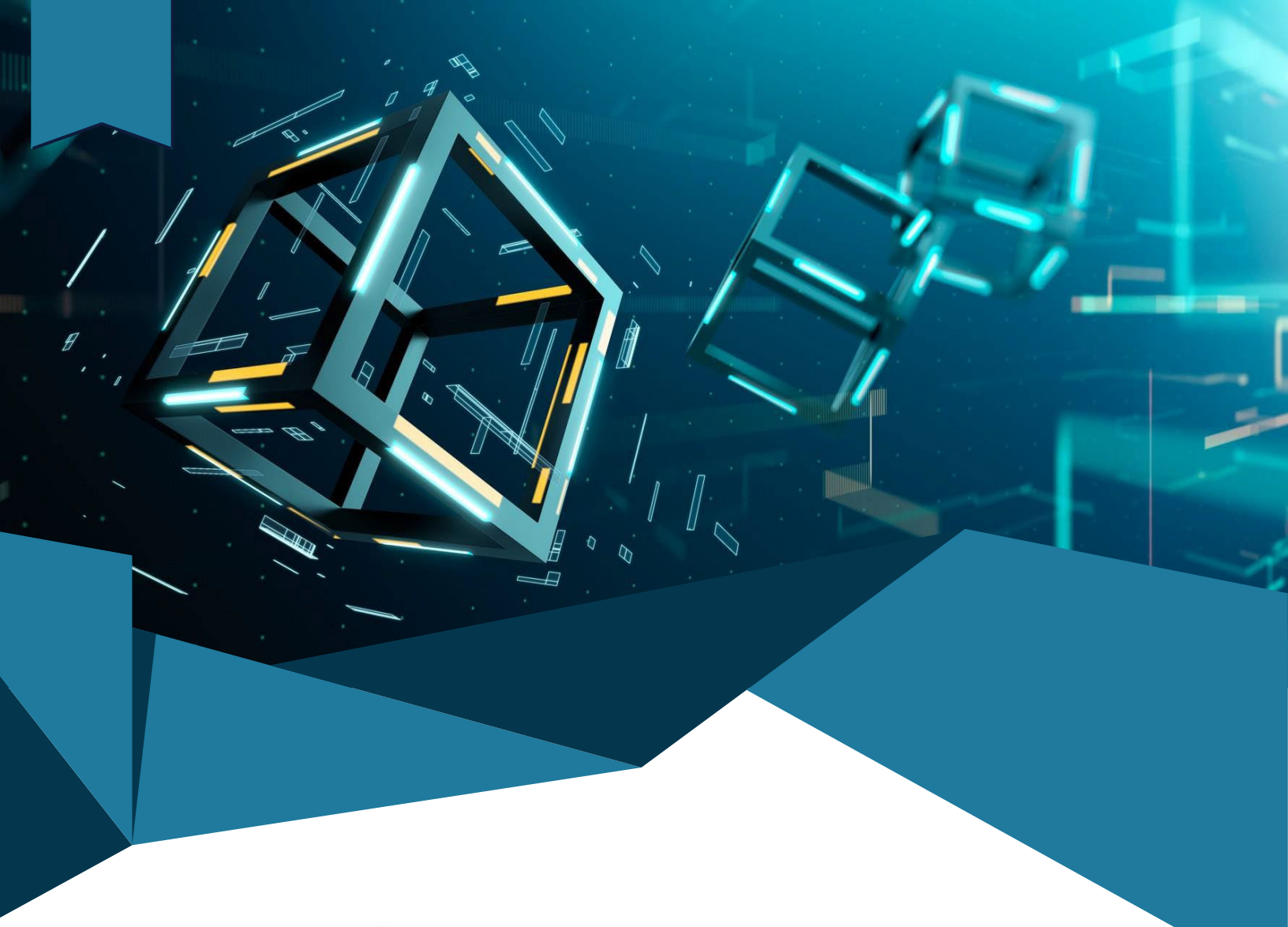


DECENTRALIZED FINANCE

REPORT OF THE SUBCOMMITTEE ON DIGITAL ASSETS AND BLOCKCHAIN TECHNOLOGY,
TECHNOLOGY ADVISORY COMMITTEE (TAC) of the
U.S. COMMODITY FUTURES TRADING COMMISSION

This report has been approved by the Subcommittee on Digital Assets and Blockchain Technology (Subcommittee) of the Technology Advisory Committee's (TAC). The views, analyses, and conclusions expressed herein reflect the work of the Subcommittee, and do not necessarily reflect the views of the TAC, the Commodity Futures Trading Commission or its staff, or the U.S. Government. Reference to any products, services, websites, organizations, or enterprises, or the use of any organization, trade, firm, or corporation name is for informational purposes only and does not constitute endorsement, recommendation, or favoring by the U.S. Government.

To view individual Technology Advisory Committee members' statements, please see cftc.gov.

Table of Contents

DECENTRALIZED FINANCE

REPORT BY THE SUBCOMMITTEE ON DIGITAL ASSETS AND BLOCKCHAIN TECHNOLOGY, TECHNOLOGY ADVISORY COMMITTEE (TAC) of the U.S. COMMODITY FUTURES TRADING COMMISSION

Commissioner Christy Goldsmith Romero, Sponsor
Scott W. Lee, Senior Counsel & Policy Advisor, Office of Commissioner Goldsmith Romero
Carole House, Co-Chair
Dan Awrey, Co-Chair
Anthony Biagioli, Designated Federal Officer

Executive Summary

Decentralized Finance (DeFi) presents promising opportunities and complex, significant risks to the U.S. financial system, consumers, and national security. Since the launch of Bitcoin, applications leveraging blockchain and other distributed ledger technologies have grown exponentially. These technologies hold out the promise of greater transparency and efficiency, expanded access to basic financial products and services, and a more resilient financial system. Yet this promise has also come with very significant risks. In the absence of effective regulation, enforcement, and compliance, many of these DeFi projects, enterprises, and ecosystems have been vulnerable to fraud, mismanagement, and serious regulatory violations. These risks have been compounded by periods of extremely high market volatility, exposing investors, customers, and other stakeholders to significant losses.

The benefits and risks of DeFi depend significantly on the design and features of specific systems. We outline a conceptual framework for understanding and taking steps to address these opportunities and risks across these diverse enterprises, projects, and ecosystems. This framework is not grounded in the sometimes grandiose visions of DeFi industry leaders, but instead a more technical understanding of the core features of DeFi, the current state of play, and the likely consequences—both positive and negative—stemming from its continued development and growth.

A central concern relating to DeFi systems is the *lack of*, and some industry designs to avoid, *clear lines of responsibility and accountability*. This feature of DeFi systems may present the clearest way in which DeFi poses risks to consumers and investors, as well as to financial stability, market integrity and illicit finance—it implicates no clear route to ensuring victim recourse, defense against illicit exploitation, or the ability to insert necessary changes and controls during periods of crisis and network stress. Policymakers have little incentive, and in fact would be remiss in their duties, to permit the growth of financial ecosystems with no mechanisms to ensure necessary protections for their consumers, nations, and societies. The DeFi industry must come to terms with accountability and would benefit from being a leading voice in shaping what that looks like.

The central message of this report is that both government and industry should take timely action to work together, across regulatory and other strategic initiatives, to better understand DeFi and advance its *responsible* and *compliant* development. Simply ignoring the emergence, development, and adoption of DeFi, or failing to fully engage with broader international efforts to build and regulate DeFi projects, enterprises, and ecosystems, pose great risks for irresponsible and destabilizing developments that could harm markets, consumers, and U.S. national security. Responsible innovations in regulatory strategies, DeFi solutions, and regulatory technologies (RegTech) can help the United States better manage DeFi risks and best harness their positive potential.

Key Findings of the Report

The defining feature of DeFi enterprises, projects, and ecosystems is that they are 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. DeFi proponents aim to achieve a financial system running on self-executing computer code, available to anyone on the planet with a computer and internet connection. In reality, only some business models meet this vision of high decentralization, with many systems featuring network designs that have highly centralized information flows, control rights, and, ultimately, risks.

Understanding DeFi systems is extremely complex, requiring an examination of features of decentralization in enterprises, projects, and ecosystems across several dimensions: *access*, *development*, *governance*, *finances*, and *operations*. DeFi enterprises, projects, and ecosystems employ a variety of technologies to achieve various aspects of functional decentralization—which also typically includes a high degree of automation. These technologies include open source software, smart contracts, decentralized applications (DApps), distributed ledgers, decentralized autonomous organizations (DAOs), and oracles. Not all of these dimensions will be present in every DeFi project, nor will each dimension be equally important from a policy perspective.

Most DeFi systems are not completely decentralized or centralized, but instead fit on a multi-level spectrum of (de)centralization, varying along each of the functional and technical dimensions. This creates a challenge in defining specific business and technology models that would make a system "sufficiently decentralized," especially given the incentives for policymakers to ensure that accountability exists in systems supporting high risk activity. The more dimensions of decentralization observed, and the greater the use of technologies designed to achieve decentralization, as well as lesser concentration across the economic functions performed by the application or system, the more likely it is that an enterprise, project, or ecosystem should be viewed as decentralized.

The architecture of DeFi involves key components across mutually supporting layers of technology and functionality critical to the delivery of financial products and services, specifically the *physical/hardware*, *protocol*, *network*, *data*, *application*, *user*, *asset and market*, and *governance* layers; all working to support operations and communications across networks with varying degrees of core characteristics of *programmability and composability*, *automation*, *transparency*, *openness*, and *immutability and censorship resistance*. Understanding the risks associated with a given project, enterprise, or ecosystem requires an in-depth understanding of the nature and level of decentralization as well as the extent of the system features supported at each individual layer. Each layer may also present opportunities to embed technical features designed to support system security, transparency, privacy, interoperability, and regulatory compliance.

FIGURE A: 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)

Policymakers should align regulatory strategies in pursuit of a balance across all desired regulatory objectives or outcomes in DeFi innovation, including: customer and investor protection, promoting market integrity, ensuring microprudential safety and soundness, financial stability and mitigating systemic risk, combating illicit finance and protecting national security, reinforcing and securing U.S. competitiveness and leadership, and expanding access to safe and affordable financial services. Defining these policy objectives, and the system attributes needed to support them, can serve as a touchstone for examination and debate around what regulation can and should be designed to achieve, in assessing existing coverage and potential changes to the regulatory perimeter for DeFi, and for policymakers to evaluate the success of regulatory frameworks, compliance, and enforcement.

Decentralized networks and technologies operating largely on public, un-obfuscated ledgers present opportunities to leverage efficiency improvements in payments and financial markets, more transparent and auditable financial services, enhanced financial sector resilience, dismantled barriers to access to financial services, promotion of innovation and competition, and reinforced U.S. leadership in technology and finance. There has been significant experimentation in DeFi across both institutional and disruptive actors that brings realized and potential benefits for areas like illicit finance investigations, market and system monitoring, promotion of competition, and enabling greater consumer control and access offered in open and decentralized financial services. However, the current reality of the market, technology, and policy environment may not reflect conditions necessary to most fully realize the opportunities presented by these systems.

Policymakers should understand the type, nature, sources, probability, and potential impact of identified risks presented by DeFi. The decentralized structure of DeFi networks poses a number of significant and, in many respects, unique risks for:

- **Investors and consumers.** Risks include lack of technology and DeFi literacy across consumers, fraud, market manipulation, conflicts of interest, data breaches and undesirable privacy violations, custody risk, bankruptcy risk, and algorithmic discrimination that can harm consumers, as well as a lack of clear lines of responsibility that can minimize recourse for victims.

- **Market integrity.** Risks include vulnerabilities to wash trading, front running, and pump and dump schemes, as well as oracle exploitations that could be used to undermine markets. These are complicated further by the lack of clear lines of responsibility to embed mitigation mechanisms, inhibiting systems' abilities to respond to unexpected events and foster trust.

- **DeFi projects, enterprises, and ecosystems.** These include complex and hard to map counterparty risks, enhanced reliance on outsourcing relationships, limited control rights during periods of institutional or systemic stress, software security vulnerabilities, and the potential for automated "hardwired" failure.

- **Financial system stability.** While the scale, scope, and importance of DeFi does not currently threaten financial system stability, as these projects grow they may present cross-sectoral systemic risks as well as risks derived from complex interconnections with significant economic and technological exposures, concentration risks, and hardwired procyclicality.

- **Combating illicit finance, protecting national security, and maintaining U.S. leadership.** Experts have long discussed risks that the ongoing development and growth of financial institutions and networks outside of the United States may pose to national security and U.S. leadership—including the risks stemming from the emergence of geopolitical competitors. While these challenges transcend DeFi, further transitioning significant financial projects, enterprises, and ecosystems offshore—including those related to DeFi—could potentially compound these challenges in the long term. Associated risks presented by this loss in leadership could include loss or diminishing of geopolitical status as provider of the global reserve and transaction currency, and loss of surveillance and accountability enforcing capacity to combat illicit finance and safeguard national security.

- **Climate.** Risks include significant energy consumption, pollution, noise, and other environmental impacts.

To successfully develop and implement regulatory strategies in a space with very complex business models and technologies, as well as a challenging environment for dialogue, policymakers will have to address several core issues:

- **Determining whether and how DeFi systems fall within the existing regulatory perimeter.** This will involve assessing subject matter and geographic jurisdiction over DeFi, evaluating coverage of *financial* and *non-financial* policy and regulatory regimes, and navigating the nuances of focusing on technology-neutral activities that can face challenges with scaling application versus technology-specific approaches that face challenges of coverage as technology evolves.

