

Regulating DeFi Platforms

Law Working Paper N° 937/2026

June 2026

Gina-Gail S. Fletcher

Duke University and ECGI

Veronica Root Martinez

Duke University and ECGI

Steven L. Schwarcz

Duke University

© 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:
http://ssrn.com/abstract_id=6870918

<https://ecgi.global/content/working-papers>

ECGI Working Paper Series in Law

Regulating DeFi Platforms

Working Paper N° 937/2026

June 2026

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

We are grateful for comments from Ilya Beylin, Vanessa Villanueva Colloa, Carole House, Kristin Johnson, Carla Reyes, 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.

© 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. By implementing capital adequacy rules, disclosure regimes, and anti-money laundering and know-your-customer conventions, these entities constrain opportunism, provide reliable recordkeeping, and enable regulators to monitor systemic risk. Decentralized finance (“DeFi”) disrupts this model by replacing 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 chokepoints that historically enabled oversight and consumer protection. As a result, DeFi magnifies familiar risks that fueled the Great Depression and the 2008 Global Financial Crisis, while also introducing novel vulnerabilities tied to computer code, governance, and cross-border anonymity. This Article argues that because DeFi platforms disaggregate traditional intermediary functions, effective regulation must focus on (i) embedding compliance safeguards directly into platform design and (ii) holding accountable the actors who build, operate, and maintain those platforms. These safeguards are essential to preserve market integrity, mitigate systemic risk, and protect investors in the absence of conventional intermediaries. Specifically, regulators should develop reforms that require platforms to incorporate technological and governance tools that replicate the critical compliance and risk-management functions historically supplied by intermediaries. 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 global effort.

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

JEL Classifications: K22, K23, K42, K33, K14, D82, D18, D02, D23, D62

Gina-Gail S. Fletcher

Professor of Law

Duke University

210 Science Drive

Durham, NC 27708, USA

e-mail: fletcher@law.duke.edu

Veronica Root Martinez*

Simpson Thacher & Bartlett Distinguished Professor of Law

Duke University

210 Science Drive

Durham, NC 27708, USA

e-mail: martinez@law.duke.edu

Steven L. Schwarcz

Professor of Law

Duke University

210 Science Drive

Durham, NC 27708, USA

e-mail: schwarcz@law.duke.edu

*Corresponding Author



Regulating DeFi Platforms

Gina-Gail S. Fletcher

Professor of Law
Duke University School of Law

Veronica Root Martinez

Simpson Thacher & Bartlett Distinguished Professor of Law
Duke University School of Law

Steven L. Schwarcz

Stanley A. Star Distinguished Professor of Law & Business
Duke University School of Law

Forthcoming MINNESOTA LAW REVIEW (2026)

REGULATING DeFi PLATFORMS

Gina-Gail S. Fletcher,^{*} Veronica Root Martinez,⁺ & 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. By implementing capital adequacy rules, disclosure regimes, and anti-money laundering and know-your-customer conventions, these entities constrain opportunism, provide reliable recordkeeping, and enable regulators to monitor systemic risk. Decentralized finance (“DeFi”) disrupts this model by replacing 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 chokepoints that historically enabled oversight and consumer protection. As a result, DeFi magnifies familiar risks that fueled the Great Depression and the 2008 Global Financial Crisis, while also introducing novel vulnerabilities tied to computer code, governance, and cross-border anonymity.

This Article argues that because DeFi platforms disaggregate traditional intermediary functions, effective regulation must focus on (i) embedding compliance safeguards directly into platform design and (ii) holding accountable the actors who build, operate, and maintain those platforms. These safeguards are essential to preserve market integrity, mitigate systemic risk, and protect investors in the absence of conventional intermediaries. Specifically, regulators should develop reforms that require platforms to incorporate technological and governance tools that replicate the critical compliance and risk-management functions historically supplied by intermediaries. 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 global effort.

^{*} Professor of Law, Duke University School of Law. Research Member, the European Corporate Governance Institute.

⁺ Simpson Thacher & Bartlett Distinguished Professor of Law, Duke Law School. Research Member, the European Corporate Governance Institute.

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

We are grateful for comments from Ilya Beylin, Vanessa Villanueva Colloa, Carole House, Kristin Johnson, Carla Reyes, 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.

TABLE OF CONTENTS

INTRODUCTION	2
I. THE RISE OF DeFi	10
A. <i>Traditional Finance & Regulation through Intermediaries</i>	10
B. <i>What is DeFi?</i>	13
C. <i>The Benefits of DeFi</i>	15
II. THE RISK ARCHITECTURE OF DECENTRALIZED FINANCE	17
A. <i>Traditional Risks</i>	18
B. <i>New Risks</i>	27
C. <i>Overview of Regulatory Challenges</i>	33
III. TARGETED COMPLIANCE & ENFORCEMENT FOR DeFi	
PLATFORMS.....	43
A. <i>Ex Ante Architectural Constraints</i>	45
B. <i>Small vs Large Firm Architecture</i>	49
C. <i>Ex Poste Enforcement & Multijurisdictional Accountability</i>	53
IV. ADDITIONAL QUESTIONS & CONCERNS.	58
A. <i>DeFi – A Public Good?</i>	58
B. <i>Collective Action and Public–Private Partnerships</i>	60
C. <i>Administrative Feasibility and Capacity Constraints</i>	61
CONCLUSION.....	62
APPENDIX	64

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 According to subsequent analysis, Forsage’s founders allegedly promised investors outsized, “guaranteed” returns generated automatically by computer code—but in reality, participant funds were partly siphoned off to the founders and otherwise recycled to pay earlier investors rather than deployed in genuine market activity.² The scheme succeeded precisely because of the technological opacity and legal fragmentation that characterize what has come to be known

¹ Press Release, U.S. Dep’t of Justice Office of Public Affairs, Forsage Founders Indicted in \$340M DeFi Crypto Scheme (Feb. 22, 2023), archived at <https://www.justice.gov/archives/opa/pr/forsage-founders-indicted-340m-defi-crypto-scheme>.

² Ari Redbord, U.S. DOJ Charges Four Russian-Nationals for Role in DeFi Ponzi Scheme Forsage, TRM LABS (June 13, 2023), <https://www.trmlabs.com/resources/blog/law-enforcement-spotlight-forsage>.

as DeFi, which refers to financial products and services that use public, permissionless, decentralized technology to facilitate payments,³ trading, lending, and other financial services⁴ without the involvement of traditional financial intermediaries.⁵

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 those intermediaries with self-executing computer programs known as smart contracts.⁶ These programs automatically execute algorithms on blockchain or other encrypted computer code that enable users to trade, lend, or borrow without relying on a centralized exchange or custodian.⁷ 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

³ Digital payment systems, using cryptocurrencies evidenced by blockchain technology, provide a well-known example of FinTech. *See 5 FinTech Examples Transforming Everyday Life*, WAKE FOREST UNIV. SCH. OF PRO. STUD., <https://sps.wfu.edu/articles/fintech-examples-transforming-everyday-life/>.

⁴ *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> (reporting that “Recent technological advances have streamlined and reshaped traditional financial services [and that] FinTech has expanded rapidly in the past decade”).

⁵ *See, e.g., What is Decentralized Finance (DeFi)?*, FIDELITY, <https://www.fidelity.com/learning-center/trading-investing/crypto/decentralized-finance-defined> (“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> (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*, 3 (2026) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5119593 (stating that DeFi does not eliminate intermediaries, but it merely redistributes and reconfigures intermediaries).

⁶ King & Spalding, *Decentralized Finance – Risks, Regulation, and the Road Ahead*, JD SUPRA (Sep. 1, 2021), <https://www.jdsupra.com/legalnews/decentralized-finance-risks-regulation-9351911/>.

⁷ *See, e.g., Illicit Finance Risk Assessment of Decentralized Finance*, U.S. DEP'T OF THE TREASURY 11 (Apr. 2023), <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf> (noting that DeFi transactions, especially those that are blockchain-based, could speed up settlement and be more cost efficient). *Cf. 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> (arguing that financial intermediaries can create “inefficiencies, structural inequalities, and hidden risks”).

persons do not have access to an account,”⁸ smart contracts arguably could perform those functions⁹—including enabling investors and other parties to directly access financial services, including securities trading and borrowing.¹⁰

In principle, this architecture can reduce transaction costs and broaden market access, thereby expanding financial inclusion¹¹ and advancing FinTech’s¹² oft-touted “democratization of the financial system.”¹³ In practice, however, the removal of intermediaries also removes the compliance infrastructure—recordkeeping, internal controls, anti-money-laundering

⁸ 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.

⁹ See, e.g., *What Are Smart Contracts on Blockchain?*, IBM, <https://www.ibm.com/topics/smart-contracts> (last accessed Jan. 22, 2026) (stating that “all [smart contract] participants can be immediately certain of the outcome, without any intermediary’s involvement or time loss”).

¹⁰ 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/> (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”).

¹¹ See, e.g., Carter Faust, et al., *FinTech and Financial Inclusion: A Review of the Empirical Literature*, 95 S. CAL. L. REV. 136, 136 (2023). 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.*

¹² FinTech generally refers to the use of technology to facilitate financial innovations. Cf. *What Is Financial Technology (FinTech)? A Beginner’s Guide*, COLUMBIA UNIV. SCH. ENG’G, <https://bootcamp.cvn.columbia.edu/blog/what-is-fintech/> (stating that FinTech “is a catch-all term referring to software, mobile applications, and other technologies created to improve and automate” finance). Not being officially defined, the term FinTech is imprecise; it can also refer to financial innovations that are facilitated by technology. Cf. Julia Kagan, *Financial Technology “Fintech”: Its Uses and Impact on Our Lives*, INVESTOPEDIA, <https://www.investopedia.com/terms/f/fintech.asp> (“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.”); *Innovation, Fintech, and AI*, BANK INT’L SETTLEMENTS, <https://www.bis.org/topic/fintech.htm> (“Fintech refers to technology-enabled innovation in financial services.”).

¹³ 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/?sh=728c64d4582b> (interviewing FinTech venture capitalist Spiros Margaris on how FinTech is transforming the financial industry). Cf. Steven L. Schwarcz & Robert Bourret, *Fractionalizing Investment Securities: Using FinTech to Expand Financial Inclusion*, 84 OHIO ST. L.J. 773 (2024) (examining how FinTech has led to the development of fractionalization which greatly expands financial inclusion by creating affordable securities).

(“AML”) and know-your-customer (“KYC”) conventions, and supervisory accountability—that has long served as the backbone of financial regulation.¹⁴ Eliminating traditional intermediaries can create anonymity—at worst—or confusion—at best—over whom should be regulated, creating a compliance conundrum.¹⁵ 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.¹⁶

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.¹⁷ 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. 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.¹⁸ Additionally, despite not having a qualified 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

¹⁴ Cf. *Weighing the Interconnected Risks Technology Poses to Financial Systems*, BAKER MCKENZIE (2025), <https://www.bakermckenzie.com/en/insight/publications/resources/fintech-and-financial-stability> (stating that “[f]or 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, 735 (2019) (showing “how and why specific fintech applications—cryptocurrencies, distributed ledger technologies, digital crowdfunding, and robo-advising—are poised to amplify the effect of these destabilizing mechanisms, and thus potentially exacerbate the tensions and imbalances in today’s financial markets and the broader economy. It is this potential that renders fintech a public policy challenge of the highest order.”).

¹⁵ 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> (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).

¹⁶ This shift is similar to, but different than, that of shadow banking. Cf. *infra* notes 103-114 and accompanying text (discussing shadow banking).

¹⁷ Amber Seira, et al., *Governance of Permissionless Blockchain Networks*, BD. OF GOV. OF THE FED. RESERVE SYS. (Feb. 9, 2024), <https://www.federalreserve.gov/econres/notes/feds-notes/governance-of-permissionless-blockchain-networks-20240209.html> (defining “permissionless blockchain network”).

¹⁸ See *supra* notes 1-5 and accompanying text.

components.¹⁹ Moreover, the broader DeFi ecosystem lacked the compliance safeguards traditionally supplied by financial intermediaries, such as KYC screening, AML monitoring, or risk-based disclosures. As regulators have repeatedly emphasized,²⁰ DeFi transactions can generate severe information asymmetries, depriving investors of visibility into how funds move through a system and preventing regulators from deploying traditional surveillance tools. In Forsage’s case, these gaps allowed hundreds of millions of dollars to flow through transparently recorded—but functionally opaque—smart-contract pathways, with no mechanism to flag the scheme’s inherently unsustainable and unlawful structure for investors.

The upshot is that today’s DeFi platforms exist in an ecosystem prone to anonymity, regulatory arbitrage, and jurisdictional evasion—conditions that allow fraudulent schemes like Forsage to flourish and, according to the U.S. Treasury, can even threaten national security by facilitating the financing of rogue states and other illicit actors.²¹

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”).²² In January 2025, the SEC also sanctioned Robinhood for failing to “observe a broad array of significant regulatory requirements, 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.”²³ Three 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

¹⁹ The Department of Justice refers to Forsage as “a purportedly decentralized finance (DeFi) cryptocurrency investment platform,” 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 help elucidate the challenges associated with applying standard regulatory requirements to emerging FinTech platforms.

²⁰ See, e.g., Caroline A. Crenshaw, *Statement on DeFi Risks, Regulations, and Opportunities*, S.E.C. (Nov. 9, 2021), <https://www.sec.gov/newsroom/speeches-statements/crenshaw-defi-20211109> (discussing the information gap between retail investors and professional investors in DeFi transactions); *Illicit Finance*, *supra* note 7, at 29 (describing potential limits to “access of information critical to supporting financial investigations”).

²¹ See, e.g., Talley, *supra* note 15 (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”).

²² *About Us*, ROBINHOOD, <https://robinhood.com/us/en/about-us/> (last visited Jan. 22, 2026).

²³ Press Release, U.S. Sec. & Exch. Comm’n, *Two Robinhood Broker-Dealers to Pay \$45 Million in Combined Penalties for Violating More Than 10 Separate Securities Law Provisions* (Jan. 13, 2025), <https://www.sec.gov/newsroom/press-releases/2025-5>.

potential misconduct.”²⁴ 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.²⁵ When Robinhood violated supervisory and customer-protection obligations, regulators were able to identify the responsible entity, investigate the misconduct, and impose meaningful sanctions. That outcome demonstrates how intermediation, though costly, sustains the transparency, compliance culture, and enforceable accountability that disintermediated systems can lack.²⁶

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.²⁷ As former Commodity Futures Trading Commission (“CFTC”) Commissioner Kristin N. Johnson has emphasized, this “largely unregulated” structure deprives regulators of “foundational” safeguards such as customer identification programs, internal controls, and conflict-of-interest governance.²⁸ Importantly, recent enforcement actions confirm that even when DeFi platforms replicate traditional derivatives trading or lending, they frequently do so outside the compliance frameworks that govern registered futures commission merchants and swap execution facilities.²⁹

This Article situates these developments within the broader evolution of financial technology with a particular focus on the platforms, like Forsage, that

²⁴ 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-fra/82012940007/>.

