[For Conference Participants: This is preliminary and incomplete draft. We would love to hear your thoughts/get your comments.]

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. Immense gratitude for research assistance from . . .

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

TABLE OF CONTENTS

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, when 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] U.S. Dep't of Justice, Office of Public Affairs, *Forsage Founders Indicted in $340 M DeFi Crypto Scheme*, (Pub. L. No. 23-208) (Feb. 22, 2023), archived at https://www.justice.gov/archives/opa/pr/forsage-founders-indicted-340m-defi-crypto-scheme.

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

as DeFi, which refers to financial transactions that are facilitated by FinTech—technological systems that facilitate payments,[3] trading, and lending through digital infrastructure[4]—without the involvement of banks, broker-dealers, or other 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. 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 persons do not have access to an account,"[8] smart contracts arguably could perform those

---

[3] Digital payment systems, using cryptocurrencies evidenced by blockchain technology, provide a well-known example of FinTech. Steph Nagl, *5 FinTech Examples Transforming Everyday Life*, Wake Forest Univ. School Prof. Studies, (Dec. 5, 2023), https://sps.wfu.edu/articles/fintech-examples-transforming-everyday-life/.

[4] *See, e.g.*, Santa Clara University, Leavey School of Business, "FinTech in Finance and Analytics: Advancements and Applications" (Oct. 18, 2023) (reporting that "Recent technological advances have streamlined and reshaped traditional financial services [and that] FinTech has expanded rapidly in the past decade."), https://onlinedegrees.scu.edu/media/blog/applications-of-financial-technology-in-finance-and-analytics.

[5] *See, e.g.*, 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 (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"), https://www.nytimes.com/interactive/2022/03/18/technology/what-is-defi-cryptocurrency.html. This Article later explains why there is always some third-party involvement.

[6] Curtis Miles, *Blockchain Security: What Keeps Your Transaction Data Safe?*, IBM (Dec. 12, 2017), https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/.

[7] *See, e.g.*, U.S. DEPARTMENT OF THE TREASURY, ILLICIT FINANCE RISK ASSESSMENT OF DECENTRALIZED FINANCE 12 (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 & DIGITAL 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").

[8] Igor Makarov & Antoinette Schoar, *Cryptocurrencies and Decentralized Finance (DeFi)*, BROOKINGS 4 (Mar. 11, 2022), https://www.brookings.edu/wp-content/uploads/2022/03/SP22_BPEA_MakarovSchoar_conf-draft.pdf.

functions[9]—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 inclusion [11] and advancing FinTech's[12] 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 ("AML") and know-your-customer ("KYC") conventions, and supervisory

[9] *See, e.g.*, *What Are Smart Contracts on Blockchain*, IBM, https://www.ibm.com/topics/smart-contracts (last accessed Sept. 25, 2022) (stating that "all [smart contract] participants can be immediately certain of the outcome, without any intermediary's involvement or time loss").

[10] Prash Raval, *Compare the Best DeFi Platforms in 2022*, INVEZZ (Dec. 13, 2022), https://invezz.com/cryptocurrency/defi/platforms/. 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." 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/.

[11] *See, e.g.*, Carter Faust, Anthony Dukes, & D. Daniel Sokol, *FinTech and Financial Inclusion: A Review of the Empirical Literature*, 95 S. CAL. L. REV. POSTSCRIPT 135, 136 (2022). In relevant part, those authors find that FinTech "can play" an "important role . . . in promoting financial inclusion—the availability and equality of opportunities to access financial services." 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." 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).

accountability—that has long served as the backbone of financial regulation.[14] Eliminating traditional intermediaries can create anonymity 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. 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—without intervention from a centralized intermediary capable of monitoring and halting suspicious activity or conducting customer verification. 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,[17] 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.

---

[14] *Cf.* Baker McKenzie, *Weighing the Interconnected Risks Technology Poses to Financial Systems* (2025) ("For all the benefits that fintech has brought to consumers, businesses and societies, it has also introduced new sources of vulnerability to financial systems, raising questions about the latter's fragility."), https://www.bakermckenzie.com/en/insight/publications/resources/fintech-and-financial-stability; Saule T. Omarova, *New Tech v. New Deal: Fintech as a Systemic Phenomenon*, 36 YALE J. REG. 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 97-100 and accompanying text (discussing shadow banking).

[17] [cite]

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.[18]

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").[19] In 2025, FINRA resolved claims with Robinhood for alleged supervisory failures that led to a failure to appropriately respond to "'red flags' of potential misconduct."[20] Robinhood agreed to pay almost $30 million in penalties to FINRA and to overhaul its internal controls and customer-support infrastructure.[21] In 2025, the SEC also sanctioned Robinhood for failing to "observe a broad array of significant regulatory requirements, including . . . to accurately report trading activity, comply with short sale rules, submit timely suspicious activity reports, maintain books and records, and safeguard customer information."[22] 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.[23]

For example, DeFi platforms often distribute—or diffuse—governance responsibility across pseudonymous (that is, falsely named) developers,

---

[18] *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 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").

[19] About Us, Robinhood Markets, Inc., https://robinhood.com/us/en/about-us/ (last visited Nov. 11, 2025).

[20] Jonathan Stempel, *Robinhood paying $29.75 million to end Financial Industry Regulatory Authority probes*, USA Today (Mar. 7, 2025), https://www.usatoday.com/story/money/business/2025/03/07/robinhood-paying-fira/82012940007/

[21] Stempel, supra note 20.

[22] 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.

[23] 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.

decentralized autonomous organizations (sometimes called "DAOs"), and token holders. 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.[24] 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.[25]

This Article situates these developments within the broader evolution of financial technology with a particular focus on the platforms, like Forsage, that facilitate and exploit DeFi transactions. Advances in finance increasingly depend on FinTech, and DeFi represents FinTech's most radical extension: a financial ecosystem operating without banks, brokers, or any other institutional intermediary. While proponents claim that DeFi replaces human discretion with "immutable code" and thereby reduces 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 a realm of structural transformation—one that redefines 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 approaches risk chilling innovation and misclassifying open-source

---

[24] Statement of Comm'r Kristin N. Johnson, Regarding CFTC Resolving Charges Against Three Decentralized Finance Companies: The Need for Oversight (Sept. 7, 2023), https://www.cftc.gov/PressRoom/SpeechesTestimony/johnsonstatement090723b.