- **Identifying whether, where, and how the regulatory perimeter might need to be expanded.** After thoroughly evaluating and understanding the risks presented by each of the diverse business models, features, and operations across DeFi systems, policymakers should determine where in the DeFi stack to locate responsibility for regulatory compliance. Defining an appropriate regulatory approach will require examining the *feasibility*, *proportionality*, *usefulness*, and *costs* of different strategies.

- **Crafting the appropriate regulatory response.** Having determined appropriate targets for regulation, policymakers can leverage a variety of regulatory strategies: disclosure, reporting, third-party auditing, entry

restrictions, regulatory supervision, governance regulation, conduct regulation, product regulation, balance sheet regulation, activity restrictions, structural regulation, and resolution planning.

- **Allocating responsibility and accountability for regulatory compliance in a world of decentralized governance.** Locating and enforcing responsibility in DeFi systems, needed to ensure their security and stability, can be difficult; it involves navigating complex and novel issues such as regulation and accountability involving software code and First Amendment arguments, as well as determinations of entities and "personhood."

- **Mapping counterparty exposures in a world of decentralized balance sheets.** Policymakers should consider how to identify and monitor critical interdependencies across DeFi balance sheets, along with the potential channels they create for the spread of contagion and cross-sectoral systemic risks.

- **Mapping key service providers and services in a world of decentralized operations.** Even highly decentralized systems often involve a small group of core developers and other key service providers. Mapping providers, roles, and their risk indicators could be critical for detecting the actions of malevolent actors or potential threats to network stability.

- **Oversight of new and rapidly evolving technology.** Industry and RegTech solutions as well as regulatory authorities' own capabilities will have to evolve to enable oversight to keep pace with technological evolutions. The potential promise of DeFi's transparency and ability to build in regulatory compliance features will not be realized without regulators gaining greater confidence that DeFi systems will work as designed and intended in times of crisis.

- **Ensuring DeFi lives up to critical policy objectives like expanded access, necessary transparency, and responsible governance.** Ensuring achievement of these goals involves a combination of "stick" and "carrot" approaches, with responsibilities owed by industry and by government. Policymakers will have to consider addressing lagging implementation of policy frameworks across many jurisdictions, challenges with timeliness and efficacy of enforcement, as well as identifying key partnerships with industry to drive needed market shifts.

- **Mitigating the unique threats DeFi poses.** Policymakers should address the specific and unique threats posed by DeFi to ensure a properly calibrated risk-based approach that does not inadvertently box in regulation and compliant innovation targeting antiquated risks, nor permit the unconstrained build-up of concentration or interconnectedness, along with the corresponding cascading risks, as DeFi grows and becomes more integrated with the broader financial system.

- **Identifying the best role for policymakers in building DeFi, including in standards, research, and fostering identity infrastructure.** Agencies cannot bring the DeFi space into compliance through enforcement alone, but must also determine how to best use long-leveraged authorities to drive positive developments in the ecosystem. Given long lead times for these efforts and the potential benefits for certain building blocks of DeFi to also reap utility across TradFi and beyond, policymakers should consider how to accelerate standards development, research and development (R&D), and identity solutions that can support responsible DeFi.

- **Fostering a robust and constructive dialogue with industry.** Tensions between different sides on DeFi debates have delayed meaningful progress on critically needed regulatory agendas, as well as partnerships to foster greater responsibility in the space like standards and information sharing efforts. Policymakers should consider how to sponsor, tailor, and participate in robust and constructive dialogue with major stakeholders in the DeFi ecosystem to drive consequential change.

Industry players also hold distinct responsibility and capabilities to shape responsible development in DeFi, especially through integration of compliance and security measures that will likely enhance the sector's success with wider adoption and trust across enterprises and consumers. To achieve this trust and fulfill this role in shaping the sector, the DeFi industry will have to address key issues:

- **Promoting industry leadership in technical standard setting and infrastructure and solutions development.** The DeFi industry has struggled to organize around building and implementing technical standards for security and compliance features in DeFi platforms, and has even struggled to integrate long-existing standards into their systems. Industry stakeholders must consider how they can effectively convene and participate in standards efforts that can give critical roadmaps to entrepreneurs and builders as they develop new applications in DeFi.

- **Incorporating regulatory considerations at an early stage in DeFi development.** Engineers will have to look to policy objectives and regulatory obligations as technical requirements for DeFi projects, considering where within the architecture of their systems the most effective and economical application of controls and security features would best meet these requirements.

- **Building dynamic regulatory compliance into DeFi protocols and systems.** Features to secure against market manipulation, illicit finance, and cybercrime will need to evolve as new typologies and vulnerabilities are discovered, changing their risk profiles, and as automation by both licit and illicit actors demands an increase in sophistication, timeliness, accuracy, and assurance of compliance mechanisms, which at present have generally not achieved a level of automation that would make them useful in DeFi systems.

- **Fostering a robust and constructive dialogue with regulators and policymakers.** Industry will need to consider how to adapt messaging and engagement to improve perceptions by and collaboration with policymakers. This may benefit from industry adopting an honest accounting for failures and successes in the current state of the industry and prioritizing wherever possible data-driven examination and debate of specific measures to drive forward progress.

Key Recommendations

A complete discussion of the report's recommendations, and key questions needed to be addressed for their implementation, can be found in Chapter V of this report.

Resource assessment, data gathering, and mapping. The first priority for policymakers should be to increase their technical capacity and understanding, including by identifying what they do and do not yet know about DeFi. To better map and understand these systems, we recommend that policymakers take the following actions:

- Increase their capacity to understand DeFi, including through mapping their data, expertise, and resources needed.
- Conduct a gap analysis and address critical capability gaps.
- Research and analyze key factors driving emergence, evolution, and growth of DeFi.
- Create a strategy for continuous data gathering and monitoring state of DeFi.
- Scale partnerships and information sharing across regulatory authorities to harmonize regulatory frameworks, data collection, and enforcement actions.

In conducting resource assessments and mapping of DeFi systems, policymakers will generally have to address key questions related to the types of data needed to understand DeFi, where to get it, and what issues DeFi versus TradFi systems may be better positioned to address.

Survey the existing regulatory perimeter. Policymakers should use the mapping exercise as the basis for determining whether and how DeFi systems, including the wide range of activities and functions they perform, currently bring them within the perimeter of U.S. financial and non-financial regulation. We recommend the following actions in conducting this survey:

- Identify existing regulatory frameworks applied to mapped DeFi systems.
- Assess the compliance level of DeFi projects.
- Identify needed points of expansion to address residual risks presented by DeFi.
- Partner with state and self-regulatory bodies to more fully assess the U.S. regulatory touchpoints of DeFi.
- Compare U.S. regulatory perimeter and compliance against peer nations.
- Support state and international capacity building.

Policymakers will be faced with key questions in conducting this survey, relating to threshold conditions for application of the frameworks, mapping regulatory objectives to DeFi, and degrees of control and influence over DeFi warranting regulation.

Risk identification, assessment, and prioritization. Policymakers should seek to systematically identify, define, and catalogue the risks arising in connection with DeFi, including those pertaining to asymmetric information and conflicts of interest, operational and security vulnerabilities, liquidity and maturity mismatches, over-leverage, hardwired algorithmic failures and procyclicality, complexity and concentration risks in DeFi compositions, and market manipulation and illicit finance. This process can help policymakers distinguish between categories of DeFi and prioritize policy and enforcement efforts. We recommend that policymakers:

- Comprehensively map and catalogue players and interconnections across DeFi ecosystems and their specific risks.
- Identify and prioritize projects of greatest concern based on nature and scale of the risk and gaps in existing frameworks.
- Identify and address discrete information gaps, whether caused by information availability or analytic capability.
- Prioritize policy goals for DeFi, accounting for at least the objectives outlined in this report: customer and investor protection, promoting market integrity, ensuring microprudential safety and soundness, financial stability and mitigating systemic risk, combating illicit finance and protecting national security, reinforcing and securing U.S. competitiveness and leadership, and expanding access to safe and affordable financial services.

Policymakers will face key questions related to how specific risks map onto specific DeFi systems as well as the specific information needed by policymakers, industry, and consumers to make critical measurements and decisions pertaining to risks presented by DeFi.

Identifying and evaluating the range of potential policy responses. In conjunction with the risk assessments, policymakers should evaluate the range and likely effectiveness of regulatory strategies and risk mitigations for DeFi. This requires assessing specific measures and obligations as well as identifying the key points of responsibility and control that can provide the basis for imposition of regulatory obligations. Policymakers should take a series of actions to evaluate the range of policy responses to DeFi:

- Inventory range of existing regulatory and risk-mitigating mechanisms (*e.g.,* disclosure, third-party auditing, etc.).

- Determine which mitigation mechanisms would be most effective for specific risks.
- Identify additional regulatory authorities needed to address residual risks.
- Drive strategies and resourcing to scale timeliness and efficacy of regulatory enforcement.
- Debate and define information and identity privacy, availability, and discoverability requirements for DeFi.
- Surge policy and infrastructure development efforts for digital identity.

Policymakers should address questions related to the calibration of regulatory treatment of both financial and non-financial activities occurring over the same rails; how to define the best information to inform consumers of DeFi risks; how to harmonize approaches to software security across various related issues like cybersecurity, artificial intelligence, and DeFi; and how best to measure tradeoffs in security and innovation, including in regulatory mandates.

Fostering greater engagement and collaboration with domestic and international standard setters, regulatory efforts, and DeFi builders. Policymakers should develop a strategy for fostering greater engagement and collaboration within the domestic regulatory community, with standards and research bodies (such as the National Institute of Standards and Technology NIST), as well as with the DeFi industry to establish not only policy objectives but also the means by which to achieve them. There are several specific actions that we recommend policymakers take:

- Leverage Federal Advisory Committee Act (FACA) and other engagement authorities, as well as interagency collaboration fora, to foster greater dialogue and information sharing.
- Drive development of real-time, operational information sharing partnerships to detect, identify, and disrupt illicit financial flows in DeFi and address cybersecurity issues.
- Promote U.S. leadership in international standards setting and R&D efforts, including through bilateral and multilateral pilots and experimentation.
- Stand up coordinated, outcome-oriented R&D efforts across agencies, DeFi, and RegTech sectors, including through outcome-defined tech sprints, grants, and risk-based regulatory relief.

To create a more robust set of partnerships and discourse across key government and industry stakeholders, policymakers should consider key questions relating to defining and scoping limited and broad relief from regulatory obligations in sandboxes to promote experimentation, along with impacts of international framework timelines and implementations on efficacy of the U.S. approach.

Apply recommended framework to drive near-term, prioritized progress on digital identity, "know your customer" (KYC) and anti-money laundering (AML) regimes, and calibration on privacy in DeFi. The pseudonymity and disintermediation provided in most DeFi systems presents serious concerns for policymakers focused on ensuring AML and countering financing of terrorism (AML/CFT) regimes are effective and provide appropriate protections and victim recourse for consumers. In high-value, highly sensitive activities like finance, there must be a balance between discoverability and validation with privacy and burden considerations, achieved through rigorous debate and evaluation to determine (a) what information should (b) be discoverable to whom (c) under what conditions.

Policymakers should prioritize a surge of policy and R&D efforts, informed by persistent engagement with key government and industry stakeholders, to address identity and privacy issues in DeFi:

- Map ecosystem players and business operations involving identity processes and data, as well as what identity data is possible to exist or collected at different DeFi layers.

- Assess identity information compliance and requirement gaps against what is most useful to support regulatory objectives like AML/CFT and illicit finance investigations.
- Identify the specific risks, vulnerabilities, and unintended consequences associated with identity discoverability, verification, and monitoring across DeFi.
- Evaluate options, benefits, and costs for KYC, such as identity discoverability and verification across DeFi, including considering options for gradations of identity information and privacy at different layers in the stack, permitting reliance on regulated identity service providers to a DeFi system, and differentiating between financial and non-financial activity.
- Surge partnerships in R&D, standards efforts, and operational action, such as through issuance of strong digital credentials and infrastructure development, across government and industry stakeholders.

Near-term action on identity is both warranted and possible: the perils presented by the absence of sufficient identity controls and solutions are already present within the ecosystem, and there are also clear areas for government and industry action that can drive creation of frameworks and identification of key roadblocks to address, to ultimately arrive at acceptable solutions that help not just DeFi, but future digital infrastructure across payments and broader digital commerce.

Members of the Subcommittee on Digital Assets and Blockchain Technology

The CFTC seeks to ensure that all of its advisory committee and subcommittee memberships are fairly balanced. To that end, the selection of the Subcommittee on Digital Assets and Blockchain Technology members was consistent with the TAC Federal Advisory Committee Act Charter and Membership Balance Plan. The Subcommittee members were selected to ensure that the subcommittee's membership consists of a wide range of perspectives and interests, including representation from industry, public interest groups, and academia.

