WILMERHALE

CFTC Advisory Subcommittee Releases Report on DeFi: Issues, Findings and Recommendations

FEBRUARY 16, 2024

Introduction

On January 8, 2024, the Digital Assets and Blockchain Technology Subcommittee (the Subcommittee) of the Commodity Futures Trading Commission's (CFTC or the Commission) Technology Advisory Committee (TAC) presented a 79-page report titled "Decentralized Finance" (DeFi) to the CFTC.[1] The Subcommittee's work, which is sponsored by Commissioner Christy Goldsmith Romero, does not represent the views of the CFTC. Rather, it "provid[es] a framework for policymakers and industry in approaching the regulation of DeFi."[2]

Commissioner Goldsmith Romero explained that the report is "intended to help inform ongoing policy debates in the U.S. Congress, state legislatures and regulators including the CFTC."[3] She also expressed hope that the report "can serve as a first step to facilitate a dialogue between policymakers and industry particularly because DeFi remains at the center of illicit finance risks, cyber hacks and theft."[4]

The report begins with some conceptual background for policymakers seeking to understand DeFi and goes on to discuss potential policy objectives related to DeFi, including both opportunities and

---

[1] Digital Assets and Blockchain Subcommittee of the CFTC Technology Advisory Committee, *DeFi Report* (Jan. 8, 2024), available at https://www.cftc.gov/PressRoom/SpeechesTestimony/romerostatement010824b.

[2] *Id*. at 17.

[3] Commodity Futures Trading Commission, *Statement of Commissioner Christy Goldsmith Romero on CFTC's Digital Assets and Blockchain Technology Subcommittee Release of Decentralized Finance Report* (Jan. 8, 2024), https://www.cftc.gov/PressRoom/SpeechesTestimony/romerostatement010824b.

[4] *Id.*

risks. It also examines the regulatory and policy issues that policymakers and industry need to address, and it concludes with a series of recommendations.

The Subcommittee acknowledges that there are difficult strategic issues for policymakers and regulators, including determining who in the DeFi ecosystem should be subject to regulation. However, perhaps recognizing the challenges surrounding policy development on this topic, the Subcommittee concludes that "[t]he nature of engagement between government and private sector on DeFi at present is not constructive."[5] The report does not seek public comment or feedback, but one could expect the TAC and the Subcommittee will continue to discuss the report and DeFi issues in the future.

In this alert, we summarize the Subcommittee's conceptual approach to DeFi in its report, as well as its key findings and recommendations.

Background

The CFTC's TAC was formed in 1999 to advise the Commission on issues at the intersection of technology, law, policy and finance, and the Subcommittee includes various stakeholders from industry and academia.[6] The TAC has three subcommittees, and it has recently addressed a variety of issues, including artificial intelligence, cybersecurity, electronic trading risk principles and volatility of digital assets.

The TAC's DeFi report is one of several DeFi-related reports and enforcement actions published by the CFTC and other government agencies in recent years. In April 2023, the US Treasury Department issued a "risk assessment" related to illicit finance risks in DeFi. The Treasury Department ultimately recommended that federal regulators conduct further engagement with industry "to explain how relevant laws and regulations apply to DeFi services, and take additional regulatory actions and publish further guidance informed by this engagement."[7] In her statement regarding the publication of the report, Commissioner Goldsmith Romero noted that the report "reflects the start of such engagement."[8]

This is not the CFTC's first interaction with DeFi. In January 2022, the CFTC settled an enforcement action against Blockratize, Inc., for offering off-exchange event-based binary options contracts and for failure to register as a designated contract market or swap execution facility.[9]

---

[5] DeFi report, at 65.

[6] "Technology Advisory Committee," Commodity Futures Trading Commission (accessed on Jan. 10, 2024), https://www.cftc.gov/About/AdvisoryCommittees/TAC; DeFi report, at 14–15.

[7] *Id.*; US Department of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* (Apr. 6, 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

[8] Commodity Futures Trading Commission, *supra* note 3.

[9] In the Matter of Blockratize, Inc., CFTC Docket No. 22-09 (Jan. 3, 2022).

