Bridging Policy and Practice: A Pragmatic Approach to Decentralized Finance, Risk, and Regulation

Eric W. Hess*

ABSTRACT

Confronted with a Hobson's choice of either implementing stringent enforcement of uncertain regulation or geo-fencing the United States, regulators and stakeholders must consider collaborative alternatives for shaping the future of decentralized finance ("DeFi"). Championing collaboration, this Article emphasizes the need for all DeFi stakeholders, from intermediaries to builders, to proactively enhance transparency and risk management, irrespective of regulatory dictates.

* Eric Hess has decades of experience in top legal, compliance, risk, technology, advocacy, board level, and management roles for equities exchanges, broker-dealers, investment advisors, and fintech, digital asset and cybersecurity companies. He is the founder of Hess Legal Counsel and host of the "Encrypted Economy" podcast.

Starting with the Security and Exchange Commission's (SEC) formation in the 1930s, this Article explores the evolution of the SEC's initial technology-forward approach to regulating intermediaries and disruptive technologies. The 2008 financial crisis marked a shift by both the SEC and Commodity Futures Trading Commission ("CFTC") towards regulating disruptive technologies, like automated trading and digital assets, as potential threats to financial stability, reflecting a reactive, top-down regulatory response. Collaborative efforts between stakeholders and regulators are essential for regulations that are well-informed by market and technological developments.

DeFi offers an opportunity to reconsider that approach by pursuing achievable initiatives aimed at bolstering transparency and risk management. Public-private collaborations are explored as a reasoned alternative to a blunt application of the "same risk, same rules" paradigm to DeFi. In contrast, the proposed collaborative approach would foster actionable risk mitigation practices and resilience through an informed, pragmatic process.

This Article explores the possibilities for innovative anti-money laundering verification and risk processes for DeFi as part of an open collaborative approach. It also evaluates potential adaptations of existing SEC and CFTC rules and guidance to diligence; risk management; and pre-transaction, smart contract-encoded controls for institutional DeFi users.

Pursuing this path would substantially enhance outcomes for both regulators and stakeholders. It would aim to strike a balance between regulatory objectives, risk management, and innovation, while facilitating a more efficient enforcement paradigm.

Table of Contents

I.   INTRODUCTION

The rapid adoption of digital assets, combined with the potential of decentralized finance ("DeFi") protocols to disintermediate traditional financial institutions, has raised concerns among regulators and policymakers alike. These concerns stem from perceived threats to market and financial system integrity, investor protection, monetary stability, and financial system resilience.

A controversial topic in the initial years of the 2020s has been whether the conventional intermediary-based regulatory framework should be modified to accommodate digital assets and DeFi. This issue underscores a divide between regulators. On one hand, the Securities and Exchange Commission (SEC) has challenged the adoption of disruptive financial technologies ("fintech"), and, on the other hand, proponents of innovative fintech must confront the constraints of a harsh regulatory and politicized environment.[1] This tension is amplified by a growing mutual distrust,[2] despite the SEC's historical openness to disruptive fintech prior to the 2008 financial crisis.[3]

In the stream of real-time analysis concerning legal and regulatory altercations impacting digital assets, the broader historical context can easily become obscured. The first two parts of this Article aim to shift this perspective, providing an overview of how disruptive technologies have historically interacted with regulation, the events that seemingly damaged this relationship, and the implications of this dynamic for DeFi.[4] The remaining three parts of this Article aim to accomplish two goals. First, to provide an alternative perspective for regulators and policymakers by suggesting a more collaborative and efficient model to adapt to disruptive fintech. Second, to present DeFi ecosystem participants with a practical approach to begin adapting to a rapidly evolving regulatory and risk environment. Utilizing case studies and real-world examples, this Article identifies compelling areas for attention and outlines potential steps toward progress. These potential steps foster cooperation across diverse

---

1.   *See infra* Sections III.G and IV.C.

2.   *See, e.g.*, Gary Gensler, Chair, U.S. Sec. & Exch. Comm'n, "*We've Seen This Story Before," Remarks before the Piper Sandler Global Exchange & Fintech Conference* (June 8, 2023), https://perma.cc/ZN4V-PJ2Z (referring to an unspecified set of actors and schemes in crypto as "Hucksters. Fraudsters. Scam artists. Ponzi schemes. The public left in line at the bankruptcy court").

3.   *See, e.g.*, Douglas W. Arner et al., *The Evolution of FinTech: A New Post-Crisis Paradigm?*, 47 GEO. J. INT'L. L. 1271, 1272–73 (2016); Chris Brummer, *Disruptive Technology and Securities Regulation*, 84 FORDHAM L. REV. 977, 1037 (2015); Dirk A. Zetzsche et al., *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, 23 FORDHAM J. CORP. & FIN. L. 31 (2017).

4.   *See infra* Parts II–III.

stakeholders—referred to as hybrid finance stakeholders—in the DeFi ecosystem over alterations to the underlying protocols.

Part II of this Article is primarily a case study of the SEC, as it historically embraced decentralization of market functions and disruptive fintech as tools to accomplish regulatory goals. Prior to 2008, the SEC adopted a proactive and forward-thinking approach towards disruptive fintech, in contrast with its more recent stance on digital assets and DeFi technologies. The SEC even compelled the adoption of technological advancements to bring about changes in market structure and facilitate competition.

Part III discusses the 2008 financial crisis and the period that followed it, focusing specifically on the regulation of automated trading and the intense political pressure faced by both the SEC and Commodity Futures Trading Commission ("CFTC") to address automated trading as a systemic risk concern in the fallout from the crisis. Many of the risk concerns raised regarding automated trading during this period mirror those later raised regarding digital assets. This heightened systemic risk sensitivity impacted regulators across federal departments and agencies, as underscored by the establishment of the Financial Stability Oversight Council ("FSOC"). The FSOC created a bias towards top-down regulation of disruptive fintech such as automated trading and digital assets. This bias, together with the politicization of emerging financial technologies and associated risks, goes to the heart of why regulators like the SEC and the CFTC have chosen enforcement over creating a viable regulatory framework for digital assets and DeFi. Notably, the CFTC's stringent regulatory approach to DeFi, particularly in 2022 and 2023, comes despite the CFTC's prolonged experience with recognizing the short comings of its initial stringent regulatory approach to automated trading.

Part IV explores established and promising applications of DeFi technologies in both permissioned and permissionless forms,[5] with traditional finance adoption being a vastly under-reported category. It examines ongoing digital asset market structure legislation in the United States, alongside legislative developments in jurisdictions with a more progressive stance towards DeFi, in addition to the shortcomings of a simplistic application of the "same risks, same rules" approach to DeFi.

---

5. For the purposes of this Article, "permissionless DeFi" means open and decentralized access to a DeFi protocol that does not require permission from a governing authority. Thus, any user can join the network, send transaction instructions, view and verify all the transactions that have been recorded onto the blockchain, and participate in any supported consensus process. "Permissioned DeFi" encompasses any controlled access to an underlying permissionless DeFi protocol when such access requires authorization. Access to these networks is restricted and governed by a set of rules or criteria established by an overseeing entity or consortium. This could involve identity verification or other forms of vetting before one is allowed to participate.

Part IV also urges a collaborative strategy to better inform policymaking processes and to bridge the intervening period prior to the implementation of a viable regulatory framework. This involves active initiatives between regulators and other DeFi stakeholders to further develop risk-mitigated, economically viable processes and services—termed "hybrid finance services"—to integrate both existing and emergent DeFi services with the traditional financial system.[6]

The core of the collaborative efforts for which Part IV advocates lies in fostering agile, dynamic collaboration among hybrid finance stakeholders such as regulators, intermediaries, technology providers, and users within the DeFi ecosystem, with the goal of harmonizing innovation and protection. However, United States regulators and policymakers need to recalibrate their increasingly adversarial regulatory approach to avoid compromising the United States' historically influential role balancing innovation with shaping international standards and norms for emerging technologies. This Article acknowledges the intricacies of this undertaking within a multifaceted financial regulatory framework. Further, Part IV identifies anti-money laundering ("AML") and risk management as foundational areas for building consensus and progress.

Part V briefly reviews existing regulations applicable to DeFi before exploring counterparty AML risk management for permissionless networks. AML is a compelling area for collaboration as it is a prominent concern of legislators, regulators, and hybrid finance stakeholders.[7] Addressing permissioned and permissionless access is a necessary predicate for hybrid finance services, with the promise of associated cybersecurity and privacy benefits. We review the Monetary Authority of Singapore's ("MAS") experiment with verified credential technology using DeFi technologies and other permissioned and permissionless options for accessing hybrid finance services. Lastly, Part V discusses the limitations of applying these potential solutions to hybrid finance services.

---

6. The term "hybrid finance" acknowledges the coexistence and interplay of various actors and services in the entirety of the DeFi ecosystem—centralized and decentralized, regulated and unregulated. Much like a hybrid car engine which alternates between combustion and electric power based on various conditions, "hybrid finance" contemplates the strategic use of both centralized service providers and decentralized services, guided by considerations like specific use cases, efficiency requirements, and risk factors. Fundamentally, the concept of hybrid finance services recognizes that DeFi protocols exist within larger supporting ecosystems that can have both decentralized and centralized components. Further reliance on, or integration of, any component should be based on a reasoned balance of considerations along a spectrum of decentralization.

7. *See, e.g.*, Crypto-Asset National Security Enhancement and Enforcement Act of 2023, S. 2355, 118th Cong. (July 18, 2023) (introduced in U.S. Senate as part of the National Defense Authorization Act) [hereinafter Cansee Act]; Digital Asset Anti-Money Laundering Act of 2023, S. 2669, 118th Cong. (July 27, 2023) [hereinafter Digital Asset Anti-Money Laundering Act of 2023].

Part VI outlines a comprehensive strategy for risk management, with an emphasis on cybersecurity and adaptations to existing risk management frameworks, and pre-transaction risk controls for hybrid finance users. The proposed bottom-up approach would repurpose existing SEC and CFTC third-party risk management guidelines and adapt the Financial Stability Board's ("FSB") DeFi framework for macroprudential and systemic risk to micro-level risk management. Further, this Article explores the adaptation of current SEC market access rule logic to pre-transaction risk management processes. A focus on user level collaboration in these areas would enhance the self-regulation of the hybrid finance ecosystem and facilitate valuable risk management guidance for all participants.

Recent responses of regulators and policymakers to disruptive technologies such as digital assets have exhibited an excessive tilt towards top-down approaches influenced by perceptions of hypothetical systemic risks. Examining the failure of top-down approaches to mitigate risk or foster innovation underscores the need for a more discerning and informed bottom-up approach. Instead of endeavoring to address more complex issues such as how DeFi would be treated within a comprehensive digital asset regulatory framework ("boiling the ocean") or legislative delegation of agency oversight, this Article advocates for a pivotal shift towards fostering productive dialogue concerning DeFi utilization and addressing its persistent challenges strategically and tactically.[8] The recommendations posited herein are designed to construct a risk-mitigation framework that aligns and reflects the dynamics within the DeFi ecosystem. In addition to mitigating risks (including hypothetical systemic risks), the approach would also avoid inadvertent negative impacts on national competitiveness and security arising from unintended policy consequences.

II. A BRIEF HISTORY OF INTERMEDIATION AND DISRUPTIVE
     TECHNOLOGIES IN FINANCIAL REGULATION

"The past is the future unfurled." — Thomas Carlyle

A. Early History of Intermediary-Based Financial Regulation

The rapid evolution of digital asset markets in its brief history since the publication of the Bitcoin whitepaper in 2008 starkly contrasts with the gradual development of the securities markets,[9] which underwent a significant period of transformation before a federal framework was

---

8. *See infra* Sections IV.E–F and Parts V–VI.
9. *See, e.g.*, 17 C.F.R. § 23.607 (mandating that direct electronic access implement systems and controls to manage financial risk, including pre-trade automated controls).

established in the 1930s. The Buttonwood Agreement, signed in 1792, marked the first formal system for securities trading between brokers in the United States and led to the development of trusted relationships between brokers and investors.[10] In 1817, the New York Stock & Exchange Board (NYSE) was voluntarily created by securities industry participants to self-regulate U.S. securities trading.[11] For over a century, its rules covered aspects such as admission requirements, trading hours, record-keeping, ethics, and enforcement without any comprehensive, intervening federal regulatory scheme.[12]

Following a decade characterized by speculative activity and fraud leading to the Great Depression,[13] Congress passed the Securities Act of 1933 (the "33 Act") to regulate securities offerings.[14] Congress passed the Securities Exchange Act of 1934 (the "34 Act") to extend the federal securities laws beyond offerings and establish a U.S. regulatory framework for the secondary trading of securities through financial intermediaries, creating categories of regulated participants like stock exchanges, clearing agencies, and broker-dealers.[15] The 34 Act also formed the SEC and granted the SEC authority to regulate "registered national securities associations,"[16] leading to the creation of the National Association of Securities Dealers ("NASD") as a self-regulatory organization ("SRO") in 1939.[17] Although this legislation greatly expanded the scope of financial intermediary regulation, this regulatory

---

10. *See* Olivia B. Waxman, *How a Financial Panic Helped Launch the New York Stock Exchange*, TIME (May 17, 2017, 9:00 AM), https://perma.cc/AX2A-ZHQ4.

11. *See The History of NYSE*, N.Y. STOCK EXCHANGE, https://perma.cc/FJ22-W767 (last visited June 28, 2023).

12. *See id*.

13. *See* Brummer, *supra* note 3, at 983. As Brummer recounts:

> By the early 1920s, individuals such as Ivar Krueger graced the cover of *Time* magazine after raising millions of dollars to fund a Ponzi scheme built on repaying loans and doling out dividends to investors . . . . neither the [NYSE] nor brokers monopolizing its trade contacted or discussed the financial statements of the presumed auditor. Similarly, increasingly complex frauds were committed against the public—like that perpetrated by the Musica brothers, who created an entire network of fictitious firms to bolster false financial statements . . . .

Id.

14. *See* The Securities Act of 1933, 15 U.S.C. §§ 77a et seq. (1934) [hereinafter The 33 Act].

15. *See* The Securities Exchange Act of 1934, 15 U.S.C. §§ 78a et. seq. (1934) [hereinafter The 34 Act].

16. *See id.* § 78d.

17. *See* The Maloney Act, Ch. 677, § 1, 52 Stat. 1070 (1938) (codified as amended at 15 U.S.C. § 78o–3 (1982)).

framework remained largely unchanged over three subsequent decades, and the SEC was largely a caretaker of this status quo.[18]

Thereafter, the SEC became more adaptive to technological innovation, increasingly permitting—and, at times, requiring—the use of disruptive technologies, such as financial data processing and electronic communications networks, to facilitate greater quote and trade transparency and as a tool to functionally redistribute the concentrated powers of exchanges and other market intermediaries.[19] This stance reflected a shift in the regulatory landscape that recognized and adapted to evolving market and technology dynamics.

B. The Role of Technology in Early National Market Structure

The 1963 Special Study of the Securities Markets marked a turning point in financial intermediary regulation. The comprehensive 3,000-page report assessed the various phases of securities trade processing.[20] The study shed light on the negative impacts of conflicts of interest and abuses tied to the actions of intermediaries and the very structure of securities markets, which ultimately harmed investors and market efficiency.[21] Issues such as wide spreads, high markups, and profiteering by market makers and specialists led to recommendations for increased regulation of intermediaries and broader dissemination of quotes in the equities marketplace.[22] In the early 1970s, the SEC, guided by this report, took measures to transition the market towards a more integrated system. It published the "Future Structure of the Securities Markets" statement that emphasized the need for creating a consolidated disclosure of transaction reports and quotations from all markets, permitting broker-dealer access to all exchanges, and integrating off-exchange or over-the-counter ("OTC") trading into the disclosure system.[23] Crucially, while the electronic marketplace had, by that point, streamlined interactions

---

18. *See* Brummer, *supra* note 3, at 978–79 ("For the first three decades following the birth of U.S. federal securities regulation in the 1930s, . . . the market ecosystem subject to securities regulation was quite stable and experienced only incremental change.").

19. *See infra* Section II.B.

20. *See generally* U.S. SEC. & EXCH. COMM'N, REP. OF SPECIAL STUDY OF SECURITIES MARKETS OF THE SEC. AND EXCH. COMM'N TO THE H. COMMERCE COMMITTEE, H.R. Doc. No. 95, Pt. 1, 88th Cong., 1st Sess. [hereinafter SPECIAL STUDY OF SECURITIES MARKETS]. (1963); *see also* JOEL SELIGMAN, THE TRANSFORMATION OF WALL STREET: A HISTORY OF THE SECURITIES AND EXCHANGE COMMISSION AND MODERN CORPORATE FINANCE 86 (3rd ed. 2003) (noting that the 1963 study was "undoubtedly the single most influential document published in the history of the SEC").

21. *See* SPECIAL STUDY OF SECURITIES MARKETS, *supra* note 20, at Ch. III §§ B, C; Ch. IV § B; Ch. VI §§ C, D; Ch. XI § A.

22. *See id.* at Ch. I, § A (other reforms included decimalization and establishment of the Securities Investor Protection Corporation).

23. *See* STATEMENT OF THE U.S. SEC. & EXCH. COMM'N ON THE FUTURE STRUCTURE OF THE SECURITIES MARKETS (Feb. 2, 1972), available at https://perma.cc/3QQT-W6ED.

between intermediaries, the SEC's statement highlighted a concern that these benefits were not reaching investors.[24]

These actions set the stage for the growth of financial technology innovation in the decades to come, leading regulators not only to adapt to technological advances but to increasingly view technology as a tool to accomplish greater transparency and competition in national markets.[25] In 1971, the NASD created a computerized system for trading securities not listed on stock exchanges—the National Association of Securities Dealers Automated Quotation system (NASDAQ).[26] In 1975, the CFTC was established to unify federal jurisdiction over traded commodity futures.[27] That same year, Congress tasked the SEC to create a national system with rules designed to reduce informational asymmetries and ensure intermediaries were meeting their obligations to customers.[28] These mandates prominently addressed the areas set forth in Figure 1 below.

---

24. *See id.*

25. *See infra* Section II.C.

26. *See* Ellen Terrell, *History of American and NASDAQ Stock Exchanges*, LIBRARY OF CONGRESS, (Oct. 2012), https://perma.cc/47WZ-PBZN.

27. *See* Commodity Futures Trading Commission Act of 1974, Pub. L. No. 93-463, 88 Stat. 1389 (codified as amended at 7 U.S.C. § 4a) (creating the CFTC); *see also* Futures Trading Act of 1982, Pub. L. No. 97-444, 96 Stat. 2294 (renewing the CFTC's mandate for four more years).

28. *See* Securities Acts Amendments of 1975, Pub. L. No. 94–29, 89 Stat. 97, 112 (1975). The amendments revised Section 11A of the 34 Act to mandate:

> [T]he protection of investors and the maintenance of fair and orderly markets to assure (i) economically efficient execution of securities transactions; (ii) fair competition among brokers and dealers, among exchange markets, and between exchange markets and markets other than exchange markets; (iii) the availability to brokers, dealers, and investors of information with respect to quotations for and transactions in securities; (iv) the practicability of brokers executing investors' orders in the best market; and (v) an opportunity, consistent with the provisions of clauses (i) and (iv) of this subparagraph, for investors' orders to be executed without the participation of a dealer.

Id. The amendments also required: "(D) The linking of all markets for qualified securities through communication and data processing facilities will foster efficiency, enhance competition, increase the information available to brokers, dealers, and investors, facilitate the offsetting of investors' orders, and contribute to best execution of such orders." *Id*; *see also* Dave A. Oesterle, *Congress's 1975 Directions to the SEC for the Creation of a National Market System*, AM. ENTER. INST. (May 7, 2003), https://perma.cc/96E2-X248.

Figure 1.[29]

The Beginnings of the National Market System

✔ **Publish Prices:** Exchanges & dealers should publish prices at which they will execute trades

✔ **Disintermediate:** Investors' orders should be executable without mandatory dealer participation

✔ **Network:** Markets should be linked electronically so the best prices are accessible

✔ **Best Execution:** Regulated brokers must obtain best execution for their clients

This Congressional action expanded the goal of the SEC's mandate from the protection of investors to the efficient operation of capital markets. It marked the beginning of a more concerted effort by the SEC to leverage the benefits of technology to directly address the informational asymmetries benefiting floor brokers and market makers to the detriment of investors. In the years immediately following, the NYSE rolled out an order delivery system that disintermediated floor brokers' privileged access to specialists, and the exchanges established interlinkages to facilitate price competition.[30] In 1984, building on this momentum, NASDAQ introduced the disruptive Small Order Execution System ("SOES") that enabled market makers to automatically execute small retail orders at their best displayed price.[31] This upended the broker-intermediated model. In a controversial move, the NASD made market maker participation mandatory following the inability of retail users to get executions during the 1987 crash.[32] Mandatory participation meant that

---

29. Figure derived from information contained within 7 U.S.C. § 4a and the Futures Trading Act of 1982, Pub. L. No. 97-444, 96 Stat. 2294.

30. *See Transformation & Regulation: Equities Market Structure, 1934 to 2018*, SEC HISTORICAL SOCIETY, https://perma.cc/BD8N-AE3J (last visited June 29, 2023). In 1978, various exchanges created an automated linkage system. For discussion, see Adoption of Amendments to the Intermarket Trading System Plan to Expand the ITS/Computer Assisted Execution System Linkage to all Listed Securities, Exchange Act Release No. 42212, 64 Fed. Reg. 70297 (Feb. 14, 2000).

31. *See Nasdaq National Market Execution System*, NASDAQ (July 10, 2000), https://perma.cc/56PE-VQFE.

32. *See Notice to Members 88-43: Adoption of Amendments to the Rules of Practice and Procedures for the NASD Small Order Execution System and to Schedule D to the NASD By-Laws*, FINRA (June 22, 1988), https://perma.cc/J3B3-MHTS. Opportunistic traders, nicknamed the "SOES bandits," were able move in and out of positions faster than the institutional players, cutting into their profitability. *See* Scott Patterson, *Man vs.*

market makers could not choose to disable SOES participation in periods of high volatility when they needed the momentary flexibility to pull and repost their quotes. Mandatory participation also reduced information asymmetries that benefited market makers due to their prior ability to make such quote adjustments even after an order was received. Large brokers lobbied aggressively to minimize the impact of retail day traders leveraging their brokers' technology to directly execute against orders that had previously required their intervention.[33] Despite the forces aligned against it, this disintermediating technological capability empowered unregulated market participants and would set a new benchmark for capital markets that is considered unremarkably standard today.[34] The SOES phenomenon provides a powerful analogy for the inevitability of disruptive fintech adoption and the forces that oppose their adoption. This phenomenon also set the stage for a more active period of reliance on disruptive financial technologies by the SEC to achieve its policy objectives in the following two decades.

C. Financial Regulators Adapt to, and Embrace, Disruptive Technologies

During the 1990s and 2000s, the CFTC proactively adapted to electronic trading, albeit in a less interventionist manner than the SEC. In 1990, the CFTC adopted ten principles for screen-based trading.[35] In 1994, it imposed enhanced disclosure requirements on regulated entities, in large part due to the growth in futures volumes driven by electronic trading.[36]

Machine: How the Crash of '87 Gave Birth to High-Frequency Trading, CNBC (Sept. 14, 2010, 9:24 AM), https://perma.cc/C4LK-N2KD.

33. *See* Thierry Foucault, et al., *Market Making with Costly Monitoring: An Analysis of the SOES Controversy*, 16 THE REV. OF FIN. STUDIES 345 (2003).

34. *See e.g.*, discussion *infra* notes 52–58 and accompanying text (regarding Reg NMS).

35. The ten principles, first adopted by the International Organization of Securities Commissions ("IOSCO") in 1990, applied to sponsors of trading systems and provided proscriptive principles for sponsors to demonstrate ongoing legal and regulatory compliance. The principles provided for equitable access to trading data and fair operation for all market participants; risk identification and management, including identification of potential system vulnerabilities and risks from interactions with other financial systems; education to ensure user competence and understanding of inherent risks; capability of system surveillance; and responsiveness to regulatory directives. *See* Policy Statement Concerning the Oversight of Screen-Based Trading Systems, 55 Fed. Reg. 48670 (Nov. 21, 1990), https://perma.cc/L7A9-WSL9. IOSCO defined "system sponsor" as the organization responsible for the system, such as an exchange. *See* Andrea M. Corcoran et al., *Screen-Based Trading Systems for Derivative Products,* TECH. COMM. OF THE INT'L ORG. OF SEC. COMM'N, at 8 (June 1990), https://perma.cc/N6LK-KHQH.

36. At the end of 1994, the CFTC published notice of the adoption of Rules 1.14 and 1.15 to implement the risk assessment authority. *See* Risk Assessment for Holding Company Systems, 59 Fed. Reg. 66674 (Dec. 28, 1994) (codified at 17 C.F.R. pt. 1). For corrections to final rules implementing risk assessment authority, see Risk Assessment for

The CFTC's approach to disruptive technology was not interventionist and left matters largely in the hands of market participants. Significant rulemaking related to electronic trading would gain additional momentum following the 2008 financial crisis.[37]

In 1994, when the SEC published its "Market 2000" report, it recognized the success of technological development and enhanced competition, but it also criticized that the playing field was "not level" due to "different regulatory obligations."[38] The report noted that the SEC would need to ensure that regulatory responsibilities were "rationally allocated without stifling the ability of alternative markets and services to emerge" and further, in some cases, that "this goal will justify different regulatory guidelines."[39] This response marked a period when the SEC was increasingly focused on adapting to the growing significance of electronic trading. These adaptations, based on a bottom-up approach, reframed intermediary roles and enhanced market transparency, competition, and efficiency within an evolving national market structure. An example of this was the Order Handling Rules implemented by the SEC in 1997 after it fined a number of NASDAQ market makers for collusion, price fixing, and trading ahead of customer orders.[40] The rules required market makers and other trading venues to publicly display their best-priced customer limit orders (orders to buy or sell a security at a specified price or better) and mandated that broker-dealers provide their customers with the opportunity to have their orders executed at better prices displayed in other markets.[41]

Holding Company Systems; Correction, 60 Fed. Reg. 13901 (Mar. 15, 1995) (codified at 17 C.F.R. pt. 1), https://perma.cc/7JWA-GM7E. For an adoption history and amendments (effective Aug. 24, 1995) to Commodity Pool Operator and Commodity Trading Advisor Disclosure Rules, see Amendments to Commodity Pool Operator and Commodity Trading Advisor Disclosure Rules, 60 Fed. Reg. 38146 (July 25, 1995) (codified at 17 C.F.R. pts. 1, 4, 30, and 150), https://perma.cc/KU66-N9CD.

37. *See infra* Sections III.D–E.

38. SEC DIVISION OF MARKET REGULATION, MARKET 2000 AN EXAMINATION OF CURRENT EQUITY MARKETS DEVELOPMENT 2 (Jan. 1994), https://perma.cc/FUM6-L3ER (noting the efficiency and effectiveness of the equity markets but also noting that improvements could be made to improve fairness for investors, timely and comprehensive disclosure of market information, fair competition among markets and market participants, and market accessibility).

39. *Id.*

40. *See* Nat'l Assoc. of Securities Dealers, Inc., *Order Instituting Public Proceedings*, Exchange Release Act No. 37538 (Aug. 8, 1996), https://perma.cc/B3B9-99C7; *see also* U.S. SEC. & EXCH. COMM'N, REP. PURSUANT TO SECTION 21(A) OF THE SEC. EXCH. ACT OF 1934 REGARDING THE NASD AND THE NASDAQ MARKET (Aug. 8, 1996), available at https://perma.cc/3SS6-9YFN.

41. *See* U.S. SEC. & EXCH. COMM'N, *NASD Rulemaking: Order Approving a Proposed Rule Change to Permanently Expand the NASD's Rule Permitting Market Makers to Display Their Actual Quotation Size* (July 15, 1998), https://perma.cc/B5SB-ESQM.

