD8].

263. Born et al., *supra* note 165.

264. *See* Press Release, Off. of Foreign Assets Control, Settlement Agreement Between the U.S. Department of the Treasury's Office of Foreign Assets Control and Binance Holdings, Ltd. (Nov. 21, 2023), https://ofac.treasury.gov/recent-actions/20231121 [https://perma.cc/34NS-FM29]; Press Release, U.S. Dep't of Just., Binance and CEO Plead Guilty to Federal Charges in $4B Resolution (Nov. 21, 2023), https://www.justice.gov/archives/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution [https://perma.cc/R6NS-54UB] (explaining that Binance was facilitating transactions between U.S. and non-U.S.-based customers).

265. *See* Press Release, U.S. Dep't of Just., *supra* note 264 (explaining how Binance, a company registered outside the U.S., tried to operate outside U.S. law despite serving U.S. based customers).

266. Press Release, Off. of Foreign Assets Control, *supra* note 264.

267. Press Release, U.S. Dep't of Just., *supra* note 264.

268. Press Release, Off. of Foreign Assets Control, *supra* note 264.

269. *Illicit Finance*, *supra* note 8, at 26.

accountability.[270] Indeed, across various jurisdictions, some regulators may lack the authority, capacity, or willingness to go after crimes related to digital assets, making enforcement even more difficult.[271] Additionally, evidence gathering can be complicated for DeFi platforms that have their operations and customers spread across multiple countries.[272] Regardless, the cross-border nature of DeFi and the ease with which transactions are executed globally make it exceedingly likely that law enforcement efforts will be duplicated across agencies and countries in the event of misconduct.[273]

* * *

The regulatory challenges identified in this Section do not counsel regulatory restraint. Rather, they underscore the need for regulators to gather better information about DeFi markets, monitor how those markets develop, and use that information to determine what additional regulatory measures may be warranted.[274] As that information is being gathered, however, enforcement actors need to begin to lay the groundwork to incentivize robust compliance by those who build, operate, and maintain DeFi platforms via a coordinated, global enforcement effort.[275]

III. TARGETED COMPLIANCE & ENFORCEMENT FOR DEFI PLATFORMS

Part III sets forth this Article's central claim: Because DeFi platforms disaggregate the functions historically performed by financial intermediaries, effective regulation must (1) embed compliance safeguards directly into platform design and (2) hold accountable the actors who build, operate, and maintain those platforms. The absence of embedded compliance constraints or credible accountability mechanisms within DeFi is itself destabilizing to the financial

270. *How to Strengthen International Law Enforcement Cooperation For Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets*, U.S. DEP'T OF JUST. 11 (June 6, 2022), https://www.justice.gov/d9/pages/attachments/2022/06/07/ncet_executive_order_report.pdf [https://perma.cc/GT74-9MC3].

271. *Id.* at 8.

272. *Id.* at 9.

273. *Id.*

274. *See supra* Part II.C.1 (discussing the macroprudential and microprudential concerns in the regulatory challenges of DeFi).

275. We note that international law scholars have also identified that cross-border regulation is essential to addressing the problems DeFi presents to the financial markets. *See* Douglas W. Arner, Dirk A. Zetzsche, Ross P. Buckley, & Jamieson M. Kirkwood, *The Financialisation of Crypto: Designing an International Regulatory Consensus*, 53 COMPUT. L. & SEC. REV., no. 105970, July 2024, at 17.

markets and potentially harmful to consumers.[276] Even incrementally developed architectural safeguards via compliance requirements—paired with targeted, multijurisdictional enforcement—may work to materially improve market discipline and the deterrence of misconduct. The point is not to restore traditional intermediaries, but to create sufficient incentives for the compliance and risk-management functions they once supplied to be performed within DeFi platforms and protocols.

A. EX ANTE ARCHITECTURAL CONSTRAINTS

DeFi operates primarily through smart contracts.[277] The primary ex ante architectural constraints should therefore focus on reducing the risks of using smart contracts.

Smart contracts can create risk in at least three ways: They foster disintermediation by substituting computerized algorithms for responsible financial intermediaries; they obscure the identities of the contracting parties, thereby limiting counterparty interaction; and they enable unchecked automatic contract execution.[278] Regulation therefore should focus on attempting to reduce these risks by (1) re-intermediating responsible parties, (2) creating a process to identify the counterparties, and (3) controlling unchecked automation. Any regulatory attempt to reduce these risks should be designed not to unduly interfere with DeFi's benefits.

There is, however, a threshold question about regulatory scope. Just as the law does not purport to regulate all contracts even though some may be problematic,[279] DeFi-focused regulation should only address smart contracts that would be reasonably likely to cause material problems. Experience will be needed to fully identify those contracts. At the outset, however, regulators should focus on financially complicated smart contracts, such as those that facilitate money lending or the sale or trading of securities or commodities (as opposed, for example, to smart contracts that merely facilitate the sale of

276. *See* Zetzsche, Arner, & Buckley, *supra* note 38, at 201–02 (proposing design-based safeguards that constrain risky DeFi activity before losses occur).

277. OECD, *supra* note 64, at 18.

278. *See supra* Part II.B (discussing the new risks that DeFi poses compared to traditional financial risks).

279. To the extent contracts individually may be problematic, consumer protection law may apply if consumers could be harmed. *See* Emilie K. Aguirre, Gina-Gail Fletcher & Veronica Root Martinez, *Profiting from Prediction*, __ CAL. L. REV. (forthcoming 2027). Consumer protection law would not, however, necessarily affect the ex ante architectural design of smart contracts.

goods).[280] As a matter of materiality, regulators should initially prioritize financially complicated smart contracts that have significant market activity or exposure or that can transmit losses through interconnection and common dependencies (including shared price feeds). In practice, regulators could focus first on DeFi platforms that (1) handle substantial transaction volume, (2) hold significant value, (3) serve large numbers of users, or (4) are closely connected to other protocols, instead of using a single transaction-size cutoff.[281]

1. Re-intermediating Responsible Parties

To re-intermediate responsible parties, regulators could require that parties who arrange or meaningfully enable the use of smart contracts be identified or at least identifiable. For example, regulators could require such parties to register centrally.

In practice, such identification should include but not necessarily be limited to individuals who program smart contracts. Such identification should also include any groups or other organizations for which those individuals act.[282] It may also need to extend, where relevant, to stablecoin issuers and cross-chain bridges that may supply leverage over access and execution.[283] In this context, regulators may wish to consider whether to limit parties arranging the use of smart contracts to responsible institutions. Congress has recently

280. *Cf.* Imad D. Abyad, Note, *Commercial Reasonableness in Karl Llewellyn's Uniform Commercial Code Jurisprudence*, 83 VA. L. REV. 429, 455 (1997) (observing that simple business transactions such as those involving the sale of goods "are peculiarly devoid of the use of experts in ascertaining commercial reasonableness").

281. Concentration evidence supports this kind of targeting. In an OECD sample of Uniswap v3 pools, between March 2021 and April 2023, 20% of pools accounted for 92.46% of trading volume among the pre-selected pools. *See* Iota Kaousar Nassr, Elefteria Kostika & Anastasia Melachrinos, *Concentration of DeFi's Liquidity: Evidence from Decentralised Exchanges (DEXs) and Automated Market Makers (AMMs)* 14–15 (OECD Working Papers on Finance, Insurance and Private Pensions No. 49, 2024), https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/04/concentration-of-defi-s-liquidity_5df1e8f9/4ed08440-en.pdf [https://perma.cc/CA3Y-8PLR].