[25] *See e.g.*, CFTC Wins Default Judgment Against Ooki DAO, 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); see also CFTC Wades into DeFi Enforcement Again, Blockchain and the Law (Oct. 16, 2023), https://www.blockchainandthelaw.com/2023/10/cftc-wades-into-defi-enforcement-again (describing settled charges against Opyn, Inc. and Deridex, Inc. for operating unregistered trading platforms and failing to implement customer-identification programs).

protocols.[26] 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 no longer exist.

In response, 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. 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, underwriters, 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 lowers costs and expands 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 and human actors, 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/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: how these layered risks defeat ordinary enforcement levers,

[26] See 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* (2025) (manuscript on file with author) (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).

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 IV . . .

The Article then concludes.

Finally, the Appendix defines the critical terms used throughout 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 institutional intermediaries—banks, broker-dealers, underwriters, 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."[27] 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.[28] To take an everyday example, consider the role of banks in facilitating lending. In theory, a company capital 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

[27] Tom C.W. Lin, *Infinite Financial Intermediation*, 50 Wake Forest L. Rev. 643, 643 (2015)

[28] 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.").

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.[29] In its position as lender, the bank can acquire information to determine to whom it should extend loans and on what terms.[30] The bank is also able to serve as a long-term monitor of the borrower's condition, ensuring the return of the capital loaned and an increase in the value of the investment made.[31]

Although the intermediation can be and 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.[32] To accomplish this goal, intermediaries serve key, critical roles in the financial markets. First, intermediaries facilitate capital aggregation and reallocation, through deposit-taking, lending, and securitization, among other mechanisms.[33] In so doing, intermediaries improve market liquidity and smooth the transfer of capital within the markets.[34] Second, intermediaries disseminate information throughout the markets.[35] Exchanges, for example, facilitate the flow of information by allowing available information to be reflected in the price of assets through trading.[36] Other intermediaries, like underwriters and analysts, act as information brokers, reducing asymmetric information between companies and investors.[37] 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.[38] Underwriters in an initial public offering, for example, serve a risk management function both for the issuer—by helping with the pricing, marketing, selling of the issuance—and the investors—by acting as reputational agent and attesting to the worth of the issuance.[39]

---

[29] [cite]
[30] [cite]
[31] [cite]
[32] Hans Genberg, *The Changing Nature of Financial Intermediation and Its Implications for Monetary Policy*, *in* Financial Market Developments and Their Implications for Monetary Policy 101 (Bank for Int'l Settlements 2008), http://www.bis.org/publ/bppdf/bispap39.pdf
[33] *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.");
[34] Whitehead, *supra* note [x], at 9.
[35] [cite]
[36] [cite]
[37] [cite]
[38] [cite]
[39] Lin, *Infinite Financial Intermediation*, *supra* note [x], 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;[40] on exchanges to provide equitable access to exchange pricing information;[41] and on underwriters to ensure reliable and complete issuer disclosures in an initial public offering.[42] With other intermediaries, like banks and insurers, regulations are concerned with ensuring that these intermediaries do not take on excessive risks, thereby jeopardizing their clients' money.[43]

Given their importance and involvement in financial transactions, intermediaries are often the primary mechanism through which financial regulation occurs. 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 several 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.[44]

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.[45] 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.

---

[40] [cite to regulations]
[41] [cite to regulations]
[42] [cite to regulations]
[43] Cite to deposit insurance and limits on risk taking
[44] [cite]
[45] Kathryn Judge, *Intermediary Influence*, 82 U. Chi. L. Rev. 573, 590-591 (2015).

B.What is DeFi?

DeFi refers to financial transactions that are facilitated by FinTech without the involvement of traditional financial intermediaries.[46] More specifically, decentralized finance operates across multiple architectural layers, and analytical clarity requires distinguishing between the underlying encrypted computer codes—such as Ethereum, Binance Smart Chain, or Tron—that are programmed to execute the smart contracts that provide DeFi products and services and the protocols that guide that programming. Analytical clarity also requires distinguishing the persons—developers, operators, and supporting entities—that create those protocols. We focus on the protocols and the persons who create them.

Smart contracts epitomize how DeFi can remove the need for a traditional financial intermediary.[47] A smart contract is a self-executing computer program that automatically performs its steps when specified conditions are met.[48] Depending on their programming, smart contracts implement the rules that govern lending decisions, trade execution, collateral management, and other financial activities[49] 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. 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.[50] Loans can be disbursed nearly instantaneous, cutting lending costs.[51] In these ways, smart contracts allegedly can "eliminate

---

[46] See supra note 5 and accompanying text.

[47] *See, e.g.*, U.S. DEPARTMENT OF THE TREASURY, ILLICIT FINANCE RISK ASSESSMENT OF DECENTRALIZED FINANCE 12 (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 & DIGITAL 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").

[48] See supra notes 6-8 and accompanying text.

[49] Miles, *supra* note 6.

[50] Sirio Aramonte, Sebastian Doerr, Wenqian Huang & Andreas Schrimpf, *DeFi Lending: Intermediation Without Information?*, BIS 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.*

[51] *See id.*

the need for intermediaries in financial transactions—replacing exchanges, market-makers, asset managers, banks, and other lenders with software protocols."[52]

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 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.[53] Additionally, some treat these benefits as inherently welfare-enhancing.[54]

By removing banks and other financial intermediaries, who charge for their services, DeFi also reduces transaction costs.[55] Moreover, investors 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.

Furthermore, DeFi can help to democratize finance by broadening market access,[56] making it accessible to anyone with an internet connection and a crypto wallet.[57] That would offer global access to borrowing, securities trading,

---

[52] 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.

[53] [cite]

[54] 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.

[55] See supra notes 10-11 and accompanying text.

[56] See supra notes 11-13 and accompanying text.