Then-Acting Director of Enforcement Vincent McGonagle warned that "all derivatives markets must operate within the bounds of the law regardless of the technology used, and particularly including those in the so-called decentralized finance or 'DeFi' space."[10] Later that year, the Commission brought an action against bZeroX, LLC, and its founders, Tom Bean and Kyle Kistner, when they "designed, deployed, marketed, and made solicitations concerning a blockchain-based software protocol that accepted orders for and facilitated margined and leveraged retail commodity transactions."[11] The Commission also obtained a default judgment against the Ooki decentralized autonomous organization (DAO), a successor to bZeroX, LLC, as an unincorporated association.[12] Since then, the CFTC has taken enforcement actions against DeFi protocols that automatically execute crypto-derivatives transactions in a manner that is inconsistent with the Commodity Exchange Act (CEA) and the CFTC regulatory framework, which requires trading platforms to register with the Commission. In September 2023, the Commission brought charges against the developers of three DeFi protocols for failing to register as a swap execution facility or designated contract market, failing to register as a futures commission merchant, failing to adopt a customer identification program, and illegally offering leveraged and margined retail commodity transactions in digital assets.[13]

In her dissenting statement related to the September 2023 enforcement actions, Commissioner Summer Mersinger urged the CFTC not to take an "Enforcement First" approach to DeFi regulation.[14] Similarly, Commissioner Kristin Johnson observed that "the absence of regulation directly addressing the supervision of the growing digital asset marketplace leaves vulnerable retail customers exposed and lacking long-established customer protections available in other asset classes."[15]

The publication of a report by a CFTC advisory committee can be the beginning of meaningful dialogue between regulators and industry. In the past few years, other CFTC advisory committees and subcommittees have published papers and recommendations on various topics, which helped

---

[10] *CFTC Orders Event-Based Binary Options Markets Operator to Pay $1.4 Million Penalty* (Jan. 3, 2022), https://www.cftc.gov/PressRoom/PressReleases/8478-22; *see also Keynote Address of Commissioner Dan M. Berkovitz Before FIA and SIFMA-AMG, Asset Management Derivatives Forum 2021* (Jun. 8, 2021), https://www.cftc.gov/PressRoom/SpeechesTestimony/opaberkovitz7 ("Not only do I think that unlicensed DeFi markets for derivative instruments are a bad idea, I also do not see how they are legal under the CEA. … DeFi markets, platforms, or websites are not registered as DCMs or SEFs. The CEA does not contain any exception from registration for digital currencies, blockchains, or 'smart contracts.'").

[11] In the Matter of bZeroX, LLC; Tom Bean; and Kyle Kistner, CFTC Docket No. 22-31 (Sept. 22, 2022).

[12] *Commodity Futures Trading Comm'n v. Ooki DAO*, 2023 WL 5321527 (N.D. Cal. 2023).

[13] In the Matter of Opyn, Inc., CFTC Docket No. 23-40 (Sept. 7, 2023); In the Matter of ZeroEx, Inc., CFTC Docket No. 23-41 (Sept. 7, 2023); In the Matter of Deridex, Inc., CFTC Docket No. 23-42 (Sept. 7, 2023).

[14] Summer K. Mersinger, *Dissenting Statement of Commissioner Summer Mersinger Regarding Enforcement Actions Against: 1) Opyn, Inc.; 2) Deridex, Inc.; and 3) ZeroEx, Inc.* (Sept. 7, 2023), https://www.cftc.gov/PressRoom/SpeechesTestimony/mersingerstatement090723.

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

frame and spur conversation among market participants, stakeholders and policymakers.[16] Though the DeFi report is styled as a policy paper rather than a request for comments, interested parties who have reactions or comments to this paper should still consider both formal and informal opportunities to offer feedback to the Subcommittee and CFTC staff.

DeFi Report – Basic Framework

The Subcommittee declines to "advance a definitive definition of DeFi that might one day provide the basis for a new or expanded regulatory perimeter," and it warns against designing regulatory frameworks around a single technology.[17] Instead, the Subcommittee "functionally" defines DeFi as "enterprises, projects and ecosystems characterized by highly automated financial networks that have no single point of failure, do not rely on a single source of information, and are not governed by a central authority that is capable of altering or censoring this information in order to perform tasks central to delivery of one or more financial services."[18]

The functional definition recognizes that DeFi projects vary with respect to decentralization across several different dimensions (e.g., governance, access, operations), which in turn results in different business models. The report discusses in detail the different aspects of decentralization, with the goal of highlighting the various types of DeFi ecosystems so policymakers can have a framework for identifying and categorizing the types of potential risks.[19]

The report also focuses on the "architecture" of DeFi and, more specifically, the DeFi technology stack.[20] Later in the report, for each layer of the stack, the Subcommittee suggests specific technical features and controls that could be embedded to promote regulatory compliance and to reduce risk:[21]

---

[16] *See, e.g.,* Market Risk Advisory Committee, *Interest Rate Benchmark Reform Subcommittee SOFR First Recommendation* (Jul. 13, 2021); Global Markets Advisory Committee, *Recommendations to Improve Scoping and Implementation of Initial Margin Requirements for Non-Cleared Swaps* (May 19, 2020).