282. That should include the application-tier and other access points through which users interact with protocols: front-end interfaces, application programming interfaces (APIs), and other operational touchpoints that are often hosted off-chain. *See Illicit Finance*, *supra* note 8, at 3, 8 (noting DeFi is often "not functionally decentralized" and defining the "application tier" as front-end user interfaces and APIs hosted primarily off-chain).

283. FIN. STABILITY BD., *supra* note 166, at 6 (discussing liquidity risks in stablecoins and lending protocols and identifying oracles and cross-chain bridges as DeFi-specific risks).

used a similar "permitted-entity" approach in the payment-stablecoin context.[284]

This registration approach is not intended to imply that all meaningful DeFi activity occurs at the application layer. As explained in Part I.B., DeFi operates across multiple layers, and sophisticated users may interact directly with protocol-layer smart contracts without using any particular front-end interface.[285] Registration requirements therefore should not turn on the layer that an actor sits. Instead, registration requirements should focus on whether the actor meaningfully controls, enables, or maintains access to covered financial activity. At the application layer, for example, the persons or entities that design, host, maintain, or materially control a web interface, mobile application, API, wallet integration, or other user-facing access point may be appropriate registration targets when their access point enables them to translate complex smart-contract interactions into executable user transactions.[286] Beyond the application layer, a lending protocol, for example, may be governed by developers or entities with upgrade authority, DAO participants exercising managerial control, stablecoin issuers with mint-and-redemption leverage, or bridge operators that facilitate the movement of assets across chains.[287] The relevant question in determining which actors require registration, then, is whether the actor has enough practical control over access, governance, deployment, maintenance, or execution to make registration a useful tool for monitoring risk and assigning responsibility.

A related problem would be identifying parties that fail to register. One possible solution would be to provide that such non-registering parties could not enforce their smart contracts.[288] For example, non-registering parties could not enforce repayment of loans and may have to return the purchase price of

284. *See* Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act, Pub. L. No. 119-27, 139 Stat. 419 (2025) (restricting stablecoin issuance to qualified nonbanks, state-qualified entities, or bank subsidiaries that are licensed under applications for Permitted Payment Stablecoin Issuers (PPSI) to ensure full reserves and other protections).

285. *See supra* notes 73–96 and accompanying text (describing DeFi's structure).

286. *See* IOSCO, *supra* note 69, at 1, 3 (describing the DeFi application layer as including front-end user interfaces through which users interact with protocols); *Illicit Finance*, *supra* note 8, at 8 (defining the "application tier" to include front-end user interfaces and APIs hosted primarily off-chain).

287. *See* FIN. STABILITY BD., *supra* note 166, at 1, 3, 18–19 (identifying stablecoins, oracles, and cross-chain bridges as sources of DeFi-specific risk); CFTC v. Ooki DAO, No. 3:22-CV-05416-WHO, 2023 WL 5321527 (N.D. Cal. June 8, 2023) (treating DAO governance as a basis for regulatory enforcement).

288. *Cf.* Investment Company Act of 1940 § 47(b)(1), 15 U.S.C. § 80a-46(b) (providing that any contract made or performed in violation of the Investment Company Act is unenforceable).

transferred securities and commodities. This approach would reduce the need for regulators to identify every non-registering party in advance by allowing the consequences of nonregistration to be enforced naturally in individual transactions and disputes.

2. Identifying Counterparties

It sometimes can be important to identify the counterparties to smart contracts. For example, a counterparty may become subject to liability because it breaches the contract, the contract may need modification because it fails to provide for a contingency, or the contract's underlying computer code may be defective or otherwise in error. For these purposes, the re-intermediating responsible parties should be required to maintain, and to make available as appropriate, a list of all counterparties.

This also could help to redress incentives for actors to take advantage of investors through excessive risk taking or fraudulent behavior, such as "rug pull" scams, in which DeFi developers disappear with funds raised after a token issuance, leaving investors with a worthless asset.[289] Victims at least should be able to sue identifiable parties for recourse.

3. Controlling Unchecked Automation

Controlling unchecked automation would need to start with monitoring. That raises at least three questions: (1) Who should monitor, (2) what should they monitor, and (3) what should they do if they see a problem?

To answer the first question: Presumably a government agency should monitor. That would be complicated for two reasons. The first reason has to do with the difficulties in monitoring cross-border smart contracts; these issues are discussed in Part II.C.3. The second reason has to do with the lack of personnel at regulatory agencies who are adept in reading the code underlying smart contracts.

Answering the second question would depend on what could be problematic. As a practical matter, monitoring presupposes legibility. Covered platforms (or major access points) should maintain a public inventory of core contract addresses (with versioning) and a basic change log for upgrades and parameter changes that affect execution risk.[290] For lending and securities or commodities transfers, the problems might include fraud, highly correlated collateral enforcement and/or liquidation, or risky initial conditions (such as

289. *See supra* note 190 and accompanying text (defining "rug pull" scams).

290. FIN. STABILITY BD., *supra* note 166, at 31 (discussing data transparency/consistency gaps in DeFi and calling for targeted public-sector approaches to enhance market transparency and risk monitoring).

the one-way-out lending conditions) that trigger smart-contract execution. Requiring pre-approval of smart contracts could help to mitigate these problems, though it could be expensive and awkward to operate.[291]

Monitoring for fraud may be especially difficult because fraud promoters try to hide their nefarious intentions and actions. For example, investors were unaware that Forsage's smart contracts were programmed to follow the fraudulent payout logic of a classic Ponzi scheme—diverting funds from later investors to pay earlier participants and siphoning a portion of the funds into the pockets of Forsage's founders.[292] It is unclear whether monitoring could have identified and halted this suspicious activity.

Answering the third question—what should monitors[293] do if they see a problem—would depend on the nature of the problem. For example, where liquidation is triggered by price information supplied by an oracle, monitors should have authority to pause or slow the process when the price appears distorted or when simultaneous liquidations threaten to produce a fire-sale spiral.[294] This would represent the equivalent of programming circuit breakers into smart contracts, which would parallel the use of circuit breakers in high-frequency trading markets. Circuit breakers have been needed in that context because advances in computing power allow parties to analyze market conditions and execute orders in fractions of a second[295]—effectively (somewhat

291. *Cf.* Omarova, *supra* note 228, at 66 (proposing ex ante regulatory control through "pre-market government licensing of complex financial instruments").

292. U.S. Dep't of Just., *supra* note 1.

293. One of us has written extensively about monitors—"(i) an independent, private outsider, (ii) employed after an institution is found to have engaged in wrongdoing, (iii) who effectuates remediation of the institution's misconduct, and (iv) provides information to outside actors about the status of the institution's remediation efforts." *See* Veronica Root Martinez, *Public Reporting of Monitorship Outcomes*, 136 HARV. L. REV. 757, 759 (2023). The use of the word monitors in this Article is unrelated to that strain of scholarship.

294. FIN. STABILITY BD., *supra* note 166, at 1–2, 23–24 (describing risks from automatic liquidation of collateral and noting that orderly liquidation mechanisms and market circuit breakers are generally absent in DeFi); *cf.* Zetzsche, Arner, & Buckley, *supra* note 38, at 202 (proposing supervisory modification of risk factors during system operation and technical restrictions that make certain conduct contingent on supervisory consent).