Name	Entity Representing	Position Title
Carole House (Co-Chair; TAC Chair)	Terranet Ventures, Inc.	Executive in Residence
Dan Awrey (Co-Chair)	Special Government Employee	Professor of Law, Cornell Law School
Nikos Andrikogiannopoulos	Metrika	Founder & CEO
Christian Catalini	Lightspark	Co-Founder & Chief Strategy Officer
Jonah Crane	Klaros Group	Partner
Sunil Cutinho	CME Group	Chief Information Officer
Cantrell Dumas	Better Markets	Director, Derivatives Policy
Dan Guido	Trail of Bits	Co-Founder & CEO
Jill Gunter	Espresso Systems	Chief Strategy Officer
Stanley Guzik	S&P Global Commodity Insights	Chief Technology Officer
Ben Milne	Brale	Founder & CEO
John Palmer	Cboe Global Markets, Inc.	Representative
Ari Redbord (TAC Vice Chair)	TRM Labs	Head of Legal and Government Affairs

Name	Entity Representing	Position Title
Michael Shaulov	Fireblocks	CEO
Emin Gün Sirer	Ava Labs	Founder & CEO
Justin Slaughter	Paradigm	Policy Director
Corey Then	Circle	Vice President, Global Policy
Adam Zarazinski	Inca Digital	CEO
Jeffery Zhang	Special Government Employee	Assistant Professor of Law, University of Michigan Law School

List of Tables and Figures

Executive Summary

Report

I. Introduction

This report is presented to the CFTC with the aim of providing a framework for policymakers and industry in approaching the regulation of DeFi. Its objective is to identify and analyze the nature and dimensions of DeFi, the current and future opportunities and risks presented by it, and the key issues for both policymakers and industry leaders. The report concludes by identifying a number of outstanding questions for policymakers and articulating a series of recommendations for further action.

The report frames the opportunities and risks presented by DeFi in light of several important policy objectives. These objectives include consumer and investor protection, promoting market integrity, ensuring microprudential safety and soundness, maintaining financial stability, expanding access to safe and affordable financial products and services, combatting illicit finance, and strengthening U.S. leadership and competitiveness in the realm of both finance and technology. The analysis considers the diversity of DeFi applications, the unique risk profiles of different business models, network structures, and use cases, and critical questions around where and how to allocate responsibility for regulatory compliance within decentralized actors and ecosystems, along with the appropriate role for both regulators and industry players in addressing the myriad of risks posed by DeFi.

More broadly, the report is intended to help inform ongoing policy debates in Congress, state legislatures, regulatory agencies, and international financial standards bodies. The report's recommendations should also be of interest to industry leaders that are ultimately responsible for adopting a constructive posture towards regulatory compliance, implementing any necessary regulatory controls, and driving socially desirable innovation. The report will also be of interest to the American people, the ultimate consumers of the financial products and services offered by the DeFi industry, who for better or worse will be the ones most affected by the decisions made by both policymakers and industry leaders. And more generally, this report reflects the reality that policymakers, industry, and consumers would all benefit from a deeper understanding of the key features of DeFi projects, enterprises, and ecosystems, along with a detailed roadmap for how to make the most of its opportunities while mitigating its attendant risks.

This past October marked 15 years since the launch of Bitcoin (BTC).[1] Over this span, applications leveraging blockchain and other distributed ledger technologies have grown exponentially. These technologies hold out the promise of greater transparency and efficiency, expanded access to basic financial products and services, and a more resilient financial system. This promise was at the heart of a boom in blockchain-based financial technology (FinTech) innovation: with thousands of new DeFi projects, enterprises, and ecosystems emerging to harness this new technology for purposes ranging from asset tokenization, to improving trade finance and supply chain management, to coordinating humanitarian relief efforts.[2] At their peak, these DeFi projects, enterprises, and ecosystems enjoyed a collective market capitalization of over $3 trillion[3].

[1] *See* Bitcoin genesis block (2009); Satoshi Nakamoto, Bitcoin White Paper, "Bitcoin: A Peer-to-Peer Electronic Cash System" (October 31, 2008).

[2] *See, e.g.*, United Nations High Commissioner for Refugees, "UNHCR launches pilot Cash-Based Intervention Using Blockchain Technology for Humanitarian Payments to People Displaced and Impacted by the War in Ukraine" (December 15, 2022).

[3] *See* CoinGecko, Global Cryptocurrency Market Cap (November 9, 2021).

Yet this promise has also come with very significant risks. In the absence of effective sufficient regulation, enforcement, and compliance, many of these DeFi projects, enterprises, and ecosystems have been vulnerable to fraud, mismanagement, and serious regulatory violations. These risks have been compounded by periods of extremely high market volatility, exposing investors, customers, and other stakeholders to significant losses. In 2022 alone, the cryptocurrency market lost over $2 trillion in market capitalization.[4] While some of these losses were connected to the bankruptcy of centralized cryptocurrency exchanges, they nevertheless illuminate ongoing concerns surrounding insufficient due diligence by investors, significant regulatory gaps, a lack of effective industry self-policing, and the widespread failure to promote a culture of regulatory compliance. Like almost any new technology or business model, DeFi thus presents both significant promise and perils.

This report develops a conceptual framework for understanding and taking steps to address these opportunities and risks. This framework is not grounded in the sometimes grandiose visions of DeFi industry leaders, but instead a more technical understanding of the core features of DeFi, the current state of play, and the likely consequences—both positive and negative—stemming from its continued development and growth. Part II begins by defining DeFi, outlining its key technological and functional dimensions, and describing some of its current and potential future use cases. This is followed in Part III by a discussion of key policy objectives, opportunities, and risks. Part IV then outlines the key issues identified by the TAC for further considerations by policymakers and industry stakeholders. Building on these key issues, Part V closes with a list of specific questions for further examination and a series of recommendations for further action.

[4] *See* Cheyenne DeVon, CNBC, "Bitcoin Lost Over 60% of Its Value in 2022—Here's How Much 6 Other Popular Cryptocurrencies Lost" (December 23, 2022).

II. Defining DeFi: A Technological and Functional Approach

There is nothing particularly new about business models that disaggregate economic functions or allocate responsibility for the delivery of vital inputs to multiple different actors. At the firm level, the canonical business decision about whether to "make" or "buy" is ultimately a question of whether an enterprise should produce a given intermediate product or service internally, or purchase it from an arm's-length party on the open market.[5] These firm- level decisions can then be observed at the industry level, where the length and complexity of modern supply chains reflect the value of specialization, and thus decentralization, across vast swathes of the global economy.[6] Even in finance, where centralized financial intermediaries have long played a dominant role, there is still often a high degree of decentralization: witness for example the "fragmentation nodes"[7] and "shadow intermediation chains"[8] that emerged in the years leading up to the global financial crisis and, more recently, the rise of "banking-as-a-service" (BaaS) and other platform-based business models.[9]

This observation—that decentralization is itself neither particularly novel nor uncommon—raises an important question. Specifically: what, if anything, sets DeFi apart from more conventional financial markets and institutions? The first part of this report explores this critical threshold question. The objective of this exploration is not to advance a definitive definition of DeFi that might one day provide the basis for a new or expanded regulatory perimeter. Given that DeFi is still a nascent and rapidly evolving technology, articulating a single, tractable, and all-encompassing definition would be extremely difficult. For the same reasons, designing regulatory frameworks around a specific technology may not be particularly desirable from a policy perspective. Accordingly, while we offer a working definition of DeFi for the purposes of this report, our objective at this stage is to provide a functional definition that highlights the combinations of features and technologies that DeFi can reasonably be understood to encompass. This understanding then provides a springboard for the discussion and analysis in subsequent sections of the report about the specific opportunities and risks that DeFi presents, the challenges it poses for both the DeFi industry and policymakers and, ultimately, how best to move forward.

[5] *See* Ron Coase, *The Nature of the Firm*, 4 Economica 386 (1937); Oliver Williamson, *Transaction-Cost Economics: The Governance of Contractual Relations*, 22(2) Journal of Law and Economics 233 (1979). For a more detailed discussion of blockchain technology using a Coasian frame, see Michael Casey, Jonah Crane, Gary Gensler, Simon Johnson & Neha Narula (eds.), "The Impact of Blockchain Technology on Finance: A Catalyst for Change", 21 Geneva Reports on the World Economy 13-16 (July 16, 2018).

[6] *See, e.g.*, White House, "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-based Growth" (June 2021).

[7] *See* Kathryn Judge, *Fragmentation Nodes: A Study in Financial Innovation, Complexity, and Systemic Risk*, 64 Stanford Law Review 657 (2012).

[8] *See* Zoltan Pozsar, Tobias Adrian, Adam Ashcraft & Hayley Boesky, *Shadow Banking*, 19(2) Federal Reserve Bank of New York Economic Policy Review 1 (2013).

[9] *See* Erik Feyen, Jon Frost, Leonardo Gambacorta, Harish Natarajan & Matthew Saal, "Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy", Bank for International Settlements Paper No. 117 (July 2021).

(A) Dimensions of Decentralization

FUNCTIONAL DEFI DEFINITION

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.

DeFi has been heralded as both the future of finance and as an existential threat to the integrity and stability of the global financial system. Yet both proponents and critics of DeFi tend to view it as something of a monolith—as if decentralization was a question of all or nothing.[10] This monolithic view stems from the widespread misperception that any project, enterprise, or ecosystem that combines blockchain or other distributed ledger technology with algorithmic automation must necessarily be decentralized. Under this view, the use of this specific technology to provide financial products or services is, by construction, DeFi.

There is a second view of DeFi rooted in the design of financial networks and their technological architecture. Pursuant to this second—often more aspirational—view, ***the defining feature of DeFi enterprises, projects, and ecosystems is that they are 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***.[11] As recently described by the Bank for International Settlements: ***"DeFi is a competitive, contestable, composable and non-custodial financial ecosystem built on technology that does not require a central organization to operate and that has no safety net."***[12] While some blockchain or other distributed ledger networks may fall within this narrower and more precise definition, many will not—typically because their network design envisions highly centralized information flows, control rights and, ultimately, risks. Nevertheless, this second view thus gets to the pith of what many DeFi entrepreneurs ultimately hope to achieve: a financial system that runs on self-executing computer code, available to anyone on the planet with a computer and an internet connection.

In reality, DeFi projects, enterprises, and ecosystems can exhibit decentralization across several different dimensions. These dimensions can be combined in a variety of ways, using a variety of different technologies, thus giving rise to a wide range of different business models. While some of these business models are highly decentralized, others envision important roles for centralized financial, technological, and other intermediaries. Yet others seek to exploit widespread misperceptions about the fundamental nature of DeFi—engaging in so-called "decentralization theatre"—to attract capital and customers. This section seeks to demarcate the different dimensions of decentralization, identify the technologies that make decentralization possible, and create a framework for understanding what business models can be understood as falling into this still nascent and rapidly evolving category. Identifying the dimensions of DeFi can help illuminate the diversity of these projects and provides policymakers with a conceptual framework for describing and categorizing different types of DeFi ecosystems and for identifying and addressing the myriad of potential risks.

[10] *See, e.g.*, Raphael Auer, Bernhard Haslhofer, Stefan Kitzler, Pietro Saggese & Friedhelm Victor, *The Technology of Decentralized Finance (DeFi)*, Bank for International Settlements Working Paper No. 1066 (January 2023).

[11] *Id.* (defining DeFi as "a competitive, contestable, composable and non-custodial financial ecosystem built on technology that does not require a central organization to operate and that has no safety net.").

[12] *Id.*

FIGURE 1. THE DIMENSIONS OF DEFI

		***Functional* dimensions**				
***Technological* dimensions**		access	development	governance	balance sheet	operational
	open source software					
	smart contracts					
	distributed ledgers					
	DApps					
	DAOs					
	Oracles					

The decentralization at the heart of DeFi projects, enterprises, and ecosystems can be observed across at least five dimensions:

- **Decentralized access**. Decentralized access is a function of the legal, technological, and governance barriers to participation in a DeFi project, enterprise, or ecosystem. Where participants can gain access subject only to compliance with the relevant software protocols, this would represent a high degree of decentralized access. Conversely, where participation is limited—by law, technological requirements, or otherwise—to specific types of participants, or where participation is determined by a centralized governance mechanism (*see* below), this would represent a relatively low degree of decentralized access. In the context of blockchain and other distributed ledgers, decentralized access is often associated with "permissionless" networks, whereas centralized access is associated with "permissioned" networks.

- **Decentralized development**. Decentralized development is a function of the number of and distribution of, and relationships between, software developers and engineers working to build, maintain, and update a given DeFi project, enterprise, or ecosystem. Viewed on a spectrum, whereas a small, close-knit team of developers working together at a single firm to build proprietary software would represent a high degree of centralized development, a large number of otherwise independent and potentially anonymous developers working on a project using open source software would represent a high degree of decentralized development. The distribution of the developers can also be further decentralized where DeFi projects, enterprises, and ecosystems use multiple software clients for execution and consensus nodes.

DIMENSIONS OF DEFI

The dimensions of decentralization of DeFi enterprises, projects, and ecosystems can be observed by analyzing five major dimensions: access, development, governance, finances, and operations. The more dimensions of decentralization observed, and the greater the use of technologies designed to achieve decentralization, as well as lesser concentration across the economic functions performed by the application or system, the more likely it is that an enterprise, project, or ecosystem should be viewed as decentralized.

- **Decentralized governance.** Decentralized governance is a function of the distribution of residual control rights in connection with a DeFi project, enterprise, or ecosystem. In theory, DeFi projects, enterprises, and ecosystems seek to use self-executing software to anticipate, capture, and completely automate the decision-making process. In practice, however, reflecting both fundamental uncertainty[13] and the inevitability of incomplete contracting[14], most projects, enterprises, and ecosystems allocate some degree of residual discretion and control to human agents.

  These residual control rights can include decisions about, for example, the design of financial products and services, the technological architecture supporting the delivery of those products and services, or any measures taken to manage the attendant risks. Importantly, they can also include the ability of human agents to override any automated functions where the software malfunctions, the network architecture breaks down, or in other unusual and exigent circumstances. The distribution of these residual control rights can vary greatly across projects, enterprises, and ecosystems. In some cases, and with respect to some decisions, these rights may be concentrated in the hands of a small handful of "core" developers. In other cases, and with respect to other decisions, these rights may be highly dispersed amongst a potentially very large network of passive token holders.