[17] DeFi report, at 25.

[18] *Id.* at 20.

[19] *Id.*

[20] *Id.* at 26.

[21] *Id.* at 58.

FIGURE 9: MECHANISMS TO SUPPORT SECURITY AND COMPLIANCE IN THE DEFI TECH STACK

Layer	*Key Players and Components*	*Examples of Technical Features and Controls*
Governance	• Developers, issuers, owners, voters • Governance tokens	• On-chain governance, token distribution, certifications
Asset/Market	• Liquidity providers • Tokens, capital, collateral, prices	• Capital requirements, audits, market metrics and reports
User	• Developers (including layer 2 builders), consumers, businesses, financial intermediaries	• Digital identity, geolocation information, activity and transaction thresholds and monitoring
Application	• Exchanges and other service providers • DApps, smart contracts, wallets, APIs, oracles	• Trust registries, terms of service, redundancy and diversity of data sources, performance monitoring, authentication, authorization, access control, encryption
Data	• Ledgers/blockchains, explorers, addresses, other on-chain data	• Parent-child keys, block headers, information fields
Network	• Miners, validators, block builders, pools, voters • Nodes, relayers, bots, mempools	• Consensus mechanisms, internet protocol screening, validation requirements, network allow/do not allow lists, domain name system seeds
Protocol	• Code repositories • Software code	• Software updates and patches, distribution, tiered version control, interoperability standards
Physical/Hardware	• Mobile devices, computers, servers, and other physical infrastructure	• Mining hardware specifications, physical security (*e.g.*, compromise, natural disasters, temperature changes)

Policy Objectives, Opportunities and Risks Identified in DeFi Report

The report lists seven policy objectives related to DeFi: (i) protecting investors and consumers; (ii) promoting market integrity; (iii) ensuring microprudential safety and soundness (i.e., the safety and soundness of individual intermediaries); (iv) maintaining US and global financial stability and mitigating systemic risks; (v) expanding access to safe and affordable financial products and services; (vi) combating illicit finance; and (vii) reinforcing and strengthening US leadership and competitiveness in finance and technology.[22]

In light of these objectives, the report lists both the opportunities presented by DeFi and its risks. Opportunities include improving efficiency in the delivery of financial products and services, promoting greater transparency within the financial services industry, enhancing resiliency within the financial system, dismantling barriers to financial access and inclusion, promoting innovation and competition, and strengthening US leadership in technology and financial services.[23] With

[22] *Id.* at 34–37.

[23] *Id*. at 37–43.

respect to each opportunity, the report discusses both theoretical and practical limitations. For example, decentralized, interoperable networks may result in a reduction in overall transaction costs, but they also may "expand the sources and destinations of possible technological and financial contagion."[24] In addition, "despite the transparency of the underlying [blockchain] networks, much of the raw data cannot be effectively used by investors, consumers, or regulators without first devoting significant time and effort to building the core technological competency and capacity necessary to collect, manipulate, and analyze it."[25] Regarding US leadership in technology and financial services, the report acknowledges that "the US regulatory environment is perceived by many in the DeFi industry as ambivalent, if not hostile, toward its future development."[26] However, it also concludes that "given the size of the US market, there are still powerful incentives for [industry participants] to provide financial products and services to US citizens and residents," suggesting that many of these projects may move onshore if the United States adopts a "clear, consistent, and comprehensive approach to the regulation of DeFi."[27]

More specific risks identified in the report are listed below.

- For investors and consumers:[28] There are risks related to information asymmetries (e.g., investors and consumers may not have the technological expertise to understand DeFi projects, and more complex DeFi projects may require an unrealistic amount of time and effort to fully understand); conflicts of interest (e.g., developers may also be market participants); degree and transparency of decentralization (e.g., there may be large voting blocs unknown to most participants); the design of DeFi (e.g., operational, technological and security risks related to open source software, smart contracts, decentralized governance protocols, oracles and bridges); and the lack of clear lines of responsibility associated with decentralized development and governance.
- For market integrity:[29] Pseudo-anonymity makes DeFi projects susceptible to abusive market practices, and as with consumer protection, a lack of clear lines of responsibility compounds the problem. Moreover, "[t]he absence of sufficient governance systems, backstopped by regulation and accountability, inhibits the systems' abilities to respond to unexpected events and to foster trust."
- For DeFi projects, enterprises and ecosystems:[30] Malicious actors may exploit open source software to manipulate consensus protocols. The use of smart contracts (i.e., self-

[24] *Id.* at 38.