[57] 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, Sokjoon Lee, Moonseong Kim & Woochan Lee, *Comparative Analysis of Security*

and other investment opportunities without needing approval from traditional financial institutions,[58] thereby benefitting those who are financially excluded or underserved.

DeFi's proponents also argue that by replacing human-managed intermediaries, smart contracts reduce the chance of human error.[59] 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.[60] In these ways, DeFi offers a level of speed, predictability, and user autonomy that conventional intermediaries struggle to match.[61]

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."[62]

* * * *

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 eliminate 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

---

Features and Risks in Digital Asset Wallets, **14** *Electronics* 2436, 2440–42 (2025), https://doi.org/10.3390/electronics14122436.

[58] [cite]

[59] [cite]

[60] [cite]

[61] [cite]

[62] Erik Vorhees, *A Response to SBF and Principled Crypto Regulation*, MONEY & STATE (Oct. 20, 2022), https://www.moneyandstate.com/blog/response-to-sbf.

consumers, and applying jurisdiction-bound regimes to a borderless, disintermediated system.

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 intermediaries and increases efficiency, DeFi reproduces familiar dangers under a new technological guise. The first subsection explores how disintermediation undermines the AML and KYC safeguards[63] 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 by rediscovering the very vulnerabilities financial regulation was designed to contain.

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

A longstanding risk is that financial market participants might engage in money laundering, which would threaten monetary integrity,[64] or that they might even finance terrorists, jeopardizing national security. [65] The decentralization of finance would make it more difficult to enforce the laws against money laundering and terrorist financing.[66] Enforcement difficulties would arise for at least two reasons: other things being equal, it would be

---

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

[64] Money laundering and terrorist financing threaten the integrity of domestic payments. U.S. DEP'T OF THE TREASURY, 2015 NATIONAL MONEY LAUNDERING RISK ASSESSMENT 6 (2015), https://home.treasury.gov/system/files/246/National-Money-Laundering-Risk-Assessment-06-12-2015.pdf [https://perma.cc/UK6E-QKSK]; U.S. DEP'T OF THE TREASURY, 2015 NATIONAL TERRORIST FINANCING RISK ASSESSMENT 4 (2015), https://home.treasury.gov/system/files/246/National-Terrorist-Financing-Risk-Assessment-06-12-2015.pdf [https://perma.cc/UUB6-WMLM].

[65] Talley, *supra* note **Error! Bookmark not defined.**.

[66] 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.").

harder to identify decentralized, rather than centralized, financial market participants; and enforcement costs would increase because there likely would 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.[67] 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.[68]

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. 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,[69] while FINRA concluded that Robinhood lacked "reasonable anti-money-laundering programs" and failed to respond to "red flags of potential misconduct." [70] 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

---

[67] 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").

[68] FINRA Rule 3310, Anti-Money Laundering Compliance Program, FINRA Manual (2024).

[69] 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/news/press-release/2025-5

[70] Jonathan Stempel, *Robinhood Paying $29.75 Million to End Financial Industry Regulatory Authority Probes*, Reuters (Mar. 7, 2025)

unlawful activity in violation of the Travel Act.[71] In parallel, the Financial Crimes Enforcement Network ("FinCEN") entered into a consent order finding that the exchange willfully failed to implement an effective AML program, lacked meaningful 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.[72]

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.[73] 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.[74] DeFi platforms typically have no physical headquarters, no compliance officers, and no practical mechanism for conducting customer identification or monitoring transactions in real time. The absence of centralized control makes it exceedingly 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.[75] Although some

---

[71] 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, Legal Update, Dec. 23, 2025), https://connect.mayerbrown.com/584/18748/december-2025/legal-updatevirtual-currency-exchange-pleads-guilty-to-criminal-charges-related-to-anti-money-laundering-violations-and-pays-multi-million-dollar-fine-to-fincen.asp.

[72] Resnikoff, supra note 71.

[73] Resnikoff, supra note 71.

[74] 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).

[75] 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 U.S. Dep't of the Treasury, FinCEN Advisory on Customer Due Diligence Requirements for Financial Institutions (May 11, 2016). These

DeFi platforms claim to employ geofencing—blocking internet protocol ("IP") addresses associated with sanctioned jurisdictions [76] —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.[77]

Enforcement experience confirms these compliance deficiencies. In 2023, the CFTC brought actions against DeFi platforms Opyn, Inc., Deridex, Inc., and ZeroEx, Inc., finding that each offered leveraged or margined digital asset transactions without registering as required under the Commodity Exchange Act and that Opyn and Deridex failed to adopt KYC and AML programs consistent with the obligations imposed on registered futures commission merchants under 17 C.F.R. § 42.2.[78] 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. The Financial Crimes Enforcement Network ("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. [79] Centralized intermediaries thus provide regulators with both data and jurisdictional hooks—compliance officers, transaction records, and identifiable management—necessary to enforce AML and know-your-customer obligations.

---

measures underpin effective AML programs by linking transactions to identifiable actors and ensuring accountability within the financial system.

[76] *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.

[77] See Office of Foreign Assets Control, Sanctions Compliance Guidance for the Virtual Currency Industry (Oct. 15, 2021), https://ofac.treasury.gov/media/608/download?inline (discussing crypto-wallet-address screening and sanctions exposure in the virtual currency sector); U.S. Department of the Treasury, Illicit Finance Risk Assessment of Decentralized Finance 22–24 (Apr. 6, 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).

[78] See CFTC v. Ooki DAO, No. 3:22-cv-5416 (N.D. Cal. 2023); see also Elanit Snow & Jonathan Mollod, CFTC Wades into DeFi Enforcement Again, Blockchain & the Law (Oct. 16, 2023) (describing the CFTC's charges against Opyn, Inc., Deridex, Inc., and ZeroEx, Inc. for failing to register as required and for lacking required KYC and AML programs).

[79] 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 Nov. 11, 2025).

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.[80] 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 remembering that this case was not actively litigated and the CFTCs authority to bring the case was therefore not questioned by a litigant.[81] 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 what traditional finance has long recognized as "two ways out" lending: having two independent sources of repayment—cash flow and asset value.

---

[80] 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, CFTC Wins Default Judgment Against Ooki DAO (June 20, 2023), https://www.cftc.gov/PressRoom/PressReleases/8715-23.