- **Decentralized balance sheets**. Balance sheet decentralization is a function of the distribution of legal and beneficial ownership rights over any assets that are held within a DeFi project, enterprise, or ecosystem, along with the nature, number, distribution, and intertwining of any corresponding liabilities or other legal claims. The defining feature of conventional financial intermediaries is that they use a single, centralized balance sheet to both raise and deploy capital and provide financial products and services to their customers. At the system level, the balance sheets of these intermediaries are then intertwined in a myriad of ways that create dense and often opaque networks of legal and economic exposures.
  In the context of conventional financial intermediation, any decentralization is limited to two specific and relatively narrow circumstances. The first arises where an intermediary raises capital from a large number of investors, especially where this results in the dispersion of residual control rights. The second arises in the limited case where an intermediary's business model envisions that its customers retain beneficial ownership rights in any assets held by the intermediary. Against this backdrop, DeFi theoretically enables balance sheet decentralization along two additional dimensions. First, DeFi—at least in its most extreme forms—envisions replacing centralized financial intermediaries with automated protocols as conduits for pooling capital, allocating this capital for investment, trading the assets connected to these investments, and offering other financial products and services. Second, DeFi enables individual customers to retain direct and full legal ownership over their assets via, for example, the use of encrypted private keys and "unhosted" wallets (*see* below).

- **Decentralized operations**. Operational decentralization is a function of the nature or extent to which a DeFi enterprise, project, or ecosystem outsources critical functions or processes to third parties. These functions and processes can theoretically include: software design, maintenance, and upgrades; transaction processing, validation, and recordkeeping; cybersecurity; and regulatory compliance. Viewed on a spectrum, whereas outsourcing one of these functions or processes to a single-source vendor would represent a relatively low degree of operational decentralization, outsourcing several of these functions or processes to other DeFi projects, enterprises, or ecosystems would represent a relatively high degree of operational decentralization.

[13] *See* Frank Knight, *Risk, Uncertainty and Profit* (1921).

[14] *See* Oliver Hart, *Incomplete Contracts and the Theory of the Firm*, 4:1 Journal of Law, Economic, and Organization 119 (1988).

Not all of these dimensions will be present in every DeFi project, enterprise, or ecosystem. And insofar as these dimensions are not strictly binary, we should also expect to observe significant variance along a spectrum from centralization to decentralization. Nor is it necessarily the case that these dimensions are all equally important from a policy perspective. As explored in greater depth below, many of the key policy challenges that arise in connection with DeFi stem from the question of how to advance important policy objectives like consumer protection, market integrity, and financial stability in a world of decentralized *governance*. Nevertheless, identifying these dimensions can help illuminate the diversity of DeFi, along with the perils of attempting to craft a single, all-encompassing definition. As we shall see, it also provides policymakers with a conceptual framework for describing and categorizing different types of DeFi projects, enterprises, and ecosystems, and for identifying and addressing the myriad of potential risks.

DeFi enterprises, projects, and ecosystems employ a variety of different technologies designed to achieve decentralization across one or more of these dimensions. While some of these technologies—like open source software—are already widely used across a range of commercial contexts, others—like DApps, distributed ledgers, and DAOs—are more closely associated with DeFi. The common denominator underpinning all of these technologies is that they seek to use algorithmic automation to perform tasks central to the delivery of one or more financial products or services.

- **Open source software**. Open source software is source code that is released under a license or other legal framework that enables anyone to freely view, modify, and build on that code. Open source software includes open application programming interfaces or APIs that specify a freely available protocol by which software developers can access software applications or query information available in an open library.

- **Smart contracts**. A smart contract is a computerized protocol that automatically executes an instruction upon the satisfaction of a set of predetermined conditions.[15] Smart contracts generally take the structure of a modus ponens—or "if, then"—statement. While smart contracts may also represent legally binding contracts, this is not necessarily the case.

- **DApps**. A decentralized application or DApp is a software application that is built on a decentralized network and combines one or more smart contracts with a front-end user interface.

- **Distributed ledgers**. A distributed ledger is a database that relies on multiple participants or "nodes" to enter, store, update, and/or verify information in the database. These ledgers rely on consensus algorithms to ensure that the database is accurate and up-to-date across all the nodes in a given network. Participation as a node can either be limited to certain designated participants ("permissioned") or open to anyone that complies with the relevant software protocols ("permissionless").

- **DAOs**. A decentralized autonomous organization or DAO is an organization of individuals making decisions about how to govern a software protocol that enables collective decision-making in connection with a DeFi project, enterprise, or ecosystem. These collective decisions are then typically executed using smart contracts and employing the assets that the DAO's members have contributed to the project, enterprise, or ecosystem.

- **Oracles**. An oracle is a software application that connects blockchains and other distributed ledgers to external—i.e. "off-chain"—systems for the purpose of collecting, verifying, and transmitting "real world" data. Amongst other uses, this data can be used to determine whether the predetermined conditions programmed into a smart contract have been satisfied. In many cases, oracles will use decentralized consensus mechanisms to verify the provenance and accuracy of the relevant data.

[15] *See* Nick Szabo, *The Idea of Smart Contracts* (1997).

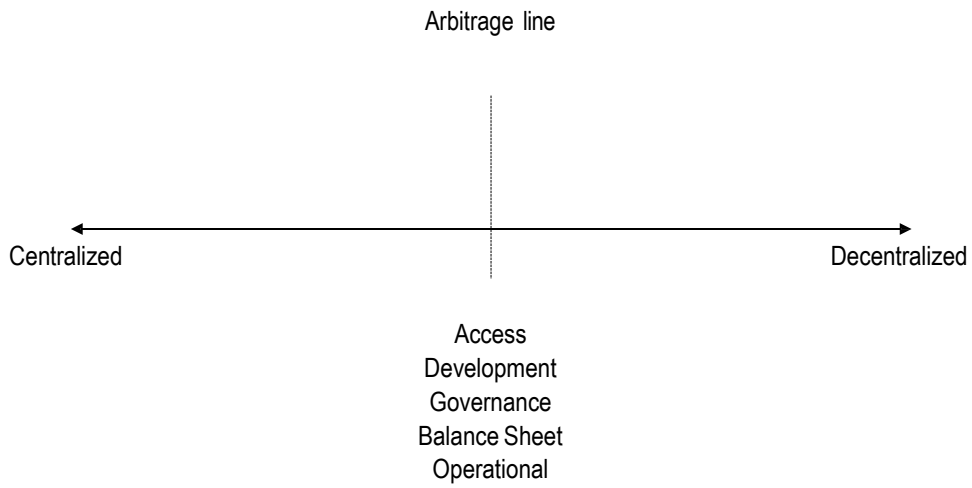
SPECTRUM OF DECENTRALIZATION

Most DeFi systems are not completely decentralized or centralized, but instead fit on a multi-level spectrum of (de)centralization (varying along each of the functional and technical dimensions), creating a challenge in trying to meet certain industry calls for either regulators or industry to coalesce around a particular defined level of decentralization for all business and technology models that would make it "sufficiently decentralized."

Within these dimensions of decentralization, there are also varying *degrees* of centralization and decentralization. As in traditional finance—or TradFi—there are few systems that operate as entirely centralized or decentralized across all of these dimensions. Most systems are not completely centralized or decentralized, but instead fall somewhere on a spectrum of (de)centralization (*see* Figure 2). This spectrum is also not one-dimensional, but can instead vary along each of the functional and technological dimensions described above.

This multi-dimensional spectrum of decentralization represents a challenge for policymakers and industry stakeholders that have called for a bright line rule, applicable to all business and technology models, that would clearly define when a DeFi project, enterprise, or ecosystem was sufficiently "decentralized." This challenge is compounded by the fact that the policy implications of decentralization depend, at least in part, on the purposes for which it is being employed. Thus, for example, while using decentralization to enhance operational resilience in the face of cyber threats and malicious actors may be desirable from a policy perspective, using it to evade responsibility for regulatory compliance is most certainly not.

FIGURE 2: THE SPECTRUM OF DECENTRALIZATION



Ultimately, no single dimension or technology will definitively serve to make a project, enterprise, or ecosystem "DeFi". Nevertheless, the more dimensions of decentralization we observe, the greater the use of technologies designed to achieve decentralization, and the lower the levels of concentration in the delivery of financial products and services, the more likely it is that a project, enterprise, or ecosystem should be viewed as falling into this category.

(B) The Architecture of DeFi

In considering the nature and level of decentralization, it is helpful to understand the basic technological architecture of DeFi projects, enterprises, and ecosystems. Figure 3 depicts the DeFi technology stack: identifying the functions performed at each layer, the key players, and primary components. This framework is adapted from the Open Systems Interconnection (OSI) model[16], widely used in information technology to depict the seven functional elements of computer systems used to communicate information across a network: *application, presentation, session, transport, network, data link, and physical*.

[16] *See* International Standards Organization (ISO)/International Electrotechnical Commission (IEC) 7498-1:1994, Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model (1994).

FIGURE 3: THE DEFI TECHNOLOGY STACK[17]

Layer	*Functions*	*Key Players and Components*
Governance	• Oversight, administration, and enforcement of decisions on network development and operations	• Developers, issuers, owners, voters • Governance tokens
Asset/Market	• Native financial assets minted on the network, along with any collateral assets	• Liquidity providers • Tokens, capital, collateral, prices
User	• End user interacting with or using products or services on the network	• Developers (including layer 2 builders), consumers, businesses, financial intermediaries
Application	• Software enabling the end user to carry out functions, distinct from the operations of the underlying network	• Exchanges and other service providers • DApps, smart contracts, wallets, APIs, oracles
Data	• Information, including its recording and presentation, used and referenced in a DeFi system	• Ledgers/blockchains, explorers, addresses, other on-chain data
Network	• Entities, infrastructure, and consensus mechanisms supporting the routing, sending, and validation of data into, across, through, and between networks	• Miners, validators, block builders, pools, voters • Nodes, relayers, bots, mempools
Protocol	• Rules, procedures, and standards for data formatting and communication to enable interaction across a network, and for building of higher order financial products and services on top of it	• Code repositories • Software code
Physical/Hardware	• Physical or tangible devices, assets, and hardware used in connection with a network	• Mobile devices, computers, servers, and other physical infrastructure

DEFI ATTRIBUTES

Operating across every layer of the DeFi technology stack, DeFi systems will exhibit varying degrees of decentralization along technological and functional dimensions, and include characteristics related to: programmability and composability; automation; transparency; openness; and immutability and censorship resistance.

At each layer of this DeFi technology stack are one or more projects, enterprises, and ecosystems that perform functions critical to the delivery of financial products and services. While some of these functions may be performed by decentralized actors and protocols, many others may be performed by more centralized enterprises and intermediaries. Understanding the risks associated with a given project, enterprise, or ecosystem thus demands an in-depth understanding of the nature and level of decentralization at each individual layer. By the same token, each layer may also present opportunities to embed technical features designed to support system security, transparency, privacy, interoperability, and regulatory compliance. This makes understanding the basic technological architecture of DeFi critically important for both industry and policymakers.

[17] Several other projects have uniquely represented the DeFi technology stack and key functions. While these other models are useful references for policymakers, the TAC felt this model better outlined the technologies, entities, and functions across whole DeFi systems to consider for understanding all entities involved and for integrating features like security and compliance controls. For examples of other DeFi technology stack illustrations, *see* Raphael Auer, Bernhard Haslhofer, Stafan Kitzler, Pietro Saggese & Friedhelm Victor, "The Technology of Decentralized Finance (DeFi)"; International Organization for Securities Commissions (IOSCO) Consultation Report, "Policy Recommendations for Decentralized Finance (DeFi)" (September 2023); Dominik Metelski and Janusz Sobieraj, "Decentralized Finance (DeFi) Projects: A Study of Key Performance Indicators in Terms of DeFi Protocols' Valuations" 10(4) International Journal of Financial Studies (November 25, 2022).

At every layer of this technology stack, DeFi projects, enterprises, and ecosystems are likely to exhibit varying degrees of decentralization along both functional and technological dimensions. They also exhibit several other characteristics, which may themselves vary across various technological and functional dimensions. These characteristics include:

- **Programmability and Composability.** Heavily leveraging protocol features and software-driven operations, DeFi projects, enterprises, and ecosystems typically support both *building in* particular features and functions—i.e. programmability—and *building with or on* different components like smart contracts and APIs in various combinations—i.e. composability—to build higher order applications and capabilities, and to meet bespoke requirements.

- **Automation.** DeFi projects, enterprises, and ecosystems leverage programmability to support the automation of financial and operational functions, thus seeking to significantly limit or even eliminate human intervention in their execution. This automation can serve several purposes: including the optimization of cost and time efficiencies, simplifying user experiences, reducing friction points, and potentially even reducing threats from malicious actors. Automation can also be used to thwart intervention from regulatory authorities and law enforcement officials.

- **Transparency.** The ability of certain stakeholders within DeFi projects, enterprises, and ecosystems to see certain information is a critical element in the security of blockchain-based and other distributed ledger networks. This transparency enables stakeholders to build trust and ensure accuracy of information that supports functions like the validation of transactions.