The Order Handling Rules provided the necessary regulatory framework for brokers to operate alternative trading systems ("ATSs"), effectively mirroring the order-matching role traditionally held by exchanges.[42] Increasingly, these networks became their own distinct pools of liquidity, leading to fragmentation despite their integration into the public markets. While this brought about certain efficiencies, it raised questions relating to exchange registration requirements and compliance. To address these challenges, the SEC issued a concept release to actively solicit feedback from market participants.[43] The SEC's goal was to harness technological innovations to reconfigure market structure, tackle fragmentation, improve market efficiencies, and serve the interests of investors.[44]

In 1998, in response to the feedback from the concept release, the SEC adopted Regulation ATS ("Reg ATS").[45] Reg ATS had broad support due to the SEC's collaborative approach with interested and impacted stakeholders.[46] Reg ATS provided a straightforward path for registered broker-dealers to operate ATSs provided they registered as an exempt exchange, subject to certain compliance, supervisory, and recordkeeping requirements.[47] To encourage competition, ATSs were required to provide "fair access" to all regulated intermediaries.[48] In addition, Reg ATS provided for the maintenance of certain systems' capacity, integrity, and security standards.[49] In doing so, it adapted its regulation to facilitate a decentralization and redistribution of public market functions that previously had only been permitted for a registered exchange. As expressed by then SEC Acting Chair Unger, Reg ATS represented the SEC's recognition that the "traditional organizational model" requiring exchange registration for such functions "may not be the most appropriate

42. *See* U.S. Sec. & Exch. Comm'n Hist. Society, *Transformation & Regulation: Equities Market Structure, 1934 to 2018*, https://perma.cc/QSM8-PRAX (last visited July 10, 2023). Order matching refers to the process by which a securities exchange (or other market center) pairs buy and sell orders based on certain criteria such as price and time priority prior to execution.

43. *See* Regulation of Exchanges, Exchange Act Release No. 38672, 62 Fed. Reg. 30485 (June 4, 1997) (codified at 17 C.F.R. pt. 240), https://perma.cc/6MB9-M3QW.

44. *See id.* at 30485 ("The [SEC] . . . is reevaluating its approach to the regulation of exchanges and other markets in light of technological advances and the corresponding growth of alternative trading systems and cross-border trading opportunities.").

45. *See* Regulation of Exchanges and Alternative Trading Systems, Exchange Act Release No. 40760, 63 Fed. Reg. 70844 (Dec. 22, 1998) (codified at 17 C.F.R. pts. 202, 240, 242, 249), https://perma.cc/S7MX-484Y.

46. *See id.* at 70847 (noting that most commenters welcomed the proposals).

47. *See id.* at 70863–84.

48. *See id.* at 70872–75.

49. *See id.* at 70875–77.

[model] in an economy operating on triple-paced 'Internet time.'"[50] The new framework provided a viable path for early-stage participants to "choose the regulatory scheme that best fits [their] business plan" and take advantage of "more flexible corporate governance structures."[51]

While Reg ATS embraced disruptive financial technologies, Regulation National Market Systems ("Reg NMS"), adopted by the SEC in 2005, extended the ability of ATSs to compete against exchanges.[52] Reg NMS marked the SEC's most consequential use of technology in reforming market structure to date. Reg NMS's interventionist regulatory approach sought to leverage advancements in technology to restructure and decentralize competition for displayed bid and ask prices in equities markets, particularly for ATSs.[53] It effectively mandated linkages across major market centers, limited access fees,[54] required incoming orders to interact with the best immediately accessible quotes at automated market centers,[55] tightened quote spreads,[56] and allowed exchanges to share quoting fees.[57] Because Reg NMS necessitated linkages across more than just national and regional exchanges and permitted market participants to ignore quotes that were slow to respond (known as "trade throughs"),[58] it forced market centers and market makers to substantially upgrade their technology infrastructures to remain competitive. Reg NMS would lead to traditional market makers becoming displaced by automated and high-frequency market making.[59]

Likely influenced by both the increased outsourcing of technology and compliance obligations associated with Reg NMS and a concurrent report on outsourcing by the Bank for International Settlements,[60] the NASD released a notice addressing its members' risk management

---

50. Laura S. Unger, Comm'r, U.S. Sec. & Exch. Comm'n, *Speech by SEC Commissioner: The Internet – Will It Be the End of the Stock Market as We Know It?* (June 22, 1999), https://perma.cc/FT4L-UVVT.

51. *Id.*

52. *See* Regulation NMS, Exchange Act Release No. 51808, 70 Fed. Reg. 37496 (June 29, 2005) (to be codified at 17 C.F.R. pts. 200, 201, 230, 240, 242, 249, 270), https://perma.cc/9W2C-ZPBW.

53. *See* Regulation NMS, Proposed Rule, Exchange Act Release No. 50870, 69 Fed. Reg. 247 (Dec. 27, 2004) (to be codified at 17 C.F.R. pts. 200, 201, 230, et al), https://perma.cc/KPD2-ZU6M.

54. *See* 17 C.F.R. § 242.610.

55. *See id.* § 242.611.

56. *See id.* § 242.612.

57. *See id.* § 242.603.

58. *See id,* § 242.610.

59. *See* MERRITT B. FOX, ET AL., SEC. MARKET ISSUES FOR THE 21ST CENTURY 174 (2018), available at https://perma.cc/E7JK-KQ59.

60. *See, e.g.*, Basel Committee on Banking Supervision, *Outsourcing in Financial Services*, BANK FOR INT'L SETTLEMENTS (Feb. 2005), https://perma.cc/4RZ3-V992.

responsibilities when outsourcing to third-party service providers.[61] The National Futures Association ("NFA"), the self-regulatory organization for the U.S. derivatives industry formally established under the oversight of the CFTC in 1981,[62] also adopted targeted guidance for specific third-party services during the same period for AML programs, automated order-routing systems, and other services.[63] The Financial Industry Regulatory Authority's (FINRA)[64] and the NFA's risk management guidance will be explored more thoroughly in Part V with regards to hybrid finance services.[65]

Following the adoption of Reg NMS, the SEC would become less interventionist in its technology-focused approach to redistributing or decentralizing intermediary market functions. The prior four decades had witnessed the creation of disruptive technologies that forced the NYSE to adapt from being the nearly singular marketplace for public securities to becoming a technology host, allowing brokers to transition from agents to dominant sources of liquidity themselves.[66] Prospectively, the SEC's focus both in rulemaking and informal guidance shifted towards managing the rapid growth of technology and its risks.[67] As discussed in Part III, the impetus for this shift would not start from within the public equities markets but from the U.S. residential housing market.[68]

---

61. *See Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers*, FINRA (July 22, 2005), https://perma.cc/E65E-LKXS.

62. *See* COMMODITY FUTURES TRADING COMM'N *ORDER OF SEPTEMBER 22, 1981*: *Application of the National Futures Association, Order Granting Registration and Approving Rules* (Sept. 22, 1981); *see also NFA History*, NAT'L FUTURES ASS'N, https://perma.cc/K5R2-WQZW (last visited Aug. 2, 2023).

63. *See Interpretive Notice 9045 – NFA Compliance Rule 2-9: FCM and IB Anti-Money Laundering Program,* NAT'L FUTURES ASS'N (Oct. 29, 2022), https://perma.cc/72WS-9BK5; *see also Interpretive Notice 9046 – Compliance Rule 2-9: Supervision of the Use of Automated Order-Routing Systems,* NAT'L FUTURES ASS'N (Dec. 12, 2006), https://perma.cc/3BKP-XPJF; *Third-Party Service Providers*, NAT'L FUTURES ASS'N, https://perma.cc/2FH2-QZ9W (last visited July 11, 2023).

64. NASD was redesignated as FINRA in 2009. *See NASD and NYSE Member Regulation Combine to Form the Financial Industry Regulatory Authority – FINRA*, FINRA (July 30, 2007), https://perma.cc/S5C3-28M4.

65. *See infra* Section V.C.

66. *See* Brummer, *supra* note 3, at 1032.

67. *See infra* Part III.

68. *See* THE FIN. CRISIS INQUIRY COMM'N, THE FINANCIAL CRISIS INQUIRY REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON THE CAUSES OF THE FINANCIAL AND ECONOMIC CRISIS IN THE UNITED STATES (Jan. 2011), available at https://perma.cc/6DXX-LKCH. In its 665-page report presented to Congress in 2011, the national commission would assign the blame for the financial crisis to a housing bubble "fueled by low interest rates, easy and available credit, scant regulation, and toxic mortgages." *But see* Paul G. Mahoney, *Deregulation and the Subprime Crisis*, 104 VA L. REV. 235 (Apr. 10, 2018) (noting that the risky practices associated with the crisis, such as credit default swaps ("CDSs"), were already permissible under the existing law and that the crisis was an outcome of the banks' pursuit of greater risk to maintain profitability in the face of the fluctuating interest rate environment prevalent since the 1970s).

Rules such as Reg ATS and Reg NMS demonstrated a forward-thinking approach by the SEC, which, at that time, viewed disruptive technology as complementary with financial regulation. These regulations reflected the belief that burgeoning electronic marketplaces, powered by disruptive technologies, could further bolster the United States's position as a global financial center and that regulations ought not just accommodate these changes but guide them towards desired outcomes. These reimagined markets were also shaped by various policy determinations, including the decentralization of liquidity, intensifying market price competition, and increased home ownership and economic growth resulting from expanded access to retail credit.[69] The pivot of U.S. policymakers and regulators towards systemic risk concerns in the aftermath of the 2008 financial crisis illustrates how dramatically regulatory responses can shift and cause new market dynamics and challenges to become embedded into policy. This pivot also illustrates how the benefits of disruptive technologies can become tainted by association with such crises and how difficult it can be to challenge the political narrative against excessive, top-down regulation as a response once such concerns are in the public spotlight.

III.   THE POST-2008 FINANCIAL CRISIS ERA: SYSTEMIC RISK AND TOP-DOWN REGULATION

   "History never repeats, but it often rhymes." — Mark Twain

The 2008 financial crisis and subsequent technology-induced volatility events across the U.S. financial markets would force policymakers and regulators to reassess the relationship of financial technology and regulation. No longer was financial technology primarily viewed as a tool to disaggregate market functions or improve price discovery. Its role in facilitating transparency, capital markets efficiency, and investor protection would also be questioned. Instead, financial technology would be increasingly viewed as a threat that challenged the existing regulatory framework and raised hypothetical systemic risk concerns.

In response to the 2008 financial crisis, Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (the "Dodd Frank Act").[70] Key provisions of the Dodd Frank Act included,

---

69. Allison Herren Lee, Comm'r, U.S. Sec. & Exch. Comm'n, *Going Dark: The Growth of Private Markets and the Impact on Investors and the Economy* (Oct. 12, 2021), https://perma.cc/9F5H-FVCU.

70. *See* Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified as amended in scattered sections of the U.S. Code).

among other things, the creation of the FSOC to monitor systemic risk,[71] promulgation of the Volcker Rule to limit speculative trading by banks,[72] and significant reforms to the OTC derivatives market.[73]

A. Electronic Market Access Risks

In the 2000s, buy-side institutions displayed an increasing desire to connect directly with exchanges and ATSs utilizing their broker's technology in what became known as direct market access ("DMA") technology.[74] The institutions wanted greater control and a means to minimize the risk of information leakage. DMA technology grew rapidly, and, in response, the SEC adopted the Market Access Rule in 2010 to address concerns that the controls to manage the risks associated with DMA orders were less rigorous than those that applied to orders that did not bypass the broker's trading desks.[75] As DMA continued to grow, the CFTC and even the European Union (EU) would follow with similar constructs.[76] The Market Access Rule required various automated filters, as noted in Figure 2 below, to screen DMA orders before such orders could be routed to a particular market.[77]

---

71. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 111, 124 Stat. 1376, 1393 et. seq. (2010) (codified at 12 U.S.C. § 5321); *see also* Martin Neil Baily, et al., *The Impact of the Dodd-Frank Act on Financial Stability and Economic Growth*, 3 THE RUSSELL SAGE FOUND. J. FOR THE SOC. SCIENCES 20–47, 39–40 (2017).

72. *See* Prohibitions and Restrictions on Proprietary Trading and Certain Interests in, and Relationships with, Hedge Funds and Private Equity Funds, 79 Fed. Reg. 5536 (Jan. 31, 2014) (codified at 12 C.F.R. pt. 44), https://perma.cc/E7WX-K3CV (prohibiting banking entities from engaging in or sponsoring hedge funds or private equity firms in proprietary trading with an eye to systemic risk).

73. *See id.*

74. *See, e.g.*, CELENT, THE EVOLUTION OF DIRECT MARKET ACCESS (DMA) TRADING SERVICES IN THE US AND EUROPE (March 13, 2008), https://perma.cc/WRY8-HTES [hereinafter CELENT REPORT].

75. *See* Risk Management Controls for Brokers or Dealers With Market Access, Exchange Act Release No. 63241, 75 Fed. Reg. 69792 (Nov. 15, 2010) (codified at 17 C.F.R. § 240), https://perma.cc/F3ED-FR2K [hereinafter SEC Market Access Rule] ("[T]he Commission is concerned that the various financial and regulatory risks that arise in connection with [DMA] access may not be appropriately and effectively controlled by all broker-dealers.").

76. *See, e.g.*, discussion *infra* notes 95–97 and accompanying text; Council Directive 2014/65, 2014 O.J. (L 173/349) ("An investment firm that engages in algorithmic trading shall have in place . . . appropriate trading thresholds and limits and prevent the sending of erroneous orders or the systems otherwise functioning in a way that may create or contribute to a disorderly market.").

77. *See infra* Section III.A, Fig.2; *see also* 17 C.F.R. § 240.15c3–5(c).

Figure 2.

Market Access Control Basics

Prevent the entry of orders that:

Exceed pre-set credit or capital thresholds	Exceed price or size parameters	Appear erroneous or duplicative	Violate internal trading restrictions
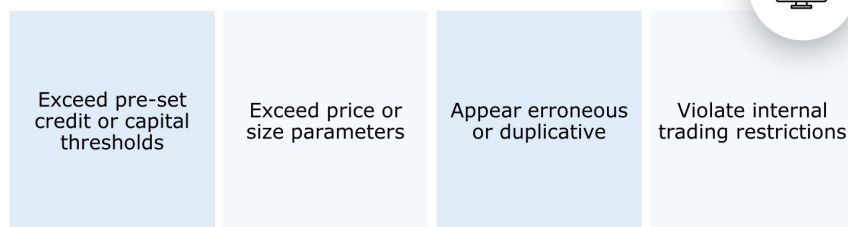
Source: 17 C.F.R. § 240.15c3-5(c)

In the years since its adoption, DMA access has become ubiquitous across regulated intermediaries and is often facilitated by third party vendors.[78] The Market Access Rule will be further explored in Section VI.C.

B. Flash Crash of 2010

The post-2008 financial crisis jitters of politicians and regulators were exacerbated in May 2010, prior to the passage of the Dodd Frank Act, when the U.S. stock market experienced a "flash crash," dropping 9% in total value in less than fifteen minutes without any negative news. This flash crash was caused by the cascading and cumulative effects of automated trading programs closing out positions in response to volatility in the equities markets.[79] Regulated intermediaries were integrating rapid advances in high-frequency and automated trading technologies, but the near instantaneous, programmatic, and interconnected responses of these systems to changing market data raised concerns that the regulations themselves were not keeping up with technological change.[80]

After the flash crash, Congress demanded an accounting from both the CFTC and the SEC.[81] Automated trading became a focus area for the newly established FSOC, as noted in its first annual report in 2011 and in subsequent years.[82] Future market-moving events caused by automated

---

78. *See* CELENT REPORT, *supra* note 74.

79. *See* Jill Treanor, *The 2010 'Flash Crash': How It Unfolded*, GUARDIAN (Apr. 22, 2015, 1:43 PM), https://perma.cc/ZH67-6M29.

80. *See* FINDINGS REGARDING THE MARKET EVENTS OF MAY 6, 2010, REP. OF THE STAFFS OF THE CFTC AND SEC TO THE JOINT ADVISORY COMM. ON EMERGING REGULATORY ISSUES (Sept. 30, 2010), available at https://perma.cc/8STX-KE9W.

81. *See id.*

82. The FSOC took notice of algorithmic/automated trading and clearing in every annual report, with mentions peaking in 2012, 2016, and 2017. *See* FSOC Annual Report Archive, U.S. DEP'T. OF TREAS., https://perma.cc/T5XX-P9JZ (last visited July 12, 2023) [hereinafter FSOC Annual Reports].

trading failures would only sharpen a growing wariness towards disruptive technologies, such as the forced sale of Knight Capital Trading following a $460 million loss induced by a trading algorithm failure.[83]

While each of the SEC and CFTC were tasked with managing substantially similar risks (albeit with different market structure and instruments), there were notable differences in their response to the rise of disruptive financial technologies.

C. SEC's Regulation of Algorithms

Throughout 2010, the SEC continued to implement rules to build a regulatory framework that endeavored to address risks resulting from the increase in automated trading. In addition to the SEC's Market Access Rule and FINRA's guidance related to vendor risk management addressed later in Part VI, the SEC adopted exchange circuit breakers in response to market volatility,[84] adopted Regulation Systems Compliance and Integrity ("Reg SCI"),[85] and stepped up enforcement against high frequency trading firms.[86] Reg SCI, adopted in 2014, addressed systemic risk through

---

83. *See* Knight Capital Americas LLC, *Order Instituting Administrative and Cease-and-Desist Proceedings*, Exchange Act Release No. 70694 (Oct. 16, 2013), https://perma.cc/MZ9C-LDUZ (settled matter); *see also* Richard Drew, *Getco and Knight Capital to Merge in $1.4 Billion Deal*, REUTERS (Dec. 19, 2012), https://perma.cc/L8KT-ZY9S. Knight Capital Trading ("Knight") had initially received a $400 million cash infusion from a group of investors, that included Getco Holdings Co ("Getco"), after an error in Knight's market open algorithms sent millions of unintentional orders into the U.S. equities market on August 1, 2012. Getco agreed to acquire Knight for $1.4 billion later that year. *See id.*

84. *See Investor Bulletin: Measures to Address Market Volatility*, U.S. SEC. & EXCH. COMM'N (July 1, 2012), https://perma.cc/EL8J-S7WF (explaining the SEC's implementation of new rules designed to limit market volatility by restricting the potential aggressivity of price movements called "Limit Up-Limit Down" mechanisms and "Market-Wide Circuit Breakers").

85. Reg. SCI required key market participants, such as exchanges, alternative trading systems, and clearing agencies, to establish, maintain, and enforce policies and procedures related to their technology systems to ensure system "capacity, integrity, resiliency, availability, . . . security," and compliance. *See* Regulation Systems Compliance and Integrity, Exchange Act Release No. 73639, 79 Fed. Reg. 72252 (Dec. 5, 2014) (codified at 17 C.F.R. §§ 242.1000–1007), https://perma.cc/G85D-M647 [hereinafter Reg. SCI]; 17 C.F.R. § 242.1001(a–b). Reg. SCI sets out obligations for crisis response during "SCI events" such as significant disruptions, compliance issues, or intrusions. *Id.* Additionally, Reg SCI has specific requirements to create and maintain business continuity and disaster recovery plans, including regular testing. 17 C.F.R. § 242.1001(a)(2)(v–vi), 1004.3.

86. *See* Athena Capital Research, LLC, *Order Instituting Administrative and Cease-and-Desist Proceedings*, Exchange Act Release No. 73369, Investment Advisers Act Rel. No. 3950, at 1 (Oct. 16, 2014), https://perma.cc/LLE4-9QC3 (ordering a HFT firm to cease and desist because they engaged in "marking the closing"—a disruptive trading practice involving placing large orders at close to artificially raise asset prices); Latour Trading LLC, *Order Instituting Administrative and Cease-And-Desist Proceedings*, Exchange Act Release No. 73125, at 2 (Sept. 17, 2014), https://perma.cc/6C6N-DF2M (arising out of "extensive failures to maintain minimum net capital" requirements under Exchange Act

significant technology and infrastructure requirements imposed on key market participants, such as exchanges, ATSs, and clearing agencies, with the aim of reducing systems issues and improving resilience.[87] Additionally, in 2016, FINRA expanded its registration requirements for "Securities Traders" to include certain developers who worked on algorithmic trading strategies for member firms.[88] While the circuit breaker rules were more limited technical implementations finely tuned to exchange quote and price volatility, the balance of these rules, regulations, and guidance—Market Access, vendor risk management guidance, developer registration, and, in particular, Reg SCI—reflected broader, top-down, systemic-risk-focused mandates which arose largely in response to advances in financial technologies. As discussed below, the CFTC's approach regarding Regulation Automated Trading initially took a bottom-up approach to regulating similar risks, but subsequently reverted to top-down mandates before ultimately scaling back the scope of the regulation in response to industry concerns.[89]

Rule 15c3-1); John McCrank, *Exclusive: SEC Targets 10 Firms in High Frequency Trading Probe - SEC Document*, REUTERS (July 17, 2014, 5:12 PM), https://perma.cc/GX3X-JLW3.

87. *See* Reg. SCI *supra* note 85, at 72253. In discussing the need for technology-focused regulation applicable to certain regulated market actors, the Commission noted:

> A confluence of factors contributed to the Commission's . . . current determination that it is necessary . . . to address the technological vulnerabilities, and improve Commission oversight, of the core technology of key U.S. securities markets entities . . . . These considerations include: the evolution of the markets to become significantly more dependent upon sophisticated, complex[,] and interconnected technology; . . . a significant number of, and lessons learned from, recent systems issues at exchanges and other trading venues, [and] increased concerns over ''single points of failure'' in the securities markets.

Id. at 72253.

88. *See* Self-Regulatory Organizations: Financial Industry Regulatory Authority, Inc.; Order Approving a Proposed Rule Change To Require Registration as Securities Traders of Associated Persons Primarily Responsible for the Design, Development, Significant Modification of Algorithmic Trading Strategies or Responsible for the Day-to-Day Supervision of Such Activities, Exchange Act Release No. 77551, 81 Fed. Reg. 21914 (Apr. 7, 2016) (codified at 15 U.S.C. § 78s), https://perma.cc/YP6R-3QCM (requiring registration of "associated persons who are (i) primarily responsible for the design, development[,] or significant modification of algorithmic trading strategies, or (ii) responsible for the day-to-day supervision or direction of such activities"); *see also* STAFF REP. ON ALGORITHMIC TRADING IN U.S. CAPITAL MARKETS, U.S. SEC. & EXCH. COMM'N, at 3 (Aug. 5, 2020), https://perma.cc/M5EP-4GZX ("The Economic Growth, Regulatory, Relief, and Consumer Protection Act of 2018 requires the staff of the [SEC] to submit to Congress a report on the risks and benefits of algorithmic trading in the U.S. capital markets.").

89. *See infra* Section III.C.

D. CFTC's Automated Trading Rulemaking

During the first half of the 2010s, spurred by the flash crash and Congress's mandate under the Dodd Frank Act, the CFTC engaged in active rulemaking designed to address risk management concerns around automated trading and clearing.[90]

In 2012, the CFTC adopted pre-trade risk management rules applicable to futures commission merchants ("FCMs"), swap dealers and major swap participants ("SDs" and MSPs"), and designated contract markets for futures and options ("DCMs") that closely aligned with the SEC's Market Access Rule.[91] Among other things, the new rules required FCMs, SDs, and MSPs to establish, maintain, and enforce risk-based limits and controls for all cleared transactions.[92] The new rules also required DCMs to impose similar automated risk management controls.[93]

The CFTC published a concept release on automated trading in 2013 to solicit feedback on pre-trade risk controls, post-trade measures, system safeguards, and further protective measures for market participants.[94]

---

90. *See* Jonathan Spicer, *Analysis – 'Flash Crash' Politicizes U.S. Stock Market*, REUTERS (Sept. 3, 2010, 3:23 AM), https://perma.cc/GB98-D58A. Titles VII and VIII of Dodd Frank directed the CFTC's new rulemaking. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010) (codified as amended in scattered sections of the U.S. Code). The CFTC identified 38 areas where rulemaking under the Dodd Frank directive would likely be necessary, including data recordkeeping, disruptive trading practices, and position limits. *See Rulemaking Areas*, COMMODITY FUTURES TRADING COMM'N, https://perma.cc/ZR9R-RY64 (last visited Oct. 4, 2023).

91. *See* Customer Clearing Documentation, Timing of Acceptance for Clearing, and Clearing Member Risk Management RIN 3038-0092 -0094, 77 Fed. Reg. 21278, 21306–8 (Apr. 9, 2012) (codified at 17 C.F.R. § 1.73 and § 23.609), https://perma.cc/C2L8-6F3J (requirements related to automated pre-trade risk management for FCMs, SDs and MSPs); Core Principles and Other Requirements for Designated Contract Markets RIN 3038-AD09, 77 Fed. Reg. 36612, 36705 (June 19, 2012) (codified at 17 C.F.R. § 38.607), https://perma.cc/9UPA-QQ3X (requirements relating to automated pre-trade risk management for DCMs); *see also* SEC Market Access Rule, *supra* note 75.

92. FCM, SD, and MSP requirements established pre-trade risk controls, such as automated position and order size limits, by clearing members and FCMs to manage financial risks, and prescribed regular stress testing of positions and assessment of margin requirements to ensure ongoing risk compliance. Controls include price collars, maximum order sizes, order cancelation features, ongoing stress testing, margin evaluation, and ability to orderly liquidate positions and assess the cost thereof. *See* 17 C.F.R. §§ 1.73(a) and 609(a).

93. Section 607 mandated that DCMs offering direct electronic access implement systems and controls to manage financial risk, including pre-trade automated controls, to prevent price distortions and market disruptions. *See* 17 C.F.R. § 23.607.

94. *See* Concept Release on Risk Controls and System Safeguards for Automated Trading Environments, 78 Fed. Reg. 56542 (Sept. 12, 2013), https://perma.cc/4E6R-HXMJ.

Many industry participants commented on the release, including a comprehensive response by the Futures Industry Association ("FIA").[95]

Following publication of the concept release, the U.S. government treasuries market experienced a destabilizing market event triggered (again) by a trading algorithm error.[96] The U.S. Department of Treasury ("DoT"), Federal Reserve, SEC, and CFTC all collaborated on a joint staff report presented to Congress in 2015.[97] Those findings would be cited in the notice of proposed rulemaking for Regulation AT that same year.[98] Figure 3 below provides a high-level summary of its main provisions.[99]

Figure 3.

Proposed Regulation AT – New and Additional Requirements

New	Additional
Categories of registration re. algorithmic trading	Trading systems testing, monitoring & supervision requirements
Algorithmic trading procedures	Compliance reporting obligations
Source code held in repositories for regulators	Controls on direct electronic access
	Transparency requirements
	Self-trade prevention requirements
	Market-maker & trading incentive program disclosures

Many risk concerns noted in this proposal resemble those discussed later with regards to DeFi.[100] These included operational risks like malfunctioning algorithms and data anomaly handling, sudden strategy shifts affecting market liquidity, potential market integrity issues due to

---

95. *See Comments for Orders and Other Announcements 79 FR 4104*, COMMODITY FUTURES TRADING COMM'N, https://perma.cc/HL5B-FMW9 (last visited July 15, 2023) (over 60 responses were received from industry participants); Walter L. Lukken, *Comment Letter on Re: Concept Release on Risk Controls and System Safeguards for Automated Trading Environments RIN 3038-AD52; 78 FR 56542*, FUTURES INDUS. ASS'N (Dec. 11, 2013), https://perma.cc/C9E7-6N6X (including an 85-page report addressing each of the questions raised in the concept release).

96. *See* U.S. DEP'T OF TREAS., ET AL., JOINT STAFF REP.: THE U.S. TREASURY MARKET ON OCT. 15, 2014 (July 13, 2015), https://perma.cc/2FT5-C8AZ [hereinafter 2015 Joint Staff Report].

97. *See id.*

98. *See* Regulation Automated Trading, 80 Fed. Reg. 78824, 78834 (Dec. 17, 2015) (codified at 17 C.F.R. pts. 1, 38, 40, and 170), https://perma.cc/U3U5-YN9U (referencing the 2015 Joint Staff Report) [hereinafter Regulation AT].

99. *See infra* Section III.D, Fig.3; *see also* Regulation AT, *supra* note 98.

100. *See infra* Sections VI.B–D.

illicit activity, and transmission risks from erroneous orders. The proposal also emphasized risk management challenges associated with increased usage of electronic platforms and the prospect of high-frequency trade execution exceeding capabilities.[101]

The CFTC's proposed Regulation AT included a comprehensive risk management regime with new controls and requirements at *each* stage of an order's lifecycle from order generation to execution to clearing and allocation in proprietary or customer accounts.[102] Proposed Regulation AT also imposed significant back-office technology management controls and sensitive provisions related to the potential compulsory production of source code for proprietary trading algorithms.[103] This extensive proposal was met with a swift and negative reaction, highlighted in Figure 4 below, from impacted market participants, largely championed through the FIA.[104]

Figure 4.