295. *See, e.g.*, James Chen, *Understanding High-Frequency Trading (HFT): Basics, Mechanics, and Example*, INVESTOPEDIA (last updated July 22, 2026), https://www.investopedia.com/terms/h/high-frequency-trading.asp [https://perma.cc/VNN7-YYXG]; Eric Budish, Peter Cramton & John Shim, *The High-Frequency Trading Arms Race: Frequent Batch Auctions as a Market Design Response*, 130 Q.J. ECON. 1547, 1548 (2015) (stating that "industry observers remarked that 3 milliseconds is an 'eternity' to high-frequency trading (HFT) firms").

like smart contracts) operating unchecked in real time[296] and, as a result of erroneous trades, causing substantial losses before being stopped.[297] Similar protections should be programmed into smart contracts.

A more general ex ante architectural constraint on smart contracts might be to incentivize limiting their use to contracts that are straightforward and unlikely to cause problems. As previously observed, experience will be needed to fully identify those contracts. The European Union has been using this type of approach to incentivize limiting potentially harmful applications of securitization, through its "STS" (simple, transparent, and standardized) regime.[298] We do not, however, appear to know enough at this time about DeFi and the risks of smart contracts to properly design such an analogous STS regime.

B. SMALL VS. LARGE FIRM ARCHITECTURE

Efforts to regulate DeFi platforms must be mindful of the differing risks that arise from large DeFi platforms versus small ones. As discussed above, for small DeFi platforms, microprudential regulation may not be appropriate but macroprudential regulation may be necessary to address the potential destabilizing impact of multiple, correlated failures of small DeFi platforms.[299] Thus, the regulatory architecture necessary to address the challenges and risks of DeFi should differ based on the risk profile of the platform, which may, in turn, depend on the size of the platform.

In financial regulation, size-differentiated regulation is neither novel nor controversial. A well-known example is bank regulation. The Office of the Comptroller of the Currency, one of several bank regulators, designates a bank as small if it has less than $1.6 billion in assets, and any bank so designated is

296. *See, e.g.*, Carol Clark, *Controlling Risk in a Lightning-Speed Trading Environment*, CHI. FED LETTER, Mar. 2010, https://www.chicagofed.org/publications/chicago-fed-letter/2010/march-272 [https://perma.cc/AC33-V87Q] (discussing the risks associated with high-speed trading).

297. *See id.*; *see also* Risk Management Controls for Brokers or Dealers with Market Access, 75 Fed. Reg. 69792, 69794 (Nov. 15, 2010) (to be codified at 17 C.F.R. pt. 240) (noting that because of the speed of high-frequency trading, a malfunctioning algorithm could enter $720 million worth of erroneous trades if there were a two-minute delay in detection). These advances in speed also can reduce liquidity in affected markets, raising the costs for other investors. Budish et al., *supra* note 295, at 1590 ("[A]ll of the expenditure by trading firms on speed technology . . . is ultimately borne by investors via the cost of liquidity . . . .").

298. *See supra* notes 229–230 and accompanying text (discussing the European Union's STS approach).

299. *See supra* Part II.C.1 (discussing the macro- and microprudential concerns of DeFi regulatory challenges).

subject to different examination procedures based on its size.[300] Examples of size-differentiated regulation are also evident in securities regulation. For example, companies classified as "smaller reporting companies" have less extensive disclosure obligations, including reduced extensive-narrative disclosures and fewer years of audited financial statements.[301]

Size-differentiated regulation has benefits for both regulators and market participants, especially in nascent markets like DeFi. Differentiated regulation allows resource-constrained regulators to tailor their focus based on the risk profiles of the firms they oversee.[302] Similarly, differentiated regulation lowers compliance costs for smaller, less complex entities, which in turn may facilitate greater innovation by lowering barriers to market entry.[303] As a new but still evolving area, DeFi platforms are well-suited for differentiated regulations to encourage innovation but ensure regulatory oversight based on the risks and complexity of the platforms' activities.

A precursor to promulgating differentiated regulations is the question of what makes a DeFi platform "small" versus "large." The distinction in size could be made in terms of the volume of transactions, the size of transactions, the number of consumers, or the number of interconnections between the platform and other financial institutions. Further, whatever metric is chosen to make size determinations of DeFi firms, data would be needed to determine where to draw the line. As such, more information on DeFi platforms—such

300. OFF. OF THE COMPTROLLER OF CURRENCY, OCC BULL. NO. 2025-48 COMMUNITY REINVESTMENT ACT: REVISION OF SMALL AND INTERMEDIATE SMALL BANK AND SAVINGS ASSOCIATION ASSET THRESHOLDS (2025), https://occ.gov/news-issuances/bulletins/2025/bulletin-2025-48.html [https://perma.cc/B5D9-C6TM].

301. *Smaller Reporting Companies*, U.S. SEC. & EXCH. COMM'N (July 12, 2024), https://www.sec.gov/resources-small-businesses/going-public/smaller-reporting-companies [https://perma.cc/CH8K-98PE].

302. *See Risk and Regulatory Policy: Improving the Governance of Risk*, OECD 16–17 (2010), https://www.oecd.org/content/dam/oecd/en/publications/reports/2010/04/risk-and-regulatory-policy_g1ghc5f1/9789264082939-en.pdf [https://perma.cc/S3DX-4TRD] (noting that a risk-based approach to regulation "should be proportionate, targeted and based on an assessment of the nature and magnitude of the risks" and that governments have "limited resources," so regulations can improve society through the "efficient allocation of regulatory resources").

303. *See* Joseph J. Cordes, Susan E. Dudley & Layvon Q. Washington, *Regulatory Compliance Burdens: Literature Review & Synthesis*, GEO. WASH. UNIV. REGUL. STUD. CTR. 1 (Oct. 2022), https://regulatorystudies.columbian.gwu.edu/sites/g/files/zaxdzs4751/files/2022-10/regulatory_compliance_burdens_litreview_synthesis_finalweb.pdf [https://perma.cc/4DBZ-5QDR] (stating that poorly designed regulations "can impose unnecessary administrative burdens as well as barriers to entry into the market of smaller and newer, more innovative, firms").

as transaction size and volume, users, and interconnections—would be needed to make size, and therefore risk, determinations from a regulatory standpoint. This disclosure will also facilitate updating the regulatory framework applicable to the platform as its size grows, thereby further fostering size-differentiated regulation of DeFi platforms.

This inquiry is especially difficult in DeFi because "size" may appear differently at different layers. At the application layer, a platform may look large because a widely used interface attracts significant user traffic. At the protocol layer, however, the more relevant measure may be total value locked, transaction volume, upgrade authority, or the number of other protocols that rely on the smart contract. At the asset layer, size may turn on the importance of a stablecoin or other token used as collateral across multiple platforms. And at the settlement layer, size may depend less on the platform's own users than on the extent to which it connects otherwise separate pools of liquidity. A workable size-differentiated framework therefore should not rely on any single firm-level measure.

To implement size differentiated regulation, a baseline level of disclosure is needed to determine the size, risk profile, operations, and governance structure of DeFi platforms. An oft-touted feature of DeFi platforms is that they provide transactional transparency, since each transaction is on the blockchain.[304] However, few can read and comprehend the underlying code, thereby reducing the benefits of transparency almost entirely.[305] Thus, at a minimum, DeFi platforms must make disclosures that clearly describe their smart contracts' functionality in a way that can be understood by users.[306]

Other minimum disclosures should include information on the platforms' risks, whether technological, operational, legal, or external. These risk disclosures serve a two-fold purpose—to force DeFi platform developers to consider the attendant risks of their products and to inform users and regulators of the ways in which the DeFi platform may fall short. Differentiated regulations would be useful in risk disclosure. Because the impact of failure or losses is greater at larger firms, large-firm risk disclosures cannot be taken at face value. Large-firm risk disclosures should be subject to third-party audit and verification to ensure accuracy and completeness. Small-firm risk disclosures, on the other hand, should be self-certified and possibly subject to third-party audit every two years.