    - To be clear, the fact that DeFi projects, enterprises, and ecosystems are designed to promote transparency does not mean that they will always publish all useful or desired information for investors, customers, regulators, law enforcement, or other stakeholders. In fact, the transparency associated with many current DeFi projects, enterprises, and ecosystems, such as in making publicly visible information about transactions, is viewed by many not as a feature of these systems, but rather as a bug. This has driven significant interest and investment in the development of privacy-enhancing technologies that can further shield certain information currently available within these systems while still enabling the use of other information to ensure the accuracy of the distributed ledger and support law enforcement.

- **Openness.** DeFi projects, enterprises, and ecosystems often exhibit a significant degree of openness, whether through decentralized access, decentralized development, or simply by making their source code publicly available. The degree of openness and community engagement can enhance or be indicative of the level of decentralization.

- **Immutability and Censorship Resistance.** A feature often championed as core to DeFi projects, enterprises, and ecosystems is their immutability: the inability of network participants to change a system's ledgers, protocols, transactions, or other features. In theory, this immutability can then be combined with decentralized (permissionless) access and freedom from confiscation to achieve full censorship resistance. Most DeFi projects, enterprises, and ecosystems do not implement full immutability and censorship resistance. Instead, they contemplate that some subset of network participants may be able to address security vulnerabilities, implement software upgrades and patches, or otherwise make changes designed to optimize the products and services provided on the network. Greater degrees of immutability and censorship resistance can increase the challenges associated with decentralized governance, making it more difficult to implement network upgrades, correct errors, and respond in a timely and comprehensive fashion to malicious actors.[18]

[18] *See* Bank for International Settlements (BIS), "The Crypto Ecosystem: Key Elements and Risks" (2023).

(C) Current and Potential Future Use Cases

In the eyes of its proponents, DeFi can be used to provide almost all of the financial products and services currently supplied by the conventional—intermediated—financial system (*see* Figure 4).[19] Customers can use DApps and other DeFi protocols to directly hold digital assets such as stocks, derivatives, bonds, money, and other financial assets in self-hosted "wallets". They can also use these DApps and protocols to lend out the financial assets held in these wallets, to pledge them as collateral against their own borrowing and, thereby, to create decentralized lending and money markets. Customers can also pool their capital in DAOs that then combine decentralized governance and algorithmic decision-making to allocate this capital for investment. In addition, DAOs and other decentralized protocols can be combined with smart contracts and oracles to provide customers with life, property, health, and other types of insurance.

[19] For a more detailed description of this vision, *see* Campbell Harvey, Ashwin Ramachandran, Joey Santoro, Vitalik Buterin & Fred Ehrsam, "DeFi and the Future of Finance" (August 2021); Fabian Schar, "Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets", 103(2) Federal Reserve Bank of St. Louis Review 153 (2021); Raphael Auer, Bernhard Haslhofer, Stafan Kitzler, Pietro Saggese & Friedhelm Victor, "The Technology of Decentralized Finance (DeFi)".

FIGURE 4: BANK OF INTERNATIONAL SETTLEMENTS ILLUSTRATION OF THE FUNCTIONS OF DEFI VERSUS TRADFI[20]

Crypto vs traditional financial system

Function	Service	Crypto financial system		Traditional finance
		Decentralised finance (DeFi)	Centralised finance (CeFi)	
Trading	Funds transfer	DeFi stablecoins	CeFi stablecoins	Traditional payment platforms
	Asset trading	Crypto asset DEX	Crypto CEX	Exchanges and OTC brokers
	Derivatives trading	Crypto derivatives DEX		
Lending	Secured lending	Crypto decentralised lending platforms	Crypto centralised lending platforms	Broker-dealers active in repo and securities lending
	Unsecured lending	Crypto credit delegation	Crypto banks	Commercial banks and non-bank lenders
Investing	Investment vehicles	Crypto decentralised portfolios	Crypto funds	Investment funds

CEX = centralised exchanges; DEX = decentralised exchanges; OTC = over-the-counter

Proponents also see DeFi technology as a way to revolutionize how financial assets are developed, issued, and traded. Financial assets can be developed using open source software. These assets can then be issued and traded on purportedly decentralized and fully-automated trading platforms that use algorithmic market-making tools to create electronic order books and support market liquidity, before using distributed ledgers to clear and settle the resulting transactions. Similarly, automated trading protocols, smart contracts, and oracles can be combined to create decentralized derivatives markets in which the entire lifecycle of a derivatives contract takes place on-chain and without the involvement of centralized financial intermediaries.

Last but not least, proponents of DeFi envision a world in which distributed ledger technology is used to create decentralized financial market infrastructure supporting domestic and cross-border payments, wholesale money markets, and trade financing. Some proponents even envision a single, decentralized and fully-interoperable clearing and settlement network connecting all these various financial markets, products, and services. In theory, this decentralized infrastructure could one day compete with—and perhaps even supplant—the highly fragmented yet deeply interconnected network of banks, brokers, clearinghouses, and custodians at the heart of the TradFi ecosystem.

The opportunities and risks stemming from the ongoing development of DeFi projects, enterprises, and ecosystems are canvassed in Part III of this report. Yet in many ways, it is difficult to imagine precisely what this future—more decentralized—financial system might look like. Not only would this system likely be very different from the one we have today, but most of it does not exist yet—and may never will. Beyond the theory and inevitable marketing hype, there is also the question of how decentralized these projects, enterprises, and ecosystems actually are in practice, and along which dimensions. Accordingly, before turning to these potential opportunities and risks, it is useful to briefly describe some of the current DeFi use cases.

[20] *See* Sirio Aramonte, Wenqian Huang, and Andreas Schrimpf, BIS Quarterly Review, "DeFi Risks and the Decentralization Illusion" (December 6, 2021).

- **Digital wallets**. Digital wallets are DApps and software protocols that enable customers to store and transfer digital assets. In most cases, customers can simply download and install these apps and protocols directly onto their computer or smartphone, resulting in a fairly high degree of decentralized *access*. So-called "self-custodial" or "unhosted"[21] wallets also enable customers to hold and store digital assets locally—i.e. on a computer or thumb drive—without ownership being recorded on the books of a centralized financial intermediary, thereby facilitating a degree of *balance sheet* decentralization. In contrast, "custodial" or "hosted wallets" can also be accessed via apps or browsers, but the actual assets are held in accounts at the centralized intermediaries requiring obligations like KYC and other controls that result in more centralized access and management of funds.

  Some of these digital wallet DApps and protocols combine self-custody with services—known as mixers—designed to break the chain of custody associated with the transfer of digital assets. These mixing services make it more difficult to trace the movement of digital assets within a given network, thereby undercutting the transparency often associated with distributed ledger technology. Accordingly, while these mixing services can enhance customer privacy, they also make the digital wallets that provide these services potential conduits for illicit transactions.

  Many of the most popular digital wallets and mixers were created and deployed using open source software. As a result, in many cases, the number and identity of their core developers is not publicly known. In some cases, these core developers continue to exercise a degree of residual control through their holdings of digital assets known as governance tokens. Amongst other matters, these governance tokens give their holders the right to vote on any changes to a digital wallet or mixer's protocols. In other cases, developers may have entirely relinquished any residual control rights, rendering the relevant protocols completely self-executing. Accordingly, digital wallets and mixers can vary greatly in terms of the degree of decentralized *governance*—with some characterized by the complete absence of any residual control rights.

- **Decentralized exchanges (DEXs)**. DEXs are software protocols that facilitate the automated exchange of digital assets. DeFi entrepreneurs, software developers, or DAOs can create or "mint" a new type of digital asset in accordance with the technical specifications associated with a given open source software platform, like Ethereum's ERC20, developed in conjunction with a given distributed ledger. This new digital asset can then be listed for trading on any DEX built on the same platform, provided that it first complies with the protocols established by the relevant DEX. Where compliance with these protocols is the only precondition to listing a digital asset, the relevant DEX can be said to exhibit a high degree of decentralized *access*.

  Once a digital asset is listed for trading, DEXs can provide two basic financial services. The first is an automated order book that matches buyers and sellers of any given pair of digital assets, thereby promoting market liquidity and price discovery. The second is a smart contract-based automated market-making (AMM) mechanism. For each pair of digital assets trading on a DEX, this AMM mechanism pools reserves of each digital asset from select market participants, with trades involving this trading pair then executed against the digital assets held in these reserves.

  DEXs bring together several different types of market participants. All DEXs seek to attract customers interested in simply trading digital assets. DEXs that employ an AMM mechanism also seek to attract market participants known as "liquidity providers" who are willing to deposit digital assets into the reserve pools supporting the liquidity of each trading pair, typically in exchange for compensation. In many cases, this compensation takes the form of digital assets known as LP tokens that represent a fractional interest in the ownership of the assets in the relevant pool. Lastly, DEXs issue governance tokens that give holders the right to vote on any proposed changes to a DEX's protocols. Whereas the presence of a large

[21] *See* Financial Crimes Enforcement Networks (FinCEN), FinCEN Guidance FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currency" (May 9, 2019).

number of dispersed liquidity providers would effectively create a decentralized *balance sheet*, the existence of a large number of dispersed holders of a DEX's governance tokens would represent a high degree of decentralized *governance*.

- **Consumer lending and credit platforms.** DeFi lending and credit platforms allow consumers to borrow and lend digital assets. Recent estimates suggest that there may be over $10 billion in "total value locked" (TVL) into these platforms worldwide.[22] These platforms typically operate by allowing lenders to earn a fixed or variable return on their digital assets by depositing them in a lending or liquidity pool that other users can then access to borrow these assets.[23] Aiming to streamline loan management, these platforms often employ smart contracts to automate elements of the lending and borrowing process, with some permitting both borrowing and posting collateral in multiple forms of assets simultaneously. These applications will either algorithmically match lenders to borrowers or, increasingly, use a peer-to-smart contract lending model, where lenders and borrowers do not interface directly but instead interact via smart contracts.

  Given the pseudo-anonymity associated with these DeFi consumer lending and credit platforms, lenders are unable to employ conventional underwriting practices based on the identity and creditworthiness of the borrower. Instead, these lenders typically require the borrower to post digital assets as collateral in excess of the loan amount. Many platforms will also set liquidation thresholds: establishing a value or percentage price drop below which the collateral will automatically be sold in order to pay back the lender. Whereas some loans will have a predetermined maturity date coded into the smart contract, others function as revolving lines of credit that charge users interest on the value of funds withdrawn. In addition to collateralized lending, these platforms also provide consumers with so-called "flash loans". In a flash loan, a user can borrow digital assets without having to put up any collateral on the stipulation that they are required to pay back the loan in the same block of transactions—typically a matter of seconds. Flash loans are used by those interested in price arbitrage between different markets, as well as for liquidations to manipulate a particular market or price in the user's favor.

- **Cross-border payment and remittance networks.** While most current DeFi activity remains highly speculative in nature,[24] revolving around digital asset trading, lending, and arbitrage, there is growing interest from both customers and merchants in the use of digital assets to facilitate cross-border payments and remittances.[25] Using distributed ledger technology, DeFi payment and remittance networks enable users to send and receive digital assets directly, without the need for banks, money services businesses (MSBs), or other TradFi intermediaries.[26] These networks can exhibit different levels of access and balance sheet decentralization: with some structured around permissionless ledgers and unhosted

[22] TVL is a DeFi industry metric referring to the amount of user funds or collateral deposited or "locked" in a DeFi platform. TVL is commonly used as a measure of the size of the DeFi lending and credit market. TVL information may not be reliable as it is not audited or verified and may double-count funds since collateral can be reused between platforms. *See* U.S. Treasury, "Illicit Finance Risk Assessment of Decentralized Finance" (April 2023); DeFi Llama, TVL Rankings; and International Monetary Fund (IMF), *Global Financial Stability Report: COVID-19, Crypto, and Climate* (October 2021).

[23] *See* U.S. Treasury, "Illicit Finance Risk Assessment of Decentralized Finance" (April 2023).

[24] *See* Sirio Aramonte, Wenqian Huang, and Andreas Schrimpf, BIS Quarterly Review, "DeFi Risks and the Decentralization Illusion" (December 2021).

[25] *See* Deloitte, in partnership with PayPal, "Merchants Getting Ready for Crypto: Merchant Adoption of Digital Currency Payments Survey" (2022).

[26] If not using a more centralized intermediary service like an exchange, individual users can generate digital asset transactions out of their digital wallets across decentralized networks. They use the beneficiary's public key or address and signal the amount in digital assets—plus a transaction fee for the operators of the network, like miners or validators—the originator wishes to send. The originator then uses their private key associated with their wallet to sign the transaction, and broadcasts the transaction to the network. From there, the transaction is routed to the "memory pool" of unconfirmed transactions for eventual formation into a transaction block and then appending to the network participants' copy of the ledger upon finalization.

wallets, and others structured around permissioned ledgers and centralized cryptocurrency exchanges. At present, most of these networks only facilitate the transfer of digital assets and do not provide seamless exchange with or between fiat currencies.

- **RegTech**. From a regulatory perspective, DeFi is something of a double-edged sword. On one hand, the transparency often associated with distributed ledger technology can in theory help advance important regulatory objectives like promoting market discipline; rooting out fraud, market manipulation, and financial crime; and monitoring potential threats to financial stability. On the other hand, many DeFi projects, enterprises, and ecosystems are designed to offer their users a high level of privacy and anonymity, creating obstacles to effective regulation and enforcement.