[81] 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, CFTC Wins Default Judgment Against Ooki DAO (June 20, 2023), https://www.cftc.gov/PressRoom/PressReleases/8715-23 (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.[82] 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.[83] 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.[84] The rationale is to enable loans to be disbursed nearly instantaneous, cutting lending costs.[85]

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.[86] 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.[87] In August 1929, however, a relatively modest decline in stock prices caused some of those loans to become under-collateralized.[88] 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.[89]

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

---

[82] *Compare* Sirio Aramonte, Sebastian Doerr, Wenqian Huang, & Andreas Schrimpf, *DeFi Lending: Intermediation without Information?*, BIS BULLETIN NO. 57, at 1 (June 2022) (reporting that DeFi lending has risen from virtually zero in 2020 to more than $50 billion by early 2022), available at https://www.bis.org/publ/bisbull57.pdf, *with* Giulio Cornelli, Leonardo Gambacorta, Rodney Garratt, & Alessio Reghezza, Why DeFi Lending? Evidence from Aave V2, 63 J. FIN. INTERMEDIATION (July 2025) (Article 101166) (reporting that the IMF estomates the overall DeFi- lending debt outstanding to be around $25 billion in 2022).

[83] *See, e.g.,* Rutgers University, Credit Standards (Feb. 6, 2015) ("Bank lenders typically look for at least 'two ways out'"), https://www.coursehero.com/file/p7emi70/Credit-Standards-Bank-lenders-typically-look-for-at-least-two-ways-out-First/.

[84] *See supra* note 50 and accompanying text.

[85] *See supra* note 51 and accompanying text.

[86] *See* Iman Anabtawi & Steven L. Schwarcz, *Regulating Systemic Risk: Towards an Analytical Framework*, 86 NOTRE DAME L. REV. 1349, 1356-57 (2011).

[87] *Id.*

[88] *Id.*

[89] *Id.*

by the homes that the borrowers purchased with the loan proceeds.[90] Those "subprime" mortgage loans were then bundled together as collateral to partially support the payment of complex asset-backed securities that were sold to banks and other institutional investors worldwide.[91] 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.[92] 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.[93] 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.[94]

DeFi's one-way-out lending model invites these same risks. The problem is that any type of asset used as collateral can unexpectedly decline in value, causing loans secured by such assets to become undercollateralized. Thus, a $100,000 loan that is initially secured, for example, by $110,000 of a certain type of cryptocurrency[95] will become significantly undercollateralized if the value of that cryptocurrency declines, say, by 20% (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.[96] 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.

---

[90] *Id.* at 1359-60.

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] See, e.g., Cornelli, et al., supra note 82: "Anonymity and crypto assets volatility leads to reliance on overcollateralisation as a risk management tool, as there is no other way to assess the borrower's ability to repay. . . . DeFi's reliance on crypto assets as collateral also makes it largely self-referential and limits its interaction with the real economy."

[96] See supra note 50 and accompanying text (discusisng that DeFi lending allows parties to access funding simply by providing pre-specified forms of standardized collateral). See also Giulio Cornelli et al., supra note 82 ("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.*

3. Shadow Banking & the DeFi Parallel

DeFi's decentralization of finance also could pose risks similar to those caused by the advent of shadow banking. Shadow banking refers broadly to the movement of financial intermediation away from traditional, regulated banks into markets and nonbank financial entities such as hedge funds, money market funds, and structured investment vehicles. 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.[97]

By encouraging regulatory arbitrage, this shift caused a significant portion of the financial system to become unregulated.[98] 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. The lack of regulatory protection allowed excessive "[m]aturity and credit transformation in the shadow banking system," which arguably "contributed significantly to asset bubbles in residential and commercial real estate markets prior to the" Global Financial Crisis.[99] 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.[100]

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

---

[97] *See generally* Victor Fleischer, *Regulatory Arbitrage*, 89 TEX. L. REV. 227 (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.").

[98] Eric Feyen et al., *Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy*, Bank Int'l Settlements Papers, July 2021, at 13, 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 DEALB%K (May 27, 2011, 1:29 PM), http://dealbook.nytimes.com/2011/05/27/ (follow "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).

[99] ZOLTAN POZSAR ET AL., FED. RESERVE BANK OF N.Y., STAFF REPORT NO. 458, SHADOW BANKING (2010) (abstract).

[100] Fleischer, *supra* note 97, 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 99, at 1.

intermediation functions without equivalent safeguards.[101] 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,[102] creating what the Federal Reserve calls funding risk: the danger of "large, sudden withdrawals of funds" and fire sales during adverse shocks.[103] Because DeFi credit and liquidity provision typically rely on crypto-native assets—including volatile cryptocurrencies and stablecoins that reference fiat currency[104] 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.[105]

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.[106] 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 the system "very fragile against the occurrence of adverse shocks."[107] 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.

---

[101] 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).

[102] Cf. supra note 96 and accompanying text (discussing DeFi lending's reliance on crypto assets as collateral).

[103] Pablo D. Azar et al., The Financial Stability Implications of Digital Assets, 30 Fed. Rsrv. Bank N.Y. Econ. Pol'y Rev. 1, 8 (Nov. 2024), (defining funding risk as the possibility of "large, sudden withdrawals of funds—a situation commonly referred to as a run").

[104] 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.

[105] Pablo D. Azar et al., The Financial Stability Implications of Digital Assets, 30 Fed. Rsrv. Bank N.Y. Econ. Pol'y Rev. 1, 25-26 (Nov. 2024), (describing automated liquidations and cascading price effects across DeFi platforms).

[106] Hilary J. Allen, DeFi: Shadow Banking 2.0?, 64 Wm. & Mary L. Rev. 919 (2023).

[107] Azar et al., supra note __, at 4 ("The lack of a strong and cohesive regulatory framework for digital assets also amplifies these vulnerabilities … rendering the crypto system very fragile against adverse shocks.").

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.