Major Criticisms of Regulation AT: Take I

Complex, prescriptive risk control framework	Unnecessarily burdensome reporting requirements
Over-reaching registration scope	Risks to intellectual property rights in source code
Inflexible software testing requirements	Substantially underestimated costs
Inconsistent with existing market practices	Disincentivized innovation

---

101. *See* Regulation AT, *supra* note 98, at 78859–60.
102. *See id.* at 78827–29, 78849–54, 78880–82.
103. See *id.* at 78857–66.
104. *See infra* Section III.B., Fig.4; Peter Schwartz, *Comment for Proposed Rule 80 FR 78824*, Public Comment No. 60575, COMMODITY FUTURES TRADING COMM'N. (Jan. 5, 2016), https://perma.cc/NE9N-X57K; Williams R. Harts, *Comment for Proposed Rule 80 FR 78824*, *Comment No. 60590*, COMMODITY FUTURES TRADING COMM'N. (Jan. 15, 2016), https://perma.cc/8DVU-4W5Q (both discussing dissatisfaction with the Regulation Automated Trading proposal); *see also* Timothy Weatherhead, *Battle Lines Drawn Over Automated Trading Rule*, THE HILL (Nov. 3, 2016, 2:50 PM), https://perma.cc/4TBR-7ZW7; Allison Lurton, *Comment for Proposed Rule 80 FR 78824*, *Comment No. 60689*, COMMODITY FUTURES TRADING COMM'N (Mar. 4, 2016), https://perma.cc/QP8D-MHDZ (noting the FIA's dissatisfaction with the Regulation AT proposal).

When Regulation AT was proposed again in 2016, the CFTC endeavored to partially scale back the scope of its initial reach.[105] However, in the face of continued "intense opposition," Regulation AT was withdrawn in 2020.[106] In withdrawing Regulation AT, the CFTC explicitly rejected the policy-related decisions of Regulation AT as excessively burdensome and overreaching.[107] Such policies were born from heightened political tensions related to systemic risk concerns despite significant negative consequences to industry participants.

In December 2020, the CFTC adopted a slimmed-down set of principles, known as the "Electronic Trading Risk Principles." These principles applied risk controls solely to DCMs.[108] Because the members of DCMs are futures and options market participants, application of risk controls to DCMs still subjects these participants to the DCM's risk controls and rules.[109]

Ultimately, as depicted in Figure 5 below,[110] Regulation AT had a nearly eight-year history that, although inefficient in its initial approach, ultimately reflected a bottom-up, pragmatic approach to address the requisition protections and needs of market participants.

---

105. *See* Regulation Automated Trading; Supplemental NPRM, 81 Fed. Reg. 85334 (Nov. 25, 2016) (to be codified at 17 C.F.R. pts. 1, 38, 40, and 170), https://perma.cc/KD6Z-GKEJ. Regulation AT risk controls in the repurposed rule were not to be applied at every level, but only to "AT Persons" or FCMs. Additionally, some proposed requirements relating to the risk control framework, registration criteria, reporting requirements, and third-party trading systems would be relaxed. *See id.*

106. Regulation Automated Trading; Withdrawal, 85 Fed. Reg. 42755, 42760 (July 15, 2020) (to be codified at 17 C.F.R. pts. 1, 38, 40, and 170), https://perma.cc/8DHA-WNP7 (noting 73 negative comment letters without mentioning a single positive comment letter).

107. *See id.* (noting Comm'r Berkovitz's recognition that "certain elements of Reg AT attracted intense opposition" and his belief the Reg AT proposal "may have been a bridge too far").

108. *See* Electronic Trading Risk Principles, 85 Fed. Reg. 42761 (July 15, 2020) (to be codified at 17 C.F.R. pt. 38), https://perma.cc/3N7B-2V5P (proposed rule); Electronic Trading Risk Principles, 86 Fed. Reg. 2048 (Jan. 11, 2021) (to be codified at 17 C.F.R. pt. 38), https://perma.cc/N8M3-AGRY (final rule adopted); *see also* 17 C.F.R. §§ 38.250, 38.251; 17 C.F.R. § 38.251(e) (requiring DCM's to implement rules reasonably designed to prevent, detect, and mitigate market disruptions or system anomalies associated with electronic trading); 17 C.F.R. § 38.251(a) (requiring DCMs to collect and evaluate individual trader's market activity to protect against price manipulation).

109. DCM's are required to impose system requirements on market participants and can implement pre-transaction risk controls and order cancellation authorities to manage market disruptions. *See e.g.*, System Safeguards Testing Requirements, 81 Fed. Reg. 64721 (Sept. 19, 2016) (to be codified at 17 C.F.R. pts. 37, 38, and 49), https://perma.cc/E8EB-EFFA.

110. *See infra* Section III.D., Fig.5.

Figure 5.
Reg AT Timeline

Concept Release re. Risk Controls and System Safeguards	Joint Staff Report re U.S. Treasury Market Flash Crash	Amended Reg AT Re-Proposal	ETRP Rule adopted
Sept '13	**July '15**	**Nov '16**	**Jan '21**
Oct '14	**Dec '15**	**July '20**	
U.S. Treasury Market Flash Crash	Reg AT Proposal	Reg AT Withdrawal and ETRP Rule Proposal	
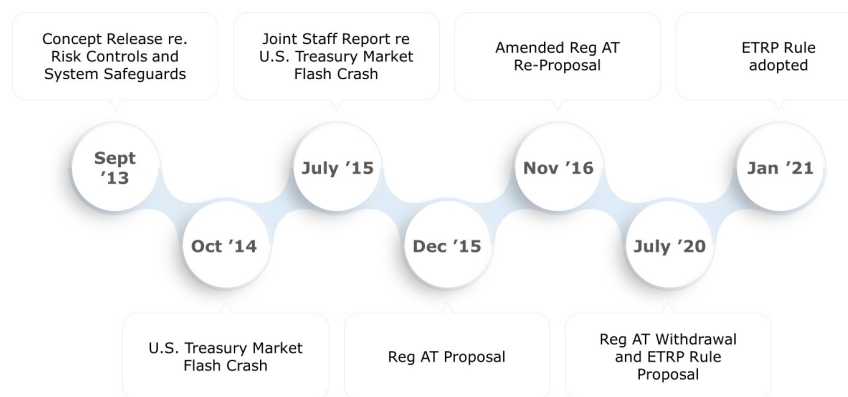
E.   Reflections on CFTC's Experience with Regulation AT

The CFTC's experience with Regulation AT presents an insightful study into the dynamics between financial regulators and industry stakeholders. Despite efforts to actively engage through a concept release and rule proposals, strong resistance from the industry demonstrated a deep divide between the two perspectives and the objectives of the regulator and its market participants.[111] This divide was not a matter of miscommunication; the submitted commentary on the release was extensive. Rather, the schism reflected an assumption by the CFTC that the industry would eventually accommodate sweeping top-down mandates despite the validity of its objections. This experience illustrates how formulating reactive regulations directed at disruptive fintech may be politically expedient but can create unworkable constructs when it proves too burdensome or when mandates exceed statutory authority.

It is noteworthy that the CFTC eventually acknowledged the stakeholders' objections, leading to the adoption of an alternative rule in place of Regulation AT. The withdrawal of Regulation AT marked a turning point, exemplifying how the regulatory process, initially falling short, can self-correct by giving due consideration to stakeholder concerns. Recognizing the shortcomings inherent in the efforts to adopt Regulation AT underscores the need for a more synergistic approach between regulators, policymakers, and disruptive technology stakeholders, moving away from a top-down regulatory paradigm to a more collaborative, bottom-up strategy.

Regulation AT serves as a powerful reminder that while macro-level risk mitigation is an important element of regulation, a politically

---

111. *See* Lurton, *supra* note 104.

expedient bias towards broad, top-down regulation as a response can stifle the development and adoption of innovative technologies. Regulation AT's proposal was a consequence of a new perspective towards the regulation of disruptive technology following the 2008 financial crisis.

F.   One Crisis, Two Paths Forward

The financial upheaval of 2008 marked a shift in how U.S. policymakers and financial regulators approached financial technology. That shift cast emergent financial technologies in two markedly different lights. On one hand, Congress and regulators moved to impose additional centralized oversight, with prescriptive mandates for regulated intermediaries to manage systemic risks amplified by disruptive fintech.[112] On the other hand, the publication of the Bitcoin whitepaper by Satoshi Nakamoto in 2008 introduced a peer-to-peer cryptographic digital asset that could not be controlled by any single entity or government and could be transferred without intermediaries.[113] Bitcoin represented a counterbalance to the systemic risks associated with government debt creation, leveraging a trustless, self-regulating code.[114] In February 2009, Satoshi Nakamoto observed that "[t]he root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust."[115] Thus, one path forward sought to re-establish trust in the financial system through government agencies imposing greater regulation on the operation of intermediaries operating within it, while the other raised more fundamental questions as to whether those governments themselves could be trusted.

In 2014, the publication of the Ethereum whitepaper further expanded the scope of decentralized possibilities.[116] By introducing a unique programming language to enable the development of decentralized applications and smart contracts on a public blockchain network,[117] the Ethereum whitepaper built on the early groundwork for DeFi laid by Bitcoin.

---

112. For a discussion of responsive laws, rules, and regulations promulgated by Congress and financial regulators, see Randall D. Guynn, DAVIS POLK & WARDELL LLP, *The Financial Panic of 2008 and Financial Regulatory Reform*, HARV. L. SCH. FORUM ON CORP. GOV. (Nov. 20, 2010), https://perma.cc/P8TG-YWXX.

113. *See* Satoshi Nakamoto, *Bitcoin: A Peer-To-Peer Electronic Cash System* (Oct. 31, 2008), https://perma.cc/JMM3-8KED.

114. *See id.*

115. Satoshi Nakamoto, *Bitcoin Open Source Implementation of P2P Currency*, SATOSHI NAKAMOTO INSTITUTE (Feb. 11, 2009), https://perma.cc/P8S2-XKPE.

116. *See* Vitalik Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, ETHEREUM.ORG (2014), https://perma.cc/Y5JX-6WCR.

117. *See infra* Part IV.

The political and regulatory attention to automated trading in the 2010s, and to digital assets in the early 2020s, politicized financial technology with an unprecedented and unfortunate intensity. This intensity was magnified in November of 2022 with the collapse of FTX, a centralized offshore digital asset trading platform.[118] The political significance of this event was made more impactful by the active role that its founder had taken in trying to shape U.S. digital asset policy.[119]

G. Digital Asset Regulation and Enforcement

To an external observer, the United States's approach to digital asset regulation has been marked by an increasingly adversarial, politicized tone.[120] Though the SEC has engaged in broader rulemaking proposals, such as amending Reg ATS and safeguarding customer assets that would impact digital asset stakeholders, a digital asset regulatory framework has yet to be established.[121] During SEC Chair Gensler's term, the Commission significantly increased the number and frequency of digital

---

118. *See* Stephen Katte, *Calls for Regulation get Louder as FTX Contagion Continues to Spread*, COINTELEGRAPH (Nov. 29, 2022), https://perma.cc/U8QP-ZKB9; *see also* Peter Whoriskey and Dalton Bennett, *Crypto's Free-Wheeling Firms Lured Millions. FTX Revealed the Dangers*, WASH. POST (Nov. 16, 2022, 1:14 PM), https://perma.cc/WSE3-XTPE.

119. *See* Shalini Nagarajan, *FTX's Sam Bankman-Fried says Crypto Adoption by Institutions is more of a Trickle than a Deluge because Regulators are Keeping them Waiting*, MARKETS INSIDER (Feb. 23, 2022, 5:04 AM) https://perma.cc/5ACV-ADBT; *see also* Cheyenne Ligon, *The 'SBF Bill': What's in the Crypto Legislation Backed by FTX's Founder*, COINDESK (Nov. 15, 2022, 10:28 PM), https://perma.cc/E789-H5AJ; *Digital Assets and the Future of Finance: Understanding the Challenges and Benefits of Financial Innovation in the United States: Hybrid Hearing Before the H. Comm. on Fin. Serv.*, 117th Cong. (Dec. 8, 2021), https://perma.cc/6RAL-UFUW.

120. *See, e.g.*, Carol R. Goforth, *Political Reality and Crypto Regulation*, 26 CHAP. L. REV. 599, 617–620 (2023).

121. The latest proposed revisions to Reg ATS—the Digital Asset Special Purpose Broker-Dealer exemptive relief and the proposed Safeguarding Advisory Client Assets rules—implicate digital asset securities but are not tailored frameworks for digital assets. *See* Amendments Regarding the Definition of 'Exchange' and Alternative Trading Systems (ATSs) that Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities, Exchange Act Release No. 94062, 87 Fed. Reg. 15496 (Mar. 18, 2022) (to be codified at 17 C.F.R. pts. 232, 240, 242, and 249), https://perma.cc/RA94-75HQ [hereinafter ATS Proposal]. The Special Purpose Broker-Dealer exemption provides limited relief from the Customer Protection Rule's "good control location" requirement for broker-dealers holding digital asset securities. *See* Custody of Digital Asset Securities by Special Purpose Broker-dealers, Exchange Act Release No. 90788, 86 Fed. Reg. 11627 (Feb. 26, 2021) (to be codified at 17 C.F.R. pt. 240), https://perma.cc/GR7L-5NNE. The proposed amendment to the Safeguarding Advisory Client Assets Rule (also known as the "custody rule") would require a wide range of investment advisers to use qualified custodians, including for digital assets, when acting as a custodian for its clients. *See* Safeguarding Advisory Client Assets, 88 Fed. Reg. 14672, Rel. No. IA-6240 (Mar. 9, 2023) (to be codified at 17 C.F.R. pts. 275, 279), https://perma.cc/5Q3G-WCJX.

asset enforcement cases that it brought to court.[122] This enforcement strategy has focused primarily on initial securities registration violations and secondarily on anti-fraud measures.[123] The strategy later expanded to include exchange, broker, and clearing agency registration violations.[124] Controversially, enforcement actions brought later in Chair Gary Gensler's term often centered around claims that certain tokens were securities as part of actions brought against crypto trading platforms without any process for impacted token issuers or allocators to challenge these designations before they were made.[125]

The CFTC has also substantially increased enforcement actions during this same period, but not to the same scale as the SEC.[126] These actions predominantly involved fraud, failure to register as a FCM, DCM, or Swap Execution Facility ("SEF"), or the lack of appropriate AML protocols for centralized entities.[127] In 2023, the CFTC won a default judgment against an unincorporated decentralized association, Ooki DAO, primarily for engaging in leveraged and margined retail commodity

---

122. From 2013 to 2021, the SEC initiated 55 digital asset related enforcement actions; 34 were resolved in administrative proceedings, and 21 were pursued in court. *See* MORRISON COHEN LLP, CRYPTOCURRENCY LITIGATION AND REGULATION TRACKER CRYPTOCURRENCY LITIGATION AND REGULATION TRACKER (Apr. 26, 2023), https://perma.cc/F8US-5YD9. From 2021 to 2023, the number of enforcement actions rose to 61; 47 were pursued in court, and 14 were resolved administratively. *See id.* These statistics exclude trading suspensions. *See also* Yuliya Guseva, *The SEC, Digital Assets, and Game Theory*, 46 J. CORP. L. 629 (2021).

123. *See* Guseva, *supra* note 122.

124. *See, e.g.*, U.S. Sec. & Exch. Comm'n v. Payward, Inc. (N.D.Cal. Nov. 20, 2023), https://perma.cc/VR5B-4JRL [hereinafter Kraken Action]; U.S. Sec. & Exch. Comm'n v. Coinbase, Compl., 23 Civ. 4738 (S.D.N.Y. June 6, 2023), https://perma.cc/58HD-MTNJ [hereinafter Coinbase Action]; U.S. Sec & Exch. Comm'n v. Binance Holdings Ltd., 23 Civ. 1599 (D.D.C. June 5, 2023), https://perma.cc/6P5Q-THSW [hereinafter Binance Action]; *see also* U.S. Sec. & Exch. Comm'n v. Beaxy Digital, Ltd., 23 Civ 1962 (N.D. Il. Mar. 29, 2023), https://perma.cc/6N5J-S6YC.

125. *See, e.g.*, Kraken Action, *supra* note 124, at 15 (identifying 16 digital assets as securities); Coinbase Action, *supra* note 124, at 33 (identifying 13 digital assets as securities); Binance Action, *supra* note 124, at 85 (identifying 10 digital assets as securities); U.S. Sec. & Exch. Comm'n v. Ishan Wahi, et.al., Docket No. 2:22-cv-01009 (W.D. Wash. July 21, 2022), https://perma.cc/N9JE-H76J (identifying 9 digital assets as securities).

126. From 2015 to 2021, the CFTC initiated 21 digital-asset-related enforcement actions, with five being resolved in administrative proceedings and 16 in court. From 2021 to 2023, there were 19 CFTC enforcement actions, with seven resolved in administrative proceedings and 12 in court. *See* MORRISON COHEN LLP, *Cryptocurrency Litigation and Regulation Tracker Cryptocurrency Litigation and Regulation Tracker* (Apr. 26, 2023), https://perma.cc/F8US-5YD9; Solidus Labs Research, *2023 Crypto Enforcement Trends: SEC & CFTC Set Records as States Take the Lead*, SOLIDUS LABS, https://perma.cc/3QDX-ZKSR (last visited Aug. 1, 2023).

127. *See* Solidus Labs Research, *supra* note 126.

transactions without being a registered DCM or FCM.[128] The action raised novel issues regarding how a decentralized organization could be served, or held liable, as a person under the CEA.[129] Later in 2023, the CFTC settled enforcement actions with three entities that developed and maintained DeFi protocols and applications.[130] The settlement with one entity, ZeroEx, Inc., related to a non-custodial protocol designed for the trading of non-margined or leveraged digital assets (known as the "spot" market), a market over which the CFTC lacks jurisdiction.[131] However, that protocol was used by unaffiliated third parties to effect exchanges of derivatives for a de minimis portion of total protocol volume.[132] In the order, the CFTC noted that a developer that deployed a decentralized protocol and operated a front-end interface met the standard for facilitating the conduct of such third parties.[133] This position contradicted the findings of an earlier federal case that refused to hold developers liable for a third party's misuse of a DeFi protocol,[134] suggesting a willingness of the CFTC to engage in a more aggressive and potentially litigious enforcement strategy. Moreover, two of the settlements related to a failure to register as an FCM and a SEF.[135] In her dissent, CFTC Commissioner Summer Mersinger noted that the cases represented "a significant shift in position on the merits of engagement with DeFi market participants" and the potential for the CFTC to create an "impossible environment for those who

---

128. *See* bZeroX, LLC, CFTC No. 22-31 (Sept. 22, 2022), https://perma.cc/W3BC-2BXM [hereinafter Ooki DAO Action] (order fining Ooki DAO, which was originally named bZeroX, for CEA registration violations).

129. *See Statement of CFTC Division of Enforcement Director Ian McGinley on the Ooki DAO Litigation Victory*, Release No. 8715-23, COMMODITY FUTURES TRADING COMM'N (June 9, 2023), https://perma.cc/TAM9-UP9R; *see also* Practical Law Finance, *CFTC Granted Default Judgment Against Ooki DAO for CEA Violations*, w-039-7921, THOMSON REUTERS (June 14, 2023), https://perma.cc/F49P-98G7.

130. *See CFTC Issues Orders Against Operators of Three DeFi Protocols for Offering Illegal Digital Asset Derivatives Trading*, Release No. 8774-23, COMMODITY FUTURES TRADING COMM'N (Sept. 7, 2023), https://perma.cc/ASL7-CV7Y; Deridex, Inc., CFTC No. 23-42 (Sept 7, 2023), https://perma.cc/6S3F-8WC9 [hereinafter Deridex Action]; Opyn, Inc., CFTC No. 23-40, (Sept 7, 2023), https://perma.cc/4Z3G-CNZT [hereinafter Opyn Action]; ZeroEx, Inc. CFTC, No. 23-41, (Sept 7, 2023), https://perma.cc/X2F7-N94A [hereinafter ZeroEx Action].

131. *See* ZeroEx Action, *supra* note 130.

132. *See* @Matcha, TWITTER (X) (Sept 07, 2023, 6:55 PM), https://perma.cc/DE88-5LXY ("[ZeroEx] . . . cooperated with the CFTC to resolve an inquiry regarding tokens constituting less than 0.1% of Matcha's trading volume since inception.").

133. *See* ZeroEx Action, *supra* note 130, at n.8.

134. *See generally* Nessa Risley v. Universal Navigation Inc. d/b/a Uniswap Labs, 22 Civ. 2780 (S.D.N.Y. Aug 29, 2023), https://perma.cc/3KM6-JSSF (dismissing a class action based on a claim that a DeFi protocol could be held liable for users who fell victim to "scam tokens" sold by third parties on the protocol).

135. *See* Deridex Action, *supra* note 130, at 5–6; Opyn Action, *supra* note 130, at 5–6.

want to comply with the law, forcing them to either shut down or shut out U.S. participants."[136]

The SEC's enforcement-driven approach, coupled with inconsistent statements about its enforcement authority over digital asset markets, has contributed to regulatory uncertainty.[137] Legal scholars have documented the lack of judicial precedent for the agency's efforts to apply an investment contract analysis to secondary sales of digital assets.[138] Subsequently, the SEC's classification of digital assets as securities (when purchased in secondary market transactions and part of programmatic sales) was rejected in a key decision in its action against Ripple Labs.[139] Conversely, that decision also supported the SEC's interpretation that the sale of tokens by Ripple Labs to institutional investors constituted an investment contract and were thus securities.[140] However, whether a specific digital asset-related enforcement action warrants a regulator, such as the SEC or the CFTC, to initiate a lawsuit is a separate consideration

---

136. *Dissenting Statement of Commissioner Summer K. Mersinger Regarding Enforcement Actions Against: 1) Opyn, Inc.; 2) Deridex, Inc.; and 3) ZeroEx, Inc.*, Release No. 8774-23, COMMODITY FUTURES TRADING COMM'N (Sept. 7, 2023), https://perma.cc/GD6Z-N964.

137. *Compare Game Stopped? Who Wins and Loses When Short Sellers, Social Media, and Retail Investors Collide, Part III*: *Hearing Before the U.S. H. Fin. Servs. Comm.*, 117th Cong. 12 (May 6, 2021), https://perma.cc/JY74-2PTZ (asserting the SEC's lack of regulatory authority over digital asset exchanges), *with* Allyson Versprille, *Gensler Asserts SEC Authority Over Crypto as Opponents Waver*, BLOOMBERG NEWS (July 11, 2023, 10:00 AM), https://perma.cc/L5S9-HV7H (reporting on Gary Gensler's assertion of authority over "crypto trading platforms" and "the vast majority of tokens").

138. *See* Lewis Cohen et al., *The Ineluctable Modality of Securities Law: Why Fungible Crypto Assets are not Securities* (Nov. 10, 2022), https://perma.cc/AM23-ERQX.

139. *See generally* U.S. Sec. & Exch. Comm'n v. Ripple Labs, 20 Civ. 10832, at 25 (S.D.N.Y. July 13, 2023) (holding that programmatic sales of XRP tokens on digital asset exchange were not investment contracts because investors could not have known whether their investments were funding the common enterprise, and evidence was not introduced showing secondary investors were aware of Ripple's marketing) [hereinafter Ripple Order]. *But see* U.S. Sec. & Exch. Comm'n v. Terraform Labs Pte. Ltd. Et. al, Case 1:23-cv-01346-JSR, at 40–42 (July 31, 2023), https://perma.cc/XD5W-ZTL9 [hereinafter Terraform Dismissal Denial Order]. There, presiding Judge Rakoff stated:

> [T]he Court declines to draw a distinction between these coins based on their manner of sale, such that coins sold directly to institutional investors are considered securities and those sold through secondary market transactions to retail investors are not. In doing so, the Court rejects the approach recently adopted by another judge of this District in a similar case, SEC v. Ripple Labs Inc . . . .

Id. at 40.

140. *See* Ripple Order*, supra* note 139, at 22; *See also* Sec. & Exch. Comm'n v. Terraform Labs Pte. Ltd. et al., No. 1:23-cv-01346-JSR, at 37–43 (December 28, 2023) [hereinafter the *Terraform Opinion and Order*], https://perma.cc/L5P3-FT2L; *see also* U.S. Sec. & Exch. Comm'n v. LBRY, Inc., No. 21 Civ. 260, 2022 WL 16744741 (D.N.H. Nov. 7, 2022); U.S. Sec. & Exch. Comm'n v. Telegram Grp. Inc., 448 F. Supp. 3d 352 (S.D.N.Y. 2020); U.S. Sec. & Exch. Comm'n v. Kik Interactive Inc., 492 F. Supp. 3d 169, (S.D.N.Y. 2020).

from the potential pitfalls of a litigation-focused enforcement strategy. This strategy could result in increased litigation, unfavorable legal precedents due to potential overreach,[141] and resource inefficiency due to the need for larger litigation teams—resources that could be better deployed to collaborative efforts with stakeholders.

Lastly, while the SEC and CFTC cite investor protection as a key objective in digital asset enforcement,[142] the pursuit of this objective has been distorted by a more complex set of considerations.[143] For example, the SEC has missed opportunities to pursue greater transparency and clearer regulations, such as adopting a tailored disclosure framework for digital asset offerings like those proposed by SEC Commissioner Hester Peirce or the digital assets advocacy group LeXpunK.[144] A heightened regulatory focus on the hypothetical systemic risks of disruptive technologies and its politicization has led to policies that are less effective in addressing investor protection and detrimental to innovation.[145]

H. FSOC's Focus on Digital Assets

The FSOC is composed of the Secretary of Treasury; the heads of the Federal Reserve, CFTC, and SEC; and others.[146] This composition is intended, among other things, to ensure that the SEC, CFTC, Treasury, and other participating agencies remain focused and coordinated on potential or hypothetical macroprudential and systemic risk concerns as part of their mandate. However, the FSOC has no mandate to contemplate innovation as a counterbalancing consideration. The FSOC has

---

141. *See* Brooke Masters, *When Tackling Crypto, the SEC should be Wary of Overreach*, FINANCIAL TIMES (Aug. 16, 2023), https://perma.cc/EZJ8-DJZ4.

142. *See e.g.*, Jesse Pound, *SEC Chairman Gary Gensler Says More Investor Protections are Needed for Bitcoin and Crypto Markets*, CNBC (May 7, 2021), https://perma.cc/4GXS-DJ7C; Gary Gensler, Chair, U.S. Sec. & Exch. Comm'n, *Remarks Before the 2022 NASAA Spring Meeting & Public Policy Symposium: Investor Protection in a Digital Age* (May 17, 2022), https://perma.cc/JU6M-LV8Q; *see Statement of Commissioner Kristin N. Johnson Calling for the CFTC to Initiate A Rulemaking Process for CFTC-Registered DCOs Engaged in Crypto or Digital Asset Clearing Activities*, Release No. 8708-23, COMMODITY FUTURES TRADING COMM'N (May 30, 2023), https://perma.cc/4BQN-XDAK [hereinafter Johnson Statement].

143. *See infra* Section III.F.

144. *See* Hester M. Peirce, Comm'n, U.S. Sec. & Exch. Comm'n, *Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization* (Feb. 6, 2020), https://perma.cc/DN86-H5MX; *see also Regulation X Proposal: An Exempt Offering Framework for Token Issuances*, LEXPUNK (Apr. 25, 2022), https://perma.cc/P4DK-QV2A.

145. *See e.g.*, *infra* Section III.F.

146. *See Financial Stability Oversight Council*, U.S. DOT, https://perma.cc/8R4G-CTDL (last visited Nov. 20, 2023). The Council is composed of ten voting and five non-voting members. The other voting members include the heads of the Federal Deposit Insurance Corporation, Federal Housing Finance Agency, and Consumer Financial Protection Bureau. *See id.*

historically given attention to automated trading,[147] but in 2018, the FSOC created a digital assets working group to facilitate coordination among the financial regulators and has since identified digital assets as a priority area of focus in its annual reports.[148]

The 2022 White House Executive Order on Ensuring Responsible Development of Digital Assets (the "Digital Assets Executive Order") tasked the FSOC with identifying financial stability risks associated with digital assets and proposing necessary regulatory adaptations.[149] This order highlighted significant concerns with the lack of uniform application of AML and countering the financing of terrorism ("CFT") regulations and standards across jurisdictions.[150] The order also underscored the significant roles of both the SEC and CFTC in maintaining systemic integrity and promoting financial stability.[151] The Digital Assets Executive Order, along with subsequent White House announcements,[152] acknowledged the influential role of the Financial Stability Board ("FSB") in identifying and addressing strategic and systemic risks associated with digital assets.[153]

In response to the Digital Assets Executive Order's mandate, the FSOC published a comprehensive report outlining systemic risks associated with digital assets and suggesting prophylactic measures, including continued enforcement, aligned with the principle of "same activity, same risk, and same regulatory outcome."[154] This approach was echoed by CFTC Commissioner Goldsmith Romero, who advocated for stricter digital asset regulations to preemptively safeguard the broader financial system from potential systemic risks, and by SEC Chair Gensler,

---

147. *See* FSOC Annual Reports, *supra* note 82.