  RegTech software is designed to bridge this gap: enabling these projects, enterprises, and ecosystems to comply with their ongoing regulatory compliance obligations while simultaneously protecting the privacy and in some cases anonymity of their users to the fullest extent permitted by applicable law. This could include the use of capabilities like artificial intelligence, APIs, and scripts for pattern recognition and anomaly detection, clustering of cryptocurrency addresses and transactions, natural language processing, and geotagging, as well as leveraging data from sources like distributed ledgers, network traffic, internal exchange records, and open source and social media. To enable obfuscation paired with discoverability, privacy-enhancing technologies like zero-knowledge proofs and homomorphic encryption, along with digital identity technologies like digital certificates issued by trusted certificate authorities, can enable actors in a DeFi ecosystem to automatically verify the identity of users for the purposes of KYC and AML/CFT regulation without the need to share detailed, sensitive, or personally identifiable information with other actors.

  RegTech DApps, smart contracts, and other protocols can also be used to automate compliance tasks, enhance real-time risk management, improve regulatory reporting and analytics, and create a single, fully transparent, and immutable audit trail. Business models for RegTech can vary from those integrated directly into a specific DeFi project—*e.g.,* building a protocol that will not validate transactions without first meeting KYC requirements—to those developed by centralized service providers to support regulatory oversight and monitoring by other DeFi projects, enterprises, and ecosystems.

  In addition to addressing individual regulatory concerns, RegTech also plays a critical role in managing and mitigating systemic risks within decentralized networks. Within this dynamic environment, DeFi service providers bear significant responsibility for ensuring the safety and soundness of their customers. DeFi ecosystems, by their very nature, introduce unique systemic vulnerabilities, necessitating rigorous risk management and compliance efforts by these service providers. RegTech solutions can offer real-time monitoring and analysis capabilities to identify and assess systemic risks, enabling both service providers and regulators to proactively respond to potential threats to financial stability. By automating risk assessment and compliance processes across interconnected networks, RegTech can also enhance the security of customer assets and contribute to the resilience and stability of the entire DeFi ecosystem.

  Importantly, where DeFi projects, enterprises, and ecosystems outsource the development, testing, and implementation of these and other RegTech solutions to third party service providers, this will necessarily result in a degree of *operational* decentralization. Where these service providers are left to make important decisions about the design of these solutions, and to update them over time in response to new learning and changing regulation, it may also translate into more decentralized *governance*.

While this list of current and potential future DeFi use cases might suggest that these financial products and services are being performed by independent projects, enterprises, and ecosystems, in reality the programmability, composability, openness, and other features of DeFi often mean that a wide range of products and services are bundled together. For example, whereas conventional exchanges focus exclusively on listing securities or derivatives, matching customer orders, and executing the resulting trades, many DEXs combine these functions with trade clearing and settlement, digital wallets, lending and borrowing platforms, and payments. To many, this level of interoperability and functional integration is an important and valuable feature of DeFi ecosystems. Nevertheless, as explored in greater detail below, it is also a source of significant and unresolved challenges and risks.

III. Debating DeFi: Policy Objectives, Opportunities, and Risks

Understanding the policy implications stemming from the emergence and evolution of DeFi projects, enterprises, and ecosystems requires that policymakers first identify the objectives that financial policy and regulation are designed to achieve. In light of the dimensions of DeFi, the technology that drives it, and the range of current and potential future use cases, policymakers should then evaluate the opportunities and risks presented by DeFi in order to determine what actions—including but not limited to new law and regulation—may be necessary to achieve these objectives. This section describes these policy objectives, along with the opportunities and risks posed by the rise of DeFi.

(A) Policy Objectives

Financial policy and regulation are called upon to advance a wide range of policy objectives. In order to advance these objectives, policymakers must successfully navigate a host of complex and interwoven challenges. As a threshold matter, in the United States, responsibility for advancing these objectives falls to a myriad of government agencies, self-regulatory organizations, and other regulatory authorities at both the state and federal level. These objectives also frequently come into conflict, forcing policymakers to grapple with thorny and potentially intractable tradeoffs. Examples of these tradeoffs include the tension between maintaining financial stability and promoting vibrant competition, along with the tension between protecting consumer privacy and effectively policing illegal activity. Compounding these challenges, differences between regulatory frameworks can create opportunities for regulatory arbitrage, increasing the complexity and opacity of the financial system and undermining the ability of regulators to effectively pursue different policy objectives. Navigating these challenges requires not only an understanding of the opportunities and risks presented by DeFi itself, but also the likely impact of any new regulation, along with the ability to effectively coordinate this regulation across jurisdictional boundaries.

POLICY OBJECTIVES FOR DEFI

Policymakers should have a firm grasp of all desired outcomes for DeFi in order to best assess approaches they can take in regulation and enforcement, to achieve an optimal balance in promoting the responsible innovation of these technologies while promoting other desired outcomes. Desired outcomes include, but are not limited to: customer and investor protection; promoting market integrity; ensuring microprudential safety and soundness, financial stability, and mitigating systemic risk; combating illicit finance and protecting national security; reinforcing and securing U.S. competitiveness and leadership; and expanding access to safe and affordable financial services.

Against this backdrop, identifying and describing these policy objectives is important for several reasons. First, these objectives serve as a touchstone for understanding and debating what financial policy and regulation can and should be designed to achieve, and for systemically navigating

any potential conflicts or tradeoffs between these objectives. Second, these objectives help guide regulators in determining whether and how DeFi falls within the existing regulatory perimeter, and identifying whether, where, and how the regulatory perimeter might need to be expanded or adjusted in order to capture DeFi actors or activities, and then ensuring effective monitoring and enforcement. They also help guide regulated actors, thereby ensuring that their activities comply with both the letter and spirit of this regulation. And lastly, these objectives provide a benchmark against which elected officials, regulated actors, and citizens can evaluate the success of this regulation, the effectiveness of regulatory compliance frameworks, and the impact of enforcement.

The core objectives of financial policy and regulation include[27]:

- **Protecting investors and consumers.** Investors and other consumers of financial products and services must have confidence that they will be protected from harm at the hands of the people and businesses that provide them. Financial policy and regulation play a number of important roles in promoting this confidence. Securities regulation, for example, typically mandates that the issuers of securities disclose detailed information about their business and finances, enabling investors to better understand the relevant risks and ultimately make informed decisions about their financial future. It also ensures that the financial intermediaries through which investors hold these securities are responsible for protecting them against the risks of loss, theft, or destruction. More generally, financial policy and regulation can help protect the consumers of these products and services from conflicts of interest, negligence, data breaches, theft, fraud, scams, and other forms of negligent or predatory conduct and practices.

    - *Desired DeFi System Attributes Supporting Objective:* Security, Privacy, Equity, Appropriate Transparency, Accountability, Adaptability

- **Promoting market integrity.** Confidence is also essential to the smooth and efficient operation of financial markets. To help foster market confidence, financial law and regulation can promote market integrity by ensuring that all market participants play by the same rules. These rules can target critical elements of market structure like order routing, matching, and execution. They can also target the conduct of market participants by, for example, prohibiting them from engaging in insider trading or artificially manipulating the market prices of securities or other financial instruments.

    - *Desired DeFi System Attributes Supporting Objective:* Security, Appropriate Transparency, Operational Resilience, Accountability, Adaptability

- **Ensuring microprudential safety and soundness.** Where financial products or services are provided by intermediaries, the failure of these intermediaries can impose significant losses on their customers, counterparties, and other stakeholders. Financial policy and regulation can reduce the probability and impact of these failures by imposing entry restrictions on these intermediaries, regulating their governance and balance sheets, and prescribing the range of activities they are permitted to undertake. It can also subject these intermediaries to ongoing reporting and supervision with the objective of ensuring that regulators are in a position to intervene before these intermediaries reach the point of failure.

    - *Desired DeFi System Attributes Supporting Objective:* Security, Appropriate Transparency, Operational Resilience, Accountability, Adaptability

[27] These policy objectives are adapted from those outlined in President Biden's Executive Order 14067, "Executive Order on Ensuring Responsible Development of Digital Assets" (March 9, 2022). The desired system attributes are adapted and expanded from those outlined in the BIS Annual Economic Report, Special Chapter III, "The Future Monetary System" (June 21, 2022). *See also* John Armour, Dan Awrey, Paul Davies, Luca Enriques, Jeffrey Gordon, Colin Mayer & Jennifer Payne, *Principles of Financial Regulation* (2016), chapter 3.

- **Maintaining U.S. and global financial stability and mitigating systemic risks.** Under certain circumstances, the failure of financial markets or intermediaries can pose a threat to the stability of the wider financial system. These systemic threats include both *cross-sectoral* and *time series* risks. Cross-sectoral risks are generated by counterparty exposures, information cascades, fire sale dynamics, and other direct and indirect transmission channels that create complex and often hard to detect interconnections among and between different financial markets and intermediaries. Time series risks are generated by the procyclicality of the financial cycle and its impact on the delivery of financial products and services to the real economy. Financial policy and regulation can help mitigate cross-sectoral systemic risks by ensuring the microprudential, or individual institutions', safety and soundness of systemically important financial intermediaries and other critical financial infrastructure. It can also regulate the size, activities, and corporate structure of these intermediaries, along with the interconnections between them, with the objective of preventing them from becoming channels for the transmission or amplification of systemic shocks. Financial policy and regulation can help mitigate time series risks through the use of tools like stress tests and targeted lending constraints. These tools can also potentially be used to help measure and address the negative environmental and climate impacts stemming from the delivery of financial products and services.

    - *Desired DeFi System Attributes Supporting Objective:* Stability, Integrity, Operational Resilience, Efficiency, Mitigated Climate Impact, Accountability, Adaptability

- **Expanding access to safe and affordable financial products and services.** Access to financial products and services—including basic savings, payments, credit, and insurance products—are an essential part of everyday life. Financial policy and regulation can help promote access to these products and services by ensuring that they are affordable and accessible to everybody, regardless of their economic or other circumstances. It can also ensure that people and businesses are not subject to discrimination by the financial intermediaries, markets, or algorithms that provide these products and services.

    - *Desired DeFi System Attributes Supporting Objective:* Inclusion, Equity, Diverse Representation, Security, Integrity, Operational Resilience, Victim Recourse, Accountability, Efficiency

- **Combating illicit finance.** Financial markets and intermediaries can be used as witting or unwitting accomplices for money laundering, terrorist financing, and other illicit activities. Especially where these activities are pervasive, they can undermine confidence in the financial system, contribute to financial exclusion, and pose a threat to national security. Financial policy and regulation typically seek to combat illicit finance by imposing an affirmative obligation on regulated markets and intermediaries to collect information about their customers, along with the source and destination of any transferred funds or other financial instruments, and to report suspicious activity. This information is used to determine whether there is credible evidence of money laundering, terrorist financing, or other illegal activities. Financial intermediaries are then typically required to pass this information on to regulators for further investigation and, where warranted, enforcement action, as well as to take action themselves on their platforms to reasonably prevent their institution from being used for money laundering and other illicit finance. More broadly, combating illicit finance is a critical component of U.S. national security, serving as a foundational pillar of strategies to combat rogue state actors, sanctions evasion, proliferation activities, cybercriminals, drug and human trafficking, and terrorism.

    - *Desired DeFi System Attributes Supporting Objective:* Accountability, Security, Appropriate Transparency, Victim Recourse, Adaptability

- **Reinforce and strengthen U.S. leadership and competitiveness in finance and technology.** The United States has long been a global leader in both finance and technology. The United States also derives a wide range of economic and national security benefits from the central role of its financial markets and intermediaries in the global financial system, along with the role of the U.S. dollar in international trade and investment. Financial policy and regulation can play an important role in reinforcing and strengthening this leadership by promoting confidence in these markets and intermediaries, through the targeted and judicious use of financial sanctions and other enforcement actions, and through active participation in the design and implementation of cross-border financial infrastructure, common technical standards, and international regulatory frameworks.

    - *Desired DeFi System Attributes Supporting Objective:* Security, Scalability, Efficiency, Adaptability, Interoperability, Innovation-Enablement

(B) Opportunities Presented by DeFi

DEFI OPPORTUNITIES

Decentralized networks and technologies operating largely on public, un-obfuscated ledgers present opportunities to leverage efficiency improvements in payments and financial markets, more transparent and auditable financial services, enhanced financial sector resilience, dismantled barriers to access to financial services, promotion of innovation and competition, and reinforced U.S. leadership in technology and finance. However, the current reality of the market, technology, and policy environment may not reflect conditions necessary to most fully exploit the opportunities presented by these systems.

Proponents of DeFi point to a number of potential benefits. In general, these benefits stem from the use of open source software, distributed ledgers, smart contracts and the other technological hallmarks of DeFi to increase decentralization, programmability and composability, automation, openness, transparency, immutability, and censorship resistance in connection with the delivery of financial products and services. This section explores these opportunities in greater detail and highlights how they can help advance the objectives of financial law and regulation. Reflecting the reality that most DeFi projects, enterprises, and ecosystems are still at a relatively early stage in their development, this section also briefly describes the current state of play: evaluating both how far DeFi has come, and how far it still has to go before it can fully capitalize on these opportunities.

- **Improving efficiency in the delivery of financial products and services.** TradFi can be very expensive, as centralized intermediaries are subject to complex and costly regulation to ensure their microprudential safety and soundness, the development of sophisticated internal compliance programs, and intensive third-party supervision and auditing. Transferring these financial assets from one intermediary to another requires costly and often duplicative investments in back office technology, along with the development and implementation of processes governing the reconciliation, clearing, and settlement of transactions. Where these processes are not technologically interoperable, the resulting network fragmentation can further increase the relevant

transaction costs. And despite recent progress, many of these processes are also still reliant on slow, costly, and error-prone manual labor.