* * * *

Taken together, these "old" risks—compliance failures, imprudent lending, and unregulated intermediation—underscore how DeFi, despite its technological novelty, replicates the structural vulnerabilities that have destabilized financial markets for over a century. 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 finance transactions away from intermediaries, DeFi poses new, novel 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.[108] This Part focuses on risks that plague DeFi, raising questions about the inherent costs of DeFi for consumers, the markets, and the DeFi platforms themselves.

1. Technological Vulnerabilities

One of the primary risks that DeFi faces relates to its very foundation—smart contracts. The compute 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.[109] This could be a particular problem given the irreversibility and finality of transactions executed on a blockchain.[110] Further compounding the issue is the absence of any centralized authority, which could leave victims without recourse in the event

---

[108] 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).

[109] https://www.ecb.europa.eu/press/financial-stability-publications/macroprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html

[110] https://www.fsb.org/uploads/P160223.pdf

of theft or fraud or other loss.[111] 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.[112] As DeFi has grown, so too have the attacks on DeFi platforms, with billions of dollars of value being lost each year.[113]

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.[114] With composability, smart contracts can interoperate to provide novel, highly sophisticated products and services not available from a single smart contract.[115]

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. 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 mechanism to determine asset values—each governed by separate smart contracts. 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.[116]

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. 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

---

111 https://www.ecb.europa.eu/press/financial-stability-publications/macroprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html

112 https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/

113 https://therecord.media/cybercriminals-stole-over-1-billion-from-crypto-funds-2023

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

115 https://www.fsb.org/uploads/P160223.pdf at 9; Francesca Carapella et al., *Decentralized Finance (DeFi): Transformative Potential & Associated Risks*, FEDERAL RESERVE BANK OF BOSTON 23 (Sep. 8, 2022).

116 *See e.g.*, https://adforensics.com.ng/flash-loan-attacks-what-they-are-how-they-work-and-how-to-stay-safe/

propagate through the DeFi ecosystem before any human actor can intervene.[117]

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.

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.[118] 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.[119] 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.[120] 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.[121] To many,

---

[117] https://adforensics.com.ng/flash-loan-attacks-what-they-are-how-they-work-and-how-to-stay-safe/

[118] https://quantstamp.com/blog/defis-composability-more-possibility-more-risk

[119] https://www.fsb.org/uploads/P160223.pdf

[120] Nic Carter and Linda Jeng, *DeFi Protocol Risks: the Paradox of DeFi* 34

[121] 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).

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.[122] Indeed, according to one study, some traders prefer decentralized exchanges over centralized ones because of their greater anonymity despite their higher costs.[123] 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.[124] Because smart contract 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.[125] 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.[126] Such malicious or manipulative behavior therefore cannot always feasibly be detected or punished.[127] 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.[128] Thus, pseudonymity can benefit malicious actors who conceal their bad behavior, thereby evading consequences for their misdeeds.

Lastly, the pseudonymity of DeFi can lead to an overall opacity that challenges efforts to see where and how DeFi is interconnected both internally and with the traditional financial system. Pseudonymity makes it nearly

---

[122] https://www.bis.org/publ/work1061.pdf
[123] https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf
[124] https://www.bis.org/publ/bppdf/bispap156.pdf
[125] https://www.bis.org/publ/bppdf/bispap156.pdf (defining a rug pull scam); see also Jared Ronis, DeFi 101: The Good, the Bad, and the Regulatory, Wilson Center (Sept. 29, 2023) available at https://acrosskarman.wilsoncenter.org/article/defi-101-good-bad-and-regulatory?gad_source=1&gad_campaignid=20397340047&gbraid=0AAAAAD3FqONYkXz_b1U6ptq4Fl7KuTdrZ&gclid=CjwKCAiAw9vIBhBBEiwAraSATglw4i4qKarsTjnDrnM48XxerRTDSK3w9mHIPQxYmVrreJV2Q5Fl-RoClYUQAvD_BwE.
[126] https://www.sec.gov/newsroom/speeches-statements/crenshaw-defi-20211109
[127] https://www.sec.gov/newsroom/speeches-statements/crenshaw-defi-20211109
[128] Vincent Gramlich et al., *Decentralized Finance (DeFi): Foundations, Applications, Potentials, and Challenges*, 44 (Aug. 22, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4535868.

impossible to assess the level of interconnections within the DeFi ecosystem, thereby leaving the system vulnerable to unknown levels of risk.[129] One developer may operate multiple crypto wallets across multiple platforms, each under a different pseudonym. Given the inability to identify any given DeFi developer, there is no way to gain meaningful insight into the developer's market concentration or vulnerabilities, such as a dependence on other parties for liquidity.[130] Further, as the interconnections between DeFi and traditional financial markets continue to grow, this lack of insight into their interconnectivity is likewise problematic. To date, fallout from DeFi has not had systemic consequences for the traditional financial system, but this is only likely to worsen as DeFi's linkages with the traditional financial system grow.[131]

3. Governance Risks

Although a central promise of DeFi is decentralization, the actual level of decentralization varies, especially with respect to DeFi governance.[132] DeFi governance refers primarily to the process by which decisions are made for a platform.[133] 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.[134] 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 were often highly centralized to better ensure their viability and stability.[135] 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.

---

[129] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf

[130] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf at pg. 14

[131] https://www.bis.org/publ/work1061.pdf

[132] Francesca Carapella et al., *Decentralized Finance (DeFi): Transformative Potential & Associated Risks*, FEDERAL RESERVE BANK OF BOSTON 21 (Sep. 8, 2022) ("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."); https://www.fsb.org/uploads/P160223.pdf

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

[134] Francesca Carapella et al., *Decentralized Finance (DeFi): Transformative Potential & Associated Risks*, FEDERAL RESERVE BANK OF BOSTON 21 (Sep. 8, 2022) ("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.")

[135] Francesca Carapella et al., *Decentralized Finance (DeFi): Transformative Potential & Associated Risks*, FEDERAL RESERVE BANK OF BOSTON 21 (Sep. 8, 2022).

First, full decentralization is unlikely.[136] And, second, governance authority is typically concentrated in the hands of a few.