148. *See* Stan Higgins, *US Finance Regulators Form Crypto Working Group, Says Mnuchin,* COINDESK (Dec. 11, 2022, 2:30 PM), https://perma.cc/F5D3-MP7Z; 2022 ANNUAL REP., FIN. STABILITY OVERSIGHT COUNCIL 79 (2022), https://perma.cc/P5RS-Q5R7 (noting that the FSOC's Digital Assets Working Group met consistently and coordinated the drafting of FSOC's Report on Digital Assets Financial Stability Risks and Regulations in response to E.O. 14067).

149. *See* Ensuring Responsible Development of Digital Assets, Exec. No. 14067, 87 Fed. Reg. 14143 (Mar. 9, 2022), https://perma.cc/44AS-6LCW.

150. *See id.* at 14144.

151. *See id.* at 14148.

152. *See* FACT SHEET: White House Release's First-Ever Comprehensive Framework for Responsible Development of Digital Assets, THE WHITE HOUSE (September 16, 2022), https://perma.cc/RPR6-KLBQ.

153. Ensuring Responsible Development of Digital Assets, Exec. No. 14067, 87 Fed. Reg. 14143, 14150 (Mar. 9, 2022), https://perma.cc/44AS-6LCW (noting the FSB is "leading work on issues related to stablecoins, cross-border funds transfers and payments, and other international dimensions of digital assets and payments").

154. REP. ON DIGITAL ASSET FIN. STABILITY RISKS AND REG., FIN. STABILITY OVERSIGHT COUNCIL 111 (2022), https://perma.cc/9NCU-4BEJ (recommending enforcement of the existing financial regulatory framework against digital assets and limiting interconnections with the traditional financial system).

who compared the financial stability risks associated with digital assets to those associated with the 2008 financial crisis and the potential for those risks to become systemic.[155]

The growing influence of the FSOC and its emphasis on systemic risk has created a bias towards a top-down regulatory approach that risks hindering the ability of financial regulators to collaboratively engage with stakeholders to advance innovation and competition. Collaborative engagement, while increasingly challenging in the current environment, can be productively pursued by hybrid finance stakeholders irrespective of regulatory recognition.[156]

IV. DeFi, Regulation, and the Case for Proactive Collaboration

> "Rational optimism is not just the belief that things will get better; it is also the understanding that we have the capability to make things better. This is the key to progress. When we solve problems, we create new problems, but they are better problems. They are the problems of success, not failure." — David Deutch

A. Introduction to DeFi

DeFi refers to a blockchain-based system composed of software designed for the conduct of peer-to-peer or system-to-system economic activities, such as exchanging, lending, borrowing, offering, managing, and tokenizing of digital assets.[157] These systems are governed by pre-set coded rules, algorithms, or protocols, eliminating the need for a financial intermediary or third-party asset custodian.[158] DeFi systems are stored and executed on a blockchain environment managed by a network of adverse nodes using a consensus protocol, which contributes to greater resilience

---

155. *See Remarks of CFTC Commissioner Christy Goldsmith Romero before the International Swaps and Derivatives Association's Crypto Forum 2022, New York*, Commodity Futures Trading Comm'n (Oct. 26, 2022), https://perma.cc/36MT-ALG5 ("[C]rypto presents many similar financial stability risks as the traditional financial system, with parallel themes to 2008, and the[re is] potential for that risk to become systemic."); Gary Gensler, Chair, U.S. Sec. & Exch. Comm'n, *Fireside Chat: A Market Regulator's View of Too-Big-To-Fail*, 15th Anniversary Lehman Collapse Conference (Sep. 13, 2023).

156. *See infra* Section IV.F.

157. *See* Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets*, 103 Econ. Res.: Fed. Res. Bank of St. Louis 1, 2–4 (Mar. 8, 2020), https://perma.cc/AJ7B-HQUU; *see also* Sumedha Deshmukh et al., World Econ. Forum, Decentralized Finance (DeFi) Policy-Maker Toolkit 1–7 (2021), https://perma.cc/7V83-CC66 [hereinafter WEF Policymakers Toolkit]; *see also* Raphael Auer, et. al., The Technology of Decentralized Finance (DeFi), Bank for Int'l Settlements, at 1–4 (2023), https://perma.cc/RC8C-5R9Z.

158. *See* Deshmukh et al., *supra* note 157, at 7.

against system failures.[159] While decentralization exists on a spectrum, decentralization in the context of DeFi governance refers to systems that are not owned or controlled by any single entity or a coordinated group of individuals.

In a DeFi system, users have open, transparent access to a DeFi protocol, and the system operates without requiring centralized intermediaries.[160] Pieces of code known as smart contracts are enforced by consensus rules and network validation and perform deterministic functions without the involvement of third parties.[161] These contracts can, for instance, secure an asset until a specific event happens or certain conditions are met.[162] The control of these assets is programmatically restricted and is subject to the logic of the DeFi protocol's smart contract and the underlying blockchain's consensus rules.[163] Public posting on the blockchain ensures validity and enables public scrutiny.[164]

Defining DeFi can, however, be challenging; DeFi has a broader set of connotations depending on perspective. Whether DeFi is characterized by a lack of intermediaries or centrally managed systems or, alternatively, exists on the spectrum of decentralization is not relevant here. Intermediaries and centrally managed systems interact with decentralized protocols and systems within a hybrid finance ecosystem wherever they fall on this spectrum.[165] Within this ecosystem, regulators, intermediaries,

---

159. *See id.* at 8; Schär, *supra* note 157, at 2. Such greater resilience can be attributed to the reduction or elimination of single points of failure; a consensus mechanism that ensures system integrity even if some nodes act maliciously or are compromised; the availability of continuous auditing due to increased transparency; the operation of smart contracts which operate without downtime; fraud or interference from third parties; interoperability across systems without single platform dependencies; replication of data across multiple nodes; censorship resistance which reduces the impact of localized failures or government actions; and upgradeability in response to identified issues and threats. *See generally* DESHMUKH ET AL., *supra* note 157; Schär, *supra* note 157.

160. *See* Schär, *supra* note 157, at 1 ("[T]his architecture can create an immutable and highly interoperable financial system with unprecedented transparency, equal access rights, and little need for custodians, central clearing houses, or escrow services, as most of these roles can be assumed by 'smart contracts.'").

161. *See id.* at 1–2, 9; WEF POLICYMAKERS TOOLKIT, *supra* note 157, at 8. The WEF Policymakers Toolkit explains the non-custodial aspect of smart contracts, which allows smart contracts to operate without depending on third parties:

> Non-custodial design means that the assets issued or managed by DeFi services cannot be unilaterally expropriated or altered by parties other than the account owner, even those providing intermediation and other services. These tokens are subject only to the explicit logic of their smart contracts and the relevant DeFi protocols.

WEF POLICYMAKERS TOOLKIT, *supra* note 157, at 7.

162. *See What is a Smart Contract, and How Does it Work?*, COINTELEGRAPH, https://perma.cc/78WG-FA5Q (last visited Oct. 23, 2023) [hereinafter *Smart Contract*].

163. *See* Schär, *supra* note 157, at 1–2, 9.

164. *See id.* at 9.

165. *See supra* Part I.

builders and other technology providers, participants in, and users of the DeFi ecosystem all comprise "hybrid finance stakeholders." DeFi protocols operate within a larger supporting ecosystem that may contain both centralized and decentralized components.[166] The delivery of certain services within this ecosystem may or may not require the performance of centrally managed services or operations;[167] such services are referred to as "hybrid finance services." Within the hybrid finance ecosystem, functional participants serve as integral components contributing to an interconnected, decentralized network. While some roles may require regulatory classification—assuming there exists a workable framework for compliance—hybrid finance necessitates a focus on these functional contributions rather than on a top-down, categorical assignment of responsibilities that could stifle innovation and deter active involvement from a diverse range of stakeholders.

DeFi services (or hybrid finance services) span a range of categories,[168] including but not limited to the following:

- *Decentralized Exchanges ("DEXs")*: DEXs enable peer-to-peer exchanges by utilizing liquidity pools[169] or auction processes managed through smart contracts.[170]
- *Liquid Staking*: Users deposit and lock digital assets into a network smart contract for the purpose of facilitating liquidity. In return, users receive a tokenized version of the deposited assets and a reward for the duration of such locked deposit.[171]

---

166. *See id.*

167. *See, e.g.*, discussion relating to permissioned systems *infra* Section V.B.

168. For a comprehensive list of DeFi services categories, see *Protocol Categories*, DEFI LLAMA, https://perma.cc/S2C7-6MCK (last visited July 16, 2023). *See also*, Francesca Carapella et al.*, Decentralized Finance (DeFi): Transformative Potential & Associated Risks*, WA: BOARD OF GOVERNORS OF FED. RES. SYS. 1, 13 (2022), https://perma.cc/9DDZ-8F5H (considering Lido, Convex Finance, Arrakis, Yearn Finance, and Beefy Finance to be DeFi asset managers); FIN. STABILITY BOARD, *The Fin. Stability Risks of Decentralized Fin.* (Feb. 16, 2023), at 15, https://perma.cc/KPY2-Z77K [hereinafter *FSB DeFi Report*]; WEF POLICYMAKERS TOOLKIT, *supra* note 157, at 11.

169. A liquidity pool can be generally defined as a smart contract that holds and transfers digital asset tokens based on an algorithm. *Liquidity Pool Meaning*, LEDGER (July 19, 2023), https://perma.cc/NDN6-2RH4.

170. *See e.g.*, *Swap - Curve*, CURVE, https://perma.cc/3WNW-WJUN (last visited Oct. 23, 2023); *Swap - Uniswap,* UNISWAP, https://perma.cc/P9JT-3P8R (last visited Oct. 23, 2023); *Swap - PancakeSwap*, PANCAKESWAP, https://perma.cc/XJT8-P8YP (last visited Nov. 20, 2023).

171. *See e.g.*, *Liquidity for Staked Coins*, LIDO, https://perma.cc/M8G3-9W5C (last visited Oct. 23, 2023); *Rocket Pool Decentralised Ethereum Staking Pool*, ROCKET POOL, https://perma.cc/7WRH-H6MX (last visited Oct. 23, 2023); *Mint,* FRAX, https://perma.cc/9UXQ-FV23 (last visited Oct. 23, 2023).

- *Derivatives*: Derivatives provide exposure to synthetic financial assets such as futures and perpetuals. This exposure is facilitated through collateralized liquidity pools.[172]
- *Lending Services*: These services offer interest-bearing loans accessed through smart contracts and facilitated by liquidity pools or bilateral agreements. The loans can be either collateralized with digital assets or unsecured.[173]
- *Stablecoins*: Stablecoins are digital tokens whose value is algorithmically pegged to a reserve of assets, which could be a fiat currency, a commodity, or another digital asset.[174]
- *Asset Management*: These services manage portfolios of digital assets based on various factors like risk tolerance, investment horizon, and more.[175]
- *Insurance pools*: Insurance pools involve paying a small, guaranteed premium in exchange for the possibility of a large payout in the event of a covered scenario.[176]

B. The Growth and Use Cases of DeFi Technologies

The growth of DeFi systems presents a complex but promising landscape for both financial market structure and global financial democratization.[177] Though potentially sizable, the market is nascent and has experienced volatility in volumes, even more so than digital assets

---

172. *See e.g.*, *Decentralized Perpetual Exchange*, GMX, https://perma.cc/2N4R-TAQ5 (last visited Oct. 23, 2023); *Trading, Decentralized*, DYDX, https://perma.cc/G4PX-Y4JU (last visited Oct. 23, 2023); *Gains Network*, GAINS NETWORK, https://perma.cc/25HS-48R4 (last visited Oct. 23, 2023).

173. *See e.g.*, Aave Liquidity Protocol, AAVE, https://perma.cc/3UDB-MRND (last visited Oct. 23, 2023); *Compound Finance,* COMPOUND FINANCE https://perma.cc/HP56-R2XF (last visited Oct. 23, 2023).

174. Popular stablecoins include USD Coin (USDC) and Tether (USDT) and are used within DeFi systems but are themselves not DeFi services, as they have centralized issuers.

175. *See e.g.*, Yearn Finance, Ondo Finance, and Range Protocol. *Homepage*, YEARN FINANCE, https://perma.cc/6SE4-55P2 (last visited Oct. 23, 2023); *Institutional-Grade Finance. On-Chain. For Everyone.*, ONDO FINANCE, https://perma.cc/WG44-RB7W (last visited Oct. 23, 2023); *The Universal Gateway to DeFi Asset Management*, RANGE PROTOCOL, https://perma.cc/4SRM-X9UT (last visited Oct. 23, 2023).

176. *See e.g.*, Nexus Mutual, Guard.Insure, and Insurace. *Industry Leading On-Chain Protection*, NEXUS MUTUAL, https://perma.cc/25VB-EZWA (last visited Oct. 23, 2023); *Making Web3 Safer*, INSURACE, https://insurace.io (last visited Oct. 23, 2023) [hereinafter the *Insurance Protocols*].

177. *See, e.g.*, Anna Stone, *Why Decentralized Finance is a Leapfrog Technology for the 1.1 Billion People who are Unbanked*, WORLD ECON. FORUM (Sept. 16, 2022), https://perma.cc/H7PQ-7APN (discussing DeFi's potential to bring financial services to the 1.1 billion unbanked people who have mobile phones); Marvin Ammori, *Decentralized Finance: What It Is, Why It Matters*, A16ZCRYPTO (June 15, 2021), https://perma.cc/RQ3V-5MJU.

have on a relative basis.[178] Despite the existence of over 3,200 DeFi services worldwide, less than 3% have asset deposits (also known as total value locked or "TVL") of over $100 million, and few experience significant user activity.[179]

As illustrated in Figure 6 below,[180] as of December 31, 2023, DeFi services had an aggregate TVL of $53.25 billion, up slightly following a downward trend and sharply off-peak volumes in the months leading up to the Terra Luna collapse in May of 2022.[181] This decline may have also been partially attributable to a rising Fed Funds rate in 2022 and 2023,[182] which attracts capital away from riskier assets, such as those associated with DeFi.

---

178. *See* DEFILLAMA, *Overview (All)*, https://perma.cc/AQB6-4LW8 (last visited Dec. 29, 2023). As of January 3, 2024, DefiLlama reported 3,233 DeFi applications and protocols, with 94 having a TVL of $100 million or more.

179. *See id.*

180. *See infra* Section IV.A., Fig.6.

181. *See* DEFILLAMA, *DeFi Aggregate TVL* (Dec. 31, 2023), https://perma.cc/JD7A-VJLK; *see also* Krisztian Sandor and Ekin Genç, *The Fall of Terra: A Timeline of the Meteoric Rise and Crash of UST and LUNA*, COINDESK (Dec. 22, 2022, 4:07 PM), https://perma.cc/VSN7-MNFH. The fall of Terra's stablecoin, TerrUST (UST), and its sister token, LUNA, created a loss of confidence in the then current design of algorithmic stablecoins which are connected to DeFi ecosystems, impacted a large number of projects with exposure to UST and LUNA, resulted in margin call liquidations across the digital asset ecosystem, and raised concerns regarding overall exposure in light of unknown impacts.

182. *See Policy Tools: Open Market Operations*, BD. OF GOVERNORS OF THE FED. RSRV. SYS., https://perma.cc/K5L7-7UC4 (last visited Dec. 29, 2023).

Figure 6.[183]
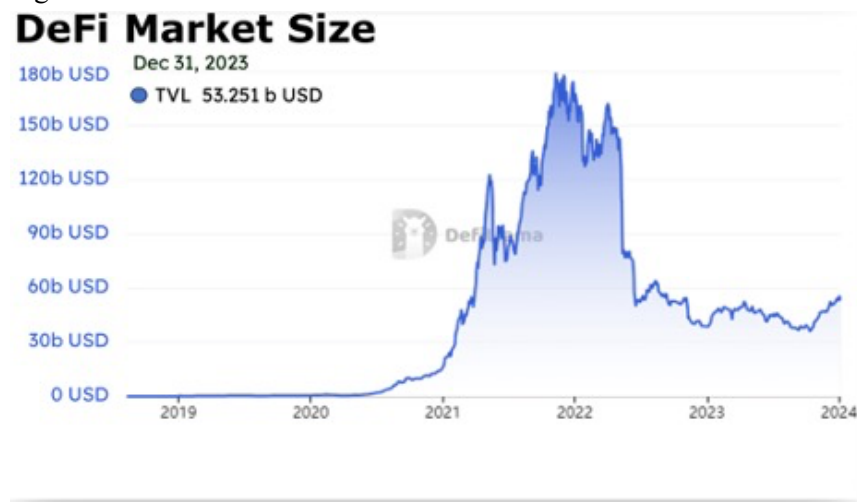
This aggregate TVL statistic also does not account for the swift adaptation of smart contract and distributed ledger technologies by traditional financial intermediaries, such as Broadridge, capitalizing on the open-source technologies offered by DeFi. This is one of the understudied and underappreciated benefits derived from DeFi technologies.

Institutions such as Broadridge, with its Distributed Ledger Repo platform,[184] have recently begun to harness the disruptive capabilities of DeFi technologies. Utilizing DeFi credit smart contracts and atomic blockchain-based settlement, the platform achieved over $50 billion in average daily volumes with only UBS and Societe Generale active on the platform.[185] Broadridge's ongoing expansion into cross-border, intraday repo facilities further underscores this impact, albeit on a proprietary, centrally managed, and permissioned network.[186]

Similarly, the Monetary Authority of Singapore ("MAS") created Project Guardian, a DeFi and asset tokenization technology pilot program,

---

183. *DeFi Aggregate TVL*, *supra* note 181.

184. A repurchase agreement, or repo, is economically equivalent to a short-term secured loan but is structured as a sale of the collateral for cash along with the seller/borrower's agreement to repurchase the security at an agreed price a short time later.

185. *See First Cross-Border Intraday Repo on Broadridge's DLT Platform*, BROADRIDGE, https://perma.cc/8D4P-AP6Q (last visited July 16, 2023) (discussing Broadridge's leadership in bringing the benefits of distributed ledger technologies ("DLT") to the global repo market, "capturing $1 trillion dollars in monthly volume"); *see also Broadridge's DLT Repo Platform Transacts $1 Trillion a Month. Just Getting Started*, LEDGER INSIGHTS (Feb. 1, 2023), https://perma.cc/2KJ9-RWFZ.

186. *See* Broadridge Fin. Serv., Inc., *UBS Executes First Cross-Border Intraday Repo Trade on Broadridge Distributed Ledger Repo Platform*, CISION PR NEWSWIRE (Apr. 3, 2023, 7:30 PM), https://perma.cc/AU7U-FVCL.

and worked with prominent participants such as JP Morgan and Deutsche Bank Securities to transact in tokenized deposits and government bonds on Polygon, a public blockchain network.[187] The project employed digital identity solutions and adapted logic from existing DeFi protocols to support its implementation.[188]

The Depository Trust & Clearing Corporation ("DTCC") also stands as a prime example of the acceptance of DeFi in mainstream finance. As the world's largest depository, the DTCC processes over $2.3 quadrillion in total value of securities annually.[189] It has rigorously tested blockchain-based security settlement with stable value tokens and smart contract encumbrance mechanisms deployed in DeFi, plus designed governance models aligned with DLT platforms.[190] The DTCC concluded that these technologies have the potential to generate enormous savings—potentially billions annually—for the traditional finance industry.[191]

The benefits of DeFi technologies, as summarized in Figure 7,[192] and as observed by Broadridge, Project Guardian, and the DTCC, are multifaceted. These advantages span across operational facets, from atomic or instantaneous settlement and reduced settlement costs to seamless collaboration across multiple services.[193] DeFi can reduce overheads associated with transfers and post-transaction reconciliation.[194]

---

187. *See Project Guardian*, MONETARY AUTHORITY OF SINGAPORE, https://perma.cc/VMB3-WHL8 (last visited Aug. 2, 2023) [hereinafter *Project Guardian Description*].

188. DBS Bank, JP Morgan, and SBI Digital Asset Holdings conducted foreign exchanges and government bond transactions against liquidity pools consisting of tokenized Singapore Government Securities Bonds, Japanese Government Bonds, Japanese Yen (JPY), and Singapore Dollar (SGD). OLIVER WYMAN FORUM, ET. AL., *Institutional DeFi: The Next Generation of Finance*, https://perma.cc/SH23-MA69 (last visited Aug. 2, 2023) [hereinafter *Institutional DeFi Whitepaper*].

189. *See* DEP. TRUST & CLEARING CORP., *2021 Progress: DTCC Annual Report*, at 4 (2021), https://perma.cc/72FF-R9H5.

190. *See* DEP. TRUST & CLEARING CORP., *Digital Dollar Project and DTCC: Security Settlement Pilot: Exploring Post-Trade Security Settlement with a U.S. Central Bank Digital Currency* (Nov. 2022), https://perma.cc/PD88-8SK7 [hereinafter *Digital Dollar Project Whitepaper*]; *see also DTCC and Accenture Unveil Governance Operating Model to Manage Risks and Promote Safety Across Distributed Ledger Technology Landscape*, DEP. TRUST & CLEARING CORP. (Sept. 4, 2019), https://perma.cc/Y2L9-AEPG.

191. *See Digital Dollar Project Whitepaper*, *supra* note 190, at 7, 29 (describing how the financial industry could save money through "simplifying trade confirmations, reconciliation, cash management, asset optimization, and other exceptions-based business logic processes").

192. *See infra* Section IV.B, Fig.7.

193. *See Institutional DeFi Whitepaper*, *supra* note 188, at 13, and *Digital Dollar Project Whitepaper*, *supra* note 190, at 9.

194. *See Institutional DeFi Whitepaper, supra* note 188, at 13. Smart contracts can automatically execute transfers and adjustments for post transaction reconciliations, eliminating the need for manual processing and human intervention. As a result, transactions can settle instantaneously versus days for traditional transactions. In addition, transparent ledgers facilitate auditability for reconciliation verification. The immutable

Beyond these operational efficiencies, DeFi can present regulatory advantages, contributing to heightened transparency, improved market efficiency, and bolstered risk management.[195]

Figure 7.[196]
Validated Institutional DeFi Benefits

Atomic settlement	Cheaper settlement	Composability
Interoperability	Reduces middle & back-office overhead	Enables collateral liquidation & new products
Amplifies token & tokenized RWA liquidity	Minimizes communication dependencies	Eliminates counterparty risk

Sources: Project Guardian, DTCC, Broadridge. See article body for citations.

The DeFi ecosystem is home to a wide range of financial experiments, benefiting from an open-source ethos and composable technology stacks. Some of the longest-running experiments have shown sustained resiliency and demonstrate significant value. For example, Uniswap, the largest DEX, has experienced more than $1.6 trillion in transactional volume since inception.[197] The protocols are sustainably profitable as well. For example, lending market leader Aave has earned more than $603 million in protocol fees since inception.[198] These protocols can programmatically lock significant value. Liquid staking service Lido currently has $14.16 billion in TVL.[199] Maker DAO, with a TVL of over $5 billion, has closely maintained the peg of algorithmic stablecoin $DAI since its first launch six years ago.[200] In addition, its ecosystem has seen

---

nature of blockchains can streamline reporting and compliance checks. *See Smart Contract*, *supra* note 162.

195. *See* Carapella et al., *supra* note 168, at 14–16.

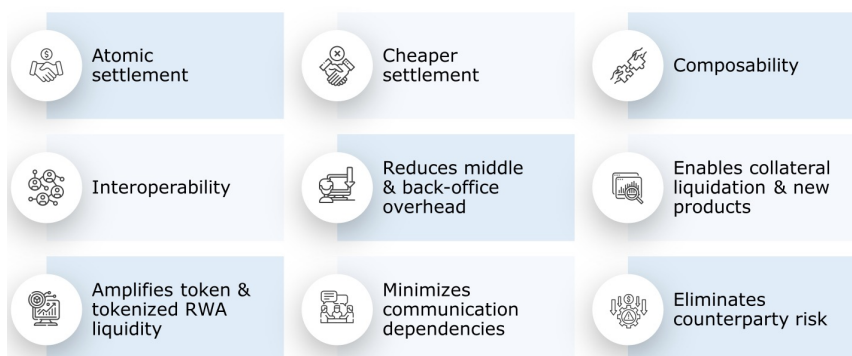196. Figured derived from *Institutional DeFi Whitepaper*, *supra* note 188, at 13, *Digital Dollar Project Whitepaper*, *supra* note 190, at 9, and Carapella et al., *supra* note 168, at 14–16.

197. *See Uniswap*, DEFILLAMA, https://perma.cc/966F-495G (last visited Oct. 23, 2023).

198. *See DeFi Llama*, AAVE, https://perma.cc/W43F-G5E9 (last visited Oct. 23, 2023).

199. *See DeFi Llama*, LIDO, https://perma.cc/EUT3-ZD25 (last visited Oct. 23, 2023).

200. *See $DAI Price*, CRYPTO.COM, https://perma.cc/MDT5-YAV4 (last visited Nov. 20, 2023).

the integration of $DAI into more than 400 applications and services.[201] Even established protocols, however, still experience security issues.[202]

There are many early-stage projects that illustrate the immense potential scope of DeFi services, even those that do not today fall into the debate of regulatory jurisdiction.[203] Centrifuge, for example, is a structured credit protocol that facilitates the financing of real-world assets ("RWA") and tokenizing them as on-chain collateral.[204] Toucan[205] and Thallo[206] are category leaders in carbon credit and offset markets. Nexus Mutual and Etherisc are current category leaders in on-chain event-triggered insurance.[207] VitaDAO facilitates the funding of early stage longevity research in exchange for tokenized IP rights.[208] Ondo Finance offers tokenized investment funds to provide institutional-grade, on-chain investment products and services to DeFi system stakeholders, albeit via a permissioned offering.[209] The potential for DeFi technologies to revolutionize supply chain management is still in its infancy but has attracted significant research.[210]

Despite DeFi's early successes and clear potential, it faced a harsh regulatory environment in the United States, particularly for services that raised potential intermediary registration issues. In contrast, other countries took a more proactive approach to developing adaptive regulatory frameworks potentially raising longer term global

---

201. *See DeFi Llama*, MAKERDAO, https://perma.cc/KYM5-2V8Z (last visited Oct. 23, 2023).

202. *See, e.g.*, Sam Kessler, *As Curve Averts DeFi Death Spiral, Fiasco Exposes Serious Risks*, COINDESK (Aug. 9, 2023, 4:27 PM), https://perma.cc/CJJ8-UXJY. Curve is one of the largest DEX's by TVL. The hack raised questions about Curve's security and even its viability.

203. Polygon Labs maintains a database that lists out multiple use cases for digital assets and DeFi. *See* POLYGON LABS, *The Value Prop*, https://perma.cc/W85B-4CZX (last visited Oct. 23, 2023).

204. *See* CENTRIFUGE, https://perma.cc/26XQ-LZZ7 (last visited Oct. 23, 2023).

205. *See* TOUCAN PROTOCOL, https://perma.cc/9DXN-UWKL (last visited Oct. 23, 2023).

206. *See* THALLO, https://perma.cc/DZG3-V3ND (last visited Oct. 23, 2023).

207. *See* NEXUS MUTUAL, https://nexusmutual.io/ (last visited Oct. 23, 2023) (noted here for DeFi risk insurance); ETHERISC, https://perma.cc/4VZ2-3L3U (last visited Oct. 23, 2023) (noted here for parametric insurance for real-world events (weather, flight delays, etc.) delivered via decentralized oracles).

208. *See* VITADAO, https://perma.cc/JZ8D-LLHP (last visited Oct. 23, 2023).

209. *See* ONDO FINANCE, https://perma.cc/D4SL-TD76 (last visited Oct. 23, 2023).