In theory, compared to centralized financial intermediaries, decentralized technological networks, DeFi projects, enterprises, and ecosystems create opportunities for reducing these transaction costs. The elimination or reduction of certain conventional financial intermediaries could potentially reduce the regulatory compliance burden for both regulators and regulated actors, with the use of open source software and public distributed ledgers in particular making supervision and auditing less complex and costly. Similarly, the development of decentralized networks can help reduce duplicative investments in back office technology, while greater automation can make transactions using these networks cheaper, faster, and less prone to errors.[28] By promoting faster settlement of transactions, decentralized networks could also reduce counterparty risks and free up capital for investment.[29] And beyond transaction processing, decentralized networks combined with greater automation could support more efficient liquidity pooling in connection with DeFi lending protocols, DEXs, and the delivery of other financial products and services.[30]

- *Relevant Policy Objectives:* Market Integrity, Safety and Soundness, Financial Stability and Systemic Risk, Safe and Affordable Access, U.S. Leadership

- *Current State of Play:* Both the speed and scale of DeFi transaction processing capability have increased significantly since the initial clunky implementations and slow transaction processing observed in the first days of Bitcoin. However, the still nascent state of many DeFi projects, enterprises, and ecosystem, as well as the underlying technology, leave many remaining issues related to scalability, interoperability, throughput, and transaction processing that threaten to delay, or perhaps even derail, the realization of these efficiency benefits.[31] Additionally, the failure to integrate sufficient compliance and security measures integrated into DeFi systems—whether due to the absence of applicable regulatory frameworks or the failure to comply with them—create the illusion of cost efficiencies that will likely evaporate once DeFi projects, enterprises, and ecosystems are fully incorporated into the regulatory perimeter. Lastly, as a theoretical matter, it is not entirely clear whether decentralized, interoperable networks will necessarily result in a reduction in overall transaction costs. For example, while interoperable networks can connect more people and businesses and create larger pools of liquidity, they also expand the sources and destinations of possible technological and financial contagion. Similarly, the technological bridges used to achieve interoperability in decentralized networks are often vulnerable to cyberattacks, posing problems for consumer protection and network reliability. Once these and other costs are considered, there is no guarantee that DeFi will yield meaningful and lasting efficiency gains.

- **Promoting greater transparency within the financial services industry**. Fully transparent distributed ledgers built using open source software provide developers, regulators, and the general public with a significant amount of data about the transactions and other activities that take place on DeFi networks. The transparency and auditability of these ledgers can be further enhanced through the use of automated processes designed to improve data quality and reliability. This data is a necessary precondition for the effective governance of DeFi projects, enterprises, and ecosystems: providing investors and consumers with important information about their financial products and services, economic and governance rights, and attendant risks. It can also be extremely valuable for regulatory and compliance purposes: enabling regulators

[28] *See* Wharton School, University of Pennsylvania, "DeFi Beyond the Hype" (May 2021).

[29] *Id.*

[30] *See* Tobias Adrian, IMF, Remarks at the BIS 21st Annual Conference, "Currencies and Decentralized Finance" (June 24, 2022).

[31] *Id.*

and law enforcement to more effectively monitor transaction activity, trace transaction chains, and identify critical dependencies and other threat vectors for the purpose of targeting and enforcing anti-money laundering and terrorist financing laws, economic sanctions, and other regulatory actions. In these and other ways, fully transparent and publicly-available digital ledgers can help foster confidence and trust in DeFi projects, enterprises, and ecosystems, while also reducing opportunities for theft, fraud, illicit finance, or corruption by malicious actors operating within DeFi networks.[32]

- *Relevant Policy Objectives:* Consumer and Investor Protection, Market Integrity, Safety and Soundness, Financial Stability and Systemic Risk, Safe and Affordable Access, Illicit Finance, U.S. Leadership

- *Current State of Play:* Many DeFi projects, enterprises, and ecosystems already make available a wealth of data about their governance, technological architecture, the transactions that take place on their ledgers, and other network features. In theory, this data can help support better governance, regulatory supervision and compliance, and law enforcement. Yet in practice, and despite the transparency of the underlying 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. This problem of usability reflects the pseudonymous nature of much of the relevant data, the ability to undertake transactions "off-chain", the fact that many regulators are still building out their technological competency and capacity, and the still nascent stage of RegTech development. It also reflects how both regulators and the DeFi industry could coordinate in the development of common technical standards designed to ensure that the structure and communication of this data render it usable by investors, consumers, regulators, auditors, and other stakeholders.[33]

- **Enhancing resiliency within the financial system.** A diverse, stable, and well-regulated DeFi ecosystem could potentially help enhance the stability and resilience of the financial system.[34] Heavy reliance on centralized intermediaries for the delivery of financial products and services can pose the risk that—because of their size, footprint, interconnectedness, or lack of substitutability—policymakers will view at least some these intermediaries as "too-big-to-fail".[35] The too-big-to-fail problem is a source of acute moral hazard problems, along with potentially significant competitive distortions, that drive increasing concentration within the financial services industry. This concentration, together with the other features of too-big-to-fail banks and other systemically important financial institutions, can generate both cross-sectoral and time series risks[36] to the stability of the U.S. and global financial system. It also undercuts the type of vigorous competition that is often critical for driving technological innovation.

[32] *See* Jared Ronis, Wilson Center, "DeFi 101: The Good, the Bad, and the Regulatory" (September 29, 2023).

[33] *See* IOSCO, Consultation Report, "Policy Recommendations for Decentralized Finance (DeFi)" (2023).

[34] *See* Financial Stability Board, *Decentralized Financial Technologies: Report on Financial Stability, Regulatory and Governance Implications* 6 (June 6, 2019), ("The application of decentralised financial technologies may reduce some of the financial stability risks associated with traditional financial institutions and intermediaries. For example, the growth and/or dispersion of financial service providers could increase diversity in the financial system and reduce the concentration of service providers.").

[35] *See* Financial Stability Board, *Evaluation of Too-Big-to-Fail Reforms: Summary Terms of Reference* (May 23, 2019).

[36] Time series risks, such as loss of confidence, result in the reduction in the delivery of financial products or services over time. As an example, in the context of DeFi, the failure of an asset whose value or stability the broader market held confidence in (such as a stablecoin) could trigger worries about the stability of the broader sector.

Theoretically, DeFi proponents posit that by shifting away from the use of centralized financial intermediaries and towards decentralized financial networks for the delivery of key financial products and services, DeFi projects, enterprises, and ecosystems can help alleviate the too-big-to-fail problem. Specifically, by reducing reliance on the large, economically important, and highly interconnected nodes at the heart of many financial networks—while simultaneously increasing their technological and institutional diversity—DeFi can potentially make these networks more resilient to financial and technological shocks.[37]

- *Relevant Policy Objectives:* Market Integrity, Safety and Soundness, Financial Stability and Systemic Risk, Safe/Affordable Access, Illicit Finance, National Security

- *Current State of Play:* While in theory decentralized networks can promote greater systemic diversity and resilience, the majority of DeFi projects, enterprises, and ecosystems still exhibit significant levels of centralization in access, development governance, balance sheets, and operations. To the extent that this centralization recreates the vulnerabilities of conventional financial intermediaries and networks, DeFi may ultimately fail to enhance systemic resilience. Part of resilience is also not just a system's ability to withstand stress and shocks, but also its ability to adapt well and recover from that stress. This ultimately presents challenges with existing DeFi implementations whose immutability features behind their purported benefits of defending against shocks may limit the systems' abilities and timeliness to then adapt with necessary changes.

- **Dismantling barriers to financial access and inclusion**. At present, 24% of the world's population—roughly 1.7 billion people—is unbanked.[38] Especially for these unbanked populations, cross-border remittances can be time-consuming and costly: with many transfers taking days and costing on average of 6.25% of the transferred funds—and upwards of 12% in some emerging markets.[39] And even in developed markets like the U.S., ensuring that citizens have safe and reliable access to basic financial products and services remains a critical and unresolved challenge. More broadly, the rights of consumers over their financial data are often weak, unclear, or difficult to enforce. As a consequence, conventional financial intermediaries have little incentive to invest in the development of interoperable platforms—like open banking infrastructure—that would lower the technological and other barriers that prevent consumers from using and sharing their data. Consumers may also have little recourse where data gaps, inaccurate data, or other factors result in algorithmic discrimination.

  In theory, DeFi projects, enterprises, and ecosystems can leverage their open technological architecture to provide financial products and services to virtually anyone, anywhere in the world, at any time. The transparency and auditability of many DeFi networks also makes them potentially desirable platforms for giving consumers more control over their financial data, and for sharing this data with DeFi lending protocols, DEXs, and other providers of financial products and services. Building on top of these networks, these providers can then use this data to more accurately evaluate the specific financial needs and risk profiles of their consumers, better tailor their protects and services to their needs, and then market them to the consumers most likely to benefit from them. The composable and accessible nature of DeFi platforms for anyone to build applications on top of them lowers thresholds to entry and access to infrastructure that could enable greater participation in digital commerce and development by marginalized and peripheral

[37] It is important to consider the nature and duration of the risk and associated events in determining how much resilience decentralization may offer. For example, in instances where performance risks span more than an instant, ranging from days to years, a centralized contract enforcing mechanism that enforces collateralization, netting, and mutualization may be more resilient than a decentralized network. This reasoning led policymakers to pursue clearing as an objective good after the global financial crisis.

[38] *See* The World Bank, "The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19" (June 2022).

[39] *See* The World Bank, "Remittance Prices Worldwide Quarterly: An Analysis of Trends in Costs of Remittance Services" (March 2023).

communities, which provide "immeasurable opportunity for economic development".[40] In these ways, DeFi can potentially help dismantle barriers to financial access and inclusion, improve the quality of financial products and services, and reduce the risk of algorithmic discrimination.

- *Relevant Policy Objectives:* Consumer and Investor Protection, Safe and Affordable Access, Illicit Finance, U.S. Leadership

- *Current State of Play:* At present, low levels of DeFi adoption reflect ongoing issues with network complexity and high barriers to entry. Moreover, in the absence of effective regulatory frameworks, any potential benefits in terms of financial access and inclusion must be weighed against the ongoing risks to investor and consumer protection, market integrity, and national security posed by many DeFi projects, enterprises, and ecosystems. At present, many of the touted benefits of DeFi in terms of financial inclusion in DeFi are not addressing several core issues resulting in exclusion from the regulated or traditional financial system: *e.g.,* improperly or arbitrarily calibrated risk decisions or insufficiency of available data or identity credentials resulting in indiscriminate red-lining. Rather than enabling a more complete and accurate understanding of risk and identity, many potential DeFi use cases seek to promote greater financial inclusion simply by removing any centralized authority for making risk-based decisions. Given inadequacies in consumer protections and measures promoting diverse representation, which DeFi technologies will not implement within deliberate design,[41] the current DeFi ecosystem presents vulnerabilities for "predatory inclusion,"[42] rather than desired inclusion in safe and affordable services, and for discounting underrepresented communities.

- **Promoting innovation and competition.** In theory, the openness and composability of DeFi ecosystems provide a supportive environment for technological and financial experimentation, innovation, and competition. Together, these features make it possible for industry to combine the functionality of different DeFi protocols to provide new, novel, and highly bespoke financial products and services. Because neither the original DeFi protocols nor the resulting combinations would be controlled by a single financial intermediary, entrepreneurs would be free to experiment with new combinations, promoting greater competition and innovation. Others in industry could then build on these new combinations, spurring further rounds of competition and innovation. Beyond finance, distributed ledgers could one day provide the technological infrastructure for higher order web3 and DeFi developments within the digital economy, including applications and infrastructure serving as the architecture for next-generation "smart cities".[43]

  The open technological architecture and envisioned transparency of DeFi also provide a supportive environment for the application of machine learning (ML) and generative artificial intelligence (AI). In particular, the integration of ML and generative AI tools into DeFi projects, enterprises, and ecosystems can help design new financial products and services, improve risk management and fraud detection, enhance cybersecurity, contribute to more effective regulatory compliance programs, and assist with the identification of potential threat vectors.[44] The transparency and immutability offered by distributed ledger technologies may help in achieving objectives like explain-ability and auditability desired in AI solutions.[45]

---

[40] *See* Robert Rueter, Executive Director of the Inclusive Design Institute, as quoted in the Nevada Entrepreneurial Ecosystem Assessment and Strategy (2023).

[41] *See* Catherine Powell and Guest Blogger for Women Around the World, "Women on the Blockchain: Moving Beyond 'Blockchain Bros'", Council on Foreign Relations (July 10, 2019).

[42] *See* Tressie McMillan Cottom, "Where Platform Capitalism and Racial Capitalism Meet: The Sociology of Race and Racism in the Digital Society", 6:4 Sociology of Race and Ethnicity 441 (October 2020).

[43] *See* Shanghai Municipal People's Government website, "Shanghai Stays on Course for Digital Upgrade" (October 2023).

[44] *See, e.g.*, Forrest Colyer, John Liu & Michael Greenwald, "The Convergence of AI and Digital Assets: A New Dawn for Financial Infrastructure", Amazon Web Services Blog (October 19, 2023).

[45] *See* White House, Office of Science and Technology Policy, "Blueprint for an AI Bill of Rights" (October 2022).