²⁵ *Id.*

²⁶ Registered intermediaries like broker-dealers operate within a regulatory framework that allows misconduct to be traced to identifiable entities and individuals, ensures restitution for injured customers, and subjects repeat offenders to escalating sanctions—all features that decentralized systems have yet to replicate.

²⁷ Aina Turillazzi et al., *Decentralised Finance (DeFi): A Critical Review of Related Risks and Regulation* 6–7 (2023), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4593242.

²⁸ *Statement of Comm’r Kristin N. Johnson Regarding CFTC Resolving Charges Against Three Decentralized Finance Companies: The Need for Oversight*, COMMODITY FUTURES TRADING COMM’N (Sep. 7, 2023), <https://www.cftc.gov/PressRoom/SpeechesTestimony/johnsonstatement090723b>.

²⁹ See e.g., *CFTC Wins Default Judgment Against Ooki DAO*, HUNTON BLOCKCHAIN LEGAL RESOURCE (June 20, 2023), <https://www.hunton.com/blockchain-legal-resource/cftc-wins-default-judgment-against-ooki-dao> (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 AND THE LAW (Oct. 16, 2023), <https://www.blockchainandthelaw.com/2023/10/cftc-wades-into-defi-enforcement-again> (describing settled charges against Opyin, Inc. and Deridex, Inc. for operating unregistered trading platforms and failing to implement customer-identification programs). See *infra* note 84 and accompanying text.

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.³⁰ While proponents claim that DeFi replaces human discretion with “immutable code,” thereby reducing the possibility of error, the absence of institutional oversight also eliminates the very mechanisms through which legal and ethical accountability are enforced. As a result, disintermediation in DeFi both enables innovation and magnifies risk.

At its core, DeFi extends the FinTech revolution beyond efficiency and inclusion into financial innovations that redefine who performs the critical gatekeeping, compliance, and risk-management functions that have historically stabilized financial markets. DeFi removes the identifiable actors who, in traditional markets, serve as the focal points of regulation and supervision. It also facilitates financial transactions through computer code rather than humans exercising informed judgment. These shifts raise profound 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. 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 intermediary-based regulation to decentralized infrastructure, cautioning that such an approach risks chilling innovation and misclassifying open-source protocols.³¹ 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 (i) no longer exist, (ii) are deliberately bypassed, or (iii) lack the capacity to provide effective oversight of increasingly sophisticated financial technologies.

In response, this Article argues that because DeFi platforms disaggregate traditional intermediary functions, continued effective regulation must focus

³⁰ But see Vanessa Villanueva Collao, *DeFi’s Premise & Promise of Decentralization and Disintermediation*, 3 (2026) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5119593 (stating that DeFi does not eliminate intermediaries, but it merely redistributes and reconfigures intermediaries).

³¹ See generally Carla L. Reyes, *Law’s Detrimental Reliance on Intermediaries*, 92 GEO. WASH. L. REV. 1343 (2024) (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) (cautioning against premature imposition of fiduciary and corporate governance frameworks on decentralized blockchain communities).

on embedding compliance safeguards directly into platform design and on holding accountable the actors who build, operate, and maintain those platforms. Because of the cross-border nature of DeFi, this regulatory, and subsequent enforcement, effort will require multijurisdictional coordination. 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 logic. Whereas banks, broker-dealers, and other intermediaries have historically reduced transaction costs while serving as natural points of regulatory control, DeFi reassigns these functions to algorithmic code, smart contracts, and decentralized governance mechanisms. This disintermediation may lower costs and expand access, but it also displaces the institutional compliance infrastructure that has historically ensured transparency, accountability, and stability. By diffusing core intermediary functions across technical systems, DeFi introduces anonymity, regulatory arbitrage, and systemic risk—conditions that can amplify rather than eliminate human error.

Part II analyzes the risk architecture that follows from moving core intermediary functions into code. It proceeds in three parts. 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 turns to novel technology-and-governance risks—irreversible smart-contract bugs and exploits, systemic fragility produced by composability, the opaque pseudonymity of participants, and governance models that are neither fully decentralized nor adequately accountable. Third, it synthesizes the regulatory implications, examining how these layered risks defeat ordinary enforcement levers, complicate consumer protection, and generate acute cross-border jurisdictional problems.

Part 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.

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

I. THE RISE OF DeFi

Part I provides the conceptual foundation for understanding how decentralized finance challenges the regulatory logic of traditional financial markets. It begins by explaining how modern financial systems have long relied on traditional institutional intermediaries—banks, broker-dealers, and other gatekeepers—to reduce transaction costs, manage risk, and serve as natural points of regulatory oversight. It then contrasts this intermediary-based structure with the architecture of DeFi, which replaces institutional actors with smart-contract-driven algorithms. Finally, Part I examines the principal benefits claimed for DeFi, including its potential to accelerate financial innovation, reduce costs, and broaden market access. Together, these sections illuminate the structural transformation that DeFi represents—and set the stage for analyzing the regulatory gaps that arise when core financial functions migrate from institutions to technical infrastructures.

A. *Traditional Finance & Regulation through Intermediaries.*

“Intermediation is a fundamental fact of (traditional) finance.”³² 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.³³ 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.³⁴ In its position as lender, the bank can acquire information to determine to whom it should extend loans and on what terms.³⁵ The bank is also able to serve as a long-term monitor of the

³² Tom C.W. Lin, *Infinite Financial Intermediation*, 50 WAKE FOREST L. REV. 643, 643 (2015).

³³ 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”).

³⁴ Nina Boyarchenko et al., *Intermediaries as Information Aggregators: An Application to U.S. Treasury Auctions* (2015) <https://www.bostonfed.org/-/media/Documents/Macro-Financial-Society-2015/session2-boyarchenko-lucca-veldkamp.pdf&ved=2ahUKewji3MjS7J-SAxWFEIkFHxWzCf4QFnoECBgQAQ&usg=AOvVaw1A0-2NDRSNV42eRgnNr1m7>.

³⁵ *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-approval-odds> (listing the commonly requested information about the business and about the owners in applying for a loan).

borrower's condition, ensuring the return of the capital loaned and an increase in the value of the investment made.³⁶

Although the 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.³⁷ To accomplish this goal, intermediaries serve key roles in the financial markets. First, intermediaries facilitate capital aggregation and reallocation, through deposit-taking, lending, and securitization, among other mechanisms.³⁸ In so doing, intermediaries improve market liquidity and smooth the transfer of capital within the markets.³⁹ Second, intermediaries collect, analyze, and disseminate information throughout the markets.⁴⁰ Exchanges, for example, facilitate the flow of information by allowing available information to be reflected in the price of assets through trading.⁴¹ Other intermediaries, like underwriters and analysts, act as information brokers, reducing asymmetric information between companies and investors.⁴² 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.⁴³ 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 reputational agent and attesting to the worth of the issuance.⁴⁴

³⁶ See Matthew T. Gustafson et al., *Bank Monitoring: Evidence From Syndicated Loans*, 139 J. FIN. ECON. 452 (2017).

³⁷ See Hans Genberg, *The Changing Nature of Financial Intermediation and Its Implications for Monetary Policy*, 39 BIS PAPERS (2008), <https://www.bis.org/publ/bppdf/bispap39f.pdf>.

³⁸ See, e.g., Carol A. Corrado & Charles R. Hulten, *Financial Intermediation in the National Accounts*, 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”).

³⁹ Whitehead, *supra* note 33, at 9.

⁴⁰ 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).

⁴¹ Will Kenton, *Understanding Exchanges: Types, Functions, and Real-World Examples*, INVESTOPEDIA (2025), <https://www.investopedia.com/terms/e/exchange.asp> (stating that “an exchange ensures fair trading and spreads price information efficiently”).

⁴² 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).

⁴³ Steven L. Schwarcz, *Intermediary Risk in a Global Economy*, 50 DUKE L.J. 1541, 1543 (2001) (stating that “markets are diversifying investment risk by interposing intermediaries”).

⁴⁴ Lin, *Infinite Financial Intermediation*, *supra* note 32, at 648–49.

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;⁴⁵ on exchanges to provide equitable access to exchange pricing information;⁴⁶ and on underwriters to ensure reliable and complete issuer disclosures in an initial public offering.⁴⁷ 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,⁴⁸ and by preventing fraud, discrimination, and other abusive practices.⁴⁹

Given their importance and involvement in financial transactions, intermediaries are often the primary mechanism through which financial regulation occurs.⁵⁰ For regulators, financial intermediaries are clear, identifiable facilitators of transactions, which are fewer in number than market actors and therefore easier to regulate. For their part, intermediaries are motivated to comply with and monitor applicable laws and regulations as their profitability and access to the markets are often tied to their reputation for reliability and legal compliance.

Notwithstanding the benefits of intermediation, it has downsides. Most significantly, it is expensive. Intermediation adds a third party to the 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.⁵¹

⁴⁵ Investment Advisers Act of 1940 § 206, 15 U.S.C. § 80b-6

⁴⁶ 17 C.F.R. § 242.603

⁴⁷ Securities Act of 1933 § 11, 15 U.S.C. § 77k

⁴⁸ See, e.g., Federal Deposit Insurance Act, 12 U.S.C. § 1811 et seq.; Nat'l Ass'n of Ins. Comm'rs, *Risk Based Capital (RBC) For Insurers Model Act* (2012).

⁴⁹ See Dodd-Frank Act §§ 1031–1036, 12 U.S.C. § 5531–5536 (2012) (authorizing the Consumer Financial Protection Bureau to regulate unfair, deceptive, or abusive acts or practices in the consumer financial markets).

⁵⁰ Ilya Beylin, *How Portfolio Netting Deters Diversification and Competition in the Derivatives Industry*, 27 U. Pa. J. Bus. L. 1 (Fall 2024) (discussing how exchanges, clearinghouses, and other intermediaries are "conscripted into the regulatory project").

⁵¹ Erin Bendig, *The Costs of Being Unbanked or Underbanked*, FORBES (2025), <https://www.forbes.com/advisor/banking/costs-of-being-unbanked-or-underbanked/> (presenting the results of a survey showing that "30.7% of households indicated that high

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.⁵² 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.⁵³ DeFi uses decentralized, publicly accessible, and permissionless computerized blockchains, smart contracts, and distributed ledgers instead of the intermediaries – such as banks, exchanges, and brokers – and infrastructure central to traditional finance (“TradFi”).⁵⁴ DeFi thus aims to provide traditional financial activities through computer code, rather than relying on traditional intermediaries for trust.⁵⁵

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.⁵⁶ DeFi utilizes programmable, composable infrastructure, that is, open-source smart contracts that can be combined to build new applications, along with community-driven governance.⁵⁷ Further, its design is non-custodial, meaning that users can self-custody their assets via digital wallets – unlike TradFi, where institutions hold custody.⁵⁸ Notably, unlike TradFi, DeFi operates without credit checks, identity verification, or underwriting standards;

monthly fees prevented them from opening a checking or savings account with a bank or credit union”).

⁵² Kathryn Judge, *Intermediary Influence*, 82 U. CHI. L. REV. 573, 590–91 (2015).

⁵³ Paul Tierno, Cong. Rsch. Serv., R48883, *An Overview of Decentralized Finance (DeFi)*, 1 (2026).

⁵⁴ *Id.* at 5.

⁵⁵ OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, 16 (2022), <https://www.oecd.org/finance/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.htm>.

⁵⁶ Sandra Waliczek & Harry Yeung, *Decentralized Finance: Financial Markets in Practice*, World Econ. Forum (Oct. 2025), <https://www.weforum.org/stories/2025/10/decentralized-finance-financial-markets-in-practice/>.

⁵⁷ OECD, *supra* note 54, at 18.

⁵⁸ *Id.*

functions largely in a crypto-only closed loop; and eliminates institutional intermediaries.⁵⁹

Although DeFi is used to refer to the ecosystem of financial services, products, and activities, DeFi activity occurs across multiple layers.⁶⁰ The foundation of DeFi is the underlying blockchain, which is the settlement layer.⁶¹ The blockchain is a public, unalterable ledger that records all transactions and asset ownership that occur, thereby eschewing the need for a centralized authority.⁶² To date, Ethereum is one of the most popular blockchains in use but other notable blockchains include Binance Smart Chain, Polygon, and Solana.⁶³ The second layer is the asset layer, which holds the digital representation of value on the blockchain.⁶⁴ 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.

The next two layers, which are the focus of this Article, are the protocol layer and the application layer. 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.⁶⁵ Smart contracts are self-executing computer programs, often deployed on a blockchain, that are triggered automatically when predetermined criteria are satisfied.⁶⁶ Software engineers typically design, code, test, and deploy the smart contracts. Importantly, the lack of licensing or auditing requirements means that any individual with the requisite skill can perform those functions.⁶⁷

Smart contracts epitomize how DeFi can remove the need for a traditional financial intermediary.⁶⁸ Depending on their programming, smart contracts

⁵⁹ Tierno, *supra* note 52, at 12–14.

⁶⁰ Bd. of the Int'l Org. of Sec. Comm'ns, *IOSCO Decentralized Finance Report*, OR01/2022, at 1 (2022).

⁶¹ *Id.*

⁶² U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-704SP, SCIENCE AND TECH SPOTLIGHT: BLOCKCHAIN & DISTRIBUTED LEDGER TECHNOLOGIES (2019) (noting that each time a transaction is added, it is verified via a consensus pool).

⁶³ See *Top Blockchains by Total Value Locked (TVL)*, COINGECKO, <https://www.coingecko.com/en/chains> (last accessed May 26, 2026) (ranking Ethereum and other blockchains by total value locked).

⁶⁴ Victor Budau & Herve Tourpe, *ASAP: A Conceptual Model for Digital Asset Platforms*, INT'L MONETARY FUND, at 18 (Feb. 2024).

⁶⁵ *DeFi Stack: Getting a Grip on the DeFi Ecosystems*, HEDERA, <https://hedera.com/learning/defi-stack/> (last accessed May 26, 2026).

⁶⁶ See *supra* notes 6–8 and accompanying text.

⁶⁷ 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).

⁶⁸ See *supra* note 7 and accompanying text.

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.⁶⁹ 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 by paying \$100 an investor receives a 1 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 by providing pre-specified forms of standardized collateral.⁷⁰ Loans can be disbursed nearly instantaneously, cutting lending costs.⁷¹ 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.”⁷²

The final layer is the application layer, which facilitates the ability of users and investors to easily interact with the underlying protocols and assets.⁷³ For example, a user could trade cryptocurrencies by using the Uniswap Web App to swap its cryptocurrencies with cryptocurrencies held by other users.⁷⁴ In sum, DeFi is changing the ways in which 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 capacity to accelerate financial innovation. At least in theory, developers can rapidly re-program smart contracts to build, modify, and combine financial applications without requiring permission from traditional institutions. This openness enables experimentation in lending, trading, insurance, and other financial functions to

⁶⁹ See Nexa Desk, *How Do Smart Contracts Ensure Trust and Transparency in DeFi Lending?*, OUTLOOK INDIA (Sep. 11, 2025).