210. *See* Yutong Bai, et al., *Supply Chain Finance: What are the Challenges in the Adoption of Blockchain Technology?*, 1 J. DIGIT ECON. 153 (2022); Rachel Wolfson, *Supply Chains Reimagined: Enterprise Defi Finances Personal Protective Equipment*, COINTELEGRAPH (May 15, 2021), https://perma.cc/TYT3-LDBG. Despite the transformative potential of DeFi for inventory-based financing, early challenges to exploration include framework identification, cross-chain interoperability, data governance, and operational challenges associated with new business processes and supply chain transformation. *See* Bai et al., *supra* note 210, at 157–61.

competitiveness concerns for the United States.[211] Given the complexity and continual evolution of DeFi, fostering open dialogue and cooperation among DeFi stakeholders, regulators, and policymakers is essential. However, incidents like the Terra Luna collapse, the downfall of FTX, and the deepening mistrust between digital asset participants and regulators have made such collaborative efforts more challenging—even for DeFi, which was not at issue in these events. The prospects for a turnaround, absent legislative intervention, have been diminished by recent controversial enforcement cases and proposed rulemaking. [212]

C. U.S. Regulatory and Legislative Status of DeFi

In 2022, the SEC published a rulemaking release that proposed broadening the statutory definition of "exchange" under the 34 Act to include "Communication Protocol Systems."[213] The proposal drew a large number of comments, with many highlighting concerns over the SEC's broad definition of Communication Protocol Systems, including its potential to include DeFi protocols and developers.[214] Critics also argued that the SEC had failed to adequately assess the broader financial impacts of this proposal on the digital asset ecosystem, invoking possible violations of the Administrative Procedures Act (the "APA").[215]

---

211. *See e.g.*, *supra* Section IV.D.

212. *See supra* Section II.G.

213. *See* ATS Proposal, *supra* note 121, at 15497 ("A 'Communication Protocol System' would include a system that offers protocols and the use of non-firm trading interest to bring together buyers and sellers of securities.").

214. *See Comments on Amendments Regarding the Definition of "Exchange" and Alternative Trading Systems (ATSs) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities,* Release No. 94062, U.S. SEC. & EXCH. COMM'N, https://perma.cc/JP5D-F8XD; Supplemental Information and Reopening of Comment Period for Amendments Regarding the Definition of 'Exchange', Exchange Act Release No. 97309, 88 Fed. Reg. 29448, 29450 (May 5, 2023) (to be codified in 17 C.F.R. pts. 232, 240, 242, and 249), https://perma.cc/P5HU-AZ4R [hereinafter SEC Supplemental Exchange Release 2023]; *see, e.g.,* Letter from Cody Carbone, Vice President-Policy, Chamber of Digital Commerce, to U.S. Sec. & Exch. Comm'n (June 19, 2023), https://perma.cc/G386-LRQQ; Letter from Kristin Smith, Executive Director, Blockchain Ass'n, and Jake Chervinsky, Head of Policy Blockchain Ass'n, to U.S. Sec & Exch. Comm'n (Apr. 18, 2022), https://perma.cc/QT4P-SW3K; Letter from Miller Whitehouse-Levine, Policy Director, DeFi Edu. Fund, to U.S. Sec. & Exch. Comm'n (Apr. 18, 2022), https://perma.cc/Y4H8-YQ2Q; Comment Letter from LeXpunK on ATS Proposal, to U.S. Sec. & Exch. Comm'n (Apr. 18, 2022), https://perma.cc/N2E3-6C2S [hereinafter LeXpunK Comment Letter]; Comment Letter from Coin Center on ATS Proposal, to U.S. Sec. & Exch. Comm'n (Apr. 14, 2022), https://perma.cc/45KH-E2WH; Comment Letter from a16z on ATS Proposal, to U.S. Sec. & Exch. Comm'n (Apr. 18, 2022), https://perma.cc/Z72L-R9Y6.

215. *See, e.g.*, LeXpunK Comment Letter, *supra* note 214 (highlighting the failure of the SEC's economic impact analysis to contemplate cost and ability of digital asset service providers and DeFi protocols to comply with the proposed rules).

A 2023 supplemental proposing release provided more clarity respecting the intended expansion of the definition of "exchange," reinforcing the apprehensions of commentators regarding its applicability to DeFi protocols and developers while acknowledging the challenges to compliance.[216] In the supplemental rule proposal, the SEC appeared to indicate that virtually any party that develops or maintains a protocol or code that facilitates the exchange of digital assets would be required to register with the SEC as an exchange or an alternative trading system,[217] notwithstanding the lack of regulatory clarity with respect to how this would be possible or whether any particular digital asset transaction would be appropriately characterized as a security transaction. The supplemental proposing release garnered considerable substantive feedback.[218]

The SEC's approach to this proposal contrasted sharply with the collaborative industry dialogue that it had engaged in prior to adopting of Reg ATS.[219] Further, the publication of the supplemental proposing release drew dissent from SEC Commissioners Mark Uyeda and Hester Peirce, who highlighted the lack of adequate consideration of "regulatory alternatives that advance the Commission's mission while preserving space for potentially disruptive innovation."[220] Alternatives embodying this sentiment are explored in Section IV.E.

In 2023, two significant bills were proposed in Congress that sought to establish a foundational regulatory framework for digital assets. The first is the revised Responsible Financial Innovation Act ("RFIA"),

---

216. *See* SEC Supplemental Exchange Release 2023, *supra* note 214 at 29450–51, 29455 (stating that "[t]he Commission understands that currently certain trading systems for crypto assets, including so-called 'DeFi' systems, operate like an exchange as defined under federal securities laws" and that exchange registration could be required of persons, including developers, who act with others to establish, maintain, or provide a marketplace). Notably, in 2018, the SEC settled charges with the founder, Zachery Coburn of EtherDelta, a website that provided a front end for a DEX, for operating an unregistered securities exchange. *See generally* Zachery Coburn, *Order Instituting Cease-and-Desist Proceedings*, Exchange Act Release No. 84553 (Nov. 8, 2018), https://perma.cc/WBY8-NE4N [hereinafter EtherDelta Action].

217. *See* SEC Supplemental Exchange Release 2023, *supra* note 214, at 29454.

218. *See Comments on Amendments Regarding the Definition of "Exchange" and Alternative Trading Systems (ATSs) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities*, Release No. 34-94062, File No. S7-02-22, U.S. SEC. & EXCH. COMM'N (2023), https://perma.cc/PVG2-T4SF.

219. *See supra* Section II.C.b.

220. *See* Mark T. Uyeda, Comm'r, U.S. Sec. & Exch. Comm'n, *Statement on Supplemental Information and Reopening of Comment Period for Amendments to Exchange Act Rule 3b-16 regarding the Definition of "Exchange"* (Apr. 14, 2023), https://perma.cc/ZKN9-PBUK; Hester Peirce, Comm'r, U.S. Sec. & Exch. Comm'n, *Rendering Innovation Kaput: Statement on Amending the Definition of Exchange* (Apr. 14, 2023), https://perma.cc/ELN8-ZBGW.

referred to the U.S. Senate Committee on Finance.[221] The second is the Financial Innovation and Technology for the 21st Century Act (the "FIT Act"),[222] introduced in the U.S. House of Representatives.[223] Despite their different approaches, both bills share a focus on key aspects such as the designation of commodities or securities, exchange registration, custodial issues, and transparency.[224] Both bills face opposition to passage, particularly within the Senate Banking Committee, chaired by digital assets critic Senator Sherrod Brown.[225] These bills, however, provide insight into the digital asset policy issues currently under consideration.

The RFIA would allow digital asset companies to decide whether to register their assets as commodities or securities, depending on the conferred rights or powers to the consumers.[226] It includes provisions for the registration of "digital asset exchanges" under the CFTC, establishes rules for custody and segregation requirements, and stipulates bankruptcy treatment of digital assets.[227] The RFIA further mandates a custom disclosure regime, enhanced consumer protections, stringent AML penalties, a market integrity authority for digital asset intermediaries, and designated funding.[228] Moreover, it prescribes risk management standards for FCMs interfacing with DeFi exchanges that includes assessing AML and market integrity monitoring; code transparency, analysis, and

---

221. *See* S.2281, 118th Cong. (2023), https://perma.cc/9FHC-68LN [hereinafter RFIA].

222. *See* Financial Innovation and Technology for the 21st Century Act, U.S. House Committees on Financial Services and Agriculture, 118th Cong. (2022), https://perma.cc/RTT2-GG4S [hereinafter FIT Act].

223. *See* Financial Innovation and Technology for the 21st Century Act, H.R. Res. 4763, 118th Cong. (2023), https://perma.cc/T7MH-7JTQ.

224. *See id.* at §§ 303, 404 (addressing revisions to the Customer Protection Rule (17 C.F.R. § 166), permitting brokers to custody digital assets with banks and permitting FCM's to place customers' digital assets with qualified digital commodity custodians).

225. *See* Cailin Reilly, *House GOP Tries Panel Collaboration on Crypto; Democrats Leery*, ROLL CALL (May 2, 2023), https://perma.cc/ZY5W-SNN2 ("[A] partisan divide may be the next hurdle that legislation addressing the [digital assets] sector needs to clear."); Michelle Price, *Analysis: U.S. Crypto Lobbyists Court Democrats in Fresh Legislative Push*, REUTERS (July 10, 2023), https://perma.cc/9CJN-SKHW ("[T]he top Democrats on the Financial Services and Agriculture committees . . . have raised concerns [the FIT Act] would weaken the SEC's powers."); Hannah Lang, *Crypto Bill Passes Congressional Committee in Victory for Industry*, REUTERS (July 26, 2023, 8:50 PM), https://perma.cc/C9F8-4G9T; Casey Wagner, *Lummis, Gillibrand Bring New Bill to the Table Hoping for a Different Outcome*, BLOCKWORKS (July 12, 2023), https://perma.cc/Z8QX-5NED (explaining that Lummis and Gillibrand will need their bill to pass markup in Committee, but Senate Banking Committee Chair Sherrod Brown is a vocal critic of the crypto industry).

226. RFIA, *supra* note 221, §§ 403, 501.

227. *See id.* §§ 203, 205, 403(b), 404, 408, 705.

228. *See id.* §§ 201–208, 302, 501(b), 601, 1001–1006.

auditing; governance; settlement; operational and cybersecurity risks; and risk disclosures.[229]

The FIT Act proposes that most digital assets would be recognized as embodying an underlying investment contract and should be classified as securities with registration exemptions.[230] Decentralized protocol tokens would be treated as commodities under the CFTC and traded on new "digital commodity exchanges."[231] The draft bill addresses the supervision of qualified custodians and regulation of digital asset custody.[232] The bill also calls for the codification of the SEC's Strategic Hub for Innovation and Financial Technology ("Finhub") and the CFTC's LabCFTC offices and accountability to Congress to ensure that they are respectively fulfilling their missions of promoting responsible financial technology innovation, and, among other things, the establishment of a joint CFTC-SEC advisory committee to ensure regulatory harmonization regarding digital assets.[233] The FIT Act would require the SEC and CFTC to deliver a comprehensive report to Congress addressing DeFi, examining benefits such as operational resilience and interoperability, market competition and innovation, transaction efficiency, and traceability and transparency.[234] The report would also cover risks relating to pseudonymity, lack of intermediaries, cybersecurity vulnerabilities, financial market stability, illicit activity, and inherent system risks.[235]

Bipartisan legislative efforts in the Senate have sought to apply various AML and sanctions list compliance obligations to certain DeFi stakeholders,[236] even implicating Bank Secrecy Act ("BSA") obligations imposed on financial institutions.[237] Given these developments and the recurrence of concerns regarding the potential role of DeFi in facilitating illicit finance,[238] no comprehensive digital assets legislation is likely to

---

229. *See id.* § 403(j)(1–2).

230. *See* FIT Act, *supra* note 222, § 201.

231. *Id*. §§ 202-204, 404.

232. *See id.* 178, § 405.

233. *See id.* §§ 501-3.

234. *See id*. § 506.

235. *See* RFIA, *supra* note 221, § 505.

236. *See* Cansee Act*, supra* note 7; Digital Asset Anti-Money Laundering Act, *supra* note 7; *see also* Jack Reed, *Bipartisan U.S. Senators Unveil Crypto Anti-Money Laundering Bill to Stop Illicit Transfers: Reed-Rounds-Warner-Romney Introduce The Crypto-Asset National Security Enhancement and Enforcement (Cansee) Act* (July 19, 2023), https://perma.cc/FUB8-VFFZ (explaining the intricacies of extending Bank Secrecy Act and sanctions compliance to DeFi exchange services, potentially making U.S. backers and facilitators of DeFi services liable).

237. *See* Pub. L. 91-508, 84 Stat. 1114, https://perma.cc/X3XP-UGG5 (codified at 12 U.S.C. §§ 1724, 1813 and 15 U.S.C. § 78a) [hereinafter BSA].

238. *See* U.S. DEP'T OF THE TREAS., ILLICIT FINANCE RISK ASSESSMENT OF DECENTRALIZED FINANCE, at 26 (2023), https://perma.cc/T8HD-WGE7 [hereinafter, the DoT 2023 REPORT].

pass Congress without addressing AML controls, potentially including user verification. In addition, the DoT has proposed rulemaking that, if adopted, could have even broader implications for many DeFi projects due to mandates requiring the reporting of the personal financial information of certain users to the Internal Revenue Service.[239]

This focus is directly relevant to the collaborative efforts envisioned here, as any hybrid finance stakeholder collaboration, particularly those engaging regulators, will need to contemplate technical solutions addressing AML concerns and educational efforts relating to other actions impacting digital assets undertaken by the DoT.

D. Foreign Regulatory Frameworks for DeFi

Many other countries seeking to establish a regulatory framework for digital assets have taken a more measured approach while prioritizing concerns such as asset categorization, token issuance, and authorized service providers.[240] Two notable examples are the EU and United Arab Emirates' regulatory approaches. The EU's Markets in Crypto Asset Regulation ("MICA") requires further examination of the necessity and feasibility of regulating DeFi, among other aspects of crypto asset regulation.[241] Currently, services provided in a fully decentralized manner without an intermediary fall outside the scope of MICA,[242] but intermediaries using DeFi services would likely require licensing under MICA.[243] The United Arab Emirates, on the other hand, has been particularly progressive, having already established a licensing regime for decentralized exchange and staking activities.[244]

---

239. *See* Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions, RIN 1545-BP71, 88 Fed. Reg. 73300 (Oct. 25, 2023) (to be codified at 26 C.F.R. Pts. 1, 31, and 301), https://perma.cc/E787-AEHU (expanding the obligation of furnishing payee statements and filing informational returns with the IRS for certain digital asset dispositions to digital asset trading platforms (defined to include websites), digital asset payment processors, and certain digital asset hosted wallets).

240. *See, e.g.*, European Parliament, *Legislative resolution of 20 April 2023 on the Proposal for a Regulation of The European Parliament and of The Council on Markets in Crypto-Assets and Amending Directive (EU) 2019/1937* (2020), https://perma.cc/2FNQ-76VJ [hereinafter MICA].

241. *See MICA, supra* note 240; *see also* Encrypted Economy Podcast, *MiCA Series: The EU and MiCA's Crypto Asset Framework* (Panel Series Pt. I) (2023), https://perma.cc/4N2T-F9VF.

242. *See* MICA, *supra* note 240, at Recital 12a.

243. *See* Jonathan Galea, *Is DeFi Really Excluded from MiCA's Scope?*, BCAS (Mar. 28, 2023), https://perma.cc/P3UH-7E4A.

244. *See* DUBAI FIN. SERVS. AUTH., *Feedback Statement on CP143 Regulation of Crypto Tokens* (Oct. 17, 2022), https://perma.cc/6Z3H-CUQC (noting that the Dubai Financial Services Authority ("DFSA") is the licensing authority for DEX's established in the Dubai International Financial Centre (DIFC) and explaining that taking for non-retail clients is a licensed activity).

As in the United States, foreign policymakers and regulatory authorities are grappling with how to address AML/CFT concerns for permissionless DeFi services, particularly regarding its use by regulated intermediaries and service providers.[245] In addition, the Financial Action Task Force ("FATF") has pressed its member organizations to enhance their AML/CFT controls with regards to digital assets.[246]

Technological innovation has emerged as a significant factor influencing financial regulation across the globe. The inability to dynamically adapt amidst accelerating innovation will force more significant legislative interventions in the future, but those interventions may take so long to develop and implement that they will also fall behind ongoing innovation.[247] A more dynamic approach is necessary, and DeFi, as a disruptive, democratizing technology, requires such an approach.

E.   The Top-Down "Same Risks, Same Rules" Approach

The "same activities, same risk, same rules" principle is often invoked in financial regulation to argue that identical regulations should govern analogous financial activities to ensure fairness and maintain a level playing field.[248] A more thoughtful variation of this theme is "same activities, same risks, same regulatory outcome." However, as generally invoked with regards to DeFi, both principles typically overlook fundamental differences inherent in the activities and are biased towards the application of existing regulation.[249] Traditional financial regulations

---

245. *See* FIN. SERV'S REG. AUTH. OF ABU DHABI GLOBAL MARKET, POLICY CONSIDERATIONS FOR DECENTRALIZED FIN., at 9, (2022), https://perma.cc/SV52-FJSH; European Parliament, *Press Release: New EU Measures Against Money Laundering and Terrorist Financing* (Mar. 28, 2023), https://perma.cc/V8SS-8WQZ (current drafts contemplate the application of the EU's new AML rules to decentralized finance when the DeFi platform is controlled by identifiable natural and legal persons).

246. *See, e.g.*, FIN. ACTION TASK FORCE, VIRTUAL ASSETS: TARGETED UPDATE ON IMPLEMENTATION OF THE FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS (2023), https://perma.cc/A9A2-SP7J.

247. *See* Brummer, *supra* note 3, at 1035–39.

248. *See, e.g.*, *International Banking and Financial Market Developments*, BIS QUART. REV 1–105 (Dec. 2021), https://perma.cc/Q4DN-5L94; *Transcript of Remarks by Michael S. Barr: Making the Financial System Safer and Fairer*, THE BROOKINGS INST. (Sept. 7, 2022), https://perma.cc/R24P-4D79; COMMODITY FUTURES TRADING COMM'N, *Transcript of Remarks from Commissioner Christy Goldsmith Romero Before the International Swaps and Derivatives Association's Crypto Forum* (Oct. 26, 2022), https://perma.cc/36MT-ALG5; Johnson Statement, *supra* note 142, at n.116.

249. *See, e.g.* OICV-IOSCO, POLICY RECOMMENDATIONS FOR DEFI CONSULTATION REP. 1–128 (2023), https://perma.cc/6WMD-FD7D (advocating for both "same risks, same rules" and "same risks, same regulatory outcome" principles (referred to collectively herein as the "same risks, same rules" approach), but recommending that global regulators broadly identify all possible responsible parties for DeFi services (Recommendation 2) and providing a detailed roadmap for applying existing regulatory frameworks to DeFi services

apply to centralized, intermediated systems, but DeFi is predicated on decentralized, disintermediated systems, which also minimizes risks inherent in the former such as conflicts of interest. Assuming away critical differences in activities leads to suboptimal regulatory outcomes.

The "same risk, sale rules" approach, as invoked, generally misses a crucial step that no seasoned risk management professional would make: it does not contemplate risk weighting. Risk weighting is influenced by the likelihood of a risk occurring and the potential consequences of the occurrence of that risk. This type of analysis is crucial to determining the extent of the preventative and detective risk mitigation measures that are recommended in response.

Risk weightings are influenced by a myriad of factors, but, for simplicity, consider the distinctions between actual, contingent, and hypothetical risks. For illustrative purposes, building a house in a community that is a known floodplain—let's call it Riverbottom—is an actual risk for which mitigation strategies might be more resource-intensive than for contingent or hypothetical risks, such as building on stilts or pilings, incorporating retaining walls, or constructing on higher elevations. Building a house near a riverbank that has experienced flooding in especially rainy years is a contingent risk to which similar mitigations are not warranted and might include basement sump pumps, stocking sandbags, and landscaping to divert water away from the foundation. Building a house on an elevation in an area away from floodplains and rivers—let's call it Riverview—when climate change models predict increased rainfall and potential flooding in decades is a hypothetical risk to which appropriate mitigations might focus on long-term planning strategies, such as following developing climate change predictions, budgeting for future water-resistant barriers, and participating in forums contemplating the same. Each of these risks can be broadly labeled as flooding risks, but in each case the likelihood or risk weighting influences the appropriate response. If Riverbottom has a mandate that all new homes must be built on stilts, and Riverview decides to copy this mandate in response to its hypothetical flooding risks, such an approach would create an unnecessary financial burden on builders, cause underlying infrastructure challenges, and discourage residents and businesses in Riverview. Moreover, this requirement might exacerbate and draw resources away from other risks, such as strong winds. Most likely, builders, residents, and businesses in Riverview will seek out other communities with policies that are more finely tuned to the differences between these risks. Similarly, regulation and policymaking (or lack

---

associated with such identified responsible parties (Recommendation 3)) [hereinafter 2023 IOSCO DeFi Policy Report].

thereof) based on a broad definition of "same risk, same rules" runs the risk of ineffective and even detrimental regulatory outcomes.

Criticisms of the "same risk, same rules" approach to DeFi also highlight the unsuitability or unenforceability of imposing specific national or regional rules to decentralized, borderless systems.[250] Such efforts may encourage regulatory arbitrage and erode the efficacy of national regulations. Further, traditional laws may not apply to, or be less efficient in application to, deterministic contexts in which "code is law" or to inherently disintermediated, trustless technologies.[251] Another perspective is that, irrespective of the appropriateness of any specific regulatory framework of DeFi, any adopted approach should minimally be informed by a functionalist understanding of the different roles within the DeFi ecosystem.[252]

At the core of the "same risks, same rules" approach, as invoked in the context of regulatory policy, is an argument against any change. However, if such an approach had been applied to equities markets in the 1970s, the NYSE would have maintained monopoly power, because no other market center would have been permissible. In the 1980s, retail investors would not have benefited from automated executions of their orders because the rules permitting such executions introduced novel risks and implicated looser controls. In the 1990s, ATSs would not have been permitted to exist and Reg ATS, which the SEC has proposed to expand to capture DeFi services and service providers, would not have been implemented. In the 2000s, technology providers servicing broker-dealers would have been forced to become regulated themselves, increasing costs and reducing efficiencies for investors. In the 2010s, the derivatives market would have lost global competitiveness as it struggled to implement stringent, duplicative, and overreaching controls across all aspects of its markets. There, the CFTC ultimately adopted a framework that achieved the "same regulatory outcome," without the detrimental inefficiencies to the futures industry.[253] In each of these cases, if a regulatory principle grounded in a refusal to adapt had been applied, none of the associated benefits to market efficiency, capital formation, or investor protection would have been realized.

---

250. *See, e.g.*, World Economic Forum, *Pathways to the Regulation of Crypto Assets: A Global Approach*, 6–8 (May 2023), https://perma.cc/YUN4-HFUS.

251. *Id.* at 7; *see Why Decentralised Finance (DeFi) Matters and the Policy Implications*, ORG. FOR ECON. COOPERATION AND DEVELOPMENT (OECD) 1–70 (2022), https://perma.cc/EM4P-39RS; *see also* Kristin N. Johnson, *Decentralized Finance: Regulating Cryptocurrency Exchanges*, 62 WM. & MARY L. REV. 1911, 1984 (2021).

252. *See* Gabriel Shapiro, *A Functionalist Framework for Defi Regulation*, LEXNODE.SUBSTACK.COM (July 27, 2022), https://perma.cc/QA4F-7XV3.

253. *See infra* Section III.D.

These points are not merely theoretical; legislative and regulatory frameworks respecting DeFi will achieve suboptimal outcomes in the absence of informed, experiential feedback. Neither the extremes of denying the paradigm shift created by DeFi nor pretending as if DeFi transcends national regulation will provide a sustainable framework for achieving its promise. Pragmatic collaboration between DeFi's stakeholders, including regulators, will help inform the understanding of regulators and policy makers of the unique complexities of DeFi, together with the potential policy ramifications of proposed changes to applicable law and norms.

F.   The Case for Bottom-Up Collaboration

In light of the political climate surrounding digital assets and the emergent nature of DeFi, U.S. financial regulators such as the SEC and CFTC appear less inclined to pursue collaboration with other DeFi stakeholders.[254] The SEC has been openly resistant to comprehensive legislative initiatives relating broadly to digital assets,[255] and both agencies seem more focused on enforcement actions against DeFi than on cooperative solutions. This adversarial approach not only creates formidable barriers to entry in the U.S. market but is a risky negative-sum gamble, hinging on the assumption that the global financial economy will fail to adopt decentralized financial technologies. The U.S. government, a historical leader in the development and nurturing of new technologies, risks relinquishing its leadership role in shaping emerging technologies such as DeFi and becoming a force resistant to global technological progress.

Collaboration offers an alternative path to a reliance on enforcement or eventual comprehensive regulation and builds upon the CFTC's efforts to engage in constructive dialogue and proactively shape the digital assets landscape. However, to be successful, this effort would also need to extend to DeFi and be pursued by the SEC. Importantly, collaboration does not require a wholesale endorsement of DeFi or a shift in either agency's policy stance, nor does it necessitate a complete overhaul of the current enforcement strategy. It is a supplement. Weighing the resources spent combating digital assets and DeFi, a constructive consensus approach is a more efficient use of public resources compared to resource-heavy and risk-laden litigation. Ex post enforcement does not protect investors ex ante. A collaborative approach seeks to maximize innovation and

---

254. *See infra* Section IV.C.

255. *See* Sarah Wynn, *SEC Chair Gensler: Existing Rules Regulate Crypto, Legislation Unnecessary*, THE BLOCK (Mar. 29, 2023), https://perma.cc/KG6B-ETH8; *see also* Jesse Hamilton*, Gensler Says SEC is Fine Going After Crypto with its Current Authority*, COINDESK (Dec. 7, 2022), https://perma.cc/GD7A-9VLA.

regulatory outcomes by emphasizing consensus rather than focusing on differences. In this model, regulators take on the vital role of creating a framework that promotes risk mitigation, aligning with their core mission without the burden of directly pushing DeFi maturation. By fostering these incentives and integrating themselves as hybrid finance stakeholders, regulators can mitigate the hypothetical risk of costly, reactive interventions in the later stages of DeFi's evolution.

Public-private collaborations can be pursued expeditiously, without waiting for digital assets legislation to be enacted. This approach gains early and meaningful insights that can help refine untested laws and improve their implementation. Acknowledging the need for regulatory clarity among DeFi stakeholders and for regulators to understand DeFi, a cooperative approach could create tools for both permissioned and permissionless hybrid finance models, spurring diverse use cases vital to their success.

The initial phase of such collaborations would require the engagement of hybrid finance stakeholders that can productively contribute to viable regulatory outcomes. Hybrid finance stakeholders would establish objectives, governance structure, responsibilities, and criteria for collaboration, and they would assess the necessity of and conditions for exemptive relief or interpretive guidance. Assuming that there is consensus on the foregoing, identification of the appropriate projects and the logistics of managing progress should be contemplated.

Various mechanisms, both formal and informal, exist to ensure stakeholder and investor representation before the SEC and CFTC. [256] These include formal rulemaking, exemptive relief, concept releases, interpretive guidance, and no-action letter relief. The SEC's Regulation ATS and the CFTC's Regulation AT are examples of collaborations that were ultimately successful.[257]

Exemptive relief could be granted by the SEC and CFTC to hybrid finance participants in a public-private strategic collaboration.[258] This

---

256. Informal mechanisms include interpretations offered through published interpretations, guidance, bulletins, and no-action letters. No-action relief is generally a time-consuming process and has been very limited in its application to digital assets to date. *See, e.g.*, U.S. SEC. & EXCH. COMM'N, DIV. OF CORP. FIN., *No-Action Letter on TurnKey Jet, Inc.* (Apr. 3, 2019), https://perma.cc/L2KW-4WUU; U.S. SEC. & EXCH. COMM'N, DIV. OF CORP. FIN., *No-Action Letter on Pocketful of Quarters, Inc.* (July 25, 2019), https://perma.cc/U8UU-JLYD.

257. *See supra* Sections II.C and III.D.

258. *See* The 33 Act, *supra* note 14, at 15 U.S.C. § 77z-3 (authorizing the SEC to "exempt any person, security, or transaction, or any class or classes of persons, securities, or transactions, from any provision" of the Securities Act). The Securities Exchange Act of 1934 authorizes the Commission:

> by rule, regulation, or order, to exempt, either conditionally or
> unconditionally, any person, security, or transaction, or any class or classes

collaboration could provide for the requisite relief to permit participation without unnecessary regulatory uncertainty.[259] In this regard, the exemption should define the criteria for "qualified purchasers" within its scope or otherwise ensure that the relief is functional.[260]

Contemplating such exemptive relief is fruitless if there is not a cooperative and constructive dialogue that precedes it. Building such a productive collaborative relationship requires trust, open communication, and engagement from hybrid finance stakeholders. This dialogue could be coordinated through the CFTC's Office of Technology Innovation ("OTI", formerly LabCFTC)[261] and the SEC's FinHub[262] with a representative working group (which would also achieve some of the objectives of the proposed FIT Act).[263] However, enforcement staff's visibility into FinHub's engagement with participants and the risk of enforcement targeting represents a significant concern.[264] Any collaborative effort should seek to address these concerns. In addition, various hybrid finance stakeholders may opt to participate through representative groups to limit such risks.[265]

---

of persons, securities, or transactions, from any provision or provisions of the Exchange Act or any rule or regulation thereunder, to the extent that such exemption is necessary or appropriate in the public interest, and is consistent with the protection of investors.