304. Chris Brummer, *Disclosure, Dapps and DeFi*, 5 STAN. J. BLOCKCHAIN L. & POL'Y 137, 152 (2022).

305. Allen, *supra* note 160, at 936.

306. Brummer, *supra* note 304, at 153.

Disclosures would also be needed on the processes and procedures that are in place to address the identified risks, should they manifest. To date, this has proven to be a significant issue with DeFi platforms, particularly because the platforms lack a person or entity to address risks as they arise.[307] When there are failures or losses on DeFi platforms, some claim that the platforms' decentralized nature means that there is no one with the authority or capability to act.[308] However, few DeFi platforms are truly that decentralized. What is needed, instead, is the identification of persons or entities who can be held accountable for the platforms' failures. This may require identification of the developer or founder of the platform, or, if the platform has a DAO, the large token holders.

Relatedly, DeFi platforms, regardless of their size, must make public basic information on their ownership and governance structure. Many of the worst DeFi platform scams involved anonymous or pseudonymous founders. Forsage, once again, provides a key example in this regard. The founders operated the platform pseudonymously, allowing them to defraud victims of hundreds of millions of dollars.[309] Another example is the AnubisDAO rug pull, which occurred in 2021.[310] Within hours of launching, AnubisDAO raised almost $60 million.[311] But hours later, all the funds were withdrawn and siphoned to an "unknown Ethereum address."[312] To date, the anonymous developers of AnubisDAO have not been identified, no one has been charged for the scam, and investor funds have not been returned.[313]

Public identification of the founders of DeFi platforms, therefore, is crucial to imposing accountability for the risks, failures, and losses that may occur

307. *See The Crypto Ecosystem: Key Elements and Risks*, BANK FOR INT'L SETTLEMENTS 10 (July 2023) (discussing how DeFi platforms must rely on third party oracles to import data into blockchains, which centralizes the system, overrides the reliance on consensus, and introduces a central point of failure); *cf.* Zetzsche, Arner, & Buckley, *supra* note 38, at 184–87 (discussing the difficulties that DeFi creates for entity-based regulation).

308. *See* Gogel, *supra* note 8, at 6 (contending that because of the governance structure of DeFi, no one has "special power to countermand" decisions).

309. U.S. Dep't of Just., *supra* note 1.

310. David Yaffe-Bellany, *Millions for Crypto Start-Ups, No Real Names Necessary*, N.Y. TIMES (Mar. 2, 2022), https://www.nytimes.com/2022/03/02/technology/cryptocurrency-anonymity-alarm.html [https://perma.cc/2VUY-8RRE].

311. Bitcoinworld, *AnubisDAO Rug Pull Back After Nearly 3 Years with Suspicious Transactions*, BINANCE SQUARE (Aug. 11, 2024), https://www.binance.com/en-ZA/square/post/12028514221577 [https://perma.cc/85CZ-BX4U].

312. *Id.*

313. *Id.*

because of the platforms' shortcomings. Similarly, it is also important for there to be disclosure of other key players who may have a significant impact on the governance of the platform. This would include, for example, any persons or entities with control rights, decision-making authority, significant ownership of governance tokens, and/or emergency authority (such as the authority to override the platforms' operations).

Disclosures on the governance structure of the platforms would also be important for those platforms that claim to be operating as a DAO and, therefore, are truly decentralized. However, research suggests that having some elements of decentralization, even without being fully decentralized, is associated with higher capitalization.[314] This incentivizes DeFi platforms to be community-governed through DAOs, but in reality, the founder or large-token holders may still be able to make decisions without community input. For example, after suffering a significant loss in asset value when it was revealed that the pseudonymous chief financial officer of Wonderland DAO was a convicted felon, the founder of the platform proposed to wind down the project.[315] The proposal was rejected by fifty-five percent of the users voting; regardless, the founder decided to shut down the project, overriding the vote of a majority of users.[316]

In sum, disclosures are necessary to address many of the attendant risks of DeFi platforms and to protect users and the broader markets from the risks that arise from the platforms.[317] Importantly, there is a minimum level of information that all DeFi platforms must provide to create a threshold level of accountability: ownership and governance information. This also requires a regulatory stance against DeFi founders being anonymous and pseudonymous given the higher likelihood of fraud with such platforms. Beyond this baseline, however, other disclosures should be differentiated based on the size of the DeFi platform. Given their potential impact on the broader markets, these disclosures should be more onerous for large firms, requiring third-party verification and more extensive oversight. For small firms, however, third-party verification, to the extent it is needed, should be biennial to reduce the compliance and regulatory burden of disclosures for early-stage firms. At this time,

314. Yan Chen, Jack I. Richter & Pankaj C. Patel, *Decentralized Governance of Digital Platforms*, 47 J. MGMT. 1305, 1307 (2021).

315. Prashant Jha, *Wonderland's Treasury Saga Exposes the Fragility of DAO Projects Today*, COINTELEGRAPH (Feb. 8, 2022), https://cointelegraph.com/news/wonderland-s-treasury-saga-exposes-the-fragility-of-dao-projects-today [https://perma.cc/T83L-KRFV].

316. *Id.*

317. *Cf.* Zetzsche, Arner, & Buckley, *supra* note 38, at 202–03 (discussing the importance of disclosure and transparency to address DeFi risks).

however, more information would be needed to know where to draw the line between a large firm versus a small firm and to fully assess the risks that come with various sizes of DeFi platforms.

C. EX POST ENFORCEMENT & MULTIJURISDICTIONAL ACCOUNTABILITY

Embedded compliance mechanisms are necessary but not sufficient to regulate DeFi systems. Architectural safeguards via compliance requirements will not, on their own, deter intentional misconduct or prevent the strategic evasion of legal and regulatory requirements. As the International Organization of Securities Commissions (IOSCO) has emphasized, DeFi firms magnify the risk of misconduct absent effective substitutes for traditional financial intermediaries.[318] To create incentives for the adoption of compliance protocols, however, firms often need external pressure as motivation.[319] Enforcement therefore plays an indispensable role not merely by punishing violations ex post, but by reshaping incentives ex ante due to the threat of enforcement activity.[320] Importantly, sufficiently designed external enforcement strategies can serve to motivate firms to consider how to carefully craft the design and implementation of their internal compliance programs.[321]

A 2025 enforcement action against Exodus, a Delaware-incorporated financial technology company, illustrates this point.[322] Exodus operated a non-custodial wallet that did not itself execute transactions.[323] One of its exchange partners used IP-address blocking to prevent users in Iran from accessing its services, but Exodus customer-support personnel nevertheless advised users to use Virtual Private Networks (VPNs) to mask their location and regain access.[324] The Exodus action shows that technical restrictions (from either regulators or the firm itself) may not be sufficient if individuals remain able to help

318. IOSCO, *supra* note 69, at 36.

319. *See* Veronica Root Martinez, *Purpose-Driven Compliance*, 13 TEX. A&M L. REV. 1349, 1358, 1361–64 (2026) (explaining that external enforcement incentives have encouraged firms to create and implement compliance programs and that, absent the threat of sanctions, firms may lack sufficient incentives to engage in effective self-policing).