⁷⁰ Sirio Aramonte et al., *DeFi Lending: Intermediation Without Information?*, BANK FOR INT’L SETTLEMENTS 2 (June 14, 2022), <https://www.bis.org/publ/bisbull57.pdf>. DeFi requires all loans to be collateralized due to the anonymity of the transactions. *Id.*

⁷¹ See *id.*

⁷² Jai Massari & Christian Catalini, *DeFi, Disintermediation, and the Regulatory Path Ahead*, REG. REV. (May 10, 2021), <https://www.theregreview.org/2021/05/10/massari-catalini-defi-disintermediation-regulatory-path-ahead>.

⁷³ Bd. of the Int’l Org. of Sec. Comm’ns, *supra* note 59, at 1, 3.

⁷⁴ *Uniswap 101: What is Uniswap?*, UNISWAP LABS (June 1, 2023), <https://blog.uniswap.org/what-is-uniswap>

occur far more quickly than in conventional markets. Proponents argue that this flexibility can promote competition and creativity, facilitating innovative forms of financial products and services.⁷⁵ Additionally, some treat these benefits as inherently welfare-enhancing.⁷⁶

By removing banks and other financial intermediaries, who charge for their services, DeFi also reduces transaction costs.⁷⁷ Moreover, users can in theory verify key information—such as collateral levels, liquidity, and execution prices—without relying on a centralized intermediary to supply that data. This transparency, combined with automated execution, arguably may reduce opportunities for rent-seeking or discriminatory practices that can arise when human intermediaries control access to financial services.⁷⁸

Furthermore, DeFi can help to democratize finance by broadening market access,⁷⁹ making it accessible to anyone with an internet connection and a crypto wallet.⁸⁰ That would offer global access to borrowing, securities trading, and other investment opportunities without needing approval from traditional financial institutions,⁸¹ thereby benefitting those who are financially excluded or underserved.

⁷⁵ Campbell R. Harvey & Daniel Rabetti, *International Business and Decentralized Finance*, 55 J. INT. BUS. STUD. 840, 849 (2024) (referring to the “creative possibilities in the DeFi world” and the “seemingly endless” possibilities for innovation).

⁷⁶ Whether faster financial innovation and disintermediation necessarily improve social welfare—particularly when they externalize risk, undermine consumer protection, or exacerbate systemic fragility—is contested and addressed in Part IV.

⁷⁷ See *supra* notes 10–11 and accompanying text.

⁷⁸ See Harvey & Rabetti, *supra* note 75, 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”).

⁷⁹ See *supra* notes 11–13 and accompanying text.

⁸⁰ 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. 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. 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. Wallets are also commonly classified as “hot” or “cold” depending on their internet connectivity, reflecting tradeoffs between convenience and security. In decentralized finance, crypto wallets function as the primary technical interface through which users initiate transactions and interact with smart contracts, while key loss, compromise, or misuse can result in irreversible asset loss. Hyung-Jin Lim et al., *Comparative Analysis of Security Features and Risks in Digital Asset Wallets*, 14 ELECTRONICS 2436, 2440–42 (2025), <https://doi.org/10.3390/electronics14122436>.

⁸¹ Harvey & Rabetti, *supra* note 75, at 845–46.

DeFi's proponents also argue that by replacing human-managed intermediaries, smart contracts reduce the chance of human error.⁸² 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.⁸³ In these ways, DeFi offers a level of speed, predictability, and user autonomy that conventional intermediaries struggle to match.⁸⁴

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.”⁸⁵

* * * *

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. The very qualities that promise efficiency, openness, and automation also obfuscate the identifiable actors, compliance mechanisms, and supervisory chokepoints upon which legal oversight has historically relied. Part II turns to these tensions directly, examining the risks that arise when core financial functions are delegated to decentralized technical infrastructures rather than institutional intermediaries.

II. THE RISK ARCHITECTURE OF DECENTRALIZED FINANCE

Part II proceeds in three steps. Part II.A surveys the traditional financial risks that DeFi reintroduces, including money-laundering vulnerabilities, one-way-out lending, and shadow-banking–style maturity and liquidity risks. Part II.B then examines the new risks created by DeFi's technical architecture, such as smart-contract failures, pseudonymity, and fragile or opaque governance. Finally, Part II.C identifies the regulatory and enforcement challenges these risks generate, focusing on the difficulty of assigning responsibility, protecting consumers, and applying jurisdiction-bound regimes to a borderless, disintermediated system.

⁸² Khaitan & Co, *Artificial Intelligence and Smart Contracts*, LEXOLOGY (2025), https://www.lexology.com/library/detail.aspx?g=865220f0-e722-4c73-89ca-c58ce2120c64#_ftn3.

⁸³ Max Beinke et al., *Breaking the Chains of Traditional Finance: A Taxonomy of Decentralised Finance Business Models*, 34 ELEC. MKTS. 29, at 3 (stating that “DEX utilize smart contracts to tackle trust issues inherent in centralized exchanges by allowing users to retain control over their private keys”).

⁸⁴ See Rakesh Sharma, *Understanding Decentralized Finance (DeFi): Basics and Functionality*, INVESTOPEDIA (2025), <https://www.investopedia.com/decentralized-finance-defi-5113835>.

⁸⁵ Erik Voorhees, *A Response to SBF and Principled Crypto Regulation*, MONEY & STATE (Oct. 20, 2022), <https://www.moneyandstate.com/blog/response-to-sbf>.

A. *Traditional Risks.*

This Section examines how DeFi revives—and in some cases amplifies—the same prudential and compliance risks that have long challenged financial regulators. Though marketed as an innovation that eliminates, or at the very least reconfigures, intermediaries and increases efficiency, DeFi reproduces familiar dangers under a new technological guise. The first subsection explores how disintermediation undermines the AML and KYC safeguards⁸⁶ that anchor the domestic Bank Secrecy Act’s and international Financial Action Task Force’s regulatory regime. The second turns to DeFi lending, showing how smart-contract–based credit markets violate the traditional “two-ways-out” principle that once constrained excessive risk-taking by banks. The third 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. Together, these sections demonstrate that DeFi’s promise of innovation often comes with the very vulnerabilities financial regulation was designed to contain.

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,⁸⁷ or that they might even finance terrorists, jeopardizing national security.⁸⁸ The decentralization of finance would make it more difficult to enforce the laws against money laundering and terrorist financing.⁸⁹ Enforcement difficulties would arise for at least two reasons: other things being equal, it would be harder to identify decentralized, rather than centralized, financial market participants; and enforcement costs would increase because there likely would

⁸⁶ Recall that AML refers to anti-money-laundering safeguards and KYC refers to know-your-customer safeguards. See *supra* note 14 and accompanying text.

⁸⁷ 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>]; *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://perma.cc/UUB6-WMLM>].

⁸⁸ Talley, *supra* note 15.

⁸⁹ 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 FATF, *What Do We Do*, <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”).

be more such participants to enforce against (plus, the benefit-to-cost ratio would decrease if each decentralized participant on average has a smaller financial stake).

In traditional intermediated markets, firms such as broker-dealers, banks, and payment processors 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 KYC protections to identify and verify customer identity as well as ongoing monitoring and the filing of Suspicious Activity Reports.⁹⁰ Broker-dealers are further subject to FINRA Rule 3310, which requires them to maintain written AML compliance programs reasonably designed to detect and report suspicious transactions.⁹¹

These obligations are not merely aspirational; they are enforceable and auditable. In 2025, for example, Robinhood 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.⁹² 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,⁹³ while FINRA concluded that Robinhood lacked “reasonable anti-money-laundering programs” and failed to respond to “red flags of potential misconduct.”⁹⁴ These enforcement actions underscore how regulators can identify responsible parties, compel remediation, and verify compliance through the firm’s centralized recordkeeping systems—demonstrating that the presence of an intermediary provides both the infrastructure and the accountability necessary for effective AML oversight.

Recent enforcement actions against cryptocurrency intermediaries further 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 (“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.⁹⁵ In parallel, the Financial

⁹⁰ See Bank Secrecy Act of 1970, 31 U.S.C. §§ 5311–5332 (2021); see also 31 C.F.R. §§ 1023.210, 1023.320 (2024) (requiring broker-dealers to maintain AML programs and file Suspicious Activity Reports, or “SARs”).

⁹¹ FINRA Rule 3310, Anti-Money Laundering Compliance Program, FINRA Manual (2024).

⁹² See *supra* notes 22–**Error! Bookmark not defined.** and accompanying text.

⁹³ Press Release, U.S. Sec. & Exch. Comm’n, *supra* note **Error! Bookmark not defined.**.

⁹⁴ Stempel, *supra* note 24.

⁹⁵ 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->

Crimes Enforcement Network (“FinCEN”) entered into a consent order finding that the exchange willfully failed to implement an effective AML program, lacked meaningful know-your-customer 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.⁹⁶

The CVC Exchange matter underscores a critical point for decentralized finance: AML enforcement is possible in crypto markets precisely when an identifiable actor exists. Because the exchange operated as a money services business with centralized control over customer onboarding, transaction monitoring, and recordkeeping, regulators were able to impose criminal penalties, mandate remediation, and require ongoing compliance reporting—even though the underlying assets were pseudonymous and blockchain-based.⁹⁷ By contrast, DeFi platforms that eliminate centralized operators, compliance personnel, and legal entities remove the institutional hooks that made enforcement against the CVC Exchange feasible. What appears as a firm-level compliance failure in intermediated crypto markets thus becomes a systemic blind spot in decentralized finance.

Indeed, in DeFi, the structural features that enable disintermediation— anonymity, self-custody, and automated execution through smart contracts— also frustrate compliance with even the most basic requirements of the Bank Secrecy Act.⁹⁸ DeFi platforms typically have no physical headquarters, no compliance officers, and no practical mechanism for conducting customer identification or monitoring transactions in real time.⁹⁹ The absence of centralized control makes it difficult to implement KYC and AML programs, both of which serve as foundational tools for preventing illicit finance by verifying user identity, assessing counterparty risk, and facilitating the reporting of suspicious activity to law enforcement.¹⁰⁰ Although some DeFi

[currency-exchange-pleads-guilty-to-criminal-charges-related-to-anti-money-laundering-violations-and-pays-multi-million-dollar-fine-to-fincen.](#)

⁹⁶ *Id.*

⁹⁷ *Id.*

⁹⁸ Bank Secrecy Act of 1970, 31 U.S.C. §§ 5311–5332 (2021); see also 31 C.F.R. §§ 1023.210, 1023.320 (2024) (requiring broker-dealers and other covered entities to maintain AML programs and file suspicious activity reports).

⁹⁹ Dirk A. Zetsche, et al., *Decentralized Finance*, 6 J. FIN. REG. 172, 187 (2020) (noting that without a traditional “headquarters to which financial regulation will apply”, “regulatory agencies are likely to struggle to exert control”).

¹⁰⁰ Know Your Customer (“KYC”) requirements obligate financial institutions to verify customer identity, beneficial ownership, and risk profile to detect and prevent money laundering and terrorist financing. See *Customer Due Diligence Requirements for Financial Institutions*, 81 Fed. Reg. 29398 (May 11, 2016). These measures underpin effective AML programs by

platforms claim to employ geofencing—blocking internet protocol (“IP”) addresses associated with sanctioned jurisdictions¹⁰¹—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.¹⁰²

Enforcement experience confirms these compliance deficiencies. In 2023, the CFTC brought actions against DeFi platforms Opy, 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 and that Opy and Deridex failed to adopt KYC and AML programs consistent with the obligations imposed on registered futures commission merchants under 17 C.F.R. § 42.2.¹⁰³ The absence of a legal entity capable of performing—or being compelled to perform—these compliance functions thus transforms what is a firm-level obligation in traditional finance into a systemic blind spot in DeFi.

These compliance deficiencies, in turn, magnify the government’s enforcement challenges. In the traditional financial system, federal agencies rely on a dense supervisory architecture. FinCEN, within the U.S. Department of the Treasury, administers the Bank Secrecy Act and issues interpretive guidance and enforcement actions to ensure financial institutions maintain effective AML programs.¹⁰⁴ Centralized intermediaries thus provide regulators with both data and jurisdictional hooks—compliance officers, transaction

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 requires more than automated execution alone. AML systems must be calibrated, updated, monitored, and audited as illicit actors adapt their techniques. DeFi platforms frequently lack identifiable actors responsible for ensuring that these functions exist, operate effectively, and evolve in response to emerging risks. The result is not the impossibility of compliance, but the absence of reliable mechanisms to ensure that compliance functions are implemented and maintained.

¹⁰¹ *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>.

¹⁰² See Office of Foreign Assets Control, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 2021), <https://ofac.treasury.gov/media/913571/download?inline> (discussing crypto-wallet-address screening and sanctions exposure in the virtual currency sector); U.S. Dep’t of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* 35 (Apr. 2023), <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf> (noting DeFi services’ use of crypto-wallet screening, and other sanctions-compliance measures).

¹⁰³ See *CFTC v. Ooki DAO*, No. 3:22-cv-5416 (N.D. Cal. 2023); see also Snow & Molloy, *supra* note 29 (describing the CFTC’s charges against Opy, Inc., Deridex, Inc., and ZeroEx, Inc. for failing to register as required and for lacking required KYC and AML programs).

¹⁰⁴ Bank Secrecy Act of 1970, 31 U.S.C. §§ 5311–5332 (2021); see also Financial Crimes Enforcement Network, *Mission*, U.S. DEP’T OF THE TREASURY, <https://fincen.gov/about/mission> (last visited Jan. 24, 2026).

records, and identifiable management—necessary to enforce AML and know-your-customer obligations.

DeFi operates across pseudonymous networks and self-executing code, however, 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. The CFTC’s enforcement action against Ooki DAO exemplifies this mismatch: Unable to identify a single responsible entity, 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.¹⁰⁵ 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. 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.¹⁰⁶ These enforcement improvisations underscore the regulatory asymmetry between traditional financial intermediaries—where AML and KYC oversight is routine and enforceable—and the DeFi ecosystem, where disintermediation not only obscures accountability but also erodes the mechanisms through which the U.S. government safeguards monetary integrity and combats financial crime.

Taken together, these compliance and enforcement challenges reveal the fragility of a financial ecosystem that operates without institutional anchors. In traditional markets, the identification of responsible entities allows regulators to impose both ex ante obligations and ex post accountability; in decentralized finance, by contrast, anonymity and computer code-based governance leave little room for either. The result is a regulatory vacuum in which illicit transactions can proliferate undetected and unremedied. Yet the risks of DeFi extend beyond AML and KYC non-compliance. As the next section explores, the automatic execution of smart 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 traditional finance characterized by two independent sources of repayment—cash flow and asset value.

¹⁰⁵ *CFTC v. Ooki DAO*, No. 3:22-cv-5416, slip op. at 2–4 (N.D. Cal. June 8, 2023); see also Commodity Futures Trading Commission, *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>.

¹⁰⁶ *Id.* (finding Ooki DAO in violation of 17 C.F.R. § 42.2 (2023) for failing to implement a customer-identification program and AML procedures).