To participate in DeFi governance, developers and investors often must acquire a governance, or voting, token.[137] These tokens are explicitly assigned specific governance rights and do not have independent monetary value outside the ability to vote on future governance measures.[138] Insiders, such as developers, founders, and early funders of a DeFi platform, are often granted a substantial number of governance tokens, concentrating power in their hands.[139] Additionally, insiders can aggregate governance tokens, increasing their concentration of power.[140] 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.[141]

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. For example, such large token holders could congest the blockchain by engaging in artificial trades between their accounts, which would in turn increase the fees that others pay them to trade.[142] Further, if governance tokens are tradable, malicious actors could acquire enough power to alter the platform for their own financial gain.[143] 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

---

[136] https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf (calling full decentralization of DeFi illusory since all DeFi platforms have an element of centralization around governance)

[137] *See* Campbell R. Harvey, *DeFi and the Future of Finance*, SSRN 21 (Feb. 6, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3711777 (noting that to participate in the governance process, parties must acquire a token).

[138] *See* David Gogel, *DeFi Beyond the Hype*, THE WHARTON SCHOOL 13 (May 2021), https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf (explaining that the value of the token reflects investor expectations about the success of the protocol).

[139] https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf at 28

[140] *See* Aina Turillazzi et al., *Decentralised Finance (DeFi): A Critical Review of Related Risks and Regulation*, SSRN 7 (Nov. 2, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4593242 (explaining how this voting mechanism is criticised for granting a disproportionate amount of voting power in early investors or the original team).

[141] *See* Aina Turillazzi et al., *Decentralised Finance (DeFi): A Critical Review of Related Risks and Regulation*, SSRN 7 (Nov. 2, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4593242 (explaining how this voting mechanism is criticised for granting a disproportionate amount of voting power in early investors or the original team).

[142] https://www.bis.org/publ/qtrpdf/r_qt2112b.pdf

[143] 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 at 34.

DAO, liquidate its $44 million treasury, and distribute $25 million of the treasury to themselves.[144]

While some DeFi platforms closely engage investors in the decision-making process, others may require substantial participation in voting before any changes are even considered.[145] Still others may grant veto rights to particular governance-token holders, fully embracing the concept that while all governance votes are equal, some are more equal than others.[146] The problem is not necessarily that different governance models exist, but rather that these governance features are not fully transparent to investors.[147] 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

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." 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.

---

[144] Aina Turillazzi et al., *Decentralised Finance (DeFi): A Critical Review of Related Risks and Regulation*, SSRN 7 (Nov. 2, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4593242

[145] https://www.fsb.org/uploads/P160223.pdf

[146] See George Orwell, *Animal Farm.*

[147] https://www.fsb.org/uploads/P160223.pdf; 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

Macroprudential regulation typically proceeds by identifying structural market failures that can amplify localized shocks into system-wide instability. 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 asymmetric information.[148] 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.[149] 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 are typically privately owned by their developers.[150] 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.[151] These conflicts, though, are exacerbated by complexity, which greatly increases the information asymmetry between DeFi-platform managers and investors.[152] 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.[153] Accordingly, the existing macroprudential regulation that

---

[148] *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).

[149] 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).

[150] [cite1]

[151] *See supra* notes 1-2, 112-113, and 125 and accompanying text.

[152] *See supra* notes 148-149 and accompanying text.

[153] 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.

applies to those market failures should already help to protect against DeFi financial instability. For example, DeFi platforms that become significant enough to be designated as systemically important financial institutions ("SIFI"s) would be subjected to SIFI-related macroprudetial 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.[154]

For these reasons, any new macroprudential regulation of DeFi platforms should focus on fixing the potential market failure of complexity, in particular reducing the information asymmetry between developers of, and investors in, DeFi platforms caused by DeFi's complexity. A blunt way to reduce DeFi's complexity would be to prohibit decentralized finance. That, however, would stifle innovation. 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.[155]

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.[156]

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,

---

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 154 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.*

[154] *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].Regu••••

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

[156] *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").

and standardized (STS) securitization transactions.[157] This framework incentivizes, rather than mandates, STS transactions by reducing regulatory capital requirements for investors therein, thereby allowing for potential innovation. 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 FeFi'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)[158] as well as a Financial Stability Oversight Council (FSOC)[159] 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.[160] 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.[161]

Until we more fully understand DeFi and its risks, ex ante preventative regulation almost certainly will be insufficient. Regulators therefore may wish also to examine potential ex post regulation to mitigate any harmful consequences caused by the collapse of DeFi platforms.[162] In connection with the COVID pandemic, for example, the Federal Reserve provided such ex post regulation by creating the Commercial Paper Funding Facility to support "the flow of credit to households and businesses" that was lost when the

---

[157] *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).

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

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

[160] 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].

[161] 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].

[162] *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).

private commercial paper market collapsed.[163] 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.[164] 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.[165] Some argue, for example, that the Basel II capital requirements contributed to the 2008 financial crisis by globally correlating faulty rules.[166] Regulatory harmonization also, paradoxically, can invalidate existing risk-management strategies that are premised on randomness and independent action.[167] For example, the value-at-risk (VaR) model presumed that portfolio managers act independently of each other.[168] Incorporating VaR into regulation, however, can incentivize managers to act more uniformly, thereby undermining VaR's utility as a risk-management tool.[169]

(b) *Microprudential Regulation*. Regulation designed to protect the individual safety and soundness of parties acting in the financial system is referred to as "microprudential."[170] The purpose is to reduce the chance that any given party fails, thereby harming its investors and counterparties.[171] Traditional bank

---

[163] *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).

[164] *See infra* notes 178-193 and accompanying text.

[165] 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).

[166] Romano, *supra* note 165, at 13–20.

[167] Whitehead, *supra* note 156, at 347.

[168] *Id.* at 341.

[169] *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).

[170] *See, e.g.*, Lucrezia Cipriani & Andrea Minto, *Microprudential Regulation*, chapter 10 in COMPARATIVE FINANCIAL REGULATION 155 (Alessio M. Pacces, Edoardo D. Martino, & Hossein Nabilou, eds. 2025).