320. *Id.*

321. *See* Veronica Root, *Coordinating Compliance Incentives*, 102 CORNELL L. REV. 1003, 1009–10 (2017) (arguing that coordinated enforcement strategies can increase firms' incentives to undertake systematic revisions and implement more robust compliance programs).

322. Off. of Foreign Assets Control, *Settlement Agreement*, U.S. DEP'T OF THE TREASURY (Dec. 16, 2025), https://ofac.treasury.gov/media/934836/download?inline [https://perma.cc/LTL4-3R5D] (finding willful and reckless evasion of sanctions controls through operational practices and requiring enhanced compliance commitments).

323. *Id.*

324. *Id.*

users get around them. This reality makes enforcement efforts necessary to effectively deter deliberate evasion of legal and regulatory requirements.

1. Enforcement Priorities by Actor

Enforcement should turn on what an actor can actually do—such as whether the actor can modify the DeFi system's code, control access to the system, manage the system interface, or influence the DeFi system's governance—rather than on whether the platform describes itself as decentralized, non-custodial, or autonomous. In practice, this likely includes at least three categories of participants.

First, regulators should target platform developers and DeFi firms with ongoing control or upgrade authority over DeFi systems, including the ability to modify protocol code, hold or use administrative keys, change transaction or risk parameters, control treasury assets, or direct governance decisions. The CFTC's actions against Opyn and Deridex, discussed above, exemplify this approach.[325] In those actions, the protocols relied on smart contracts, but enforcement authorities focused on the corporate entities that designed, deployed, and continued to operate systems offering unregistered derivatives.[326]

Second, enforcement authorities should focus on DeFi actors who use their voting rights to make decisions about a protocol's operations. In the CFTC's enforcement action against Ooki DAO, for example, token holders could vote to change the protocol, authorize expenditures from the DAO treasury, and direct other aspects of its operation.[327] The CFTC treated token holders who actually participated in those votes as members of the Ooki DAO

325. *See generally* Order Instituting Proceedings Pursuant to Section 6(c) and (d) of the Commodity Exchange Act, Making Findings, and Imposing Remedial Sanctions, *In re* Opyn, Inc., CFTC No. 23-40 (Sep. 7, 2023); Order Instituting Proceedings Pursuant to Section 6(c) and (d) of the Commodity Exchange Act, Making Findings, and Imposing Remedial Sanctions, *In re* Deridex, Inc., CFTC No. 23-42 (Sep. 7, 2023).

326. *Id.*; *see also* Order Instituting Proceedings Pursuant to Section 6(c) and (d) of the Commodity Exchange Act, Making Findings, and Imposing Remedial Sanctions at 7, *In re* ZeroEx, Inc., CFTC No. 23-41 (Sep. 7, 2023) (illustrating the enforcement approach of targeting entities with control over systems offering unregistered derivatives).

327. Order Instituting Proceedings Pursuant to Section 6(c) and (d) of the Commodity Exchange Act, Making Findings, and Imposing Remedial Sanctions at 9–10, *In re* bZeroX, LLC, CFTC No. 22-31 (Sep. 22, 2022) (holding that Ooki DAO is a "'voluntary group of persons' (Ooki Token holders who voluntarily vote their Ooki Tokens), 'without a charter' (no Ooki DAO corporate charter exists), 'formed by mutual consent for the purpose of promoting a common objective' (Ooki Token holders who voluntarily vote for the purpose of promoting the common objective of governing the Ooki Protocol)").

instead of treating governance-token ownership alone as sufficient to trigger enforcement efforts.[328]

Third, regulators should pursue service providers that knowingly help users evade legal restrictions, even when those providers do not hold customer assets or process transactions. OFAC's settlement with Exodus, again, provides a valuable example.[329] When Exodus's customer-support personnel advised individuals from countries where U.S. sanctions were in place on how to access the platform, they knowingly facilitated the evasion of current legal restrictions.[330] The relevant question is, therefore, not whether a provider takes custody of customer assets—which might trigger different methods of gamesmanship to remain outside the crosshairs of enforcement authorities—but whether a service provider's conduct helps users circumvent legal restrictions.

2. Coordinated, Multijurisdictional Enforcement

Because DeFi utilizes smart contract technology, thereby executing transactions at rapid speed in an essentially borderless environment, it is unlikely that enforcement activity will be effective unless it mirrors these qualities. DeFi systems can be deployed, modified, and abandoned in a matter of days—or hours—while funds may move through multiple jurisdictions before any single regulator has sufficient information to respond.[331] Country-by-country enforcement, developed slowly over time, is unlikely to be effective given the realities of DeFi and its underlying technological innovations. Effective DeFi enforcement therefore depends on regulators sharing information quickly across jurisdictions, identifying the actors responsible for DeFi systems, and acting before assets are moved or the related protocol or platform is abandoned.[332]

This is not an entirely novel institutional challenge. Over the past two decades, enforcement authorities have built the relationships and capacities needed for this sort of coordination, specifically in areas related to transnational misconduct.[333] As Professor Rachel Brewster documents, Foreign

328. *See id.* at 9–11 (concluding that token holders who used their tokens to participate in governance were members of the Ooki DAO unincorporated association).

329. Off. of Foreign Assets Control, *supra* note 322.

330. *Id.*

331. *See Illicit Finance*, *supra* note 8, at 29 (explaining that "the nearly instantaneous and borderless nature of virtual asset transfers" present regulatory challenges).

332. *Cf.* Zetzsche, Arner, & Buckley, *supra* note 38, at 193–94, 202 (discussing the need for collaboration among supervisory authorities in different countries to address jurisdictional and enforcement problems).

333. *See* Steve Kwok, Bora P. Rawcliffe & Margot Sève, *Cross-Border Enforcement Priorities and Increased Cooperation Come into Focus*, SKADDEN (Jan. 13, 2026),

Corrupt Practices Act (FCPA) enforcement has shifted from unilateral, state action by one primary enforcement authority toward coordinated global settlements, in which multiple countries' enforcement authorities share information and investigative efforts, negotiate resolution outcomes with the target firm and, even, share monetary penalties extracted from sanctioned firms.[334] This model—described by her as "coordinated comity"—has allowed regulators and enforcement authorities worldwide to move more quickly and prevent regulatory arbitrage by ensuring that firms cannot exploit gaps between national systems.[335] Organisation for Economic Co-operation and Development (OECD) member countries have reinforced this shift by promoting information-sharing frameworks and peer-based capacity building among enforcement authorities.[336] DeFi enforcement should build on these sorts of existing relationships and infrastructures. Cross-jurisdictional task forces focused specifically on DeFi—integrating financial regulators, sanctions authorities, and civil and criminal enforcement activity—would allow multijurisdictional enforcement to occur in a manner more on par with the technology DeFi relies upon.[337]

Importantly, regulators and enforcement authorities already cooperate across borders in areas beyond anticorruption. Over the past two decades, they have developed mechanisms for sharing information, coordinating investigations, and pursuing misconduct that crosses national borders—many of which

https://www.skadden.com/insights/publications/2026/2026-insights/litigation-controversy/cross-border-enforcement-priorities [https://perma.cc/EA3Z-XUHL] (noting that "enforcement authorities and regulators . . . [are] pursuing cross-border cases with greater speed, consistency and operational alignment").

334. Rachel Brewster, *The Rise of Global FCPA Settlements*, 104 TEX. L. REV. 299, 301–05, 354–57 (2025).

335. *Id.* at 354–57 (describing the shift from negative comity to coordinated comity through parallel investigations and settlements).