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

DeFi lending is growing rapidly.¹⁰⁷ However, the smart contracts that underpin DeFi's functions could exacerbate old risks by undermining the prudent banking paradigm 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.¹⁰⁸ 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.¹⁰⁹ The rationale is to enable loans to be disbursed near instantaneously, cutting lending costs.¹¹⁰

Violating 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. Prior to the Great Depression, for example, many banks engaged in “margin lending” to risky borrowers, securing the loans by shares of stock that the borrowers purchased with the loan proceeds.¹¹¹ 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.¹¹² In August 1929, however, a relatively modest decline in stock prices caused some of those loans to become under-collateralized.¹¹³ 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 Depression.¹¹⁴

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.¹¹⁵ Those “subprime” mortgage loans were then bundled together as collateral to partially support the payment of complex asset-backed securities that were sold

¹⁰⁷ Compare Aramonte et al, *supra* note 70, 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 (July 2025) (reporting that the IMF estimated the overall DeFi lending debt outstanding to be around \$25 billion in 2022).

¹⁰⁸ 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”).

¹⁰⁹ See *supra* note 70 and accompanying text.

¹¹⁰ See *supra* note 71 and accompanying text.

¹¹¹ See Iman Anabtawi & Steven L. Schwarcz, *Regulating Systemic Risk: Towards an Analytical Framework*, 86 NOTRE DAME L. REV. 1349, 1356 (2011).

¹¹² *Id.*

¹¹³ *Id.* at 1356–57.

¹¹⁴ *Id.* at 1357.

¹¹⁵ *Id.* at 1359.

to banks and other institutional investors worldwide.¹¹⁶ 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.¹¹⁷ 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.¹¹⁸ 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.¹¹⁹

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 cryptocurrency¹²⁰ 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.¹²¹ If multiple loans secured by the type of collateral 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.

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

¹¹⁶ *Id.*

¹¹⁷ *Id.* at 1359–60.

¹¹⁸ *Id.* at 1360.

¹¹⁹ *Id.*

¹²⁰ See, e.g., Cornelli et al., *supra* note 107 (stating that “[a]nonymity 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”).

¹²¹ See *supra* note 70 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 107 (“Unlike traditional banks that rely on extensive credit 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.*

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.¹²² Although these entities performed bank-like functions—taking in short-term funds and making longer-term loans or investments—they operated outside of the prudential and supervisory framework that applies to banks.¹²³

By encouraging regulatory arbitrage, this shift caused a significant portion of the financial system to become unregulated.¹²⁴ Without deposit insurance, capital requirements, or direct oversight, shadow banking exposed markets to maturity and credit transformation risks—the same processes by which banks borrow short and lend long—that can destabilize credit markets in a downturn.¹²⁵ The lack of regulatory protection allowed excessive “[m]aturity and credit transformation in the shadow banking system,” which arguably “contributed to the asset price appreciation in residential and commercial real estate markets prior to the” Global Financial Crisis.¹²⁶ 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.¹²⁷

Decentralized finance replicates many of these same vulnerabilities, albeit through technology rather than balance-sheet engineering. As the Federal Reserve Bank of New York recently observed, the digital asset ecosystem exhibits “runs,” high leverage, and maturity transformation across centralized lenders, stablecoin issuers, and DeFi protocols—each performing traditional

¹²² See Michael Bromberg, Understanding Shadow Banking: Definition, Examples, and Function, INVESTOPEDIA (2025), <https://www.investopedia.com/terms/s/shadow-banking-system.asp>.

¹²³ See generally 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: efficiency is reduced by the increase in transaction costs, and the regulatory burden is shifted onto those who cannot engage in arbitrage”).

¹²⁴ Eric Feyen et al., *Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy*, BANK INT’L SETTLEMENTS PAPERS, at 13 (July 2021), <https://www.bis.org/publ/bppdf/bispap117.pdf> (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, 1:29 PM), <https://archive.nytimes.com/dealbook.nytimes.com/2011/05/27/shadow-banking-makes-a-comeback/> (explaining that the Dodd-Frank Act does not subject shadow banks to many of the regulations that the Act put into place).

¹²⁵ Zoltan Pozsar et al., *Shadow Banking*, FED. RESERVE BANK OF N.Y., Staff Report No. 458, at 1 (July 2010).

¹²⁶ *Id.*

¹²⁷ Fleischer, *supra* note 123, at 275; Frank Partnoy, *Financial Derivatives and the Costs of Regulatory Arbitrage*, 22 J. CORP. L. 211, 240–42 (1997). 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. Pozsar et al., *supra* note 126, at 3.

intermediation functions without equivalent safeguards.¹²⁸ In both systems, credit creation and liquidity transformation occur outside the banking perimeter, exposing markets to destabilizing feedback loops when prices fall or liquidity dries up. For example, DeFi lending protocols allow parties to borrow by posting volatile digital collateral,¹²⁹ creating what the Federal Reserve calls funding risk: the danger of “large, sudden withdrawals of funds” and fire sales during adverse shocks.¹³⁰ Because DeFi credit and liquidity provisions typically rely on crypto-native assets—including volatile cryptocurrencies and stablecoins that reference fiat currency¹³¹ but lack sovereign guarantees—changes in crypto-asset prices directly affect collateral values, leverage ratios, and the solvency of lending protocols. When crypto prices decline, these protocols automatically liquidate collateral positions, amplifying downward price spirals—a dynamic strikingly similar to the “runs” and forced liquidations that destabilized shadow banking during the Global Financial Crisis.¹³²

From a financial-stability perspective, DeFi thus functions as what commentators have called shadow banking 2.0: a network of algorithmic intermediaries conducting credit, liquidity, and maturity transformation without prudential supervision.¹³³ Yet unlike the pre-2008 shadow-banking system, DeFi’s risk propagation is accelerated by automation and global pseudonymity. The Federal Reserve warns that the “lack of a strong and cohesive regulatory framework” for digital assets—combined with high leverage, liquidity mismatches, and cross-platform interconnections—renders

¹²⁸ Pablo D. Azar et al., *The Financial Stability Implications of Digital Assets*, 30 FED. RSRV. BANK N.Y. ECON. POL’Y REV. 1, 4 (Nov. 2024), (identifying “runs” on centralized lenders, stablecoins, and DeFi protocols as evidence of systemic fragility).

¹²⁹ Cf. *supra* notes 120–121 and accompanying text (discussing DeFi lending’s reliance on crypto assets as collateral).

¹³⁰ Azar et al., *supra* note 128, at 2 (defining funding risk as the possibility of “large, sudden withdrawals of funds—a situation commonly referred to as a run”).

¹³¹ 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. 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. 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. See GENIUS Act, Pub. L. No. 119-27, 12 U.S.C. §§ 5901–5916 (2025). 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.

¹³² Azar et al., *supra* note 128, at 25–26 (describing automated liquidations and cascading price effects across DeFi platforms).

¹³³ Hilary J. Allen, *DeFi: Shadow Banking 2.0?*, 64 WM. & MARY L. REV. 919 (2023).

the system “very fragile against the occurrence of adverse shocks.”¹³⁴ Just as policymakers after 2008 sought to bring shadow banking within the regulatory perimeter through capital and liquidity standards, regulators today face the challenge of applying those same prudential concepts to code-based markets that lack identifiable legal entities or centralized control.

These parallels underscore that while DeFi’s design promises efficiency and openness, it reintroduces the same maturity, liquidity, and leverage vulnerabilities that made shadow banking a source of systemic instability.

* * * *

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. 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. Unlike traditional institutions, DeFi transactions operate without identifiable management, jurisdictional boundaries, or human discretion, transforming long-familiar financial threats into complex technological ones. The next section therefore turns to these “new” risks—arising from anonymity, operational fragility, and the absence of legal recourse—to examine how the mechanics of decentralization themselves 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 could impose significant costs on DeFi investors and DeFi platforms. Further, with the increased interconnectedness of DeFi with traditional finance, these risks may spill over into the broader financial markets, especially as DeFi continues to grow at an accelerated pace.¹³⁵ This Part focuses on three risks that plague DeFi, raising questions about the inherent costs of DeFi for consumers, the markets, and the DeFi platforms themselves.

¹³⁴ Azar et al., *supra* note 128, at 4 (“The lack of a strong and cohesive regulatory framework for digital assets also amplifies these vulnerabilities”, which renders “the crypto system very fragile against the occurrence of adverse shocks”).

¹³⁵ Joseph Abadi, *Making Sense of Decentralized Finance*, FED. BANK OF PHILADELPHIA (2024), <https://www.philadelphiafed.org/-/media/FRBP/Assets/Economy/Articles/economic-insights/2024/q1/eiq124-making-sense-of-decentralized-finance.pdf> (providing data showing a ten-fold increase in the amount invested in DeFi platforms from 2020 to 2023).

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.¹³⁶ This could be a particular problem given the irreversibility and finality of transactions executed on a blockchain.¹³⁷ 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.¹³⁸ 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.¹³⁹ As DeFi has grown, so too have the attacks on DeFi platforms, with billions of dollars of value being lost each year.¹⁴⁰

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.¹⁴¹ With composability, smart contracts can interoperate to provide novel, highly sophisticated products and services not available from a single smart contract.¹⁴²

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.¹⁴³ Flash loans depend on the interoperability of multiple DeFi protocols—such as a lending protocol to originate the loan, a decentralized exchange to execute trades, and a pricing oracle or governance

¹³⁶ Alexandra Born et al., *Decentralised Finance – A New Unregulated Non-Bank System?*, EUR. CENT. BANK (2022), https://www.ecb.europa.eu/press/financial-stability-publications/macprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html.

¹³⁷ *The Financial Stability Risks of Decentralised Finance*, FIN. STABILITY BD., at 18 (Feb. 16, 2023), <https://www.fsb.org/uploads/P160223.pdf> (stating that smart contracts “may be impossible to stop, modify, or reverse”).

¹³⁸ Born et al., *supra* note 136.

¹³⁹ 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/>.

¹⁴⁰ Jonathan Greig, *Cybercriminals Stole \$1.7 Billion From Crypto Funds in 2023 as Attacks Proliferated*, THE RECORD (Jan. 24, 2024), <https://therecord.media/cybercriminals-stole-over-1-billion-from-crypto-funds-2023>.

¹⁴¹ Francesca Carapella et al., *Decentralized Finance (DeFi): Transformative Potential & Associated Risks*, FED. RESERVE BANK OF BOS. 5 (Sep. 8, 2022), <https://www.bostonfed.org/publications/risk-and-policy-analysis/2022/decentralized-finance-defi-transformative-potential-and-associated-risks.aspx>.

¹⁴² *Id.* See also *Financial Stability Risks*, *supra* note 137, at 9.

¹⁴³ *What Are Flash Loans?*, CHAINLINK (May 24, 2023), <https://chain.link/education-hub/flash-loans>.

mechanism to determine asset values—each governed by separate smart contracts.¹⁴⁴ Because these steps occur atomically, the transaction either executes in full or is automatically reversed, enabling rapid, multi-step strategies that have no close analogue in traditional finance.¹⁴⁵

Although flash loans can facilitate legitimate activities such as arbitrage and liquidity rebalancing, they also introduce significant systemic vulnerabilities. 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.¹⁴⁶ These episodes demonstrate how composability can magnify the consequences of a single design flaw: A vulnerability in one smart contract may be leveraged instantaneously across several protocols, allowing losses to propagate through the DeFi ecosystem before any human actor can intervene.¹⁴⁷

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 and uses it to push up the price of a particular asset on the trading platform. Because the lending platform automatically relies on that price, it treats the asset as more valuable than it really is and allows the attacker to borrow more funds than should be possible. The attacker immediately repays the flash loan—so the transaction is 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 shows how DeFi’s composability allows a short-lived distortion in one protocol to trigger losses in another, turning what might have been a contained vulnerability into a cascading failure across interconnected systems. The same dynamic often turns on the integrity of price inputs. Because smart contracts generally cannot observe market conditions directly, they rely on oracles and other mechanisms to bring external information on-chain, and those dependencies can be points of fragility when feeds are thin, stale, or manipulable.¹⁴⁸

¹⁴⁴ See *id.*

¹⁴⁵ See e.g., Abraham, *Flash Loan Attacks: What They Are, How They Work, and How to Stay Safe* (Aug. 12, 2025), <https://adforensics.com.ng/flash-loan-attacks-what-they-are-how-they-work-and-how-to-stay-safe/>.

¹⁴⁶ *Id.*

¹⁴⁷ See *id.*

¹⁴⁸ Fin. Stability Bd., *The Financial Stability Risks of Decentralised Finance* 21–22 (Feb. 16, 2023), <https://www.fsb.org/uploads/P160223.pdf> (explaining “oracle risk” and noting that errors or attacks may trigger liquidations and propagate shocks). See also Chanelle Duley et al.,

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.¹⁴⁹ Further, composability increases complexity as smart contracts build on and interact with each other; that in turn makes it harder to track and identify interdependencies that could transmit contagion.¹⁵⁰ 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.¹⁵¹ Thus, the failure of a single protocol could impact multiple DeFi platforms, creating a cascading effect through the DeFi ecosystem.

2. Transparent Yet Anonymous

As discussed above, DeFi is often built on public blockchains and, as such, anyone can see the transactions being executed, limiting the need for verification by intermediaries. 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.¹⁵² To many, the pseudonymity of blockchain and DeFi transactions is “a feature, not a bug,” viewing it as one of the primary improvements of DeFi over traditional, centralized financial markets.¹⁵³ Indeed, according to one study, some traders prefer decentralized exchanges over centralized ones because of their greater anonymity despite their higher costs.¹⁵⁴ 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.¹⁵⁵ Because smart contract

The Oracle Problem and the Future of DeFi, BIS Bull. No. 76, at 2 (Sept. 7, 2023), <https://www.bis.org/publ/bisbull76.pdf> (describing oracle manipulation triggering liquidations).

¹⁴⁹ *DeFi's Composability: More Possibility, More Risk*, QUANTSTAMP (July 15, 2021), <https://quantstamp.com/blog/defis-composability-more-possibility-more-risk>.

¹⁵⁰ *Financial Stability Risks*, *supra* note 137, at 21.

¹⁵¹ Lewis Gudegon et al., *The Decentralized Financial Crisis: Attacking DeFi*, at 2 (Feb. 2020), available at <https://arxiv.org/pdf/2002.08099>.

¹⁵² Matteo Aquilina et al., *Cryptocurrencies and Decentralised Finance: Functions and Financial Stability Implications*, BIS PAPERS NO. 156, at 16 (Apr. 2025), <https://www.bis.org/publ/bppdf/bispap156.pdf> (stating that crypto wallets are “anonymous and cannot be linked to physical or legal entities” or persons).

¹⁵³ Igor Makarov & Antoinette Schoar, *Cryptocurrencies and Decentralized Finance*, BIS WORKING PAPERS NO. 1061, at 26–27 (Dec. 2022), <https://www.bis.org/publ/work1061.pdf>.