[25] *Id.* at 39.

[26] *Id.* at 43.

[27] *Id.*

[28] *Id.* at 46–47.

[29] *Id.* at 47.

[30] *Id.* at 48–49.

executing computer code) "introduces the risk that developers will fail to anticipate all the potential future states of the world, identify the optimal actions or outcomes in each of these states, or accurately and completely incorporate these potential states, actions, and outcomes into the relevant software code." The report also notes that DeFi projects frequently rely on more centralized network nodes for the delivery of critical inputs.

- For financial stability:[31] The report predicts that, among other things, "the use of open source software to create complex DeFi compositions would likely generate a dense thicket of economic and technological exposures, making it difficult to identify, measure, or monitor the build-up of potential systemic risks." There are also risks related to hardwired procyclicality, highly correlated and automated liquidation of collateral, and DeFi's reliance on a small number of nodes for critical functions.
- For combatting illicit finance, protecting national security and maintaining US leadership:[32] Anti-money laundering (AML) laws generally rely on intermediaries to identify and report suspicious transactions. With decentralization, it is not clear who should be responsible for AML monitoring. DeFi could also undermine US government control over the international financial system.
- For the climate:[33] Proof-of-work may increase greenhouse gas emissions.

Issues for DeFi Policymakers and Industry

Issues for Policymakers

According to the report, policymakers will need to (i) determine whether and how DeFi projects, enterprises and ecosystems fall within the existing regulatory perimeter; (ii) identify whether, where and how the regulatory perimeter might need to be expanded in order to capture DeFi projects, enterprises or ecosystems; (iii) craft an appropriate regulatory response; (iv) allocate responsibility and accountability for regulatory compliance in a world of decentralized governance (which the Subcommittee considers the "most critical issue");[34] (v) map counterparty exposures in a world of decentralized balance sheets; (vi) map key service providers and services in a world of decentralized operations; (vii) oversee new and rapidly evolving technology; (viii) ensure that DeFi lives up to critical policy objectives like expanded access to safe and affordable financial services, necessary transparency and responsible governance; (ix) mitigate the unique threats that DeFi poses to security, illicit financing, system stability, consumers and investors, market integrity, and the climate; (x) identify the best role for policymakers in building DeFi ecosystems, including

[31] *Id.* at 49.

[32] *Id.* at 49–50.

[33] *Id.* at 50.

[34] The report suggests that there could be First Amendment issues related to regulation involving open source software. *Id.* at 59.

standard setting, promoting foundational research and development, and long-term policy projects like digital identity; and (xi) foster a robust and constructive dialogue with the DeFi industry.[35]

The Subcommittee observes that "[m]ost existing regulatory frameworks target the application layer of the DeFi technology stack," but "where risks are not effectively addressed at the application layer, authorities must look elsewhere within DeFi projects."[36] In particular, regulators may target actors at the network, protocol and governance layers since (1) they often wield significant power over network functionality, and (2) they are the actors "most willing and able to work with policymakers to mitigate risks that cannot be effectively addressed at the application layer."[37]

According to the Subcommittee, regulatory responses may involve disclosure, reporting, third-party auditing, entry restrictions, regulatory supervision, governance regulation, conduct regulation, product regulation, balance sheet regulation, activity restrictions, structural regulation or resolution planning.[38] In crafting an appropriate response, the report suggests that policymakers should consider the fact that "[b]usiness models built on smart contracts, automation, programmability, and composability open the door to integrating … risk monitoring and mitigation capabilities directly into the technological architecture."[39] The report also offers that policymakers may determine "what an optimal level of decentralization may be for a particular category of DeFi project, enterprise or ecosystem."[40]

Issues for Industry

The report identifies several specific issues where market participants and industry thought leaders can provide support. Those areas include (i) promoting industry leadership in technical standard setting and infrastructure and solutions development, (ii) incorporating regulatory considerations at an early stage in DeFi development, (iii) building dynamic regulatory compliance into DeFi protocols and systems, and (iv) fostering a robust and constructive dialogue with regulators and policymakers.[41]

---

[35] *Id.* at 52.