336. *See Convention on Combating Bribery of Foreign Public Officials in International Business Transactions*, OECD 3 (2025), https://legalinstruments.oecd.org/public/doc/205/205.en.pdf [https://perma.cc/EKQ8-R93Y] ("The Convention . . . establishes an open-ended, peer-driven monitoring mechanism to ensure the thorough implementation of the international obligations."); *Governments' Assessments of Corporate Anti-Corruption Compliance*, OECD 7–8 (2025), [hereinafter *Governments' Assessments*] https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/03/governments-assessments-of-corporate-anti-corruption-compliance_6100e758/e798903c-en.pdf [https://perma.cc/D93C-GK2D] (explaining that governments should "engage with and learn from the private sector" when assessing anti-corruption compliance programs).

337. Zetzsche, Arner, & Buckley, *supra* note 38, at 194 (proposing working groups and a global cooperation framework to monitor and supervise DeFi).

could also be used in DeFi enforcement. For example, IOSCO provides an established forum for coordination around market integrity, trading misconduct, and crypto-asset market oversight;[338] the Financial Action Task Force (FATF) has built robust mechanisms for aligning AML/CFT standards, risk typologies, and enforcement expectations across jurisdictions;[339] and the International Monetary Fund (IMF) and Financial Stability Board (FSB) coordinate surveillance and policy responses to cross-border threats to financial stability. [340] Additionally, bilateral and multilateral enforcement cooperation—through memoranda of understanding, joint investigations, and parallel proceedings—have become routine in legal and regulatory areas that implicate the health and safety of the financial markets.[341] The challenge in achieving greater multijurisdictional DeFi enforcement activity, then, is not the absence of ways to coordinate across borders. It is that enforcement mechanisms must be adapted—and, where necessary, supplemented—to respond to risks that move quickly, cross borders, or require technical expertise from governmental enforcement actors.

An effective multijurisdictional enforcement strategy need not create a new enforcement structure or require new legal authority for DeFi. Enforcement authorities can instead build upon existing mechanisms for cross-border investigation and enforcement while investing in the technical expertise and coordination needed to make those mechanisms effective in DeFi markets. These might include investments in rapid information-sharing channels among regulators; the development of common typologies identifying DeFi-specific risks, governance structures, and modes of evading detection; and coordinated remediation expectations and sanctions activity.[342] Just as traditional financial intermediaries historically supplied market discipline, stability, and screening through private ordering, public enforcement authorities must use their

338. IOSCO, *supra* note 69, at 6–10, 36–38 (describing IOSCO's role in coordinating regulatory responses to market integrity risks posed by DeFi).

339. *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FIN. ACTION TASK FORCE 7–12, 55–60 (Oct. 2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated
-Guidance-VA-VASP.pdf [https://perma.cc/XXK2-ACSN]; *see also Governments' Assessments*, *supra* note 336, at 7–9, 42–44 (describing FATF-based coordination, shared typologies, and cross-border alignment of enforcement expectations).

340. *Governments' Assessments*, *supra* note 336, at 32–41 (discussing IMF- and FSB-linked coordination, peer learning, and cross-jurisdictional supervisory capacity-building).

341. Brewster, *supra* note 334, at 318, 354–57 (documenting the normalization of parallel proceedings, information sharing, and coordinated resolutions across jurisdictions).

342. IOSCO, *supra* note 69, at 38–42 (emphasizing shared risk typologies); *Governments' Assessments, supra* note 336, at 38–44 (describing mutual learning, coordinated tools, and enforcement alignment as collective goods).

collective "sticks" to incentivize DeFi systems and operators to internalize compliance systems and internal controls that will replicate important features of intermediation.

From a political economy perspective, coordinated and rapid DeFi enforcement should be attractive across administrations with divergent regulatory philosophies. An administration that prioritizes executive authority and national security—priorities often associated with the Trump administration[343]—may find multijurisdictional enforcement to be useful. For instance, multijurisdictional enforcement efforts may allow regulators to respond quickly to potential misconduct without requiring (1) congressional intervention via the enactment of new legislation or (2) agencies to engage in time-intensive notice-and-comment rulemaking. At the same time, multijurisdictional coordination may advance the traditional goals of improved consumer protection, market integrity, and financial stability—objectives that have often received greater emphasis under administrations that favor an active role for financial regulators.

The upshot is that domestic regulatory regimes will remain vulnerable to regulatory arbitrage when DeFi activity can be shifted into another jurisdiction without materially changing the underlying transactions. As a result, multijurisdictional enforcement is necessary both to prevent actors from evading enforcement and to ensure that enforcement authorities have a mechanism for following the persons or firms in control of the DeFi system at issue.

* * *

In short, embedded compliance and coordinated enforcement can help to preserve the stabilizing functions historically supplied by financial intermediaries without requiring a return to traditional institutional gatekeepers.

IV. ADDITIONAL QUESTIONS & CONCERNS

Part IV addresses a set of broader questions and concerns that naturally follow from the argument and normative proposals put forth in Part III. It considers whether DeFi's potential public benefits weigh against the regulatory interventions proposed here, whether collective action and public-private partnerships can address some of the same problems, and whether regulators have the capacity to implement the proposed approach.

343. *See* Shay Dvoretzky & Parker Rider-Longmaid, *Overview of Trump's Executive Actions and Considerations for Potential Litigation*, SKADDEN (Feb. 3, 2025), https://www.skadden.com/insights/publications/executive-briefing/
overview-of-trumps-executive-actions [https://perma.cc/R5RG-8JCN] (highlighting that "[t]he Trump administration has taken, and continues to take, executive actions" that are "in connection with . . . national security").

A. DEFI—A PUBLIC GOOD?

This Article argues in favor of embedding compliance constraints into smart contracts and coordinated cross-border enforcement. One may be concerned, however, that decentralized finance itself constitutes a public good, which would be placed at risk by the compliance and regulatory interventions proposed here. Proponents of DeFi believe that its defining characteristics—permissionless access, open-source development, composability, and the ability to transact without reliance on centralized intermediaries—generate social value that extends beyond any particular platform or transaction.[344] On this view, disintermediation is a benefit, as outlined above. Some may analogize DeFi's innovations in financial transactions to the disruption caused by early internet protocols and other forms of open-source digital infrastructure. Scholars believe these technologies are important, in part, because they (1) can be used by many participants at once, (2) allow developers and users to build new applications on existing infrastructure, and (3) may lower barriers to entry, which may support future advances in innovation.[345] Under this perspective, DeFi systems are less like discrete financial products and more like a commons-like infrastructure that developers and users can build and experiment on in ways that would be difficult for a single firm to plan or control in advance.[346]

Scholars, policymakers, and industry leaders who advance the above view—or those similar—may have concerns that interventions aimed at requiring or incentivizing compliance systems[347] may chill innovation, deter open-source development, and reintroduce the very forms of centralized control that decentralization was purposefully meant to displace.[348] Critics may

344. *See, e.g.*, Brummer, *supra* note 304, at 141 (describing DeFi as an open, protocol-based ecosystem designed to reduce reliance on centralized intermediaries); Reyes, *Detrimental Reliance*, *supra* note 35, at 1348–49 (arguing that decentralization can supply social value by reducing law's dependence on centralized gatekeepers).

345. *See, e.g.*, Jan Krewer & Zuzanna Warso, *Digital Commons as Providers of Public Digital Infrastructure*, OPEN FUTURE (Jun. 30, 2024), https://openfuture.pubpub.org/pub/digital-commons-public-digital-infra/release/2 [https://perma.cc/5JEY-PYEJ] (describing a commons-like infrastructure provider).