¹⁵⁴ Sirio Aramonte, et al., *DeFi Risks and the Decentralisation Illusion*, BIS Q. REV. 21, 26 (Dec. 2021), https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf.

¹⁵⁵ Matteo Aquilina et al., *supra* note 152, at 16.

activities are not linked to legal identities, this creates an incentive for actors to take advantage of counterparties, whether through excessive risk taking or fraudulent behavior. 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.¹⁵⁶ While such fraudulent activity is possible in traditional finance, victims should have recourse through litigation to recover the value of what they lost. With DeFi, however, victims of a rug pull scam may not know whom to sue if identities are unknown.

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.¹⁵⁷ Such malicious or manipulative behavior therefore cannot always feasibly be detected or punished.¹⁵⁸ As such, notwithstanding the transparency of smart contracts, DeFi 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.¹⁵⁹ Thus, pseudonymity can benefit malicious actors who conceal their bad behavior, thereby evading consequences for their misdeeds.

Although smart contracts make individual transactions publicly observable on the blockchain, they do not reliably reveal the real-world identities or economic relationships of the parties involved. DeFi’s pseudonymity therefore produces a broader opacity that obscures who controls platforms, how risks are distributed, and where interdependencies lie within the ecosystem.¹⁶⁰ A single developer, for example, may operate multiple wallets across multiple protocols under different pseudonyms, making it difficult for investors and regulators to assess concentration, governance influence, or liquidity dependencies. As DeFi becomes increasingly interconnected both internally and with traditional financial markets,¹⁶¹ this inability to map control and

¹⁵⁶ *Id.* at 17 (defining a rug pull scam); see also Jared Ronis, *DeFi 101: The Good, the Bad, and the Regulatory*, WILSON CTR. (Sept. 29, 2023), <https://acrosskarman.wilsoncenter.org/article/defi-101-good-bad-and-regulatory>.

¹⁵⁷ Crenshaw, *supra* note 20.

¹⁵⁸ *Id.*

¹⁵⁹ Vincent Gramlich et al., *Decentralized Finance (DeFi): Foundations, Applications, Potentials, and Challenges*, at 44 (2022), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4535868.

¹⁶⁰ *Financial Stability Risks*, *supra* note 137, at 9, 32.

¹⁶¹ See, e.g., Logan Hitchcock, *Bermuda Plots ‘Fully On-Chain National Economy’ With Help From Coinbase*, YAHOO FIN. (Jan. 19, 2026); Jona Jaupi, *J.P. Morgan Launches Tokenized Money Market Fund on Ethereum*, THE DEFIANT (Dec. 15, 2025), <https://thedefiant.io/news/defi/j-p-morgan-launches-tokenized-money-market-fund-on-ethereum>.

exposure complicates risk assessment and heightens the potential for contagion—even if systemic spillovers have, to date, remained limited.¹⁶²

3. Governance Risks

Although a central promise of DeFi is decentralization, the actual level of decentralization varies, especially with respect to DeFi governance.¹⁶³ DeFi governance refers primarily to the process by which decisions are made for a platform.¹⁶⁴ 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.¹⁶⁵ 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.¹⁶⁶ 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.¹⁶⁷ And, second, governance authority is typically concentrated in the hands of a few.¹⁶⁸

To participate in DeFi governance, developers and investors often must acquire a governance, or voting, token.¹⁶⁹ These tokens are explicitly assigned specific governance rights and do not have independent monetary value outside the ability to vote on future governance measures.¹⁷⁰ 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

¹⁶² Makarov & Schoar, *supra* note 153, at 3–4.

¹⁶³ Carapella et al., *supra* note 141, 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.”); *Financial Stability Risks*, *supra* note 137, at 11 (“the actual degree of decentralization among underlying DeFi organisational structures varies broadly”).

¹⁶⁴ Iwa Salami, *Challenges and Approaches to Regulating Decentralized Finance*, 115 *AJIL* UNBOUND 425, 427 (2021).

¹⁶⁵ Carapella et al., *supra* note 141, at 21 (“This ability to change the protocol, however, raises a governance question: what 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”).

¹⁶⁶ *Id.*

¹⁶⁷ Aramonte et al., *supra* note 154, at 27 (calling full decentralization of DeFi “illusory” since all DeFi platforms have an element of centralization around governance).

¹⁶⁸ *Id.* at 28.

¹⁶⁹ See *DeFi Beyond the Hype*, *supra* note 7, at 3.

¹⁷⁰ See *id.* (explaining that “the value of the token reflects investor expectations about the success of the protocol”).

hands.¹⁷¹ Additionally, insiders can aggregate governance tokens, increasing their concentration of power.¹⁷² This concentration of governance authority means that a small group can exert outsized influence over the platform's operation, rather than the decentralized and democratized governance that is often touted with respect to DeFi.¹⁷³

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.¹⁷⁴ Further, if governance tokens are tradable, malicious actors could acquire enough power to alter the platform for their own financial gain.¹⁷⁵ 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.¹⁷⁶

In addition to governance being concentrated, it is also opaque. While some DeFi platforms may grant veto rights to particular governance-token holders, they nonetheless fully embrace the concept that while all governance votes are equal, some are more equal than others.¹⁷⁷ The problem is not necessarily that different governance models exist, but rather that these governance features are not fully transparent to investors.¹⁷⁸ 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 preceding discussion of DeFi's traditional and novel risks exposes a deeper regulatory problem: the misalignment between existing financial oversight frameworks and decentralized market architecture. DeFi's reliance on smart contracts, pseudonymous participation, and automated execution complicates both systemic-risk regulation and investor protection, calling into question how prudential regulation should be structured in the absence of

¹⁷¹ Aramonte et al, *supra* note 154, at 28.

¹⁷² See Aina Turillazzi et al., *Decentralised Finance (DeFi): A Critical Review of Related Risks and Regulation* 7 (2023), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4593242 (explaining how the voting mechanism is “criticised for enabling... disproportionate voting power that early investors or the original team can have on their votes”).

¹⁷³ See *id.* (referring to this as “governance capture”).

¹⁷⁴ Aramonte et al, *supra* note 154, at 28.

¹⁷⁵ *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, OECD, at 34 (2022), https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/01/why-decentralised-finance-defi-matters-and-the-policy-implications_5f54eead/109084ae-en.pdf.

¹⁷⁶ Aina Turillazzi et al., *supra* note 172, at 7.

¹⁷⁷ See GEORGE ORWELL, *ANIMAL FARM* (1946).

¹⁷⁸ *Financial Stability Risks*, *supra* note 137, at 12.

institutional intermediaries. This Section addresses those issues by distinguishing between macroprudential regulation aimed at financial stability and microprudential regulation focused on individual firms and investors. In addition to prudential concerns, DeFi's disintermediation raises acute consumer-protection and cross-border enforcement challenges, as the elimination of identifiable intermediaries deprives regulators and investors of the disclosure, supervision, and 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 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."¹⁷⁹ 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). 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. 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.¹⁸⁰ Although several such failures may arise in financial markets generally, not all are equally salient in decentralized finance. In the DeFi context, the most acute macroprudential risks stem from technological and organizational complexity, which can obscure risk, impair disclosure, and magnify information asymmetries in ways that traditional regulatory frameworks are ill-equipped to detect.

Complexity represents a market failure insofar as it can distort the understanding of information and impair disclosure, thereby increasing

¹⁷⁹ Kadija Yilla & Nellie Liang, *What Are Macroprudential Tools?*, BROOKINGS (Feb. 11, 2020), <https://www.brookings.edu/articles/what-are-macroprudential-tools/>.

¹⁸⁰ *See id.*

asymmetric information.¹⁸¹ In this context, complexity refers not merely to sophisticated financial products, but to the interaction of smart contracts, governance mechanisms, composability across protocols, and opaque control rights that make it difficult for market participants—and regulators—to identify who bears risk and how losses may propagate. Complexity can also result in mutual misinformation.¹⁸² As discussed below, the macroprudential regulation of DeFi platforms will need to focus on this market failure.

Conflicts represent a distinct but closely related source of macroprudential risk, particularly when they are obscured or intensified by structural complexity. 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.¹⁸³ 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.¹⁸⁴ These conflicts, though, are exacerbated by complexity, which greatly increases the information asymmetry between DeFi-platform managers and investors.¹⁸⁵ 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.¹⁸⁶ Accordingly, the existing macroprudential regulation that applies to those market failures should already help to protect against DeFi

¹⁸¹ See, e.g., Steven L. Schwarcz, *Disclosure's Failure in the Subprime Mortgage Crisis*, 2008 UTAH L. REV. 1109, 1110–11 (2008) (observing that even sophisticated institutional investors did not fully understand certain complex financings).

¹⁸² 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: neither the sponsor of the re-securitization, nor the investors, fully understood the risks).

¹⁸³ See *DeFi Beyond the Hype*, *supra* note 7, at 6 (explaining that DeFi developers initially retain substantial control over protocol decisions, with full DAO-based decentralization as a later objective).

¹⁸⁴ See *supra* notes 1–2, 139–140, and 156 and accompanying text.

¹⁸⁵ See *supra* notes 181–182 and accompanying text.

¹⁸⁶ 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. infra* note 167 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.*

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, for example, is designed to protect against liquidity failures as well as against financial contagion—the risk of debt defaults being transmitted through the interconnectedness of SIFIs.¹⁸⁷

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.¹⁸⁸ 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.¹⁸⁹

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.¹⁹⁰

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.¹⁹¹ This framework incentivizes, rather than mandates, STS transactions by reducing regulatory

¹⁸⁷ See, e.g., IMF et al., *Guidance to Assess the Systemic Importance of Financial Institutions, Markets and Instruments: Initial Considerations*, 13 (Oct. 2009), <https://www.imf.org/external/np/g20/pdf/100109.pdf> [<https://perma.cc/TB2P-XJWN>]; Basel Committee on Banking Supervision, *Consultative Document: Global Systemically Important Banks: Assessment Methodology and the Additional Loss Absorbency Requirement 1* (July 2011) <https://www.bis.org/publ/bcbs201.pdf> [<https://perma.cc/VAA2-U5Y6>].

¹⁸⁸ Steven L. Schwarcz, *Controlling Financial Chaos: The Power and Limits of Law*, 2012 WIS. L. REV. 815, 820.

¹⁸⁹ See Letter from DeFi Educ. Fund, to Vanessa A. Countryman, Sec’y of Sec. & Exch. Comm’n, 11-12 (April 18, 2022), <https://www.sec.gov/comments/s7-02-22/s70222-20123960-280119.pdf> (stating that “the Commission cannot impede decentralization in other jurisdictions, which are taking affirmative steps to attract the disintermediated market industry” and “if 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”).

¹⁹⁰ See, e.g., Charles K. Whitehead, *Destructive Coordination*, 96 CORNELL L. REV. 323 (2011) (discussing how standardization could exacerbate systemic risk). But cf. 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: “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”).

¹⁹¹ See generally Proposal for a Regulation of the European Parliament and of the Council (EC) No. 472/2015 of 30 Sep. 2015, 2015/0226 (COD).

capital requirements for investors therein, thereby allowing for potential innovation.¹⁹² 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”) ¹⁹³ as well as a Financial Stability Oversight Council (“FSOC”) ¹⁹⁴ 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.¹⁹⁵ 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.¹⁹⁶

Until we more fully understand DeFi and its risks, ex ante preventative regulation almost certainly will be insufficient standing alone. The challenge is compounded by the fact that innovators frequently design new financial products and organizational structures specifically to operate outside existing regulatory categories or to exploit gaps between them, making it difficult for regulators to anticipate risks and craft effective rules in advance. Regulators therefore may wish also to examine potential ex post regulation to mitigate any harmful consequences caused by the collapse of DeFi platforms.¹⁹⁷ 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

¹⁹² *Id.*

¹⁹³ Dodd-Frank Act § 152, 12 U.S.C. § 5342 (2012).

¹⁹⁴ Dodd-Frank Act § 111, 12 U.S.C. § 5321 (2012).

¹⁹⁵ 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/6EPE-RRD7>].

¹⁹⁶ Press Release, European Commission, A Comprehensive EU Response to the Financial Crisis: Substantial Progress Toward a Strong Financial Framework for Europe and a Banking Union for the Eurozone 3, (Mar 28, 2014), http://europa.eu/rapid/press-release_MEMO-14-244_en.htm [<https://perma.cc/H856-CAYW>].

¹⁹⁷ 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).

lost when the private commercial paper market collapsed.¹⁹⁸ 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.¹⁹⁹ 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.²⁰⁰ Some argue, for example, that the Basel II capital requirements contributed to the 2008 financial crisis by globally correlating faulty rules.²⁰¹ Regulatory harmonization also, paradoxically, can invalidate existing risk-management strategies that are premised on randomness and independent action.²⁰² For example, the value-at-risk (“VaR”) model presumed that portfolio managers act independently of each other.²⁰³ Incorporating VaR into regulation, however, can incentivize managers to act more uniformly, thereby undermining VaR’s utility as a risk-management tool.²⁰⁴

(b) *Microprudential Regulation*. Regulation designed to protect the individual safety and soundness of parties acting in the financial system is referred to as “microprudential.”²⁰⁵ The purpose is to reduce the chance that any given party fails, thereby harming its investors and counterparties.²⁰⁶ Traditional bank

¹⁹⁸ See Board of Governors of the Federal Reserve System, *Commercial Paper Funding Facility* (2020), available at <https://www.federalreserve.gov/monetarypolicy/cpff.htm> (discussing that “The 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).

¹⁹⁹ See *infra* notes 215–209 and accompanying text.

²⁰⁰ RICHARD J. HERRING & ROBERT E. LITAN, FINANCIAL REGULATION IN THE GLOBAL ECONOMY 134–35 (1995); see also Roberta Romano, *For Diversity in the International Regulation of Financial Institutions: Critiquing and Recalibrating the Basel Architecture*, 31 YALE J. ON REG. 1, 5–7 (2014).

²⁰¹ Romano, *supra* note 200, at 13–20.

²⁰² Whitehead, *supra* note 190, at 347.

²⁰³ *Id.* at 341.

²⁰⁴ *Id.* at 347–51. see also IMF, *Global Financial Stability Report: Financial Market Turbulence: Causes, Consequences, and Policies* 62 (2007) (finding that having institutions employ the same risk model has destabilizing effects).

²⁰⁵ See, e.g., Lucrezia Cipriani & Andrea Minto, *Microprudential Regulation*, in COMPARATIVE FINANCIAL REGULATION 155 (Alessio M. Paces, Edoardo D. Martino, & Hossein Nabilou, eds. 2025).

²⁰⁶ *Id.*

regulation epitomizes such regulation, requiring each bank to act with prudence.²⁰⁷

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.²⁰⁸ 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. 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.

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.²⁰⁹

2. The Consumer Protection Conundrum

DeFi's most acute consumer-protection challenge arises from the disappearance of institutional actors who traditionally bear legal responsibility for safeguarding retail investors. Consumer-protection law in financial markets assumes the presence of intermediaries—broker-dealers, advisers, custodians, and exchanges—who can be required to disclose risks, maintain accurate records, refrain from deceptive practices, and provide redress when fraud occurs.