[171] *Id.*

regulation epitomizes such regulation, requiring each bank to act with prudence.[172]

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.[173] 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, we do 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.[174]

2. The Consumer Protection Conundrum

DeFi's most acute consumer-protection challenge arises from the disappearance of the 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.[175] Because there was no intermediary to vet disclosures, supervise sales practices, or halt abusive activity, more than $340 million was extracted from retail investors worldwide, with over 80% of those investors receiving

---

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

[173] *See supra* notes 137-141 and accompanying text.

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

[175] 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

fewer ETH back than they invested and more than half never receiving any payout at all.[176] 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. 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.[177] Even in cases where regulators succeed, the remedy often arrives years after consumer harm has occurred and provides little meaningful redress to victims.

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 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

---

[176] 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

[177] See Complaint, CFTC v. Ooki DAO, No. 3:22-cv-05416 (N.D. Cal. Sept. 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.)

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.[178] Criminals can use DeFi, for example, to launder illicit funds while obfuscating both the origin and destination of such funds.[179] 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.[180]

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.[181] For example, in March 2022, a North Korean sponsored cyber hacking group stole virtual assets worth approximately $620 million from a blockchain project.[182] A few months later, in June 2022, the same group stole another $100 million from Horizon, a DeFi cross-chain bridge.[183] North Korea is also behind numerous ransomware attacks and has dispatched thousands of hackers worldwide to steal and launder virtual assets.[184] The stolen virtual assets and revenue generated therefrom may have been used for North Korea's nuclear weapons and ballistic missile programs, in addition to providing a source of revenue for the heavily-sanctioned nation.[185]

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

---

[178] *Illicit Finance Risk Assessment of Decentralized Finance*, U.S. DEPARTMENT OF THE TREASURY 26-28 (Apr. 2023).

[179] *Illicit Finance Risk Assessment of Decentralized Finance*, U.S. DEPARTMENT OF THE TREASURY 26-28 (Apr. 2023).

[180] *Illicit Finance Risk Assessment of Decentralized Finance*, U.S. DEPARTMENT OF THE TREASURY 16-18 (Apr. 2023).

[181] See generally, *Illicit Finance Risk Assessment of Decentralized Finance*, U.S. DEPARTMENT OF THE TREASURY (Apr. 2023).

[182] https://www.fbi.gov/news/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea

[183] 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." https://www.chainalysis.com/blog/introduction-to-cross-chain-bridges/

[184] *Illicit Finance Risk Assessment of Decentralized Finance*, U.S. DEPARTMENT OF THE TREASURY 24-25 (Apr. 2023).

[185] *Illicit Finance Risk Assessment of Decentralized Finance*, U.S. DEPARTMENT OF THE TREASURY 24-25 (Apr. 2023).

complicates the application of laws and, in some instances, makes it difficult to determine which laws apply in certain transactions or instances.[186] 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.[187] 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.[188] 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.[189]

Similarly, criminal actors may seek out jurisdictions with relaxed or nonexistent regulations to carry out their illicit activity to further avoid accountability.[190] Indeed, across various jurisdictions, some regulators may lack the authority, capacity, or willingness to go after crimes related to digital assets, making enforcement even more difficult.[191] Additionally, evidence gathering can be complicated for DeFi platforms that have their operations and customers spread across multiple countries.[192] Regardless, the cross-border nature of DeFi and the ease with which transactions are executed

---

186 https://www.ecb.europa.eu/press/financial-stability-publications/macroprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html

187 https://www.cftc.gov/PressRoom/PressReleases/8837-23

188 https://www.cftc.gov/PressRoom/PressReleases/8825-23

189 *Illicit Finance Risk Assessment of Decentralized Finance*, U.S. DEPARTMENT OF THE TREASURY 26 (Apr. 2023).

190 https://www.justice.gov/d9/pages/attachments/2022/06/07/ncet_executive_order_report.pdf

191 https://www.justice.gov/d9/pages/attachments/2022/06/07/ncet_executive_order_report.pdf

192 https://www.justice.gov/d9/pages/attachments/2022/06/07/ncet_executive_order_report.pdf

globally make it exceedingly likely that law enforcement efforts will be duplicated across agencies and countries in the event of misconduct.[193]

* * * *

Taken together, the traditional, technological, and governance risks identified in Part II show how DeFi recreates well-known vulnerabilities while generating new ones. These risks are further intensified by DeFi's global, permissionless nature, which complicates oversight and weakens the effectiveness of country-specific regulatory tools. The next Part turns to the regulatory and compliance challenges that arise from this risk architecture and considers how they might be addressed.

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.

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. 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—underscore why neither "code as law" nor after-the-fact regulation can function as a complete governance strategy for DeFi in isolation.

---

193 https://www.justice.gov/d9/pages/attachments/2022/06/07/ncet_executive_order_report.pdf

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, it reframes DeFi regulation as a project of functional reconstruction: re-embedding stability, accountability, and oversight into decentralized systems without abandoning their technological form.

A. Ex Ante Architectural Constraints

- Require Smart contracts to include regulable infrastructure that mimics intermediation
    - Human override and emergency controls
    - Circuit breakers or tripwires – automatic halts during volatility, when fraud is occurring, etc.
    - Create stress-mitigation mechanisms.
- Example of why this might be important? High Frequency Trading? Shadow Banking?

B. Large v. Small Firm Ex Ante Architecture

1. Large Firms

- Third-party experts/oversight/certification?
- Disclosure requirements (governance structure/control rights, etc.)

2. Small Firms

- Economic incentives?
- Ownership disclosure requirements so enforcement can occur?

C. Ex Poste 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 IOSCO has emphasized, DeFi's elimination of traditional intermediaries removes actors

that historically served as gatekeepers for market integrity, AML/CFT compliance, and fraud prevention—thereby magnifying the risk of misconduct absent effective substitutes. Enforcement therefore plays an indispensable role not merely by punishing violations ex post, but by reshaping incentives ex 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.[194] 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.[195] 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.[196] 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.[197] Second, enforcement may extend to governance participants exercising operational power, where token-based voting or DAO

---

[194] *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).

[195] U.S. Dep't of the Treasury, Office of Foreign Assets Control, Exodus Movement, Inc. Settlement (Dec. 16, 2025) (finding willful and reckless evasion of sanctions controls through operational practices and requiring enhanced compliance commitments).