346. *See* Reyes & Cutler, *supra* note 35, at 10–18 (arguing that open-source blockchain protocols function as digital infrastructure and should be regulated functionally instead of institutionally).

347. Arguments against building enforcement capacity to stop misconduct and to protect consumers from harm seem less plausible or genuine.

348. *See* Reyes, *(Un)Corporate*, *supra* note 35, at 1879–80 (warning that imposing ill-fitting legal obligations on open-source developers risks chilling participation and innovation); *cf.* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 86–90 (1999) (discussing how regulation through architecture may entrench power and reshape systems).

therefore worry that more exacting regulatory and compliance requirements would push DeFi toward a more permissioned model, limiting the experimentation that decentralization makes possible even when its broader benefits may not be apparent for some time.[349]

This objection, however, rests on an incomplete account of both DeFi's benefits and its risks. As Part II demonstrates, DeFi creates new opportunities for decentralized experimentation, but it also introduces new risks and revives (or replicates) old risks that traditional financial regulation addresses.[350] Unlike early internet protocols, which primarily facilitated communication and information exchange, DeFi transactions directly implicate the financial markets. As this Article explains above, DeFi systems perform core financial functions—credit creation, trading, custody, and payments—that directly impact confidence in the financial system.[351]

History shows that when financial innovation develops faster than regulators can respond, private actors may capture a range of benefits while the broader public ultimately bears the costs when markets fail.[352] The years preceding the Global Financial Crisis provide a familiar example: Financial innovation developed faster than regulators could understand and respond to the risks, and the consequences became clear only after those risks had spread through the financial system.[353] Even if DeFi produces benefits that extend beyond individual platforms or users, that does not mean the costs of its failures should be borne by investors or the broader financial system. The overarching goal should be to determine how governmental intervention can

349. *See* Georg Lorenz, *Regulating Decentralized Financial Technology: A Qualitative Study on the Challenges of Regulating DeFi with a Focus on Embedded Supervision*, 7 STAN. J. BLOCKCHAIN L. & POL'Y 136, 227 (2024) (noting that a misaligned regulation of DeFi could deter innovation).

350. *See supra* Part II (explaining how the architecture of DeFi lends to traditional financial risks as well as new risks).

351. Fin. Stability Oversight Council, *Report on Digital Asset Financial Stability Risks and Regulation*, U.S. DEP'T OF TREAS. 10–15 (2022), https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf [https://perma.cc/VR3Y-CL2Q].

352. *See* Michael Barr, *Ending "Too Big to Fail"*, BROOKINGS INST. (June 14, 2011), https://www.brookings.edu/articles/ending-too-big-to-fail [https://perma.cc/4V6H-2PFH] (discussing the 2008 Financial Crisis and stating that "[f]inancial innovation often outpaced the capacity of managers, regulators and markets to understand new risks and adjust").

353. *Id.*

preserve the benefits DeFi may provide while reducing its potential financial risks.[354]

B. COLLECTIVE ACTION AND PUBLIC-PRIVATE PARTNERSHIPS

Another question is whether collective action or public-private partnerships should play a larger role in addressing DeFi's risks. Experience in anticorruption, financial crime, and corporate compliance suggests that these sorts of efforts can be quite effective.[355] For example, firms and regulators have used private-public partnerships to share information, develop common standards, and identify mechanisms to detect potential misconduct.[356] These approaches draw on "new governance" scholarship, which emphasizes regulatory strategies combining public oversight with private participation, instead of relying on top-down command-and-control regulation.[357] Recent work on collaborative compliance similarly documents how firms facing similar or shared regulatory risks often benefit from working together in an effort to share expertise and reduce duplicative compliance costs.[358]

Indeed, reliance on efforts like collective action groups or similar approaches is often considered useful where misconduct crosses borders or is difficult for a single regulator or firm to detect, as is often true in DeFi.[359] Anticorruption efforts coordinated through the OECD provide one example, combining private-sector compliance efforts with government guidance,

354. *See* Zetzsche, Arner, & Buckley, *supra* note 38, at 201, 203 (arguing that government intervention may be necessary to achieve DeFi's objectives of democratization and decentralization while addressing concentration and financial risks).

355. *See, e.g.*, Mark Pieth, *Collective Action and Corruption* 5–6 (Basel Inst. on Governance, Working Paper No. 13, 2012) (describing collective action as a response to diffuse and systemic corruption); *Collective Action*, BASEL INST. ON GOVERNANCE, https://collective-action.com [https://perma.cc/2U55-98WV] (documenting industry-government anticorruption initiatives).

356. *See id.*

357. *See generally* Orly Lobel, *New Governance as Regulatory Governance*, *in* THE OXFORD HANDBOOK OF GOVERNANCE (David Levi-Faur ed., 2012) (describing public–private collaboration as a regulatory alternative to command-and-control).

358. *See, e.g.*, Kevin E. Davis & Veronica Root Martinez, *Collaborative Compliance*, UC L.J. (forthcoming 2027) (documenting benefits and limits of inter-firm compliance collaboration).

359. *See, e.g.*, *Companies' Assessments of Anti-Corruption Compliance*, OECD 3 (2025), https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/03/companies-assessments-of-anti-corruption-compliance_363b6821/977ed5a8-en.pdf [https://perma.cc/PMH6-UJNB] (describing how the public and private sectors can collectively combat corruption); *Governments' Assessments*, *supra* note 336, at 32–38 (emphasizing collective action, peer learning, and public-private engagement as complements to enforcement).

monitoring, and enforcement.[360] At the same time, the experience of these regimes suggests an important precondition: Collective action and public-private partnerships tend to function effectively only once governments have developed sufficient regulatory capacity, agree on basic standards and expectations, and demonstrate a willingness to initiate enforcement activity to enforce those established requirements. Collective actions focused on the risks and benefits of DeFi may ultimately be useful, but they would not serve as effective substitutes for clear legal and regulatory guidance.

C. ADMINISTRATIVE FEASIBILITY AND CAPACITY CONSTRAINTS

A separate question is whether regulators can actually do what this Article asks of them. Requiring compliance to be built into DeFi protocols and platforms will present an enormous challenge given that they are both diffuse and interconnected. Moreover, coordinating enforcement across jurisdictions will require significant allocations of resources (time, money, and people) and technical expertise. Agencies will need personnel with certain technical proficiencies, including in how smart contracts function, how protocol governance works in practice, and the ways transactions move across DeFi systems. They will also need to determine which agencies should act when several domestic regulators have authority over the same conduct. Regulators will also need to determine the best methods of coordination with regulators and enforcement authorities in other countries. If agencies lack the necessary personnel, technical knowledge, or ability to work with one another, the proposals outlined here may prove difficult to implement in practice.

This concern is real, but suggests the importance of governments prioritizing efforts toward early capacity building instead of a strategy of regulatory restraint. This Article concedes that regulators will need to learn more about DeFi systems prior to developing a robust set of ex ante regulatory constraints.[361] As Part III explains, coordinated enforcement and, hopefully, accountability are likely to be most effective when regulators establish shared baselines, common typologies of risk, and delegated focal points of responsibility before DeFi markets rise to the level of systemic importance.[362] Multiple examples—from shadow banking oversight to anticorruption enforcement—demonstrate that regulators often develop technical expertise as new risks and innovations within the market emerge via tools like specialized task forces,

360. *See* sources cited *supra* note 359 and accompanying text.

361. *See supra* Part II.C.1 (discussing the challenges regarding DeFi system regulation).