Forsage illustrates the acute consumer-protection challenges posed by disintermediated financial systems. Marketed as a legitimate “decentralized matrix project [that is, platform],” Forsage 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.²¹⁰ Because there was no intermediary to vet disclosures, supervise sales practices, or halt abusive activity, approximately \$340 million was extracted from retail investors worldwide, with over 80% of those investors

²⁰⁷ *Id.* (observing that microprudential regulation is concerned with the ability of banks and other financial intermediaries individually to perform their functions).

²⁰⁸ See *supra* notes 169–173 and accompanying text.

²⁰⁹ See, e.g., Jeremy C. Kress & Matthew C. Turk, *Too Many to Fail: Against Community Bank Deregulation*, 115 NW. U. L. REV. 647 (2020).

²¹⁰ 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>.

receiving fewer ETH back than they invested and more than half never receiving any payout at all.²¹¹ The platform’s reliance on self-executing smart contracts allowed the fraud to operate at global scale and with surgical precision, while depriving investors of the ordinary protections—risk disclosures, due diligence, suitability determinations, and supervisory review—that accompany financial intermediation.

Although the Department of Justice was able to identify and indict Forsage’s founders—Russian nationals who aggressively promoted the scheme online—this case is the exception rather than the rule in DeFi, where pseudonymous developers and globally dispersed operators often render meaningful enforcement functionally impossible. In many cases, the individuals who develop, deploy, or control DeFi platforms are pseudonymous, geographically dispersed, or have intentionally structured their operations to frustrate accountability.²¹² The CFTC’s enforcement action against Ooki DAO underscores the problem: unable to locate a traditional legal entity or identifiable management, the agency sued the DAO itself as an “unincorporated association” under the Commodity Exchange Act and obtained a default judgment only because no one appeared to contest the action.²¹³ Even in cases where regulators succeed, the remedy often arrives years after consumer harm has occurred and provides little meaningful redress to victims. Indeed, 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.²¹⁴

In short, DeFi creates a consumer-protection conundrum: the very intermediaries who traditionally bear legal duties to disclose risks, monitor misconduct, and compensate harmed investors are intentionally removed from the system. As Forsage and the Ooki DAO litigation illustrate, regulators often cannot identify a responsible party, and even when they can, enforcement typically arrives long after consumers have suffered irreversible losses. In a

²¹¹ *Id.*

²¹² *Regulating Crypto: The Bid to Frame, Tame, or Game the Ecosystem*, S&P GLOBAL, 16 (July 2022), <https://www.spglobal.com/content/dam/spglobal/corporate/en/images/articles/regulating-crypto-final.pdf> (discussing the difficulty in identifying those who can be held accountable).

²¹³ *See* Complaint, CFTC v. Ooki DAO, No. 3:22-cv-05416 (N.D. Cal. Sep. 22, 2022); *see also* Default Judgment, CFTC v. Ooki DAO, No. 3:22-cv-05416 (N.D. Cal. June 9, 2023) (citing the court’s decision treating the DAO as an unincorporated association because no identifiable entity could otherwise be served).

²¹⁴ Kristopher B. Kastens, *Ooki DAO Default Judgment: Regulators Still Face Many Technical and Legal Challenges in Regulating Smart Contracts*, HERBERT SMITH FREEHILLS KRAMER (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#_ftnref7.

system built on pseudonymity, dispersed governance, and immutable code, the core mechanisms of consumer protection simply have no natural place to attach. These accountability gaps are only magnified by DeFi's global reach, a feature that turns even ordinary enforcement challenges into complex cross-border problems.

3. Cross-Border Challenges

Many of the risks, both traditional and new, associated with DeFi are further heightened because of the borderless nature of DeFi operations. The lack of AML/KYC compliance coupled with the pseudonymity of DeFi provides fertile grounds for criminals to engage in illicit financial activity that is difficult to detect, prevent, or punish.²¹⁵ Criminals can use DeFi, for example, to launder illicit funds while obfuscating both the origin and destination of such funds.²¹⁶ According to a 2023 report from the Department of Treasury, cybercriminals use DeFi to generate additional profits on their illicit funds or to purchase the means, whether tools or services, to perpetrate additional criminal activity.²¹⁷

The ease with which DeFi operations cross national borders also 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.²¹⁸ For example, in March 2022, a North Korean sponsored cyber hacking group stole virtual assets worth approximately \$620 million from a blockchain project.²¹⁹ A few months later, in June 2022, the same group stole another \$100 million from Horizon, a DeFi cross-chain bridge.²²⁰ North Korea is also behind numerous ransomware attacks and has dispatched thousands of hackers worldwide to steal and launder virtual assets.²²¹ The stolen virtual assets and revenue

²¹⁵ *Illicit Finance*, *supra* note 7, at 26–28.

²¹⁶ *Id.* at 16–18.

²¹⁷ *Id.*

²¹⁸ *See generally id.*

²¹⁹ Press Release, Fed. Bureau of Investigation, 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>.

²²⁰ Press Release, Fed. Bureau of Investigation, FBI Confirms Lazarus Group Cyber Actors Responsible for Harmony's Horizon Bridge Currency Theft (Jan. 23, 2023), <https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft#Original-Statement>. Cross-chain bridges are “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 (Dec. 5, 2024), <https://www.chainalysis.com/blog/introduction-to-cross-chain-bridges/>.

²²¹ *Illicit Finance*, *supra* note 7, at 24–25.

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.²²²

These difficulties are underscored by the jurisdictional challenges that are inherent to DeFi. DeFi operates globally, providing services and products to investors worldwide. The 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.²²³ For example, a DeFi platform registered in the Cayman Islands may facilitate transactions between U.S.-based and India-based customers. 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 legal compliance by registering in a jurisdiction with less stringent laws. The recent enforcement order against Binance provides a salient example. In 2023, 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 pornography.²²⁴ 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.²²⁵ 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 ("FCMs") try to avoid their regulatory obligations by transitioning to a decentralized autonomous organization, claiming that it insulates them from compliance with U.S. laws.²²⁶

Similarly, criminal actors may seek out jurisdictions with relaxed or nonexistent regulations to carry out their illicit activity to further avoid accountability.²²⁷ Indeed, across various jurisdictions, some regulators may lack the authority, capacity, or willingness to go after crimes related to digital

²²² *Id.*

²²³ Born et al., *supra* note 136.

²²⁴ Press Release, U.S. Dep't of Justice, 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>.

²²⁵ *Settlement Agreement Between the U.S. Department of the Treasury's Office of Foreign Assets Control and Binance Holdings, Ltd.*, OFF. OF FOREIGN ASSETS CONTROL (Nov. 21, 2023), <https://ofac.treasury.gov/recent-actions/20231121>.

²²⁶ *Illicit Finance*, *supra* note 7, at 26.

²²⁷ *How to Strengthen International Enforcement Cooperation For Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets*, U.S. DEP'T OF JUSTICE 11 (June 6, 2022), https://www.justice.gov/d9/pages/attachments/2022/06/07/ncet_executive_order_report.pdf/.

assets, making enforcement even more difficult.²²⁸ Additionally, evidence gathering can be complicated for DeFi platforms that have their operations and customers spread across multiple countries.²²⁹ 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.²³⁰

* * * *

The regulatory challenges identified in this Section do not counsel regulatory restraint, but rather a period of purposeful regulatory recalibration. Part II.C highlights the limits of traditional ex ante regulation that relies on static rules, entity-based supervision, or premature standardization in a rapidly evolving, decentralized ecosystem. At the same time, it underscores why reliance on ex post enforcement alone is insufficient in markets characterized by automated execution, pseudonymity, and global reach. The implication is not that regulators should abstain from ex ante intervention, but that such intervention must operate differently—by targeting system design, governance structures, and points of functional control rather than attempting to impose conventional prudential rules on code-based markets. Part III takes up that task, showing how ex ante architectural constraints, paired with ex post accountability, can respond directly to the regulatory failures identified here without requiring regulators to predict or preempt every risk in advance.

III. TARGETED COMPLIANCE & ENFORCEMENT FOR DeFi PLATFORMS

Part III operationalizes this Article’s central claim: because DeFi platforms disaggregate the functions historically performed by financial intermediaries, effective regulation must (i) embed compliance safeguards directly into platform design and (ii) hold accountable the actors who build, operate, and maintain those platforms. In a borderless and automated financial ecosystem, neither code-based solutions nor traditional enforcement alone can supply the public goods of market integrity, financial stability, and accountability. This Part explains how design-based compliance and coordinated enforcement together can reconstruct those functions without reinstating traditional intermediaries.

This Article does not assume that regulators can fully specify, implement, or enforce optimal design-based safeguards ex ante in a rapidly evolving technological environment. To the contrary, as Part II.C emphasizes, uncertainty, information gaps, and institutional capacity constraints make comprehensive, static regulation both impractical and potentially counterproductive. The claim instead is a narrower but more defensible one: in a system defined by automated execution, pseudonymity, and global reach,

²²⁸ *Id.* at 14.

²²⁹ *Id.* at 9.

²³⁰ *Id.*

the absence of any embedded compliance constraints or credible accountability mechanisms is itself destabilizing. Even imperfect, adaptive, and incrementally developed architectural safeguards—paired with targeted, functionally grounded enforcement—can materially improve market discipline and deterrence relative to a regime that relies exclusively on after-the-fact intervention or formalistic entity-based rules.

As one can conclude from Parts I and II, the smart contracts used by DeFi Platforms excel at executing predefined rules with speed and precision, eliminating certain forms of human discretion, and reducing transaction costs associated with intermediation. Yet these same design features expose their structural limits. Smart contracts cannot assess evolving or unforeseen risk, interpret ambiguous or manipulable inputs such as oracle data, or exercise judgment in responding proportionately to systemic stress. Instead, automation can amplify fragility: Rigid liquidation triggers can produce correlated liquidations, fire-sale dynamics, and cascading failures across interoperable protocols through composability. Ex post enforcement, standing alone, is equally inadequate to address these risks. Enforcement is slow relative to instantaneous on-chain execution, fragmented across jurisdictions, and poorly suited to preventing systemic harm before it occurs. More fundamentally, regulators may have a difficult time identifying responsible parties against whom to enforce. By the time liability attaches, funds may already be irreversibly transferred, protocols may have migrated or forked, and systemic harm may be effectively locked in. These twin failures—of code that cannot adapt and enforcement that arrives too late or has no target—underscore why neither “code as law” nor after-the-fact regulation can function as a complete governance strategy for DeFi in isolation.

As a result, DeFi regulation must operate on two complementary planes. First, DeFi requires ex ante architectural constraints that can slow, channel, or temporarily pause risk—through design features that dampen procyclical automation, constrain runaway liquidations, and introduce friction where speed itself becomes a source of systemic fragility. Second, it requires ex post accountability mechanisms capable of deterring evasion, fraud, and willful blindness by attaching responsibility to those who design, govern, or materially profit from protocol operation. This hybrid approach mirrors—but does not replicate—the risk-mitigating functions historically performed by financial intermediaries. Rather than restoring banks, brokers, or exchanges as institutional gatekeepers, this approach seeks to preserve the stabilizing functions those intermediaries historically performed by embedding safeguards for accountability, oversight, and risk management directly into decentralized systems.

A. *Ex Ante Architectural Constraints*

DeFi operates primarily through smart contracts. 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. Regulation therefore should focus on attempting to reduce these risks by (a) re-intermediating responsible parties, (b) creating a process to identify the counterparties, and (c) 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 individually may be problematic,²³¹ 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 goods²³²). As a matter of materiality, regulators should initially prioritize financially complicated smart contracts that operate at scale or that can transmit losses through interconnection and common dependencies (including shared price feeds). In practice, that suggests focusing on system-relevant platforms and access points by transaction volume, total value locked, user base, and degree of composability, rather than anchoring scope to any single transaction-size cutoff.²³³

²³¹ 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* (draft on file with authors). Consumer protection law would not, however, necessarily affect the ex ante architectural design of smart contracts.

²³² 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").

²³³ 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 Org. for Econ. Co-operation & Dev., Concentration of DeFi's Liquidity 14–15 (2024), https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/04/concentration-of-defi-s-liquidity_5df1e8f9/4ed08440-en.pdf.

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. 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.²³⁴ It should also extend, where relevant, to other practical gateways, including stablecoin issuers and cross-chain bridges, that can supply leverage over access and execution.²³⁵ In this context, regulators may wish to consider whether to limit parties arranging the use of smart contracts to responsible institutions. Congress has recently used a similar “permitted-entity” approach in the payment-stablecoin context.²³⁶

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.²³⁷ Registration therefore should not turn on the layer that an actor sits but, rather, 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.²³⁸ Beyond the application layer, a lending

²³⁴ U.S. Dep’t of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* 2, 9 (Apr. 2023), <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf> (noting DeFi is often “not functionally decentralized” and defining the “application tier” as front-end user interfaces and APIs hosted primarily off-chain).

²³⁵ Fin. Stability Bd., *The Financial Stability Risks of Decentralised Finance* 4, 6 (Feb. 16, 2023), <https://www.fsb.org/uploads/P160223.pdf> (discussing liquidity risks in stablecoins and lending protocols and identifying oracles and cross-chain bridges as DeFi-specific risks).

²³⁶ See Guiding and Establishing National Innovation for U.S. Stablecoins (“GENIUS”) Act, Pub. L. No. 119-27 (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).

²³⁷ See *supra* notes 64–78 and accompanying text.

²³⁸ See Bd. of the Int’l Org. of Sec. Comm’ns, *IOSCO Decentralized Finance Report*, OR01/2022, at 1, 3 (2022) (describing the DeFi application layer as including front-end user

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.²³⁹ In each case, the relevant inquiry should be functional rather than formal: whether the actor has practical control over access, governance, deployment, maintenance, or execution in a way that makes registration useful 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.²⁴⁰ For example, non-registering parties could not enforce repayment of loans and may have to return the purchase price of transferred securities and commodities. That would shift the burden of identifying non-registering parties to the enforcement system, which would operate at the more granular level of the counterparties themselves.

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.²⁴¹ Victims at least should be able to sue identifiable parties for recourse.

interfaces through which users interact with protocols); U.S. Dep't of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* 2, 9 (Apr. 2023), <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf> (defining the “application tier” to include front-end user interfaces and APIs hosted primarily off-chain).

²³⁹ See Fin. Stability Bd., *The Financial Stability Risks of Decentralised Finance* 4, 6, 21–22 (Feb. 16, 2023), <https://www.fsb.org/uploads/P160223.pdf> (identifying stablecoins, oracles, and cross-chain bridges as sources of DeFi-specific risk); *CFTC v. Ooki DAO*, No. 3:22-cv-05416, slip op. at 2–4 (N.D. Cal. June 8, 2023) (treating DAO governance as a basis for regulatory enforcement);

²⁴⁰ *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).

²⁴¹ See *supra* note 156 and accompanying text.