The 34 Act, *supra* note 15, at 15 U.S.C. § 78mm; 7 U.S.C. §6c(1) (authorizing the CFTC to exempt transactions (or class thereof) restrictions on futures trading if the transactions are to "promote responsible economic or financial innovation and fair competition").

259. *See* discussion *supra* notes 230–34.

260. DeFi transactions deemed to be securities transactions might trigger blue sky state securities registration laws for the issuer or seller absent an exemption. Sales to "qualified purchasers," and other defined categories, are exempt from such requirements. 15 U.S.C. § 77r(b)(3).

261. *See* Sharon Y. Bowen, Comm'r, Commodities Future Trading Comm'n, *Statement on the Launch of LabCFTC* (May 17, 2017), https://perma.cc/PJ5T-X8BG.

262. *See* FINHUB, *Strategic Hub for Innovation and Financial Technology*, https://perma.cc/595Q-MEDE (last visited Nov. 21, 2023).

263. *See supra* note 245 and accompanying text.

264. *See id.*; *see also* Caroline A. Crenshaw, Comm'r, U.S. Sec. & Exch. Comm'n, *Statement on DeFi Risks, Regulations, and Opportunities* (Nov. 9, 2021), https://perma.cc/FE3Y-ATAZ (noting "FinHub comprises representatives *across the SEC's Divisions*" thus including the Division of Enforcement) (emphasis added).

265. Examples include the Blockchain Association, DeFi Education Fund, Digital Chamber of Commerce, and LeXpunK Army. BLOCKCHAIN ASS'N, *Blockchain Association is the Collective Voice of the Crypto Industry*, https://perma.cc/9KAG-6R72 (last visited Nov. 21, 2023); DEFI EDUCATION FUND, *Policy Education and Advocacy to Help DeFi Flourish*, https://perma.cc/A7NY-9BDA (last visited Nov. 21, 2023); DIGITAL CHAMBER OF COMM., *The World's Leading Blockchain & Digital Asset Trade Association*, https://perma.cc/ED3V-43G4 (last visited Nov. 21, 2023); LEXPUNK ARMY, *LeXpunK*, https://perma.cc/V8HM-8TSP (last visited Dec. 30, 2023).

In addition to ongoing Technical Advisory Committee discussions among industry members relating to digital assets dating back to 2019,[266] the CFTC has established various stakeholder subcommittee or working groups relating to Virtual Currencies,[267] Distributed Ledger Technology,[268] Digital Asset and Blockchain Technology,[269] and the FIT Act,[270] marking important steps towards a more collaborative relationship between government agencies and digital asset stakeholders. However, no CFTC subcommittee or working group is specifically focused on DeFi, possibly reflective of CFTC's position in actions against DeFi services.[271] The SEC has also failed to create any industry committee or working group with regards to either digital assets or DeFi. However, the creation of such working groups is a critical initial step to building collaborative engagement with other hybrid finance stakeholders. Collaborative efforts can enhance existing frameworks in areas such as counterparty AML, risk management, and pre-transaction risk controls, paving the way for responsible innovation.[272]

Strategically focusing on these areas sidesteps more intricate and potentially divisive subjects such as registration requirements for

---

266. *See* Tech. Advisory Comm., *Notes,* COMMODITY FUTURES TRADING COMM'N (Mar. 27, 2019), https://perma.cc/AZQ4-43QQ.

267. *See* Tech. Advisory Comm., *Transcript*, COMMODITY FUTURES TRADING COMM'N (Feb. 14, 2018), https://perma.cc/45AM-VPKP.

268. *See* Tech. Advisory Comm., *Transcript*, COMMODITY FUTURES TRADING COMM'N (Dec. 14, 2020), https://perma.cc/ZW2X-4AW2.

269. *See Commissioner Goldsmith Romero Announces July 18 Technology Advisory Committee Meeting*, COMMODITY FUTURES TRADING COMM'N (July 18, 2023), https://perma.cc/Q8QC-CRP6.

270. *See Commissioner Goldsmith Romero Announces Technology Advisory Committee (TAC) Subcommittee Co-Chairs and* Members, Release No. 8752-23, COMMODITY FUTURES TRADING COMM'N (July 14, 2023), https://perma.cc/GJB9-32V4; *Commissioner Pham Announces New Members and Leadership of the CFTC's Global Markets Advisory Committee and Subcommittees*, Release No. 8740-23, COMMODITY FUTURES TRADING COMM'N (June 30, 2023), https://perma.cc/5V5P-9WU2.

271. *See supra* Section I.F.

272. *See infra* Parts V–VI.

exchanges,[273] broker-dealers,[274] clearing agencies,[275] SEFs,[276] FCMs,[277] or asset categorization. To circumvent these issues, initial endeavors could focus on areas like the foreign exchange ("Forex")[278] or bilateral short term collateralized lending ("repos").[279] However, the risk of narrowing the scope in this manner is that it may reduce the initiative's relevance to the wider hybrid finance services ecosystem, limit stakeholder engagement, and potentially decrease the value these controls bring to both the hybrid finance community and regulatory or legislative pursuits. Hence, striking the right balance is essential.

Inclusive collaboration among stakeholders, including small and mid-sized organizations, can provide clarity, common standards, and a viable DeFi ecosystem structure. This broad representation is important because the collaboration will fail its critical purpose if it inadvertently forces consolidation into the best-resourced participants.[280] In this regard, the representation of the interests of DeFi protocols of all sizes should also be strongly encouraged.

---

273. The registration requirement for exchanges is set forth in section 5 of the 34 Act. Section 3(a)(1) and 34 Act Rule 3b-16(a) broadly defines "exchange" as any entity that brings together securities orders and uses non-discretionary methods for these orders to interact. The CFTC also mandates registration and reporting for exchanges in commodities markets known as designated contract markets (DCMs). *See* 15 U.S.C. § 78e; 15 U.S.C. § 78c(a)(1); 17 C.F.R. § 240.3b-16(a); 7 U.S.C. §§ 1-26; 17 C.F.R. pts. 1-190 (2021).

274. The registration requirement for broker-dealers is set forth in Section 15(a) of the 34 Act. A "broker" is broadly defined as a person involved in transacting securities for others. *See* 15 U.S.C. § 78o(a); 15 U.S.C. § 78c(a)(4).

275. The registration requirement for clearing agencies is set forth in section 17A(b) of the 34 Act. A "clearing agency" is defined to include intermediaries involved in making payments or deliveries for securities transactions, reducing the number of securities settlements, allocating settlement responsibilities, or providing facilities for data comparison. The definition also includes custodians in a system that treats all securities of a particular class or series as fungible, permitting or facilitating the settlement of securities transactions, or the hypothecation or lending of securities without physical delivery. *See* 15 U.S.C. § 78q-1(b); 15 U.S.C. § 78c(a)(23)(A).

276. The registration requirement for SEFs is set forth in section 5h(a)(1) of the CEA. Section 1a(50) of the CEA broadly defines a "swap execution facility" as a trading system or platform in which multiple participants have the ability to execute or trade swaps by accepting bids and offers made by multiple participants in the facility or system. *See* 7 U.S.C. § 1a(50); 7 U.S.C. § 7b-3(a)(1)..

277. The registration requirement for FCMs is set forth in section 4d(a)(1) of the CEA. A "futures commission merchant" is broadly defined as a person who engages in soliciting or in accepting orders for or acts as a counterparty in a swap transaction to margin trades or contracts. *See* 7 U.S.C. § la(28)(A); 7 U.S.C. § 6d(a)(1).

278. *See* BANK FOR INT'L PAYMENTS, PROJECT MARIANNA: CROSS-BORDER EXCHANGE OF WHOLESALE CBDCS USING AUTOMATED MARKET-MAKERS (2023) (exploring use of CBDCs for cross-border foreign exchange trading and settlement).

279. *See supra* Section IV.B.

280. *See generally* Dan Awrey & Joshua C. Macey, *Open Access, Interoperability, and the DTCC's Unexpected Path to Monopoly*, Uni. of Chicago Coase-Sandor Inst. for Law & Econ. Research Paper No. 934, Cornell Legal Studies Rsch. Paper No. 21–20, (July 12, 2021), https://perma.cc/X9M7-JB6J.

Once a hybrid finance service achieves a significant volume of transactions, it could prioritize risk-based objectives like anomalous pattern detection, preventing manipulative trading behaviors, and even embedded supervision.[281] Collaborations among hybrid finance stakeholders could improve surveillance models and blacklisting capabilities for transactions and offer guidance on various DeFi protocols. Developing smart contracts that facilitate regulatory outcomes through public-private collaborations could catalyze the adoption of enhanced standards benefiting the broader financial system. This could encourage the maturation of critical infrastructure relating to areas like digital identity verification and real time wallet transaction history assessment.

Considering the heightened sensitivity of institutions towards AML issues both domestically and globally it is crucial for the DoT, SEC, and CFTC to cooperate in this area. Solutions to address AML concerns are compelling areas for collaborative hybrid finance stakeholder efforts due to the unity of interests.[282]

V. PERMISSIONED TRANSACTIONS: A TOUCHSTONE FOR COLLABORATION

A. Impact of AML Concerns on DeFi

In the United States, one of the principal legislative and regulatory concerns related to the use of DeFi services is AML. Thus, a tailored strategy for permissionless and permissioned interactions with DeFi technologies and protocols that enables regulatory frameworks to coexist with, and even stimulate, innovation should be established.

Prior to contemplating such a strategy, a brief historical overview of U.S. AML regulations is necessary. The BSA[283] generally requires certain regulated financial intermediaries, including broker-dealers, FCMs, and introducing brokers, to establish programs to identify and monitor for suspicious activities indicative of money laundering or other financial crimes and to file reports on such suspicious activities with the DoT's Financial Crimes Enforcement Network bureau ("FinCEN").[284]

The BSA's early focus on recordkeeping to combat tax evasion evolved with the United States's "war on drugs"[285] and new financial

---

281. Embedded supervision would replace intermediary based legal data verification with distributed ledger-based, incentivized consensus. *See e.g.*, BANK FOR INT'L PAYMENTS, EMBEDDED SUPERVISION: HOW TO BUILD REGULATION INTO DECENTRALIZED FINANCE (2022), https://perma.cc/D8S8-S539.

282. *See infra* Section IV.F.

283. *See* BSA, *supra* note 237.

284. *See* 31 C.F.R. §§ 1026.210 and 300–20.

285. *See* Linn White, *The Anti-Money Laundering Complex in the Modern Era*, 133 THE BANKING L. J. 10 at 2 (May 31, 2016).

crimes[286] to incorporate requirements, such as the establishment of AML programs;[287] Customer Identification Programs;[288] Suspicious Activity Reporting ("SAR");[289] and additional Customer Due Diligence (also often referred to as "Know Your Customer" or "KYC") procedures.[290] Additionally, requirements were introduced for identifying and verifying the beneficial owners of legal entity customers.[291]

These AML programs generally involve screening customers against the Specially Designated Nationals and Blocked Persons ("SDN") list.[292] The SDN list is composed of individuals, entities, organizations, and occasionally wallet addresses subject to sanction programs managed by the DoT's Office of Financial Assets Control ("OFAC").[293] Failure to halt transactions with sanctioned individuals can lead to severe penalties, including potential criminal charges.[294]

In 2013, FinCEN issued guidance that entities or individuals subject to BSA compliance requirements for fiat currency transactions would be similarly obligated for convertible virtual currency ("CVC") transactions.[295] In 2019, FinCEN comprehensively updated this guidance, specifically addressing various CVC business models, noting ways in

286. *See* Money Laundering Control Act of 1986, Pub. L. 99-570, 100 Stat. 3207, (codified at 18 U.S.C. §§ 981, 1956-1957, 1961), https://perma.cc/M98A-9FV4; *see also* Jimmy Gurule, *The Money Laundering Control Act of 1986: Creating a New Federal Offense or Merely Affording Federal Prosecutors an Alternative Means of Punishing Specified Unlawful Activity*, 32 AM. CRIM. L. REV. 823, 823-4 (1995) (explaining how the Money Laundering Control Act made the hiding and reinvestment of illegal profit a federal offense).

287. *See* Annunzio-Wylie Anti-Money Laundering Act, Pub. L. 102-550, 106 Stat. 3680 (1992) (requiring compliance procedures and training teams to combat money laundering at financial institutions).

288. *See* 31 C.F.R. 103.121 (implemented in 2003 after the passage of the Patriot Act).

289. *See* Money Laundering Suppression Act of 1994, Pub. L. 103-325, 108 Stat. 2160, https://perma.cc/F6ZF-J3QV.

290. *See id.*

291. *See* Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29397 (July 11, 2016) (codified at 31 C.F.R. pts. 1010, 1020, 1023, 1024, and 1026), https://perma.cc/F48E-V2RY.

292. *See* OFFICE OF FOREIGN ASSETS CONTROL, *Specifically Designated Nationals and Blocked Persons List* (Nov. 7, 2023), https://perma.cc/G2D8-94T6.

293. *See* U.S. DEP'T OF TREAS., Press Release, U*.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash* (Aug. 8, 2022), https://perma.cc/5PQ6-JSPY; *see also* U.S. DEP'T OF TREAS., Press Release, *Treasury Designates Roman Semenov, Co-Founder of Sanctioned Virtual Currency Mixer Tornado Cash* (Aug. 23, 2023), https://perma.cc/5X78-BADM.

294. *See* Economic Sanctions Enforcement Guidelines, Appendix A to 31 C.F.R. 501, https://perma.cc/M774-Q9U6.

295. *See* U.S. DEP'T OF THE TREAS. FIN. CRIMES ENFORCEMENT NETWORK, *Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Mar. 18, 2013), https://perma.cc/LPL2-3NFX.

which the BSA does not apply to noncustodial software.[296] Notwithstanding this, the U.S. Department of Justice's criminal action against Tornado Cash developers in 2023 broadly interpreted the potential applicability of these requirements to decentralized digital asset projects and those associated with it, invoking national security.[297] This action underscores the ongoing prevalence of AML concerns as it relates to such projects generally, including DeFi.

In early 2023, a policy arm of the DoT published a risk assessment of DeFi for illicit finance.[298] The report, which largely reaffirmed the applicability of the 2019 guidance to DeFi services,[299] called for increased supervision and enforcement of AML/CFT compliance.[300] However, the report identified mitigating factors such as the inherent transparency of public blockchains, the intermediary role of centralized Virtual Asset Service Providers in fiat currency access, and emerging industry solutions, suggesting an openness to collaborative approaches.[301] The assessment also proposed potential solutions that would address AML/CFT concerns while prioritizing user privacy.[302] The report concluded with a call for increased collaboration to promote the responsible innovation of mitigation measures.[303] The inclusion of FinCEN would be vital for any collaborative engagements that facilitate and enhance AML/CFT and BSA regulatory objectives and compliance given their role in issuing regulations, data collection and analysis, coordination and support, guidance and outreach, and enforcement related to the same.[304] The report's recommendations are summarized in Figure 8 below.[305]

---

296. *See* FinCEN, *Application of FinCEN's Regulations to Certain Business Model Involving Convertible Virtual Currencies* (May 9, 2019), https://perma.cc/92YC-QLTX.

297. *See generally* United States of America v. Roman Storm et al., 23 Crim. 430 (S.D.N.Y. Aug. 23, 2023) (alleging conspiracies to commit money laundering, violate sanctions, and to operate an unlicensed money transmitting business, and conspiracy to violate the International Emergency Economic Power Act with respect to the transfer, payment, withdrawal, and dealing in blocked property and interests of the Lazarus Group).

298. *See* DoT 2023 REPORT, *supra* note 238. Note that FinCEN and OFAC, the regulatory and enforcement bodies within the DoT, did not co-author the report.

299. *See id.*

300. *See id.* at 2.

301. *See id.* at 31–32.

302. *See id.* at 35.

303. *See id.*

304. *See, e.*g., 31 U.S.C § 310 and Treasury Order 180-01 (July 1, 2014), https://perma.cc/82S4-Q85T; *see also FinCEN's Legal Authorities*, FIN. CRIMES ENF'T NETWORK, https://perma.cc/75B5-6CDY (last visited Nov. 21, 2023).

305. *See infra* Section V.A.

Figure 8.
Select Recommendations from Department of Treasury's DeFi Report

Balancing AML/CFT with user privacy	DeFi services cyber resilience practices	Call to action for collaboration
Zero-knowledge proofs	Real-time analytics & monitoring	Tech sprints
Frequency restrictions for certain transactions	Rigorous code testing	Development & research grants
Threshold limits for certain customers	Threat intelligence & mitigations	Assess changes to regulation or guidance to support
Use of oracles to screen wallet addresses against sanction lists	Audits	

Source: U.S. Dep't of the Treas., Illicit Finance Risk Assessment of Decentralized Finance (2023))

With the DoT signaling possible cooperation and openness to innovation, it is crucial to explore how DoT objectives can shape the architecture of hybrid finance systems. The interplay of permissioned and permissionless systems provides a natural starting point for this analysis.

B. Permissioned and Permissionless Systems

As envisioned, hybrid finance services would integrate DeFi services on public blockchains ("on-chain") with various controls encoded into smart contracts. These controls could be transparently managed by hybrid finance service providers using a framework shaped by open standards, collaborative participation, and potentially, joint ventures. As part of this framework, on-chain smart contracts could verify credentials of hybrid finance counterparts as necessary to comply with a user's AML policy. Transaction-based verification, which would also support hybrid finance, is a permissionless alternative to this process and is addressed later in this section.

Striving for a balance between privacy, regulatory objectives, access, and minimized intermediation, *permissioned* access to hybrid finance services could adopt an initial user verification process that would permit verifiability of KYC processes but pursuant to an interoperable, encoded, and flexible common framework, such as was utilized by Project Guardian, explored below.[306] Such data would be securely stored in fully encrypted databases, with ongoing verification conducted through zero-knowledge proofs or other encrypted, privacy-preserving query responses.

---

306. *See infra* Section V.B., Fig.12.

The advancement of enhanced identity verification solutions could expedite the adoption of hybrid finance services by removing a significant institutional barrier to entry, making it a fitting area for collaboration. Yet, this endeavor is fraught with potential complications, including divergent standards pertaining to BSA compliance, that can lead to liquidity fragmentation. This situation is exemplified by Aave Arc.[307]

In October 2021, Aave, a leading DeFi lending protocol,[308] published a whitepaper introducing Aave Arc.[309] Aave Arc is a permissioned lending pool designed to comply with AML regulations by exclusively catering to institutions that had undergone KYC verification.[310] Aave Arc was developed in response to "enormous" institutional interest, including interest from banks.[311] Figure 9 describes how Aave Arc was structured.[312]

Figure 9.

Case Study: Aave Arc's Permissioning

To access Aave Arc, institutional users had to be **approved through a KYC process** managed by third party "whitelisters."

Whitelisters were qualified if:

| Their KYC processes were subject to **AML regulation** | **OR** | They were approved through **Aave governance** |

Whitelisters determined **standards & procedures** for whitelisting

Whitelister responsibilities:

Conduct KYC checks

Onboard users with disclosures, terms & conditions
Permission users' wallet addresses to borrow, supply, and/or liquidate
Maintain KYC & customer due diligence documentation
Conduct compliance checks as required by jurisdiction

Whitelisters had **"guardian" powers to veto** Aave governance proposals impacting their regulatory & compliance obligations.

Source: An Introduction to Aave Arc, Aave (Oct. 29, 2021)

---

307. *See* Jacquelyn Melinek, *Aave Arc to Provide 30 Financial Institutions Access to Private Pools of DeFi Liquidity*, Blockworks (Jan. 5, 2020), https://perma.cc/2Y65-VTKG. Stani Kulechov, the founder and CEO of Aave Arc, stated, "Aave Arc allows institutions to interact with the Aave Protocol the same way any other user would, but on their own separate and permissioned liquidity pool in which every user has been verified." *Id.*

308. The Aave protocol, a non-custodial digital asset lending platform, is a top DeFi protocol in terms of TVL with over $5 billion currently locked in its smart contracts. As of January 15, 2024, Aave ranks third in total value locked among all DeFi services. Defi Llama, *TVL Rankings*, https://perma.cc/R6X7-BJCM (last visited Jan. 15, 2024).

309. *See* Aave, *An Introduction to Aave Arc* (Oct. 29, 2021), https://perma.cc/SMD8-XRPS [hereinafter *Aave Arc Whitepaper*].

310. *See* Melinek, *supra* note 307.

311. Ian Allison, *Fireblocks 'Whitelists' 30 Trading Firms for Aave's Institutional DeFi Debut*, CoinDesk (Jan. 5, 2022, 9:00 AM), https://perma.cc/4C9F-CG64.

312. *See Aave Arc Whitepaper*, *supra* note 309, at 1–4.

Aave's governance process permitted the approval of 'whitelisters,' who were authorized to conduct and verify KYC for Aave Arc users, even without regulated KYC processes.[313] This was the case with their primary whitelister, Fireblocks.[314] Despite having onboarded 30 institutions to use the service and Aave's significant TVL,[315] Aave Arc was never able to build up any meaningful volume.[316] The worsening financial and regulatory environment that developed in May of 2022 might have played a role in this sluggish performance.[317] Nonetheless, given the pent-up demand that preceded Aave Arc's launch, together with Broadridge's experience with smart contract-based repo lending a few months later,[318] one would have anticipated a more powerful uptake. The lack of widespread acceptance and shared standards in the whitelisting processes,[319] possibly due to AML/CFT concerns, may have also hindered Aave Arc's adoption. This theory aligns with Broadridge's swift success, a regulated intermediary with BSA compliance obligations, compared to Aave Arc's struggles. Aave's experience with the lack of sufficient trusted BSA regulated entities supporting more rigorous KYC credentialing and verification requirements underscores the crucial role of institutional confidence in the permissioning process and credentialing standards, in addition to the ability to adapt to their requirements.

Another variation of permissioning was undertaken as part of the MAS's Project Guardian, a public-private partnership that proactively engages and facilitates the participation of regulated intermediaries in DeFi and digital asset technologies through live pilots, collaborative policy development, and technical standardization.[320] As noted in Figure 10 below, one area of focus is the development of a common trust layer

---

313. *See Aave Arc Whitepaper*, *supra* note 309, at 3 (defining 'whitelisters' as entities that "have permission to whitelist Ethereum wallet addresses for participation in any deployment of Aave Arc Address").

314. Fireblocks, Aave Arc's primary whitelister, is a self-custody technology provider that is not required by regulation or license to comply with BSA AML requirements. *See* Allison, *supra* note 311.

315. *See* Allison, *supra* note 311.. The 30 licensed financial institutions approved by Fireblocks included Anubi Digital, Galaxy Digital, Canvas Digital, CoinShares, GSR, Hidden Road, Ribbit Capital, Covario, and Wintermute.

316. Despite Aave Arc's ability to onboard financial institutions and Aave protocol's size, Aave Arc peaked $42.5mm in TVL in June 2022 and dropped precipitously thereafter. *See* AAVE, *DeFi Llama*, https://perma.cc/SYG8-HLZ3 (last visited Nov. 21, 2023).

317. *See* Robert Stevens, *How Institutional Investors Are Handling the Crypto Crash*, COINDESK (June 8, 2023), https://perma.cc/PA54-3NYH (noting decreased institutional appetite for DeFi due to regulatory concerns and the collapse of Terra).
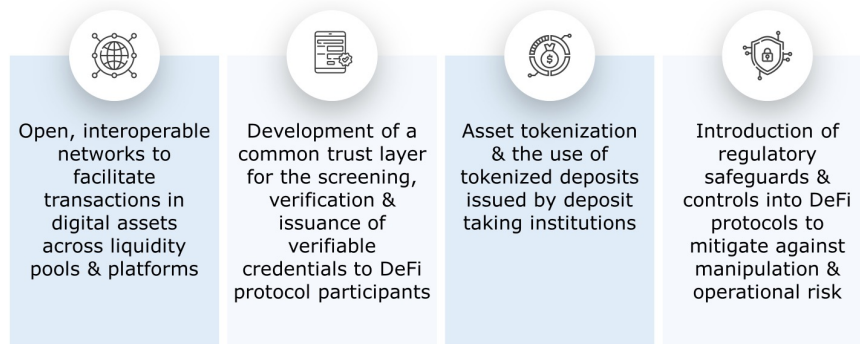
318. *See infra* Section IV.B.

319. *See Aave Arc Whitepaper*, *supra* note 309, at 2–3.

320. *See Project Guardian Description*, *supra* note 187.

for screening, verifying, and issuing verifiable credentials to DeFi protocol participants, thus addressing one of the primary challenges of Aave Arc.[321]

Figure 10.[322]

Project Guardian's Public Private Partnership Focus Areas

Source: Monetary Authority of Singapore website. http://mas.gov.sg/schemes-and-initiatives/project-guardian

A notable Project Guardian pilot program engaged reputable regulated financial intermediaries to transact in tokenized deposits and government bonds on a public blockchain network.[323] This pilot utilized Verifiable Credentials ("VCs"), issued by regulated intermediaries acting as administrators or "trust anchors."[324] As detailed in Figure 11 below, after screening and verifying KYC submissions by liquidity providers ("LPs") or a user's traders, such trust anchors issued credential tokens into the LP or trader's wallet. The permissions and identity of the LP or trader were verified through the VC by a Verifier Smart Contract that accessed the registry. Once completed, digital assets could be withdrawn from the LP or trader's wallet to deploy to a liquidity pool. The credentials featured controls such as revocation, expiry, and trading limits that could be controlled by the participating entities.[325] In this way, participants were able to ensure that their employees' access to a permissionless network was authorized.[326] Such on-chain verification could also condition for liquidity pool participation. Notably, the Aave Arc and Project Guardian

---

321. *See infra* Section V.B, Fig.10.

322. See *Project Guardian Description*, *supra* note 187.

323. *See* MONETARY AUTHORITY OF SINGAPORE, PROJECT GUARD–AN - OPEN AND INTEROPERABLE NETWORKS 25 (June 26, 2023), https://perma.cc/6PEN-F6CE [hereinafter MAS OPEN AND INTEROPERABLE NETWORK PAPER]; *Institutional DeFi Whitepaper*, *supra* note 188, at 27.

324. MAS OPEN AND INTEROPERABLE NETWORK PAPER, *supra* note 323 at 26; *Institutional DeFi Whitepaper*, *supra* note 188, at 26.

325. *See Institutional DeFi Whitepaper*, *supra* note 188, at 26, 32.

326. *See* MAS OPEN AND INTEROPERABLE NETWORK PAPER, *supra* note 323, at 15.

experiences underscore the importance of tailored and highly trusted verification processes.

Figure 11.[327] On-chain Registry for Verified Credentials

Adapted from Monetary Authority of Singapore, "Project Guardian - Open and Interoperable Networks" (June 26, 2023)
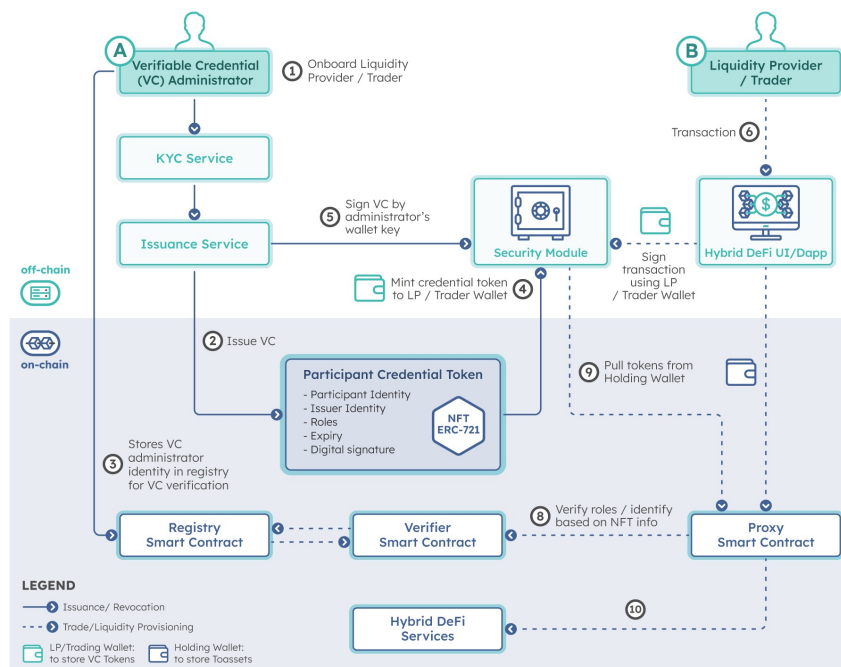
    While employing off-chain permissioning controls for employees to transact with DeFi protocols promotes efficiency, applying on-chain permissioning controls to facilitate compliance with even a subset of users' AML policies would compromise key advantages of DeFi, such as democratized access, composability, interoperability, elimination of intermediaries, and resistance to censorship. Fully permissioned ecosystems that leverage smart contract code and private blockchains as part of their technology stack cease are neither DeFi nor can be considered hybrid finance. Rather, they are simply traditional intermediated financial systems that are not optimized for these key advances.[328] Furthermore, management of access to services on permissionless systems can span a spectrum of control. For example, even whitelisting can be deployed as a permissioning system.