362. *See supra* Part III (setting forth a solution based on targeted compliance and enforcement).

interagency coordination, and international standard-setting bodies.[363] Regulators across the globe should focus on how to build the institutional capacity necessary to properly oversee DeFi before decentralized markets grow large enough to pose broader risks to financial stability.

CONCLUSION

Decentralized finance poses significant challenges for regulators and policymakers because it purposefully moves away from the regulatory and compliance architecture through which financial transactions have historically operated. By disaggregating the functions of banks, broker-dealers, exchanges, and other intermediaries into smart contracts and dispersed governance structures, DeFi diminishes the role of financial intermediaries that have traditionally supported market discipline, implemented consumer-protection safeguards, and served as key points of regulatory and systemic oversight. This Article argues that because DeFi platforms disaggregate traditional intermediary functions, effective regulation must focus on (1) embedding compliance safeguards directly into platform design and (2) holding accountable the actors who build, operate, and maintain those platforms. Recognizing that DeFi activity is inherently borderless, effective interventions cannot succeed without coordinated, multijurisdictional enforcement capable of operating at a speed and scale commensurate with DeFi and the underlying technologies it exploits and builds upon.

This Article makes three principal contributions to legal scholarship. First, it puts forth an account of DeFi's risks, showing how familiar financial vulnerabilities—excessive leverage, maturity transformation, information asymmetry, and illicit-finance risk—are amplified by automation, composability, pseudonymity, and cross-border execution. Second, it explains why effective DeFi regulation should focus less on restoring traditional intermediaries and more on preserving the functions those intermediaries historically performed. Third, it advances a regulatory framework that pairs ex ante architectural constraints that embed compliance requirements on DeFi systems with external, multijurisdictional enforcement efforts. The goal is not to eliminate DeFi's capacity for innovation, but to ensure that such innovation develops in a manner that does not put the financial markets at risk from unnecessary harm.

363. *See supra* notes 269–272 and accompanying text (discussing anticorruption enforcement); *see also Shadow Banking: Strengthening Oversight and Regulation*, FIN. STABILITY BD. (Oct. 27, 2011), https://www.fsb.org/uploads/r_111027a.pdf [https://perma.cc/Z6XS-5GRZ] (discussing shadow banking oversight).

APPENDIX

- **Algorithm:** A sequence of programmed steps embedded in smart contracts that directs the automatic execution of specified financial functions, such as lending, trading, collateral liquidation, or asset transfer, without the exercise of human discretion at the time of execution.
- **Architectural Constraints:** Ex ante design features embedded into DeFi platforms or smart contracts that are intended to slow, channel, limit, or pause automated activity in order to mitigate concerns like systemic risk, fraud, or market instability.
- **Composability:** The ability of smart contracts and DeFi protocols to interoperate with, build upon, or integrate the functionality of other smart contracts or protocols, enabling complex, multi-step financial transactions. Composability can amplify the potential for cascading failures within the financial markets.
- **Decentralized Autonomous Organization (DAO):** A governance structure used in decentralized finance where decision-making authority is exercised through token-based voting or other on-chain mechanisms instead of through a centralized, identifiable corporate entity. The identity of those operating a DAO can be difficult to ascertain.
- **Decentralized Finance (DeFi):** A system of financial activities—including lending, trading, derivatives, payments, and asset management—conducted through smart contracts on blockchain networks without reliance on traditional financial intermediaries such as banks, broker-dealers, or exchanges.
- **DeFi Matrix Project:** This term is sometimes used as a synonym for a platform. For example, the Internet sometimes defines Forsage as a "DeFi matrix project," whereas Forsage in particular, and DeFi matrix projects in general, are more simply platforms. The term "DeFi matrix" is also sometimes used as a conceptual expression to refer to the interconnected ecosystem of various DeFi platforms.
- **Embedded Compliance:** Compliance requirements and mechanisms implemented directly into the design and operation of DeFi platforms or smart contracts.
- **Ex Ante Regulation:** Regulatory intervention that operates before harm occurs, including disclosure requirements or structural safeguards intended to prevent or mitigate risk or misconduct in advance.
- **Ex Post Regulation:** Regulatory intervention that operates after misconduct or harm has occurred, including enforcement actions, penalties, liability, and remedial measures.

- **Flash Loan:** A DeFi transaction that allows a user to borrow large amounts of digital assets without posting collateral, provided that the loan is borrowed and repaid within a single blockchain transaction. Flash loans create opportunities for arbitrage, exploitation, and a number of other risks.
- **Governance Token:** A digital asset that confers voting or governance rights within a DeFi platform or DAO, often allowing holders to propose, approve, or veto changes to protocol rules, upgrades, or treasury management.
- **Macroprudential Regulation:** Regulation designed to protect the stability of the financial system as a whole by identifying, monitoring, and mitigating systemic risks that can arise from interconnected markets, correlated failures, or widespread leverage.
- **Microprudential Regulation:** Regulation designed to protect the safety and soundness of individual firms or market participants, typically by reducing the likelihood of firm-level failure and protecting investors and counterparties.
- **One-Way-Out Lending:** A lending model where repayment depends solely on the liquidation value of posted collateral, instead of on both collateral and borrower cash flow. One-way-out lending may increase vulnerability to asset price declines and systemic instability.
- **Permissionless:** A characteristic of DeFi platforms that allows users to participate, transact, or deploy smart contracts without obtaining prior approval from a centralized authority, intermediary, or gatekeeper.
- **Platform:** A DeFi-based business organization or system—such as Forsage—that uses smart contracts to provide financial services, often combining on-chain code with off-chain components such as user interfaces, governance processes, or support functions.
- **Protocol or Protocols:** The rules, logic, and instructions encoded into smart contracts that govern how a DeFi platform operates, including transaction execution, risk parameters, and governance processes; the term is distinct from the platform as a whole.
- **Pseudonymity:** Participants in DeFi transact through persistent digital identifiers, such as blockchain addresses, that are publicly visible but not directly linked to real-world legal identities.
- **Self-Custody:** Holding digital assets in a way that enables one who controls private keys to access and transfer those assets.
- **Shadow Banking (as applied to DeFi):** The performance of bank-like functions—such as credit creation, liquidity provision, and maturity transformation—outside the traditional banking regulatory perimeter; in DeFi accomplished through smart contracts instead of balance-sheet intermediaries.

• **Smart Contract:** A self-executing computer program, often deployed on a blockchain, that automatically performs predefined actions when specified conditions are met, typically without the ability to pause, reinterpret, or exercise discretionary judgment once deployed.

european corporate governance institute

About ECGI

ECGI is an international non-profit membership organisation that provides a platform for debate and dialogue among academics, policymakers, and business leaders, with a focus on major corporate governance, ESG, and stewardship issues.

The views expressed in this working paper are those of the authors, not those of the ECGI or its members.

www.ecgi.global

european corporate governance institute

ECGI Working Paper Series in Law

Editorial Board

Editor	**Amir Licht,** Professor of Law, Harry Radzyner Law School, Reichman University
Consulting Editors	**Hse-Yu Iris Chiu,** Professor of Corporate Law and Financial Regulation, University College London **Martin Gelter,** Professor of Law, Fordham University School of Law **Geneviève Helleringer,** Professor of Law, ESCP and Oxford Law Faculty **Kathryn Judge,** Professor of Law, Columbia Law School **Wolf-Georg Ringe,** Professor of Law & Finance, University of Hamburg
Series Manager	**Asif Malik,** ECGI Working Paper Series Manager

https://www.ecgi.global/publications/working-papers