3. Controlling Unchecked Automation.

Controlling unchecked automation would need to start with monitoring. That raises at least three questions: (i) Who should monitor?; (ii) What should they monitor?; and (iii) 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.²⁴² 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 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.²⁴³

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.²⁴⁴ It is unclear whether monitoring could have identified and halted this suspicious activity.

Answering the third question—what should monitors²⁴⁵ do if they see a problem—would depend on the nature of the problem. For example, where

²⁴² Fin. Stability Bd., *The Financial Stability Risks of Decentralised Finance* 34–35 (Feb. 16, 2023), <https://www.fsb.org/uploads/P160223.pdf> (discussing data transparency/consistency gaps in DeFi and calling for targeted public-sector approaches to enhance market transparency and risk monitoring).

²⁴³ Cf. Saule T. Omarova, *License to Deal: Mandatory Approval of Complex Financial Products*, 90 WASH. U. L. REV. 64 (2012) (proposing ex ante regulatory control through pre-market government licensing of complex financial products).

²⁴⁴ See *supra* note 18 and accompanying text.

²⁴⁵ 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 e.g. Veronica Root Martinez, *Public Reporting of Monitorship Outcomes*, 136 HARV. L. REV. 757 (2023). The use of the word monitors in this Article is unrelated to that strain of scholarship.

collateral enforcement is triggered by oracle-fed price moves, monitors should have the authority to pause or slow liquidation when the input appears distorted or when correlated liquidations threaten a fire-sale spiral.²⁴⁶ 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 second²⁴⁷—effectively (somewhat like smart contracts) operating unchecked in real time²⁴⁸ and, as a result of erroneous trades, causing substantial losses before they were stopped.²⁴⁹ 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.²⁵⁰ We do not, however, 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

²⁴⁶ Fin. Stability Bd., *The Financial Stability Risks of Decentralised Finance* 4–5, 23–24 (Feb. 16, 2023), <https://www.fsb.org/uploads/P160223.pdf> (describing fire-sale risks from automatic liquidation of collateral and noting that orderly liquidation mechanisms and market circuit breakers are generally absent in DeFi).

²⁴⁷ See, e.g., James Chen, *Understanding High-Frequency Trading (HFT): Basics, Mechanics, and Example*, INVESTOPEDIA (2025), <https://www.investopedia.com/terms/h/high-frequency-trading.asp>; Eric Budish et al., *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”).

²⁴⁸ See, e.g., Carol Clark, *Controlling Risk in a Lightning-Speed Trade Environment*, CHI. FED. LETTER (Mar. 2010), <https://www.chicagofed.org/publications/chicago-fed-letter/2010/march-272> (discussing the risks associated with high speed trading).

²⁴⁹ See *id.* See also Risk Management Controls for Brokers or Dealers with Market Access, 75 Fed. Reg. 69792 (Nov. 15, 2010) (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 247, at 1590 (“[A]ll of the expenditure by trading firms on speed technology [] is ultimately borne by investors via the cost of liquidity”).

²⁵⁰ See *supra* notes 191–192 and accompanying text.

destabilizing impact of multiple, correlated failures of small DeFi platforms.²⁵¹ 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 subject to different examination procedures based on its size.²⁵² 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.²⁵³

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.²⁵⁴ Similarly, differentiated regulation lowers compliance costs for smaller, less complex entities, which in turn may facilitate greater innovation by lowering barriers to market entry.²⁵⁵ 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 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

²⁵¹ See *supra* Part II.C.1.

²⁵² Office of the Comptroller of Currency, *Community Reinvestment Act: Revision of Small and Intermediate Small Bank and Savings Association Asset Thresholds*, OCC Bulletin 2025-48 (Dec. 23, 2025), <https://occ.gov/news-issuances/bulletins/2025/bulletin-2025-48.html>.

²⁵³ *Smaller Reporting Companies*, U.S. SEC. & EXCH. COMM’N (July 12, 2024), <https://www.sec.gov/resources-small-businesses/going-public/smaller-reporting-companies>.

²⁵⁴ See *Risk and Regulatory Policy: Improving the Governance of Risk*, ORG. FOR ECON. CO-OPERATION & DEV. 16–17 (Apr. 9, 2010), https://www.oecd.org/content/dam/oecd/en/publications/reports/2010/04/risk-and-regulatory-policy_g1ghc5f1/9789264082939-en.pdf (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”).

²⁵⁵ See Joseph J. Cordes et al., *Regulatory Compliance Burdens: Literature Review & Synthesis*, GEO. WASH. U. REGUL. STUD. CTR. (Oct. 2022), https://regulatorystudies.columbian.gwu.edu/sites/g/files/zaxdzs4751/files/2022-10/regulatory_compliance_burdens_litreview_synthesis_finalweb.pdf (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”).

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 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.²⁵⁶ However, few can read and comprehend the underlying code, thereby reducing the benefits of transparency almost entirely.²⁵⁷ 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.²⁵⁸

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.

²⁵⁶ Chris Brummer, *Disclosure, Dapps and Defi*, STAN. J. OF BLOCKCHAIN & POL’Y 137, 152 (2022).

²⁵⁷ Allen, *supra* note 133, at 936.

²⁵⁸ Brummer, *supra* note 256, 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. 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. 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 provide 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.²⁵⁹ Another example is the AnubisDAO rug pull, which occurred in 2021.²⁶⁰ Within hours of launching, AnubisDAO raised almost \$60 million.²⁶¹ But hours later, all the funds were withdrawn and siphoned to an "unknown Ethereum address."²⁶² 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.²⁶³

Public identification of the founders of DeFi platforms, therefore, is crucial to imposing accountability for the risks, failures, and losses that may occur 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 (to override the platforms' operations, for example).

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

²⁵⁹ See *Forsage Founders Indicted*, *supra* note 1.

²⁶⁰ 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#>.

²⁶¹ 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>.

²⁶² *Id.*

²⁶³ *Id.*

associated with higher capitalization.²⁶⁴ 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. The proposal was rejected by 55 percent of the users voting; regardless, the founder decided to shut down the project, overriding the vote of a majority of users.²⁶⁵

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. 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, 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 alone cannot deter intentional misconduct, prevent strategic evasion, or sustain a durable culture of compliance where profit incentives favor circumvention. As the International Organization of Securities Commission (“IOSCO”) has emphasized, DeFi’s transformation of traditional intermediaries diminishes the importance of actors that historically served as gatekeepers for market integrity, AML/CFT compliance, and fraud prevention—thereby magnifying the risk of misconduct absent effective substitutes.²⁶⁶ Enforcement therefore plays an indispensable role not merely by punishing violations *ex post*, but by reshaping incentives *ex*

²⁶⁴ Yan Chen et al., *Decentralized Governance of Digital Platforms*, 47 J. MGMT 1305, 1307 (2021).

²⁶⁵ Felix Ng, *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>.

²⁶⁶ IOSCO *Decentralized Finance Report*, INT’L ORG. OF SEC. COMM’N 36 (2022), <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf>.

ante, influencing behavior at the design, governance, and operational stages of DeFi platforms.

Recent enforcement actions underscore this point. In *CFTC v. Ooki DAO*, the court rejected the premise that decentralization confers immunity from law, holding that a DAO could be treated as a juridical person subject to regulatory obligations despite its on-chain governance structure.²⁶⁷ Similarly, OFAC's settlement with Exodus demonstrates how firms operating ostensibly "non-custodial" or infrastructure-level services can still engage in willful or reckless evasion, and how enforcement compels the integration of compliance controls into business functions that code alone failed to constrain.²⁶⁸ Exodus operated a non-custodial wallet that did not itself execute transactions, yet enforcement findings showed that its customer support practices actively enabled sanctioned users to circumvent geographic restrictions through technical guidance.²⁶⁹ The case underscores a critical point for DeFi regulation: embedded compliance fails where human actors retain discretion over interfaces, support, governance, or deployment, and enforcement is necessary to deter willful blindness at those margins. Enforcement is not antithetical to embedded compliance; it is the mechanism that makes embedded constraints credible.

Enforcement in DeFi should focus on actors who exercise actual operational control, rather than on formal labels such as "decentralized," "non-custodial," or "autonomous." In practice, this includes three categories of participants.

First, regulators can target developers and entities with ongoing control or upgrade authority, such as those who deploy protocols, retain administrative keys, or materially direct governance and maintenance. The CFTC's actions against Opyn and Deridex exemplify this approach: although the protocols relied on smart contracts, enforcement focused on the corporate entities that designed, deployed, and continued to operate systems offering unregistered derivatives.²⁷⁰

²⁶⁷ *Commodity Futures Trading Comm'n v. Ooki DAO*, No. 3:22-cv-05416, slip op. (N.D. Cal. June 8, 2023); see also CFTC Press Release, *CFTC Wins Default Judgment Against Ooki DAO* (June 20, 2023). Importantly, the judgment was entered on a default posture, but it remains instructive as to how courts may treat collective governance as an unincorporated association when governance decisions function as managerial control.

²⁶⁸ U.S. Dep't of the Treasury, Office of Foreign Assets Control, Exodus Movement, Inc. Settlement Agreement (Dec. 16, 2025), available at <https://ofac.treasury.gov/media/934836/download?inline> (finding willful and reckless evasion of sanctions controls through operational practices and requiring enhanced compliance commitments).

²⁶⁹ *Id.*

²⁷⁰ *In re Opyn, Inc.*, CFTC Docket No. 23-40 (Sep. 7, 2023); *In re Deridex, Inc.*, CFTC Docket No. 23-42 (Sept. 7, 2023); see also *In re ZeroEx, Inc.*, CFTC Docket No. 23-41 (Sep. 7, 2023).

Second, enforcement may extend to governance participants exercising operational power, where token-based voting or DAO structures are used to make decisions that substitute for managerial control. In *CFTC v. Ooki DAO*, the court rejected the argument that collective governance insulated the protocol from liability, emphasizing that those who vote to operate and maintain a trading protocol can constitute an unincorporated association subject to the Commodity Exchange Act.²⁷¹

Third, regulators can pursue service providers that knowingly facilitate evasion, even where those providers do not custody assets or execute transactions. OFAC's settlement with Exodus illustrates that wallet providers and interface operators may incur liability when their operational practices—such as customer support, technical guidance, or interface design—enable users to circumvent sanctions or compliance controls.²⁷² This enforcement strategy aligns liability with functional control over risk, access, and compliance outcomes, rather than with the formal architecture or rhetoric of decentralization.

Because DeFi activity executes at machine speed and across borders, enforcement cannot be effective if it remains siloed within national jurisdictions or proceeds sequentially. Protocols can be deployed, upgraded, exploited, and abandoned in a matter of days—or hours—while funds move frictionlessly through multiple jurisdictions before any single regulator can act. Country-by-country enforcement thus suffers from a significant structural lag: by the time jurisdiction is asserted and the process unfolds, the relevant actors may have dispersed, the code may have forked, and the assets may be beyond practical reach. Effective DeFi enforcement therefore requires coordinated, cross-border action that prioritizes speed, attribution, and early intervention, rather than after-the-fact remediation. This is not a novel institutional challenge. Over the past two decades, enforcement authorities have built the relationships and capacities needed for this sort of coordination: specifically, in domains characterized by transnational, fast-moving misconduct—most notably anticorruption.²⁷³

The evolution of global anticorruption enforcement demonstrates how coordination can overcome both jurisdictional fragmentation and timing constraints. As Professor Rachel Brewster documents, FCPA enforcement has

²⁷¹ *In re bZeroX, LLC, et al.*, CFTC Docket No. 22-31, at 9–10 (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”).

²⁷² Exodus Movement, Inc. Settlement Agreement, *supra* note 268.

²⁷³ See Steve Kwok et al., *Cross-Border Enforcement Priorities and Increased Cooperation Come Into Focus*, SKADDEN (Jan. 13, 2026), <https://www.skadden.com/insights/publications/2026/2026-insights/litigation-controversy/cross-border-enforcement-priorities>.

shifted from unilateral action toward coordinated global settlements, in which multiple sovereigns share evidence, align investigative strategies, synchronize resolutions, and allocate penalties.²⁷⁴ This model—described as “coordinated comity”—has allowed regulators to move more quickly, expand the evidentiary record, and prevent regulatory arbitrage by ensuring that firms cannot exploit gaps between national systems.²⁷⁵ OECD institutions have reinforced this shift by promoting joint investigations, information-sharing frameworks, and peer-based capacity building among enforcement authorities.²⁷⁶ DeFi enforcement should build on these sorts of infrastructures. Cross-jurisdictional task forces focused specifically on DeFi—integrating financial regulators, sanctions authorities, and criminal enforcement—would allow regulators to act at a tempo commensurate with the technology itself. In a system where misconduct propagates globally and instantaneously, enforcement must do the same.

This conclusion follows directly from Part III’s core claim that effective DeFi regulation must pair architectural constraint *ex ante* with accountability *ex post*. Where enforcement operates unilaterally, that approach breaks down. National rules, while necessary, invite regulatory arbitrage and will not be sufficient, as protocols respond to enforcement pressure by migrating code, relocating front-end interfaces, or reconstituting governance structures across jurisdictions without altering underlying economic activity. Fragmented enforcement further weakens deterrence by misaligning incentives: individual regulators bear the costs of investigation while the benefits of enforcement—market integrity, risk reduction, and deterrence—spill over globally. In such an environment, neither embedded compliance nor *ex post* liability can function as intended. Because DeFi’s architecture is inherently borderless, enforcement coordination is not simply a matter of international cooperation layered onto domestic law. It is a constitutive condition of effectiveness, necessary to ensure that design-based safeguards are not rendered meaningless by jurisdictional exit and that accountability mechanisms attach to control wherever it reappears.

The institutional capacity for coordinated DeFi enforcement already exists, even if it has not yet been fully mobilized for this purpose. Over the past two decades, regulators have developed dense networks for cross-border

²⁷⁴ Rachel Brewster, *The Rise of Global FCPA Settlements*, 104 TEX. L. REV. 299, 300–05, 354–57 (2025).

²⁷⁵ *Id.* at 354–56 (describing the shift from negative comity to coordinated comity through parallel investigations and settlements).

²⁷⁶ OECD, *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions* (2025), <https://legalinstruments.oecd.org/public/doc/205/205.en.pdf>; OECD, *Governments’ Assessments of Corporate Anti-Corruption Compliance* 7–9 (2025), https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/03/governments-assessments-of-corporate-anti-corruption-compliance_6100e758/e798903c-en.pdf.

cooperation in adjacent domains that map closely onto DeFi’s risk profile. IOSCO provides an established forum for coordination around market integrity, trading misconduct, and crypto-asset market oversight;²⁷⁷ the Financial Action Task Force (“FATF”) has built robust mechanisms for aligning AML/CFT standards, risk typologies, and enforcement expectations across jurisdictions;²⁷⁸ and the International Monetary Fund (“IMF”) and Financial Stability Board (“FSB”) coordinate surveillance and policy responses to cross-border threats to financial stability.²⁷⁹ Bilateral and multilateral enforcement cooperation—through memoranda of understanding, joint investigations, and parallel proceedings—has become routine in sanctions, corruption, and market abuse cases.²⁸⁰ The challenge in DeFi, then, is not the absence of institutions. It is that existing institutions must be adapted—and, where necessary, supplemented—to respond to risks that move quickly, cross borders, or require technical expertise to identify and attribute.