[36] *Id.* at 54.

[37] *Id.* at 55.

[38] *Id.* at 56–57.

[39] *Id.* at 57.

[40] *Id.* at 58 (emphasis in original).

[41] *Id.* at 66.

Recommendations

In the last section of the report, the Subcommittee makes five general recommendations for policymakers and industry to better understand and mitigate the risks presented by DeFi. The report includes recommendations and key questions related to those recommendations.

"The first priority for policymakers," the report suggests, "should be to increase their capacity to understand DeFi, including by identifying what they do and do not know yet about DeFi."[42] In particular, policymakers will need to identify the "data, expertise, and other resources they need in order to gather and analyze more data about the size, scope, economic structure, and key technological features of DeFi today," and then "armed with these resources, policymakers should develop and execute a strategy for gathering … data for the purposes of constructing a more detailed map of existing DeFi projects, enterprises, and ecosystems."[43] The map should "seek to measure and highlight key financial and technological interconnections and threat vectors, including the use of leverage, concentration in the provision of key products and services, and potential cybersecurity vulnerabilities."[44] To the extent possible, "it should also seek to identify the principal users of DeFi products and services, along with their level of financial and technological sophistication."[45]

Second, policymakers should use the "mapping exercise" to determine which DeFi projects fall within the current perimeter of US financial regulation, as well as other nonfinancial regulatory regimes.[46] One difficulty for this step, according to the report, is determining the "degree of control and influence over a DeFi project, enterprise, or ecosystem [that] warrants regulating it as a common entity."[47]

Third, policymakers must "systematically identify, define, and catalog the risks arising in connection with DeFi projects, enterprises, and ecosystems."[48] Here, the report lists additional risks, including liquidity and maturity mismatches, over-leverage, algorithmic discrimination, and oracle exploitation.[49]

Fourth, policymakers must "identify and evaluate the range and likely effectiveness of regulatory strategies and other risk mitigation mechanisms that might be used to address the risks arising in

---

[42] *Id.* at 68–69.

[43] *Id.*

[44] *Id.* at 68.

[45] *Id.*

[46] *Id.* at 69.

[47] *Id.* at 70.

[48] *Id.*

[49] *Id.*

connection with DeFi projects, enterprises, and ecosystems."[50] The report lists the regulatory options described above (disclosure, regulatory reporting, etc.). Again, the difficulty will be finding "key points of responsibility or control that could theoretically provide the basis for the imposition of regulatory obligations."[51]

Finally, policymakers should "develop a strategy for fostering greater engagement and collaboration on several fronts," including by coordinating with domestic regulators; working with stakeholders like the National Institute of Standards and Technology to play a more active and constructive role in the development of common technological, operational, cybersecurity, governance and other standards for use in the DeFi industry; fostering a more constructive dialogue with entrepreneurs, developers and builders of DeFi projects; and fully engaging with efforts in various international fora.[52]

The Subcommittee also offers specific guidance on the application of its five-step process to AML and identity in DeFi. So, for example, at step four (i.e., the regulatory options step), the report explains that a potential policy response could involve "determining what level of identity information must be collected and leveraged by different financial actors in the system at different layers of the DeFi stack."[53]

Conclusions

The Subcommittee's report is an important development in the United States concerning the regulation of DeFi. While this document may only reflect the views of a few market participants and interested parties, it reinforces the CFTC's role as a thought leader and constructive contributor to US federal regulatory policymaking. Interested parties should review and provide feedback on the report, as the TAC and the CFTC will use the document as a marker for any future action.

---

[50] *Id.* at 72.

[51] *Id.*

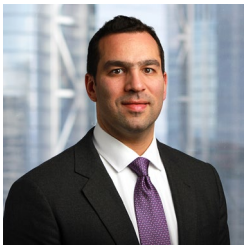
[52] *Id.* at 72–73.

[53] *Id.* at 71.

Contributors

Matthew B. Kulkin
PARTNER

Matthew.Kulkin@wilmerhale.com
+1 202 663 6075



Zachary Goldman
PARTNER

Zachary.Goldman@wilmerhale.com
+1 212 295 6309

Tiffany J. Smith
PARTNER

Tiffany.Smith@wilmerhale.com
+1 212 295 6360

Ayana Dow
ASSOCIATE

Ayana.Dow@wilmerhale.com
+1 202 663 6296

Joshua Nathanson
ASSOCIATE

Joshua.Nathanson@wilmerhale.com
+1 202 663 6193