---

327. *See id.* at 27.
328. *See supra* Sections IV.A–B.

Moreover, a permissioning system that requires any storage of personal user data and proofs for permissioning can implicate privacy and security concerns. Issues to consider include data collection protocols, the integration of multiple regulatory risk factors, the complexities of regulatory appeals processes, and the delicate balance between data requirements and privacy and security considerations.[329] Given these concerns, it is critical for regulators to actively support the development of permissionless solutions as well.

Decentralized, permissionless solutions, though still in their infancy, show substantial promise. For instance, the "Know Your Transaction" ("KYT") methodology offers a unique alternative or supplement to conventional KYC procedures, focusing on transaction monitoring and control.[330]

The KYT approach scrutinizes counterparties' wallet and smart contract addresses before executing transactions, examining potential fund flow risks and suspicious activities.[331] Such procedures usually necessitate integration with an AML services provider to provide a transaction's risk ranking. Hybrid finance users can integrate such risk rankings into the application of their internal AML processes to restrict or limit risky transactions.[332] However, the lack of a verified counterparty can present challenges for regulated entities with BSA obligations, especially for larger transactions. As illustrated by the Aave Arc case study,[333] these entities may have additional diligence requirements that need accommodation; a one-size-fits-all approach will not suffice. The solution must be flexible, considering factors like the size and frequency of transactions, different users, and various regulatory regimes.

---

329. *See, e.g.*, Gramm-Leach-Bliley Act, Pub. L. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of the U.S. Code) (repealing the 1933 era Glass-Steagall Act which had imposed regulations separating banking, securities, and insurance businesses); Gramm-Leach-Bliley Act (Privacy of Consumer Financial Information), FDIC CONSUMER COMPLIANCE EXAMINATION MANUAL, at VIII 1.6–1.7 (2021), https://perma.cc/UX9Y-G3RU; Council Regulation (EU) 2016/679, 2016 O.J. (L 119) 1; 17 C.F.R. § 248, Regs. S-P; S.B. 1121, California Consumer Privacy Act of 2018, 2017–2018 Reg. Sess. (Cal. 2018).

330. *See Combating Financial Crime in* Crypto, ELLIPTIC, https://perma.cc/U8NS-FGXK (last visited Aug. 2, 2023); *TRM Transaction Monitoring*, TRM, https://perma.cc/G43C-KWGH (last visited Aug. 2, 2023); *Cryptocurrency Intelligence and Blockchain Analytics*, CIPHERTRACE, https://perma.cc/VC99-Q8K7 (last visited Aug. 2, 2023); *Chainalysis KYT*, CHAINALYSIS, https://perma.cc/D96D-49S5 (last visited Aug. 2, 2023).

331. *See* sources cited, *supra* note 330.

332. *See, e.g.*, Nicole Adarme & Johann Bornman, *Five Things Institutions Need to Participate in DeFi*, METAMASK NEWS (Sept. 1, 2021), https://perma.cc/RT7R-LLEN; *TRM Transaction Monitoring*, *supra* note 330; *Chainalysis KYT*, *supra* note 330.

333. *See supra* notes 319–31.

A diversity of AML and KYC options should be encouraged to maintain wide service accessibility. One method might involve verified participants opting to submit to a level of KYC diligence from a VC administrator that aligns with their counterparty's anticipated AML requirements. In preparing for a transaction with this participant, the counterparty would then verify specific attributes against the registry smart contract (noted in Figure 11) using zero-knowledge proofs ("ZKPs"). This process confirms the existence of the selected verified attributes without disclosing any other personal information.

Alternatively, financial intermediaries, already in possession of customer information, could request their customers' consent to make this data verifiable through ZKP within a VC registry. This registry could incorporate multiple trust anchors, governed through on-chain voting and governance mechanisms.

Users wishing to engage with institutional liquidity through hybrid finance services could link their wallet addresses to KYC proofs, perhaps utilizing a periodically verified credential token. Such real-time verification options, among others, could support multiple standards, and wallets will increasingly permit greater options for integrating such standards. The extent of verification and monitoring could vary depending on existing AML policies and controls (whether BSA-required, regulator-required, or otherwise), the nature of the transaction itself, or other trust assumptions that reduce the risk of an anonymous cyber-attack.

To illustrate, consider a hypothetical AML process for a hybrid finance user. Mature organizations are likely to leverage their existing AML risk processes for digital assets as much as possible, but these processes alone will likely be inadequate. Thus, after applying their existing internal AML risk ratings to a counterparty's wallet or smart contract address, and before sending or confirming transaction instructions for a hybrid finance service, a user could take one of two actions: (1) initiate a verification request against an on-chain registry smart contract or other service that would check for a credential token linked to the wallet; or (2) initiate a KYT process on related addresses. Alongside this, post-transaction monitoring would adjust risk ratings on addresses and smart contracts when necessary and report per any SAR requirements. For businesses with AML processes that need not comply with the BSA, a pre- and post-transaction KYT process might be sufficient to comply with any SAR requirements. A broker-dealer or FCM, alternatively, might require the verified credentials process described in (1) due to its BSA requirements. A bank's AML/CFT obligations might cause it to deploy both KYT and VCs, perhaps even being still more selective with regards to trusted hybrid finance service providers.

Figure 12 below sets forth a workflow example integrating VCs and pre-transaction AML diligence for hybrid finance services users, integrating oracle and internal risk ratings along with suspicious activity alerts.[334] Regulated institutions may employ licensed software or in-house developments for these checks, but on-chain smart contracts solutions should be prioritized as appropriate.

Figure 12. AML Transaction Diligence Controls
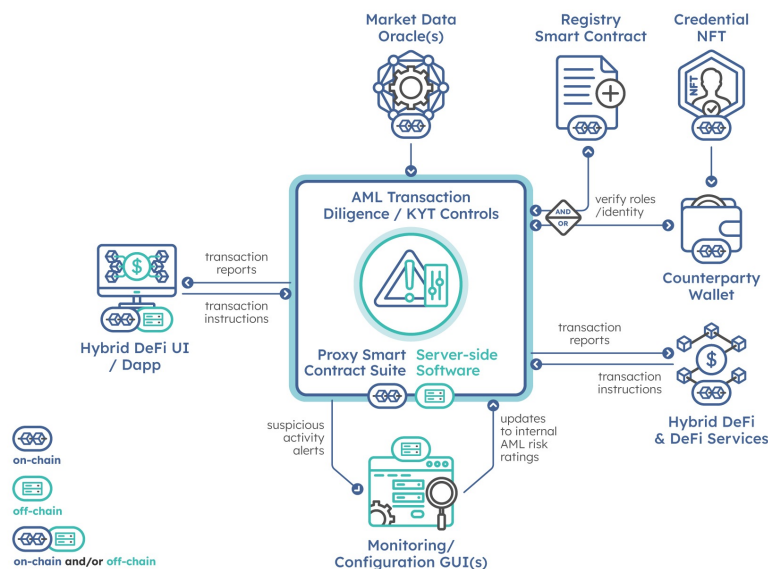
These innovations necessitate establishing trust in a diligence process, which can adhere to either regulatory mandates or common standards. As recognized by MAS, creating this structure is resource intensive and thus, service providers need to be incentivized.[335] As a result, two of MAS's key recommendations were to (1) establish public-private partnerships to create a regulatory framework that fosters sustainable market growth and innovation and (2) create a common framework and approach to minimize friction.[336]

The evolution of AML processes impacting hybrid finance services presents challenges and opportunities. The integration of on-chain verification with existing systems, like the KYT and VC methods, demonstrates the potential for more secure hybrid finance services that can also address a variety of compliance concerns, such as KYC verification, sanctions screening, privacy, and cybersecurity. However, balancing the

---

334. *See infra* Section V.B., Fig.12.
335. *See* MAS OPEN AND INTEROPERABLE NETWORK PAPER, *supra* note 323, at 16.
336. *See id.*

concerns of robust verification and with the inherent permissionless nature of DeFi is crucial. Examples like the Project Guardian pilot program demonstrate how collaborative models can produce innovative solutions within a hybrid finance framework.[337] Broader risk management strategies and pre-transaction risk controls can build on this permissioned and permissionless predicate framework.

VI. BOTTOM-UP RISK MANAGEMENT AND PRE-TRANSACTION RISK CONTROLS

The Digital Assets Executive Order highlighted the important roles of both the FSOC and the FSB in identifying financial stability risks associated with digital assets.[338] The FSOC's Digital Asset 2022 Report detailed financial stability vulnerabilities associated with digital assets,[339] whereas FSB's 2023 report (the "FSB DeFi Report") addressed financial stability risks related to DeFi.[340] However, neither report offers strategies for organization level or micro-level risk mitigation or guidance on risk weighting.

Systemic and other macroprudential risks do not exist in isolation; they embody an accumulation of micro-level risks that exist at the organizational level, such as technical, security, operational, governance, liquidity, and counterparty risks. Examining these risks in isolation relegates the more crucial role of micro-level risk management. This de-prioritization inadvertently *creates* a systemic risk that impedes market efficiency and promotes regulatory arbitrage across jurisdictions.

The process of developing a functional organizational framework for identifying and mitigating risks for a hybrid finance user must consider the organization's risk profile, its risk management maturity, the DeFi service in use, and other relevant activity metrics. As the nature of DeFi systems and related risks can vary, there is no one-size-fits-all solution. Micro-level risks can be directly managed or assessed by DeFi stakeholders. Effective micro-level risk management contributes to overall financial system stability and security. While DeFi stakeholders cannot directly control macro level risks, they can mitigate their effects through strategic planning and preemptive measures.

---

337. *See supra* notes 330–36.
338. *See supra* Section III.H.
339. *See id.*
340. *See FSB DeFi Report*, *supra* note 168, at 16–25; *see also* WEF POLICYMAKERS TOOLKIT, *supra* note 157; Carapella et al., *supra* note 168; Sandeepa Kaur et al., *Risk Analysis in Decentralized Finance (DeFi): A Fuzzy-AHP Approach* (Apr. 10, 2023), https://perma.cc/EJ4U-MR3T; 2023 IOSCO DEFI POLICY REPORT, *supra* note 249, at Annex E.

Risk assessments will vary significantly depending on whether a system is operated on a centralized or decentralized basis. In a centralized structure, services and processes are directly managed by the organization. Such structures have established procedures and comprehensive risk assessment documentation. However, such structures can be less transparent, and risk is more concentrated, posing additional challenges. Conversely, risk assessments in decentralized systems cannot rely on a single comprehensive review performed by an internal risk function due to a lack of a centralized authority to oversee and manage such a review in addition to the continuous changes that may be occurring independently across such systems. Therefore, in such systems, risk assessments should evaluate multiple interconnected systems and how they interact or are integrated with the DeFi service under review.

With the above in mind, consider an adaptation of third-party risk management requirements[341] and pre-transaction risk management rules, such as the Market Access Rules.[342] Active collaboration by financial regulators with other hybrid finance stakeholders in these areas could result in published practices and use cases that would benefit compliance and risk management professionals assessing hybrid finance services. Public knowledge sharing of solutions and practices would ensure that these benefits extend beyond its participants.

A. Risk Management of Outsourced Services

The complexity of operating and competing in the financial services industry necessitates outsourcing a variety of functions so that firms can focus on their core value propositions. Outsourcing extends even to the regulated activities and functions of regulated intermediaries.[343] As previously noted, both FINRA and the NFA require members to enact risk

---

341. *See* discussion *supra* notes 47–48; *see also* FINRA, Rule 3110 (2023) (requiring member firms to adhere to supervisory obligations relating to outsourcing of certain "covered activities"—activities or functions that, if performed directly by a member firm, would be subject to supervision); NAT'L FUTURES ASSOC., Interpretive Notice 9079 (2021) (outlining NFA Compliance Rules 2-9 and 2-36 and "plac[ing] a continuing responsibility on every Member futures commission merchant (FCM), commodity trading advisor (CTA), commodity pool operator (CPO), and introducing broker (IB) to diligently supervise its employees and agents in all aspects of their commodity interest activities").

342. *See supra* notes 54–56 and accompanying text.

343. *See* FINRA, Reg. Notice 21–29 (2021) (reminding firms of their supervisory obligations related to outsourcing to third-party vendors); NAT'L FUTURES ASSOC., Interpretive Notice 9079 (2021) [hereinafter FINRA and NFA Outsourcing Guidance]. While a "covered activity" or an activity requiring qualification and registration cannot be deemed to be "outsourced" in whole, functions associated with such "covered activities" can. *Id*. These include trade execution and reporting technologies, automated data services, information technology, operations functions, trade surveillance, and AML compliance. *Id.*

management frameworks for overseeing such outsourcing.[344] These frameworks require intermediaries to conduct risk assessments of outsourced services in accordance with their risk profile in addition to establishing and maintaining robust processes to identify and mitigate risks.[345]

A comprehensive risk assessment program, accounting for the nature and scale of the activities undertaken, has four primary stages: initial risk assessment, due diligence, onboarding, and ongoing monitoring.

The initial risk assessment is a structured process for determining whether to utilize an outsourced service including risk identification, risk weighting, assessing benefits and risks, and obtaining key stakeholder input or approval.[346]

Due diligence, as set forth with respect to hybrid finance below, considers a variety of factors including regulatory impact, operational logistics, financial stability, regulatory history, business continuity and contingency plans, notice of material failures, audit reports, and recordkeeping requirements.[347]

Drawing from the relevant experience of regulated markets,[348] such a diligence process may include all or some of the following key areas referenced in Figure 13 below.[349]

---

344. The EU has adopted similar guidance. *See* Council Regulation (EU) 2016/679, *supra* note 229. The EU has also adopted guidelines related to outsourcing arrangements for regulated intermediaries. *See* European Banking Auth., *Guidelines on Outsourcing Arrangements* (Feb. 25, 2019), https://perma.cc/49E6-KWUH.

345. *See supra* notes 61–63 and accompanying text*; see also* FINRA and NFA Outsourcing Guidance, *supra* note 343.

346. Relevant stakeholders would be represented by compliance, legal, IT, and risk management teams. Similarly, representative regulatory staff specifically tasked with exploring and facilitating such collaborations could draw from similar functional areas, including those charged with market oversight, but explicitly excluding enforcement staff.

347. *See* FINRA and NFA Outsourcing Guidance, *supra* note 343.

348. *See id.* Although the scope of this Article is primarily focused on SEC and CFTC regulation, the primary risk management frameworks promulgated by the Federal Reserve are adaptable to assessing and monitoring DeFi service risks for banks, specifically including risk management scenarios and stress testing market conditions. *See* Patrick M. Parkinson, Dir., Division of Banking Supervision and Regulation, BD. OF GOV. OF THE FED. RES. SYS., *SR No. 11-7: Guidance on Model Risk Management*, (Apr. 4, 2011), https://perma.cc/X59T-3R5W.

349. *See infra* Section VI.A. Fig.13. (adapted from FINRA and NFA Outsourcing Guidance, *supra* note 343).

Figure 13.

Hybrid DeFi Service Due Diligence Basics
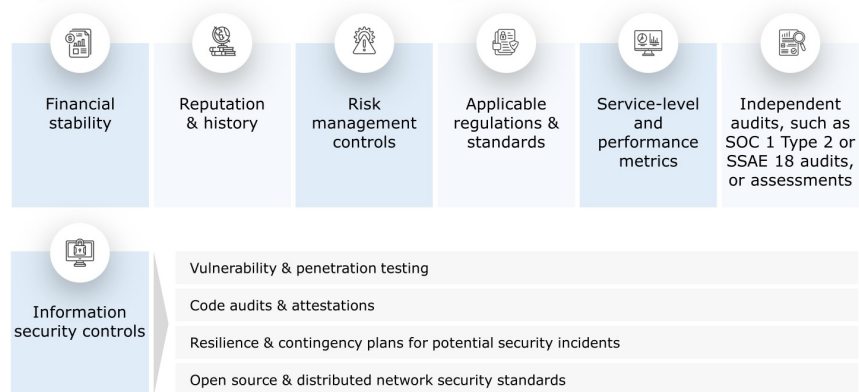
Financial stability	Reputation & history	Risk management controls	Applicable regulations & standards	Service-level and performance metrics	Independent audits, such as SOC 1 Type 2 or SSAE 18 audits, or assessments

Information security controls	Vulnerability & penetration testing
	Code audits & attestations
	Resilience & contingency plans for potential security incidents
	Open source & distributed network security standards

Source: Adapted from FINRA, Regulatory Notice 21-29 (2021); NFA, Interpretive Notice 9079 (2021)

The process for onboarding is generally intended to address the roles, responsibilities, performance expectations, and required assurances identified during the diligence process, with respect to the outsourced activities or functions.[350]

An ongoing risk management process, also informed by established practices in regulated markets, could potentially encompass activities such as those referenced in Figure 14 below.[351]

---

350. *See* FINRA and NFA Outsourcing Guidance, *supra* note 343, § III. When a function or activity is provided by a third-party provider, onboarding will generally entail documenting relationships in a written contract or obtaining some other written form of assurance.

351. *See infra* Section VI.A. Fig.14. (adapted from FINRA and NFA Outsourcing Guidance, *supra* note 343).

Figure 14.

Hybrid Finance Ongoing Monitoring

Regularly review service performance against metrics	Periodically reassess the service's risk profile	Track changes in the service's operation, risk profile, & compliance	Monitor relevant forums & information sources for service updates	Investigate publicly posted complaints
Conduct internal training & updates re. identified risks & red flags	Regularly review available information re. security controls & measures	Tracking updates and material changes	Evaluate data & systems protections	Monitor responses & postmortems to security incidents and data breaches

aSource: Adapted from FINRA, Regulatory Notice 21-29 (2021); NFA, Interpretive Notice 9079 (2021)

The process of due diligence and ongoing monitoring requires a critical evaluation of the currentness, accuracy, and completeness of available data. Identified deficiencies may require mitigation measures. How such gaps or risk concerns are addressed can play a significant role in influencing use.

With the rise of automation in finance, cybersecurity has become a critical part of due diligence and ongoing monitoring frameworks and a pressing issue for DeFi services.[352] As reliance on automated third-party and internal systems expands, standards like those published by the National Institute of Standards and Technology ("NIST"), the International Organization for Standardization ("ISO"), and the Open Web

---

352. *See, e.g.*, Office of Compliance Inspections and Exams., *National Exam Program Risk Alert: OCIE Cybersecurity Initiative*, U.S. SEC. & EXCH. COMM'N, vol. IV. no. 2 (Apr. 15, 2014), https://perma.cc/8EGZ-BASX; Office of Compliance Inspections and Exam, *National Exam Program Risk Alert: OCIE's 2015 Cybersecurity Examination Initiative*, U.S. SEC. & EXCH. COMM'N, vol. IV. no. 8 (Sept. 15, 2015), https://perma.cc/B4N3-97WB; *Interpretive Notice, 9070 - NFA Compliance Rules 2-9, 2-36 And 2-49: Information Systems Security Programs*, NAT'L FUTURES ASSOC. (Aug. 20, 2015), https://perma.cc/AH9M-LNE3 (discussing NFA Compliance Rules 2-9, 2-36 and 2-49 relating to information systems security programs); Cybersecurity and Technology Governance, Regulatory Obligations and Related Considerations, FINRA (2022), https://perma.cc/7SYB-GV3C; *see also* Richard Borden et al., *Complying with Cybersecurity Regulations in an Increasing Threat Environment*, FIA (Mar. 25, 2021), https://perma.cc/5LGX-UV6W (presentation available at: https://perma.cc/83E3-JMQL); Risk Management Program Regulations for Swap Dealers, Major Swap Participants, and Futures Commission Merchants, 88 Fed. Reg 45826 (July 18, 2023) (to be codified at 17 C.F.R. 1, 23); *Institutional DeFi Whitepaper*, *supra* note 188, at 6; Brian McPherson, *Curve Finance Exploit has 'Shaken Confidence in DeFi'*, THE BLOCK (July 31, 2023, 10:59 AM), https://perma.cc/A6S2-2PM4 (detailing the exploitation of a difficult-to-detect smart contract bug and how it resulted in at least a $24 million exploitation).

Application Security Project ("OWASP"), have become indispensable.[353] These standards offer proven frameworks and best practices that can help hybrid finance and DeFi stakeholders identify, evaluate, and mitigate cybersecurity risks.

Particularly with regards to cybersecurity, a public-private collaboration focused on a risk management framework could help advance critically important model controls for hybrid finance stakeholders and could result in service offerings, which could reside either on or off-chain depending on the use case. An example of this might be leveraging the verification controls referenced in Figure 12 above to delay or otherwise restrict withdrawals from a liquidity pool for wallets that have not been verified to mitigate the risk of a DeFi protocol being exploited. On-chain anomalous activity could trigger a temporary halt on token outflows or settlement until investigated by a hybrid finance service organization.[354] A more fully on-chain mechanism could permit voting to extend the halt beyond a certain period or liquidate the pool to its liquidity providers. While these and other options involve tradeoffs, exploring how verified credentials and halts in response to anomalous activity to minimize cybersecurity risks would be a significant contribution for a public-private collaboration. Moreover, coupled with a risk weighted due diligence process, hybrid finance stakeholders could positively shape the future of DeFi.

Hybrid finance service providers themselves might take the above actions on their own accord to mitigate risks and potentially involve DeFi protocol community members or engage with a service provider authorized by the governing body of the DeFi protocol. Regardless of whether financial regulators engage proactively, hybrid finance service providers and the communities supporting DeFi protocols should take a proactive approach to prepare for such requirements as relevant, if only for the benefit of their own cybersecurity programs.

---

353. *See, e.g.*, *Security and Privacy Controls for Information Systems and Organizations*, NAT'L INST. OF STANDARDS AND TECH. (2020), https://perma.cc/Z56Q-QCEA; *Application Security Verification Standard 4.0*, OPEN WORLDWIDE APPLICATION SEC. PROJECT (2019), https://perma.cc/7M3G-HQBZ; *see generally International Organization for Standardization, Information technology – Security Techniques*, INT'L ORG. FOR STANDARDIZATION (Aug. 2019).

354. *See* DIYAHIR, *Add EIP: Circuit Breaker #7265*, https://perma.cc/6BQW-894N (last visited Sept. 26, 2023); Laura Shin, *Circuit Breakers: Is ERC-7265 the Solution dApps Were Waiting For?* Ep. 515, UNCHAINED (Jul. 7, 2023, 7:00 AM), https://perma.cc/6Z4C-TJN5.

B. Identification and Diligence of DeFi Risks

The FSB DeFi Report, despite being more focused on financial stability and macroprudential risks uniquely associated with DeFi,[355] can generally be adapted to micro-level risk management. Figure 15 below sets forth a broad categorization of FSB's identified systemic risk concerns specific to DeFi as applied to a hybrid finance micro level construct.[356] Depending on the specific use case, each category of risk can be independently evaluated in parallel with the risk frameworks applicable to traditional financial services.

Figure 15.[357]

FSB's Financial Stability Risks of DeFi

Governance

Unclear, susceptible, or inadequately-tested governance structures can mislead users, create imbalances in power dynamics, and lead to disagreements resulting in disruptive outcomes, such as forks, network splits, and delayed responses.

Smart contracts

Complexity, reusability, and immutability of smart contracts can lead to coding errors, vulnerabilities, irreversible transactions, and difficulties in identifying accountable parties for remedies.

Composability

Systemic disruptions and adverse cascading effects could occur from a single technological failure in a smart contract due to the strong interdependencies across various protocols.

Liquidity and maturity mismatches

Discrepancies between the liquidity & maturity profiles of assets & liabilities can lead to run risks & harmful spillover effects to other parts of the financial system, particularly where immediate redemption is promised while investing in less liquid assets, such as with regards to stablecoins and lending.

Oracles and bridges

Potential inaccuracies, manipulations, or system vulnerabilities in oracles that provide off-chain data and in cross-chain bridges that connect various blockchains can lead to unintended consequences, theft, or misappropriation of assets.

Dependence on blockchain

Reliance of DeFi protocols on the underlying blockchain infrastructure can increase susceptibility to disruptions such as outages, network congestion, or consensus failure.

Critical functions, concentration and complexity

Dependence on a limited number of critical intermediaries and systems, the high concentration of activity within a few protocols or on a specific blockchain, and complex, opaque interconnections both within the DeFi ecosystem and with traditional centralized financial platforms, could create systemic disruptions.

Leverage

The use of collateralized loans can lead to automatic liquidations from a decrease in asset values, creating a cascading effect of falling prices & further liquidations.

Others

Market integrity and cross-border arbitrage issues can impact stability and trustworthiness of DeFi services.

Source: Financial Stability Board, The Financial Stability Risks of Decentralized Finance (2023)

If a hybrid finance user cannot gain adequate confidence concerning assessed risks, various mitigating strategies can be implemented. These include the establishment of dynamic pre-transaction risk controls and insurance,[358] which may itself need to be risk assessed.

---

355. *See FSB DeFi Report*, *supra* note 168, at 2-4, 20–29.
356. Cryptoisation risks, which relate to possible harms to a government's monetary policy controls and other purely macro level risk concerns, were referenced in the FSB DeFi Report but are omitted from Figure 15 because they are not adaptable to micro-level risk.
357. Adapted from the *FSB DeFi Report*, *supra* note 168, at 16–24.
358. *See infra* Section VI.D; *see also Insurance Protocols*, *supra* note 176.

There is much support for risk assessments from well-established DeFi protocols and applications.[359] Their maturity is a testament to market positioning and underscores the importance of fostering a committed community of stakeholders capable of bolstering similar risk controls. These mature protocols offer valuable examples of the processes and disclosures that hybrid finance stakeholders can assess, monitor, and improve upon. Furthermore, hybrid finance services can customize these processes and disclosures to address their unique risks and satisfy the needs of their stakeholders.

C. Adapting FSB Financial Stability Risks to the Organizational Level

As set forth in Figure 15 above, the FSB generally identifies the following specific financial stability risk categories relevant to DeFi services and protocols.[360] These risk categories can be assessed at the service and protocol micro level to create actionable bottom-up insights that are both more efficient and effective than macro level top-down mandates.

Governance risks: Poor decentralized governance can create DeFi protocol risks that can lead to user misinformation and lack of continuous protocol development. Concentration of decision-making powers, low voter participation, and disagreements over governance can cause network splits and losses.[361] However, immutable DeFi protocols do not require any governance after deployment, and, when governance is required, mature frameworks, such as those highlighted herein,[362] will generally have a reliable history of transparent governance practices. In the absence of such transparency, initial assessments and ongoing monitoring may be more challenging.

Due diligence and ongoing monitoring of governance may include whitepapers; governance process and incentive descriptions, with periodic community reviews of such processes and controls;[363] frequency and quality of community updates;[364] mechanisms that encourage public

---

359. *See infra* Section VI.C.

360. *See supra* Section VI.B, Fig.15 and *FSB DeFi Report*, *supra* note 168, at 16–24.

361. *See generally* DoT 2023 REPORT, *supra* note 238; *see also FSB DeFi Report*, *supra* note 168, at 17–18; 2023 IOSCO DEFI POLICY REPORT, *supra* note 249, at Annex D.

362. *See supra* notes 204–07 and discussion *infra* notes 381–88 and accompanying text.

363. *See, e.g.*, *BGD. Aave Governance V3*, AAVE FORUM (Mar. 20, 2023), https://perma.cc/8VCD-676X [hereinafter *Aave Governance V3*] (reviewing Aave V2 to inform new Aave V3).