An effective implementation strategy would emphasize practical tools rather than new supranational authority. These include rapid information-sharing channels among regulators; mutual recognition or crediting of enforcement actions to reduce duplication and regulatory arbitrage; coordinated sanctions, designations, and access restrictions targeting shared control points; and the development of common typologies identifying DeFi-specific risk vectors, governance structures, and modes of evasion.²⁸¹ Framed this way, coordinated enforcement functions as a regulatory public good. Just as traditional financial intermediaries historically supplied market discipline, stability, and screening through private ordering, those public goods must now be supplied collectively by regulators operating across borders. In a decentralized and borderless financial system, coordination is not ancillary to regulation—it is the mechanism through which financial stability, market integrity, and national security can continue to be credibly protected.

From a political economy perspective, coordinated and rapid DeFi enforcement should be attractive across administrations with divergent regulatory philosophies. For an administration oriented toward executive

²⁷⁷ *IOSCO Report*, *supra* note 266, at 6–10, 36–38 (describing IOSCO’s role in coordinating regulatory responses to market integrity risks posed by DeFi).

²⁷⁸ Fin. Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* 7–12, 55–60 (Oct. 2021); *see also* OECD, *Governments’ Assessments*, *supra* note 276, at 7–9, 42–44 (describing FATF-based coordination, shared typologies, and cross-border alignment of enforcement expectations).

²⁷⁹ OECD, *Governments’ Assessments*, *supra* note 276, at 32–38 (discussing IMF- and FSB-linked coordination, peer learning, and cross-jurisdictional supervisory capacity-building).

²⁸⁰ Brewster, *supra* note 274, at 354–57 (documenting the normalization of parallel proceedings, information-sharing, and coordinated resolutions across jurisdictions).

²⁸¹ *IOSCO Report*, *supra* note 266, at 38–44 (emphasizing shared risk typologies and coordinated regulatory responses); OECD, *Governments’ Assessments*, *supra* note 276, at 38–44 (describing mutual learning, coordinated tools, and enforcement alignment as collective goods).

speed, decisive action, and national security—characteristics often associated with the Trump Administration²⁸²—cross-border enforcement task forces offer a mechanism for fast, targeted intervention without the need for new legislation or expansive domestic rulemaking. At the same time, such coordination advances interests traditionally emphasized by more regulation-forward administrations, including consumer protection, market integrity, and the mitigation of systemic financial risk. Because coordinated enforcement leverages existing authority, focuses on bad actors rather than compliant innovation, and produces visible outcomes within compressed time horizons, it avoids the typical tradeoff between deregulation and oversight.²⁸³ In this sense, DeFi enforcement coordination represents a rare win-win institutional strategy: it preserves market discipline and protects users while aligning with preferences for administrative efficiency, flexibility, and international leadership across the political spectrum.

* * * *

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 objections that naturally follow from the regulatory framework developed in Part III. These concerns do not challenge the need for embedded compliance and coordinated enforcement so much as they test its limits—asking whether DeFi should be understood as a public good, whether collective action and public-private partnerships might substitute for formal regulation, and whether the proposed approach is administratively feasible given current institutional capacity. Taken together, these questions probe the tradeoffs between innovation and stability, private ordering and public oversight, and ambition and practicality in the governance of decentralized finance.

A. *DeFi – A Public Good?*

This Article’s call for embedding compliance constraints into smart contracts and for coordinated cross-border enforcement invites an immediate

²⁸² 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>.

²⁸³ *Deregulation: Definition, History, Effects, and Purpose*, INVESTOPEDIA (Mar. 11, 2025), <https://www.investopedia.com/terms/d/deregulate.asp> (defining deregulation as the “reduction or elimination of government oversight”).

objection: that decentralized finance itself constitutes a public good placed at risk by precisely the regulatory interventions proposed here. From this perspective, DeFi's defining characteristics—permissionless access, open-source development, composability, and the ability to transact without reliance on centralized intermediaries—are said to generate social value that extends beyond any particular platform or transaction.²⁸⁴ DeFi is thus analogized to early internet protocols and other forms of open-source digital infrastructure, which scholars have described as nonrivalrous, generative resources that support downstream innovation by lowering barriers to entry for developers and users alike.²⁸⁵ On this view, decentralized financial protocols function less as discrete financial products than as commons-like infrastructure, enabling experimentation and coordination that no single firm or regulator could efficiently design or control *ex ante*.²⁸⁶

Against this backdrop, embedding compliance logic directly into smart contracts or subjecting DeFi ecosystems to aggressive, coordinated enforcement is portrayed as threatening to chill innovation, deter open-source development, and reintroduce the very forms of centralized control that decentralization was meant to displace.²⁸⁷ Regulatory friction, critics argue, risks transforming DeFi from a generative and permissionless ecosystem into a *de facto* permissioned financial system—one in which the social surplus produced by decentralized experimentation is sacrificed in the name of risk mitigation, even though the benefits of that experimentation may be diffuse, long-term, and difficult to quantify *ex ante*.²⁸⁸

This objection, however, rests on an incomplete account of both DeFi's benefits and its risks. As Part II demonstrates, DeFi does not merely enable decentralized experimentation; it also reintroduces—and in many cases

²⁸⁴ See, e.g., Chris Brummer, *Disclosure, Dapps and DeFi*, 5 STAN. J. BLOCKCHAIN L. & POL'Y 137, 139–41 (2022) (describing DeFi as an open, protocol-based ecosystem designed to reduce reliance on centralized intermediaries); Carla L. Reyes, *Law's Detrimental Reliance on Intermediaries*, 92 GEO. WASH. L. REV. 1343, 1348–52 (2024) (arguing that decentralization can supply social value by reducing law's dependence on centralized gatekeepers).

²⁸⁵ 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>.

²⁸⁶ See Carla L. Reyes & Joseph P. Cutler, *Ready Layer One: Functional Regulation for Blockchain Infrastructure* (2025) (manuscript at 10–18) (on file with authors) (arguing that open-source blockchain protocols function as digital infrastructure and should be regulated functionally rather than institutionally).

²⁸⁷ See Carla L. Reyes, *(Un)Corporate Crypto-Governance*, 88 FORDHAM L. REV. 1875, 1879–83 (2020) (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 can entrench power and reshape systems).

²⁸⁸ 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 (noting that a misaligned regulation of DeFi could deter innovation).

amplifies—longstanding sources of financial fragility, including excessive leverage, maturity and liquidity transformation, opacity, and correlated failure. Unlike early internet protocols, which primarily facilitated communication and information exchange, DeFi protocols perform core financial functions—credit creation, trading, custody, and payments—that directly affect asset prices, liquidity, and confidence in the financial system. The social costs of failure in these markets are therefore categorically different. As history illustrates, financial innovation that outpaces regulatory capacity can generate diffuse private gains during periods of growth while imposing concentrated, system-wide losses when market conditions turn.²⁸⁹

Moreover, the public-good framing obscures a second, equally critical problem: Absent embedded safeguards and coordinated enforcement, many of the risks DeFi generates are not amenable to traditional regulatory responses. As Part III explains, ex post enforcement alone is structurally ill-suited to an ecosystem characterized by automated execution, pseudonymous participation, and instantaneous cross-border activity. By the time liability attaches, losses may already be locked in through irreversible smart-contract execution, liquidity runs, or cascading liquidations across composable protocols. This dynamic mirrors earlier episodes in which regulators underestimated the systemic consequences of novel financial architectures—most notably in the years preceding the Great Depression and the Global Financial Crisis—when regulatory hesitation allowed fragile structures to scale unchecked until market discipline arrived in the form of collapse.²⁹⁰ Taking DeFi’s risks seriously at an early stage is therefore not an attack on innovation, but a recognition that financial systems impose externalities that private ordering and experimentation cannot internalize on their own. Without proactive, design-sensitive regulation and credible enforcement, the very features that make DeFi innovative also threaten to reproduce the conditions for another major episode of market instability—one in which the costs of delay are borne not by early adopters alone, but by the broader financial system and the public at large.

B. *Collective Action and Public–Private Partnerships*

A related and increasingly salient question is why this Article does not place greater weight on collective action or public–private partnerships as primary responses to the risks posed by decentralized finance. In other regulatory domains—most notably anticorruption, financial crime, and corporate

²⁸⁹ Michael Barr, *Ending “Too Big to Fail”*, BROOKINGS (June 14, 2011), <https://www.brookings.edu/articles/ending-too-big-to-fail> (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”).

²⁹⁰ See *id.*

compliance—inter-firm collaboration and structured cooperation between private actors and public authorities have improved regulatory outcomes by facilitating information sharing, coordinating standards, and enabling earlier detection of diffuse misconduct.²⁹¹ These approaches draw on a broader “new governance” tradition that emphasizes regulatory strategies combining public oversight with private participation, rather than relying exclusively on top-down command-and-control regulation.²⁹² Recent work on collaborative compliance similarly documents how firms confronting shared regulatory risks often benefit from collective efforts that pool expertise, reduce duplicative compliance costs, and enhance the credibility of compliance commitments.²⁹³

These models are particularly attractive in contexts where misconduct is decentralized, transnational, and difficult for any single regulator or firm to observe—conditions that closely resemble those of DeFi. Indeed, anticorruption initiatives coordinated through the OECD and allied institutions increasingly rely on collective action and public–private engagement to address precisely these kinds of structural enforcement challenges, pairing private-sector compliance efforts with governmental guidance, monitoring, and incentives.²⁹⁴ 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, shared baselines, and credible enforcement backstops. Absent those foundations, collaboration risks becoming fragmented, symbolic, or unevenly adopted. As the following discussion explains, this sequencing problem is especially acute in DeFi, where regulatory capacity and coordination remain underdeveloped and where private ordering alone cannot reliably internalize systemic risk.

C. *Administrative Feasibility and Capacity Constraints*

A further concern is whether the regulatory and enforcement framework proposed here is administrable in practice. Embedding compliance into

²⁹¹ See Mark Pieth, *Collective Action and Corruption*, in COLLECTIVE ACTION: INNOVATIVE STRATEGIES TO PREVENT CORRUPTION 3, 7–12 (2012) (describing collective action as a response to diffuse and systemic corruption); *Collective Action*, BASEL INST. ON GOV., <https://collective-action.com> (documenting industry–government anticorruption initiatives).

²⁹² See 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).

²⁹³ Kevin E. Davis & Veronica Root Martinez, *Collaborative Compliance* (Working Draft Jan. 11, 2026) (on file with authors) (documenting benefits and limits of inter-firm compliance collaboration).

²⁹⁴ See OECD, *Companies’ Assessments of Anti-Corruption Compliance* (2025), https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/03/companies-assessments-of-anti-corruption-compliance_363b6821/977ed5a8-en.pdf; OECD, *Governments’ Assessments*, *supra* note 276 (emphasizing collective action, peer learning, and public–private engagement as complements to enforcement).

protocol design and coordinating cross-border enforcement presuppose a level of technical capacity, institutional coordination, and regulatory clarity that many financial regulators are still in the process of developing. DeFi platforms operate through novel combinations of code, governance, and economic incentives, and evaluating their risk profiles requires expertise that historically sat outside the core competencies of securities, commodities, and banking regulators. At the same time, overlapping jurisdiction among domestic agencies—combined with uneven capacity across national regulators—raises the possibility of fragmented or inconsistent application.

This concern is real, but it cuts in favor of early capacity-building rather than regulatory restraint. 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 focal points of responsibility before DeFi markets scale to systemic importance. Historical experience—from shadow banking oversight to anticorruption enforcement—demonstrates that regulators routinely develop technical expertise in response to emerging market structures, often by leveraging specialist units, interagency coordination, and international standard-setting bodies.²⁹⁵ In this sense, the administrability challenge is not a reason to defer regulation, but a reason to sequence it: building institutional capacity now is a prerequisite to avoiding the far more difficult task of crisis management after decentralized markets have grown large enough to threaten financial stability.

CONCLUSION

Decentralized finance poses a fundamental regulatory challenge not because it is novel, but because it dismantles the institutional architecture through which financial law has 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 the compliance gatekeepers that have long supplied market discipline, consumer protection, and systemic oversight. This Article argues 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. And because DeFi activity is inherently borderless, this regulatory project cannot succeed without coordinated, multijurisdictional enforcement capable of operating at a speed and scale commensurate with the technology itself.

²⁹⁵ See *supra* notes 242–45 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 (discussing shadow banking oversight).

This Article makes three principal contributions to the legal scholarship on decentralized finance. First, it offers an integrated account of DeFi’s risk architecture, 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: monitoring, verification, disclosure, risk management, and accountability. Third, it advances a regulatory framework that pairs *ex ante* architectural constraints with *ex post* accountability by grounding liability in functional control and relying on coordinated enforcement to prevent decentralization from becoming a tool for evading regulatory oversight. The goal is not to eliminate DeFi’s capacity for innovation, but to ensure that financial activity conducted through decentralized systems remains subject to the safeguards necessary for market integrity, consumer protection, and financial stability.

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 systemic risk, correlated failures, 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 but also amplifying the potential for cascading failures.
- **Decentralized Autonomous Organization (DAO):** A governance structure used in decentralized finance in which decision-making authority is exercised through token-based voting or other on-chain mechanisms rather than through a centralized corporate hierarchy, often without formal legal personality.
- **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:** Regulatory safeguards and compliance mechanisms implemented directly into the design and operation of

DeFi platforms or smart contracts, rather than relying exclusively on ex post enforcement or institutional gatekeepers.

- **Ex Ante Regulation:** Regulatory intervention that operates before harm occurs, including design-based constraints, disclosure requirements, or structural safeguards intended to prevent or mitigate risk 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, creating opportunities for both arbitrage and exploitation.
- **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 in which repayment depends solely on the liquidation value of posted collateral, rather than on both collateral and borrower cash flow, increasing 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:** A condition in which 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 rather than 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.

about ECGI

The European Corporate Governance Institute has been established to improve *corporate governance through fostering independent scientific research and related activities*.

The ECGI will produce and disseminate high quality research while remaining close to the concerns and interests of corporate, financial and public policy makers. It will draw on the expertise of scholars from numerous countries and bring together a critical mass of expertise and interest to bear on this important subject.

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

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, ESSEC Business School and Oxford Law Faculty Kathryn Judge, Professor of Law, Columbia Law School Wolf-Georg Ringe, Professor of Law & Finance, University of Hamburg
Editorial Assistant	Asif Malik, ECGI Working Paper Series Manager

<https://ecgi.global/content/working-papers>

Electronic Access to the Working Paper Series

The full set of ECGI working papers can be accessed through the Institute's Web-site (<https://ecgi.global/content/working-papers>) or SSRN:

Finance Paper Series	http://www.ssrn.com/link/ECGI-Fin.html
Law Paper Series	http://www.ssrn.com/link/ECGI-Law.html

<https://ecgi.global/content/working-papers>