[196] U.S. Dep't of the Treasury, Office of Foreign Assets Control, Exodus Movement, Inc. Settlement Agreement (Dec. 16, 2025).

[197] In re Opyn, Inc., CFTC No. 23-18 (Sept. 7, 2023); In re Deridex, Inc., CFTC No. 23-17 (Sept. 7, 2023); In re ZeroEx, Inc., CFTC No. 23-16 (Sept. 7, 2023).

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.[198] 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.[199] 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 structural lag: by the time jurisdiction is asserted and 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 habits needed for this sort of coordination: specifically, in domains characterized by transnational, fast-moving misconduct—most notably anticorruption.

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 shifted from unilateral action toward coordinated global settlements, in which multiple sovereigns share evidence, align investigative strategies, synchronize resolutions, and allocate penalties.[200] 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

---

[198] *Commodity Futures Trading Comm'n v. Ooki DAO*, No. 3:22-cv-05416, slip op. (N.D. Cal. June 8, 2023).

[199] **U.S. Dep't of the Treasury, Office of Foreign Assets Control**, *Exodus Movement, Inc. Settlement Agreement* (Dec. 16, 2025).

[200] Rachel Brewster, *The Rise of Global FCPA Settlements*, 104 Tex. L. Rev. 299, 300–05, 354–57 (2025).

cannot exploit gaps between national systems.[201] OECD institutions have reinforced this shift by promoting joint investigations, information-sharing frameworks, and peer-based capacity building among enforcement authorities.[202] 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 fuse architectural constraint ex ante with accountability ex post. Where enforcement operates unilaterally, that fusion 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 natively 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 cooperation in adjacent domains that map closely onto DeFi's risk profile. The International Organization of Securities Commissions (IOSCO) provides an established forum for coordination around market integrity, trading misconduct, and crypto-asset market oversight;[203] the Financial Action Task Force (FATF) has built robust mechanisms for aligning AML/CFT standards,

---

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

[202] OECD, *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions* (1997); OECD, *Governments' Assessments of Corporate Anti-Corruption Compliance* 7–9 (2025).

[203] **Int'l Org. of Sec. Commissions**, *Decentralized Finance (DeFi) Report* 6–10, 36–38 (Mar. 2022) (describing IOSCO's role in coordinating regulatory responses to market integrity risks posed by DeFi).

risk typologies, and enforcement expectations across jurisdictions;[204] and the International Monetary Fund (IMF) and Financial Stability Board (FSB) coordinate surveillance and policy responses to cross-border threats to financial stability.[205] Bilateral and multilateral enforcement cooperation—through memoranda of understanding, joint investigations, and parallel proceedings—has become routine in sanctions, corruption, and market abuse cases.[206] The challenge in DeFi is therefore not institutional absence, but institutional adaptation: existing bodies must be leveraged and, where necessary, supplemented with task-specific coordination focused on speed, attribution, and technical expertise.

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.[207] 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 speed, decisive action, and national security—characteristics often associated with the Trump Administration—cross-border enforcement task forces offer

---

[204] **Fin. Action Task Force**, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* 7–12, 55–60 (2021); see also **OECD**, *Governments' Assessments of Corporate Anti-Corruption Compliance* 7–9, 42–44 (2025) (describing FATF-based coordination, shared typologies, and cross-border alignment of enforcement expectations).

[205] **OECD**, *Governments' Assessments of Corporate Anti-Corruption Compliance* 32–38 (2025) (discussing IMF- and FSB-linked coordination, peer learning, and cross-jurisdictional supervisory capacity-building).

[206] Rachel Brewster, *The Rise of Global FCPA Settlements*, 104 Tex. L. Rev. 299, 354–57 (2025) (documenting the normalization of parallel proceedings, information-sharing, and coordinated resolutions across jurisdictions).

[207] Int'l Org. of Sec. Commissions, Decentralized Finance (DeFi) Report, supra note 1, at 38–44 (emphasizing shared risk typologies and coordinated regulatory responses); OECD, Governments' Assessments of Corporate Anti-Corruption Compliance, supra note 2, at 38–44 (describing mutual learning, coordinated tools, and enforcement alignment as collective goods).

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. 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.

* * * *

Taken together, embedded compliance and coordinated enforcement reconstruct the stabilizing functions historically supplied by financial intermediaries without reinstating traditional institutional gatekeepers.

IV. ADDITIONAL QUESTIONS & CONCERNS.

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 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.[208] 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. 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.[209]

---

[208] 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, *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).

[209] 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

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.[210] 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.[211]

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 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.

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

---

blockchain protocols function as digital infrastructure and should be regulated functionally rather than institutionally).

[210] 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).

[211] See Brummer, supra note 1, at 143–45 (noting concerns that premature or misaligned regulation of DeFi could suppress experimentation before its social benefits are fully realized).

regulatory hesitation allowed fragile structures to scale unchecked until market discipline arrived in the form of collapse. 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 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.[212] 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.[213] 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.[214]

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

---

[212] 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); Basel Inst. on Governance, Collective Action (documenting industry–government anticorruption initiatives).

[213] 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).

[214] 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).

guidance, monitoring, and incentives.[215] 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 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, enforcement-by-design and coordinated accountability are 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. 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

[To be written]

[215] See OECD, *Companies' Assessments of Anti-Corruption Compliance* (2025); OECD, *Governments' Assessments of Corporate Anti-Corruption Compliance* (2025) (emphasizing collective action, peer learning, and public–private engagement as complements to enforcement).

APPENDIX

- Platform: A DeFi-based business organization, such as Forsage, that uses smart contracts to provide financial services.

- 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.

- Protocol or Protocols: Protocols refer to the rules, logic, and/or instructions to be used for programming computer code into a platform's smart contracts in order to enable those contracts algorithmically to perform specific financial functions without relying on a central authority. The terms protocol and platform are sometimes, incorrectly, used interchangeably.

- Algorithm: The steps programmed into smart contracts that enable them, typically in a self-executing manner, to perform financial services or provide financial products.

- Permissionless*:* This means that persons do not require permission to invest in or otherwise use a DeFi platform.