364. *See, e.g.*, nickmartitsch, *Compound Developer Community Call – Dec. 9, 16:30 GMT*, COMPOUND FORUM https://perma.cc/P38L-8DD7 (last visited Oct. 22, 2023); *see also* duncand, *Governance Weekly Recap*, COMPOUND FORUM, (Sept. 9, 2022, 1:21 PM), https://perma.cc/SUG2-46ZL.

scrutiny of decisions;[365] voting histories;[366] modifiability and impact of voting rights;[367] automated decision-making;[368] and crisis management capabilities.[369] Additionally, further investigation may be required to determine the conditions relating to the use of administrative keys, multi-sig controls, and contract upgradeability, which creates control touchpoints relevant to assessing the protocol or service.[370] Transparency and clarity respecting governance will ensure the appropriate feedback mechanism for continuous monitoring. Such oversight mechanisms will facilitate user trust, foster informed and robust protocol development, and ensure that necessary governance actions are carried out with an understanding of their potential impact on the protocol's integrity and user interests.

Smart contracts and composability risks: Smart contract complexity can increase the risk of coding errors, unexpected behaviors, and shared vulnerabilities attributable to reuse and interconnected protocols.[371] Due to the general immutability of DeFi transactions, errors or fraudulent transactions cannot be easily undone and may limit ex-post remedies. From a risk assessor's perspective, the first step is to verify that the hybrid finance service's smart contract addresses are readily identifiable and updated. Effective due diligence for such an assessment might include code reviews or formal code verification,[372] code audits,[373] testnet deployment results, third-party expert and community reviews for

365. *See* devinwalsh, *Community Governance Process Update [Jan 2023]*, UNISWAP GOVERNANCE, https://perma.cc/6DPB-4YAZ (last visited Oct. 1, 2023).

366. *See, e.g.*, *Uniswap Proposals*, TALLY, https://perma.cc/8GBM-3CUG (last visited Oct. 1, 2023).

367. *See id.*

368. *See, e.g.*, *Aave Governance V3*, *supra* note 363.

369. *See id.*

370. Aave, Compound, and Uniswap are examples of DeFi protocols whose control over administrative keys has been relinquished to the community. *See* Alexander Behrens, *Aave Officially Hands Over Governance Keys to DeFi Community*, DECRYPT.COM (Oct. 28, 2020), https://perma.cc/BAP6-R7BM.

371. *See FSB DeFi Report*, *supra* note 168, at 19.

372. *See, e.g.*, *MakerDAO – GemJoin9 for PAXG Smart Contract: Security Audit*, CHAINSECURITY (Jan. 10, 2023), https://perma.cc/X7T7-LZB6; *Certora Continuous Formal Verification Report November 2022*, AAVE FORUM, https://perma.cc/VF5S-BBUF (last visited Oct. 19, 2023) (discussing code verification of various software services provided by Aave's service providers).

373. *See, e.g.*, AAV3 *Security & Audits*, AAVE FORUM, https://perma.cc/7HV5-CDQ8 (last visited Oct. 19, 2023); *Completion: SAFEGUARD AUDIT*, AAVE FORUM, https://perma.cc/Y98G-36VH (last visited Oct. 19, 2023) (discussing a completed audit for a new software service that can be integrated with Aave smart contracts); *OpenZeppelin Security Partnership - 2022 Year in Review*, COMPOUND FORUM, https://perma.cc/5B3R-TFWZ (last visited Jan. 6, 2024) (discussing Compound's continuous software auditing processes, including as applied to system upgrades and the current system version).

vulnerabilities or coding errors,[374] bug bounty programs, and results.[375] Rigorous smart contract audits and monitoring can minimize the risk of errors and vulnerabilities in protocols and platforms by safeguarding against irreversible transaction risks and maintaining system integrity.

Oracle and bridge risks: Oracles and bridges present risks that are unique to decentralized systems, including oracle manipulation and malfunction leading to misinformed user response and cross chain bridge vulnerabilities putting wrapped assets at risk.[376]

Relevant diligence for such an assessment might include reports and reviews related to security, reliability and accuracy for oracle sources,[377] data provenance,[378] utilization of off-chain computation by oracles,[379] security history of integrated bridges, independent third-party audits of oracle and bridge integrations,[380] and security roadmaps.[381] Such diligence can identify potential vectors for manipulation and malfunction that could lead to user errors and asset theft. Security assessments, including independent audits and reviews of security histories, roadmaps, and remediations, can help to ensure the reliability and integrity of cross-chain interactions.

---

374. *See, e.g.*, MCERFS, *Certora Continuous Formal Verification Report November 2022*, AAVE FORUM https://perma.cc/UAQ9-8AE5 (last visited Oct. 19, 2023) (discussing code verification of various software services provided by Aave's service providers).

375. *See, e.g.*, *Maker DAO: Submit a Bug*, IMMUNEFI, https://perma.cc/VN6R-PDZC (last visited Oct. 18, 2023); *Aave Bug Bounty*, GITHUB, https://perma.cc/6M5Y-ALH4 (last visited Oct. 18, 2023). For a more comprehensive bounty list, see *Explore Bounties*, IMMUNEFI, https://perma.cc/BM53-E85U (last visited Oct. 19, 2023).

376. Examples of oracle manipulation include manipulation of data into a protocol (affecting all dependent protocols), manipulation of the market price of an asset that an oracle is tracking, and manipulation of a single oracle provider that feeds other oracle providers. Examples of oracle malfunction include software bugs leading to incorrect data being fed to smart contracts and downtime that delays or creates inaccuracy in price data. Examples of bridge vulnerabilities include theft or misappropriation of bridge assets, collateral devaluation within a compromised bridge, and central points of failure attributable to consensus concentration. *See FSB DeFi Report*, *supra* note 168, at 19.

377. *See, e.g.*, Pauljlei, *Price Manipulation Implications on Aave: October 2022*, AAVE FORUM, https://perma.cc/FH7T-EYQK (last visited Sept. 26, 2023) (concluding a Mango Markets type of attack is much less likely on Aave due to its liquidity and overcollateralization requirements).

378. *See What are first-party oracles?*, API3, https://perma.cc/TYE9-5WM9 (last visited Aug. 1, 2023).

379. *See Off-Chain Reporting*, CHAINLINK, https://perma.cc/HHE2-MHN6 (last visited Aug. 1, 2023).

380. *See, e.g.*, cylon, *OpenZeppelin Security Updates for April 2022*, COMPOUND FORUM (May 2022), https://perma.cc/9ZHH-E95V; CODE ASSESSMENT OF THE STARKNET-DAI-BRIDGE SMART CONTRACTS, CHAINSECURITY (Oct. 18, 2022), https://perma.cc/PF9U-KNG4; CHAINSECURITY, *Code Assessment of the Optimism DAI Bridge Smart Contracts* (July 7, 2021), https://perma.cc/M7DT-YDJK.

381. *See, e.g.*, *Maker Protocol Technical Docs: Security for the Maker Protocol*, MAKERPROTOCOL https://perma.cc/3BXU-MWW5 (last visited Oct. 8, 2023).

Dependency risks, concentration, and complexity: Blockchain infrastructure dependencies, concentration risks associated with a small number of common infrastructure providers, and the complexity of such arrangements could expose DeFi protocols and hybrid finance stakeholders to technical risks and disruptions such as outages, delay, network congestion, or consensus failure.[382]

DeFi protocols are commonly integrated with multiple decentralized applications (e.g., aggregation protocols or Layer 2 solutions) for accessing their services and minimizing dependencies.[383] Assessing concentration risks and its associated complexities requires looking beyond interoperability and cross chain solutions to common single points of failure across those solutions and available mitigations.[384] Other areas for diligence and monitoring may include off-chain computation and other resource optimizations,[385] scaling solutions and roadmaps,[386] pause and timelock controls,[387] and actions to reduce concentration and centralization risks.[388] Such diligence can identify and permit mitigation of technical risks like outages or congestion that could disrupt DeFi services. Examining common points of failure and strategies deployed to address them can identify exposures to systemic risks and the maturity of a service or protocol towards achieving robust, decentralized operations.

Financial risks: liquidity and maturity mismatch; leverage: Risks associated with leverage, liquidity, and duration mismatch can negatively impact the financial resilience of a DeFi protocol by magnifying losses, depleting available funds for withdrawals, and creating insolvency during market stress if assets and liabilities are not carefully aligned. These are critical risks to hybrid finance users, as they directly put their capital at risk—for example, the risk that a forced liquidation will depress recovery on a collateralized loan.[389]

Initial diligence and ongoing monitoring for a hybrid finance service relating to lending, margin, or leveraged products may include reviewing

---

382. *See FSB DeFi Report*, *supra* note 168, at 18, 21–22.

383. *See id.* at 21.

384. *See, e.g.*, Derek, *A Multichain Strategy and Roadmap for Maker* MAKERDAO FORUM, https://perma.cc/7NXZ-RGFV (last visited Oct. 8, 2023).

385. *See, e.g.*, alex_starkware, *Launch Aave V3 on Starknet*, AAVE, https://perma.cc/B32Q-G4FK (last visited Oct. 8, 2023).

386. *See, e.g.*, Derek, *Layer 2 Roadmap – History and Future*, MAKERDAO FORUM, https://perma.cc/N8MG-AEA3 (last visited Oct. 8, 2023).

387. *See, e.g.*, GITHUB, *Volt Protocol's Audit of Compound Finance*, Link to "timelock," https://perma.cc/Z9YF-SJZG (last visited Oct. 8, 2023).

388. *See, e.g.*, IncentiveLord, *[Temp Check] Freeze MAI from Aave*, AAVE FORUM, https://perma.cc/8FN4-C52Y (last visited Oct. 8, 2023) (discussing centralization risk from MAI and proposing to remove MAI from Aave and Arbitrum).

389. *See, e.g.*, *Collateral & Borrowing*, COMPOUND FORUM, https://perma.cc/F6FH-XP3W (last visited Oct. 8, 2023); *Liquidation*, COMPOUND FORUM, https://perma.cc/BDT4-8CZV (last visited Oct. 8, 2023).

current risk parameters, the calculation methodology, and the process for revising such parameters.[390] This oversight may also include the results of third-party risk parameter reviews and stress tests if necessary. Such reviews or tests may include the impact of price shocks and loss of liquidity impacting the underlying collateral, along with external events such as cascades of liquidations impacting external prices.[391] This diligence could also include assessing the resilience and dynamic response of parameters. Both reviews and scenario testing should consider both leverage and mismatched liquidity and duration.

The level of transparency provided by dYdX, the second largest derivatives DEX,[392] and its partners on these factors, depicted in Figure 16 below,[393] serves as a benchmark of the type of information that would be relevant for risk assessment and ongoing monitoring. [394]

Figure 16.

Case Study: Financial Risk Management via the dYdX Parameter Recommendation Portal

Objective	Functionality	Transparency	Real-time Data	Algorithmic Framework
The dYdX Parameter Recommendation Portal suggests optimal margin risk parameters, aiding the DAO in managing the platform & guiding financial risk managers, including traders & risk professionals.	The portal's market-specific recommendations enable the DAO & traders to tailor their risk management strategies to individual market conditions.	The methodology behind the recommendations is detailed in a third party expert's review & assessment, thus promoting transparency & understanding for users.	The portal's visualizations of current & recommended parameters relative to market liquidity offer the DAO & traders a tool for real-time risk assessment.	By using an algorithm based on sampled liquidity data from live markets, the platform offers systematic risk parameter recommendations that the DAO & traders can leverage for informed decision-making.

The use of this tool facilitates better risk management within the dYdX ecosystem by providing actionable insights to both the DAO & traders.

Source: DyDx website & community forums. See article body for citations

---

390. *See Risk Parameters*, AAVE FORUM, https://perma.cc/P8HE-U7RD (last visited Sept. 29, 2023).

391. *See* WATSON FU, ET AL., MARKET RISK ASSESSMENT, GAUNTLET RESEARCH PROJECT, 1–44 (2022), https://perma.cc/T7ZK-AE35; AAVE, *Aave Risk Dashboard by Guantlet Launched*, (Dec. 19, 2022), https://perma.cc/R6UC-XX5U (last visited Sept. 26, 2023); OriN, *Updated Proposal: Chaos Labs – Risk & Simulation Platform* (Sept. 2022), https://perma.cc/5CG3-XRD8 (AAVE online forum).

392. dYdX is the second largest decentralized derivatives exchange by TVL. *See* DeFi Llama, *Dervatives TVL Rankings*, https://perma.cc/XKZ8-QTDL (last visited Dec. 29, 2023).

393. *See infra* Section VI.C, Fig.16.

394. *See Homepage*, CHAOS LABS, https://perma.cc/S5PM-6S2C (last visited Oct. 18, 2023); Craig Le Riche, *Proactive Management of dYdX Risk Parameters*, CONSIDERED FINANCE (Nov. 30, 2022), https://perma.cc/73XZ-2Z98; *see also* Chaoslabs, *dYdX Risk Parameter Recommendation Portal*, DYDX (May 26, 2023), https://perma.cc/M7PY-25AQ; *Parameter Recommendations*, CHAOS LABS, https://perma.cc/LB36-A7JG (last visited Aug. 1, 2023).

Other vulnerabilities: Risks linked to market integrity and cross-border regulatory arbitrage encompass unsustainable business models that are dependent on continual investor inflows for profit, material non-compliance with established regulations on financial activities, and fraud or manipulation, all of which could lead to substantial losses without recourse. Furthermore, DeFi services without a clear legal domicile might evade jurisdictional supervision, regulation, consumer protection requirements, or circumvent commercial practices.

Primary considerations for assessing these vulnerabilities include token economics, the DeFi service's governance, and its history. Any credible negative history concerning the DeFi service and identified core team members should be considered, along with their use of risk mitigating tools discussed above, such as delays on withdrawals associated with suspicious activity or, conversely, the power to terminate all DeFi protocol functions except withdrawals.[395] For market integrity concerns, the adoption of compliance controls would necessitate a shift towards more centralized governance mechanisms, creating a tradeoff with decentralized governance principles by introducing hierarchical control required for regulatory oversight and supervision. Capital loss considerations associated with market integrity and regulatory arbitrage risks are overlapping considerations with a financial risk assessment. Ongoing monitoring and insurance should also be contemplated.[396]

The existence of a collaborative effort among hybrid finance stakeholders could encourage the creation of services focused on post transaction analysis and publication of anomalous behavior. Moreover, as the DeFi landscape evolves, proactive measures are paramount. While post-transaction analysis and the identification of anomalous behaviors play a crucial role, mitigating risks at the beginning of the transaction process is a natural focal area for collaboration with regulators. The ability to anticipate and respond to risks and vulnerabilities as they develop is an effective bottom-up approach for ensuring the integrity and stability of the hybrid finance system.

D. Pre-Transaction Risk Management Control

As noted above, both the SEC and CFTC have adopted rules specifically addressing pre-trade risk controls (the "Pre-Transaction Risk

---

395. *See Emergency subDAO*, BALANCER DOCS, https://perma.cc/44AL-622W (last visited Sept. 26, 2023); *Emergency Members*, CURVE, https://perma.cc/ZF6E-P7SP (last visited Sept. 29, 2023)*; see also* Andrew Thurman, *'Curve Wars' Heat Up: Emergency DAO Invoked After 'Clear Governance Attack'*, COINDESK, (May 11, 2023, 12:08 PM), https://perma.cc/9YLM-62KH; Rob Behnke, *Best Practices For Secure Defi Governance*, HALBORN BLOG (Apr. 27, 2023), https://perma.cc/PGT6-3DE6.

396. *See, e.g.*, *Insurance Protocols*, *supra* note 176.

Rules").[397] Pre-trade risk controls (framed here as "pre-transaction") contemplate minimizing the risk of human error or flaws in trading algorithms, which could create cascading errors and implicate systemic risks. Because of this, they have attracted enforcement actions,[398] signaling to hybrid finance stakeholders the importance of understanding the implications for hybrid finance services and potential institutional adoption.

Adaptations to current pre-transaction risk management controls could, at a minimum, include the following: (1) preventing the entry of instructions exceeding credit or capital limits; (2) providing pre-approved assets and maximum positions sizes permitted over a period of time or in the aggregate; and (3) rejecting instructions that exceed appropriate price, size, or message volume limits, either individually or in aggregate, over a short period of time, or rejecting those that are duplicative. [399]

Risk limits, which could also incorporate financial risk parameters, could either be set internally or in conjunction with a third-party risk management service acting as an oracle for adjusting limits or parameters. Intermediate threshold alerts would ensure that strategies could be adjusted or acted upon as necessary prior to limit thresholds being breached. The integration of this with the AML Diligence Controls is illustrated below in Figure 17. [400]

397. Risk Management Controls for Brokers or Dealers With Market Access, Exchange Act Release No. 63241, 75 Fed. Reg. 69792 (Nov. 15, 2010) (codified at 17 C.F.R. § 240.15c3–5), https://perma.cc/F3ED-FR2K; *see* Customer Clearing Documentation, Timing of Acceptance for Clearing, and Clearing Member Risk Management RIN 3038-0092, -0094, 77 Fed. Reg. 21278, 21306–8 (April 9, 2012) (requirements related to automated pre-trade risk management were codified at 17 C.F.R. § 1.73 and 17 C.F.R. § 23.609) (relating to FCMs, SDs, and MSPs), https://perma.cc/F89B-8B3Q; Core Principles and Other Requirements for Designated Contract Markets, RIN 3038-AD09, 77 Fed. Reg. 36612, 36705 (June 19, 2012) (requirements relating to automated pre-trade risk management were codified at 17 C.F.R. § 38.607) (relating to DCMs), https://perma.cc/5Q6J-FA56; *see also* sources cited *supra* notes 75, 92–94 and accompanying text. Such rules are broadly referred to herein as "Pre-Transaction" versus "Pre-Trade" to ensure uniform references when applied to transactions occurring in hybrid finance.

398. *See* Ashley E. Bashur & Paul Eckert, *10 Years On, SEC's Market Access Rule Still Lacks Clarity*, LAW360 (Oct. 11, 2021), https://perma.cc/3R7V-2LS9.

399. *See supra* Section V.B.d.

400. *See supra* Section VI.D.

Figure 17. Integrated AML and Pre-Transaction Risk Controls
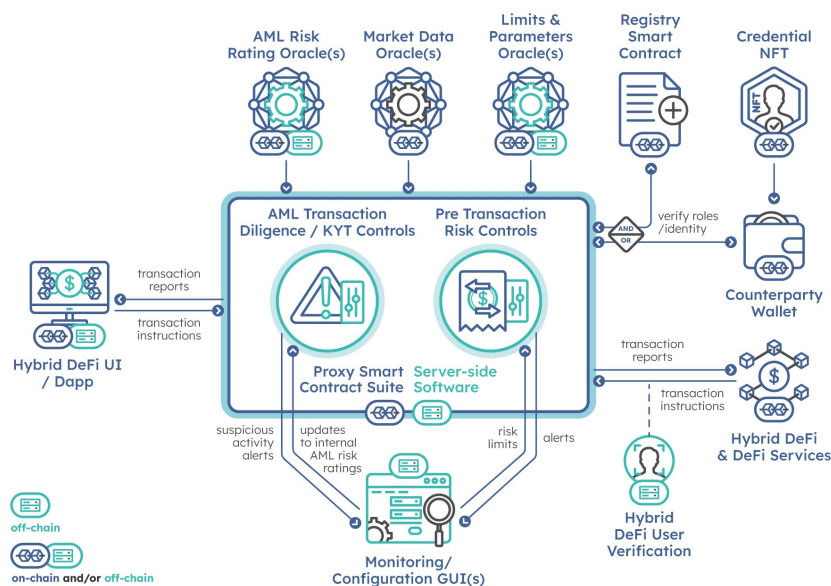
Pre-transaction risk controls, which manage a host of risk parameters and adapt to real-time market data,[401] can serve multiple functions. They can be particularly useful for managing financial risks,[402] and they can adaptively tweak maximum or baseline incremental position sizes based on real-time market data. These controls can also be customized for specific assets, introducing parameters like price ranges or collars for transaction initiation.

Implementing this pre-transaction risk framework requires structured processes and procedures. FINRA, based on its past examinations, provides relevant guidance which is further explained in Figure 18 below.[403]

---

401. *See, e.g.*, *Pre-Trade Risk*, PICO.NET, https://perma.cc/WA8V-P557 (last visited Nov. 12, 2023); *Market Access Compliance Solutions*, SUCCESSIONSYS.COM, https://perma.cc/XDN8-FSQ2 (last visited Nov. 12, 2023).

402. *See supra* Section V.C.

403. *See* FINRA, 2022 *Report on FINRA's Examination and Risk Monitoring Program* 48 (2022), https://perma.cc/3KEL-76W3. In summarizing the scope and purpose of the Market Access Rule, FINRA noted:

> [The SEC Market Access Rule] requires firms . . . that provide market access to their customers to 'appropriately control the risks associated with market access so as not to jeopardize their own financial condition, that of other market participants, the integrity of trading on the securities markets and the stability of the financial system.'

Id.

Figure 18.

Lessons From FINRA re: Internal Procedures for Pre-Transaction Risk Controls

Restricting access to authorized persons	Training firm staff managing access
Change management processes	Ongoing testing for new functionalities
Processes for ad hoc credit or capital threshold adjustments	Tailored controls for specific technology primitives, services, and market wide scenarios
Ensuring instruction & execution traceability are provided to supervisory personnel	Post transaction control reviews, including for potentially manipulative patterns

Powerpoints must flow together and be logically consistent in terms of shapes, sizes, colors, etc.

This framework addresses the establishment, documentation, and maintenance of a system for regularly reviewing the effectiveness of pre-transaction risk controls and processes for addressing issues.

Pre-transaction risk controls, which are currently operated by regulated financial intermediaries pursuant to the Pre-Transaction Risk Rules,[404] can adjust threshold participation rates in response to significant market or liquidity events. Similarly, such controls could be adapted to throttle transactions or to reduce exposure in response to a reduction in the liquidity for a particular service. Moreover, dynamic risk modeling of pre-transaction risk controls can react in real time to fluctuations in TVL or liquidity variations within protocols. These fluctuations can impact users' capabilities to withdraw or trade assets and influence the platform's stability. Provisions for 'kill switches' can halt the initiation of new transactions under specified conditions, from internal system anomalies to wider financial ecosystem events.

Despite these possibilities, both risk management and pre-transaction risk control processes and infrastructures have interdependencies with other functions and systems within mature, regulated intermediaries. This may limit the ability to scale hybrid finance transactions pending a build out of the supporting processes and infrastructure or collaborative development of supporting hybrid finance services.

The collaboration should actively contemplate building autonomous on-chain processes to mitigate conflicts of interest and to ensure universal access to risk management tools. Such tools might include benchmark standards for disclosures from DeFi service providers, such as clear and

---

404. *See infra* note 410 and accompanying text.

comprehensive information relating to underlying technology, governance (including administrative controls, multi-sig controls, and contract upgradeability), risks, fees, liquidity, and security measures. Such tools and guidance could also address security, risk management, anomalous behaviors, and other transparency concerns. This would be especially beneficial for smaller and mid-sized hybrid finance users, as it democratizes the benefits of these mechanisms.

To further bolster the integrity and accessibility of these financial services, hybrid finance services could also spur protocols to authorize adjacent entities or processes to meet new risk related demands that are independent of the DeFi protocols that they serve. Responsibilities could be delegated either to a dedicated hybrid finance servicing entity, an existing entity servicing the underlying DeFi protocol, or a combination of both.[405]

Outsourced tasks might include various ongoing functions such as onboarding diligence requirements and disclosure libraries; monitoring and reporting associated with a DeFi protocol or hybrid finance service;[406] updating pre-transaction risk controls; publication and analysis of anomalous patterns; investigation and management of temporary withdrawal delays; and oversight over autonomous processes.

The implementation of pre-transaction risk controls can mitigate both micro- and macro-level risks inherent in trading algorithms and human error. These controls, when effectively adapted and integrated with risk management frameworks and AML diligence controls, not only enhance the operational integrity of hybrid finance services but also facilitate their institutional adoption. By establishing autonomous on-chain processes and leveraging third-party risk management services, hybrid finance stakeholders can foster financial stability and transparency. This collaborative approach, which includes a mix of internal and outsourced functions, promises to bridge the gap between traditional finance and decentralized finance, thus democratizing access to sophisticated risk management tools and supporting the sustainable growth of the hybrid

---

405. *See* Chris Brummer, *Disclosure, Dapps and DeFi*, 5.1 STANFORD J. OF BLOCKCHAIN L. & POLICY 137, 169–72. Contemplating how DAO's could play a role in facilitating digital asset related disclosures, Brummer states:

> [A] crypto-native solution could include the creation of tax-exempt, nonprofit DAOs designed to promulgate disclosure frameworks, tokens[,] and compliance tools. Along these lines, DAO governance could be structured whereby participants could vote on a spectrum of disclosure-related issues—from specific disclosures necessary for dapps to open-source model disclosures to standardized credentials for accessing regulated financial opportunities.

Id. at 169.

406. *See id.* at 168 (contemplating an open-source disclosure library structured after GitHub).

finance sector. By leveraging the existing guidance of regulators like FINRA, hybrid finance can facilitate the continuous improvement, documentation, and evaluation of these risk controls, bolstering both resilience and responsibility in the face of evolving market dynamics.

VII. CONCLUSION

The U.S. financial regulatory framework historically relied on intermediaries to effect its objectives, even actively restructuring the roles of intermediaries to drive market efficiencies, democratization of access, and transparency.[407] This history underscores the fact that it is entirely consistent and firmly rooted in tradition for a financial regulator to purposefully steer and even champion the adoption of disruptive technologies in the pursuit of such regulatory outcomes.

The events of the 2008 financial crisis instigated a notable shift in this approach, with regulators and policymakers prioritizing the prevention of hypothetical systemic risk over technological innovation.[408] This tendency towards overcorrection hampers progress, imposes unnecessary burdens on small-to-medium stakeholders, and stifles the vibrant potential of the United States as a global financial center.

Historical lessons from the SEC and CFTC's regulatory adaptations to, and even the reshaping of, market structures through disruptive technologies, such as electronic communication networks and trade automation, provide valuable guidelines for a more proactive and constructive bottom-up approach.[409] This guidance is especially relevant as we grapple with the still nascent potential of DeFi.

Examining DeFi through the lens of disruptive fintech regulation, it becomes evident that it poses unique challenges (and opportunities) compared to traditional finance. Regulatory complexities arise from DeFi's evolving innovation outside the traditional financial ecosystem. The current political climate and DeFi's immaturity add to these challenges, but its potential should not be surrendered either as a matter of principle or due to global competitive and policy implications.

Conversely, DeFi stakeholders cannot wait for regulation-induced maturation; immediate commitment is required by stakeholders to ensure DeFi's growth. Nonetheless, if there is only the risk of enforcement on behalf of regulators to response to that commitment, DeFi will necessarily be pursued in other jurisdictions that can either better manage or better accommodate DeFi's development and growth. It is thus imperative that

---

407. *See supra* Part II.
408. *See supra* Part III.
409. *See supra* Parts II–III.

regulators and policymakers do more to encourage standards that more closely align with desired regulatory outcomes.

DeFi, at its core, aims to address the inherent question of trust in traditional financial systems: How can users engage in financial activities with unknown parties without the need for a trusted intermediary like a bank or financial institution? Hybrid finance amplifies this core aim by acknowledging the roles that a wide range of stakeholders may play in scaling and enhancing trustless, decentralized systems. By focusing on the operational and regulatory barriers faced by these hybrid finance stakeholders, we can advance common goals and pave the way for a financial ecosystem that is robust, inclusive, and protective of stakeholders. The future of DeFi lies in collaborative endeavors that align these diverse stakeholder interests.[410] This alignment will not only shape the DeFi landscape but also have far-reaching implications for the broader financial ecosystem.

With this in mind, important pathways were explored for building the types of controls necessary for the development of hybrid finance services including the critical areas of verifying credentials or transactions of counterparties, risk management (including security risks) frameworks, and pre-transaction risk controls.[411] Taking a bottom-up, risk-based approach guided by hybrid finance stakeholders provides a way forward. Such an approach acknowledges the need to balance fostering innovation and efficiency with the regulatory objectives of preventing investor harm and systemic instability. This balance isn't just ideal; it's crucial, given the swift pace of change in DeFi ecosystems and emerging challenges to its wider implementation.[412] Public-private collaborations among hybrid finance stakeholders provide an opportunity to strike the right balance between regulatory outcomes and innovation.

Automated trading, DeFi, and artificial intelligence are rapidly evolving, disruptive technologies that will impact the delivery of financial services forever. They bring risk and opportunity, including risks of mismanaging the opportunity and opportunities to better manage the risks. To move forward, our micro- and macro-level strategies need to not only rapidly adapt to these dynamic forces but to ensure that these adaptations are thoughtfully considered and properly informed.

---

410. *See supra* Section IV.F.
411. *See supra* Parts V–VI.
412. *See supra* Sections III.G–H, Sections IV.B–C, E, and Section IV.A.