- *Relevant Policy Objectives:* Safe and Affordable Access, Illicit Finance, U.S. Leadership

- *Current State of Play:* DeFi technologies and ecosystems have not yet reached an inflection point of mass adoption, integration, or critical dependency with respect to the provision of high value financial products and services. However, interest and experimentation in DeFi, as well as other digital assets, has grown significantly across jurisdictions in recent years—within even large and well-established banks, financial market utilities, and even central banks that are now entering the market.[46] With the ongoing expansion of research and development into the potential use of decentralized networks to clear and settle payments and facilitate the trading of digital assets, along with the desire in many jurisdictions to upgrade their antiquated financial infrastructure, it seems likely that the opportunities for DeFi projects, enterprises, and ecosystems to contribute to innovation will expand over time. While it is difficult to predict, these innovations may also lead to more general applications of DeFi technology within the broader digital economy. DeFi innovations, even if not yet mature, are also catalyzing innovation in traditional financial infrastructures. Many retail and wholesale central bank digital currency (CBDC) projects, including cross-border payment proof of concept, are at least in part motivated by an acknowledgement of the nascent competitive threat posed by DeFi and other distributed ledger technology-based innovations.

- **Strengthening U.S. leadership in technology and financial services.** As a global leader in both finance and technology, the U.S. is well positioned to play an influential role in shaping the future trajectory of DeFi. In the face of a growing number of potential challengers,[47] U.S. policymakers and industry should work together to ensure that the ongoing development of DeFi projects, enterprises, and ecosystems—and the regulatory frameworks that govern them—serve to strengthen this leadership in conjunction with meeting other policy objectives. This includes playing an active role in the development of international regulatory frameworks, industry technical standards, and research and development in strategically important areas

[46] *See* Atlantic Council, *Cryptocurrency Regulation Tracker* (2023).

[47] *See* Ananya Kumar and Josh Lipsky, "The Dollar Has Some Would-Be Rivals. Meet the Challengers", Atlantic Council (September 22, 2022).

like encryption, cybersecurity, RegTech, and financial law and regulation. To protect the longstanding role of U.S. financial intermediaries and the U.S. dollar in international trade and finance, it also includes promoting the resilience and technological interoperability of payment systems and other critical financial infrastructure—both across borders and between the DeFi and TradFi ecosystems.

U.S. leadership is particularly important in the realm of money and payments. Several countries, including China— which recently announced its intention to move forward with the development of the digital yuan[48]—have already signaled their intention to invest in new technological infrastructure to support their domestic and cross-border payment systems. Nevertheless, and regardless of whether it decides to go down the same path, the still nascent state of industry development represents an opportunity for the U.S. to assert its leadership, and to articulate its vision for the future of money and payments, through various international fora. Ensuring that U.S. policymakers and industry remain engaged on the international stage is key to promoting sustainable DeFi innovation, the development of common industry technical standards, and the emergence of clear, consistent, and comprehensive regulatory frameworks. It is also key to ensuring that U.S. policymakers, financial intermediaries, and DeFi builders remain at the forefront of these developments.

- *Relevant Policy Objectives:* National Security, Illicit Finance, U.S. Leadership

- *Current State of Play:* While U.S. software developers have and continue to play an important role in building DeFi projects, enterprises, and ecosystems, the U.S. regulatory environment is perceived by many in the DeFi industry as ambivalent, if not hostile, towards its future development. As a consequence, many of these projects, enterprises, and ecosystems currently operate overseas. Nevertheless, given the size of the U.S. market, there are still powerful incentives for them to provide financial products and services to U.S. citizens and residents. Accordingly, in the presence of a clear, consistent, and comprehensive approach to the regulation of DeFi, it is possible that many of these projects, enterprises, and ecosystems would move back to the U.S.

(C) Risks Presented by DeFi

The continued development of DeFi projects, enterprises, and ecosystems holds out a myriad of opportunities for improving the delivery of financial products and services. Yet given the current state of play, DeFi builders still have a long way to go in order to capitalize on these opportunities. Compounding this challenge, the decentralized structure of DeFi networks poses a number of significant and, in many respects, unique risks. Just as the opportunities presented by DeFi can help advance the important objectives of financial policy and regulation, these risks threaten to undermine them. This section describes these risks in greater detail, focusing specifically on the risks to investors and consumers, market integrity, the reliability and resilience of DeFi networks, broader financial stability, and U.S. national security and leadership in the realms of finance and technology.

Before turning to these risks, it is worth briefly exploring how policymakers and regulators should approach the process of identifying, evaluating, measuring, and responding to them. This process is especially critical in light of the many, important, and yet often conflicting objectives of financial policy and regulation. The general approach to risk-based regulation can be captured in the following equation:

[48] *See, e.g.*, Mike Orcutt, "What's next for China's digital currency?", MIT Tech. Review (August 3, 2023) ("If [China is] successful, it could challenge the US dollar's position as the world's dominant reserve currency—and in the process shake up the global geopolitical order.").

FIGURE 5: THE RISK EQUATION

Risk = Threat x Probability x Impact – Mitigation

DEFI RISKS

Policymakers must understand the type, nature, sources, probability, and potential impact of identified risks. The decentralized structure of DeFi networks poses a number of significant and, in many respects, unique risks for:

- **Investors and consumers –** lack of technology and DeFi literacy, fraud, market manipulation, conflicts of interest, data breaches and undesirable privacy violations, custody risk, bankruptcy risk, algorithmic discrimination
- **Market integrity** – vulnerabilities to wash trading, front running, and pump and dump schemes; oracle exploitations
- **DeFi projects, enterprises, and ecosystems –** complex and hard to map counterparty risks, enhanced reliance on outsourcing relationships, limited control rights during periods of institutional or systemic stress, software security vulnerabilities, automating failure
- **Financial system stability –** cross-sectoral systemic risks, complex interconnections with significant economic and technological exposures, concentration risks, hardwired procyclicality
- **Combating illicit finance, protecting national security, and maintaining U.S. leadership –** loss of geopolitical status as provider of the global reserve and transaction currency, loss of surveillance and accountability-enforcing capacity to combat illicit finance and safeguard national security
- **Climate –** significant energy consumption, pollution, noise, and other environmental impacts

The first stage of the process involves identifying, defining, and cataloging the relevant risks. Ideally, this should include an attempt to map these risks onto the existing or potential future vulnerabilities through which they might eventually emerge and metastasize. The second stage of the process involves an assessment of the probability that a given risk might materialize.

While this can often be a highly subjective process, especially in the presence of significant data gaps, this stage involves an assessment of the nature of the relevant risks, their sources, the relationships between them, and any other factors that bear on the probability that they will materialize in a given context or over a given timeframe. The final stage of the process then involves an attempt to estimate the size, scope, and distribution of the real world impact if and when one or more of these risks does actually materialize. This includes an assessment of the impact of these risks both with and without any attempts to mitigate them. In theory, these mitigation mechanisms could include technological solutions, governance changes, or new regulation designed to minimize the probability or impact of these risks.

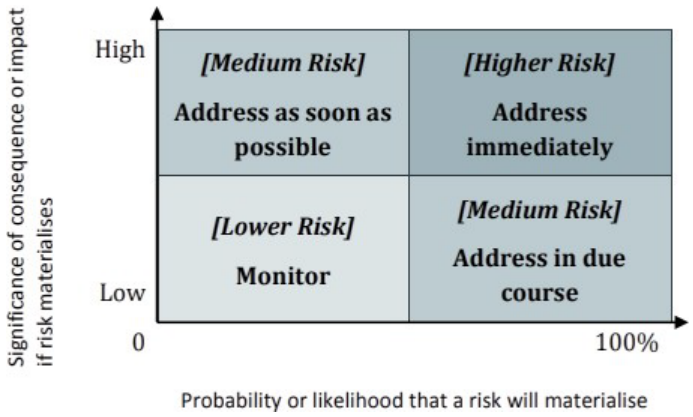
FIGURE 6: THE RISK ASSESSMENT PROCESS

Stage	Key processes
Risk Identification	• Risk identification, definition, and cataloging • Mapping risks to vulnerabilities
Probability Assessment	• Identifying the nature and sources of risks • Mapping the relationships between risks • Identifying other causal variables
Impact Assessment	• Estimating the scope, size, and distribution of risk impact
Risk Mitigation	• Identifying potential mitigation mechanisms • Estimating and comparing the impact of mitigation mechanisms

This assessment process demands a sophisticated understanding and honest intellectual accounting of the type, nature, sources, probability, and potential impact of identified risks. Even then, policymakers will often not possess all of the relevant information needed to conduct complete or accurate risk assessments. Nor do they possess a crystal ball that would enable them to predict how a particular market, institution, industry, or technology will evolve over time, or the consequences stemming from the introduction of a given mitigation mechanism. Nevertheless, this process is often extremely valuable in identifying and mapping the universe of potential risks, understanding their likely impact, and laying the intellectual and empirical groundwork for possible regulatory action.

Importantly, this risk-based approach is particularly valuable in shaping how policymakers approach the emergence of novel markets, institutions, industries, and technologies. More broadly, this approach can also help policymakers set regulatory priorities and mediate between different, and potentially conflicting, regulatory objectives. For example, probability and impact assessments can help policymakers determine where to direct scarce financial, regulatory, human, and other resources: allocating more resources to those risks with a high probability and potential impact, and less to those with a lower probability and impact (*see* Figure 7). These resources can then be used to identify where mitigation mechanisms are likely to yield the greatest reduction in risk, which mitigation mechanisms are likely to be most effective, and ultimately where to target regulatory action.

FIGURE 7: DETERMINING REGULATORY PRIORITIES[49]



The first step in the risk assessment process is identifying, defining, and cataloging the relevant risks and then mapping them onto the vulnerabilities of the markets, institutions, industries, and technologies in which they potentially arise. The principal risks arising in the context of DeFi projects, enterprises, and ecosystems include:

- **For investors and consumers.** In theory, the transparency associated with DeFi projects, enterprises, and ecosystems means that investors and consumers have at their disposal a wealth of information upon which to make informed financial decisions. Yet in practice, DeFi is still characterized by significant *asymmetries of information*. As a preliminary matter, DeFi products and services typically require investors and consumers to possess a high level of financial and technological expertise. Many DeFi products and services, especially those delivered through DeFi compositions, are also extremely complex, demanding that investors and consumers invest significant time and effort to fully understand how they work.[50] The resulting information costs make it difficult for investors and consumers to fully understand the market, liquidity, counterparty, custody, and other risks that they are taking. These costs also heighten their exposure to theft, fraud, privacy violations, market manipulation, Ponzi schemes, rug pulls, and other forms of exploitation.

  The risks associated with pervasive asymmetries of information are compounded by the deeply entrenched *conflicts of interest* within many DeFi projects, enterprises, and ecosystems. For example, the developers of DEXs or DeFi lending protocols may also be important participants in the markets for the digital assets that trade or are used as collateral on these platforms. The pseudo-anonymous nature of DeFi then makes it extremely difficult for investors or consumers to identify these conflicts of interest, and for regulators to effectively police them. These information problems and conflicts of interest will be exacerbated where DeFi projects, enterprises, and ecosystems are characterized by decentralized access: lowering barriers to entry for investors and consumers, including for less sophisticated users.

  In a similar vein, the decentralized governance of many DeFi projects, enterprises, and ecosystems poses a number of potentially significant risks. For example, the pseudo-anonymous nature of DeFi means that the holders of DAO governance tokens may be unable to ascertain the existence of large voting blocs or the presence of other token holders who, by virtue of their relationships with core developers or other key stakeholders, possess a degree of control that is disproportionate to their token holdings. In many cases, it may also be difficult for less sophisticated

[49] *See* Financial Action Task Force (FATF), *FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment* (2013).

[50] *See* Hilary J. Allen, "DeFi: Shadow Banking 2.0?", 64 William and Mary Law Review 919 (2023).

token holders to determine the level of unilateral control reserved for gatekeepers holding administrative or guardian keys. Where these blocs or gatekeepers are able to exercise a significant degree of control, decentralized governance may ultimately be an illusion.

DeFi projects, enterprises, and ecosystems can also expose investors and consumers to a wide range of more specific risks. The use of open source software, smart contracts, decentralized governance protocols, oracles, and bridges make DeFi networks particularly vulnerable to certain *operational*, *technological*, and *security risks*: exposing investors and consumers to both the loss or theft of their digital assets[51] and the unlawful or otherwise harmful disclosure of sensitive personal information. Many DeFi networks are characterized by liquidity and maturity mismatches that expose investors and consumers to conventional *run risks*. The users of DeFi lending protocols are often subject to *liquidity risk*: including the risk that the digital assets used to collateralize their exposures experience a sharp fall in value, trigging automated liquidation and deleveraging, and generating pernicious fire sale dynamics. Lastly, the use of automation in the delivery of finance products and services exposes consumers to the risk of *algorithmic discrimination*.

All of these risks are often compounded by the *lack of clear lines of responsibility* associated with decentralized development and governance, and the resulting lack of recourse for investors and consumers if and when things do go wrong. This feature of DeFi systems may present the clearest way in which DeFi poses risks to consumer and investor harm, since it implicates no clear route to ensuring the implementation of necessary mitigations for various identified risks to consumers and investors. For example, automation enabled by smart contracts can require that DeFi operations be fool-proof and robust on all possible edge cases, which presents extreme difficulties for any system of even minor complexity. Protecting DeFi consumers and investors is further challenged by the potential absence of control over, or responsibility to use, any such mechanisms. The ability to implement mitigations may be further limited due to features of immutability, which can challenge the ability to make positive changes to a system that may be needed to help defend and provide redress for consumers.

- **For market integrity.** The opaque and pervasive conflicts of interest created by the complex web of relationships between financiers, developers, and other market participants pose a number of risks to market integrity. The pseudo-anonymous nature of DeFi projects, enterprises, and ecosystems, combined with a lack of effective regulation, makes them particularly vulnerable to both *wash trading* and *front running*. The same pseudo-anonymity, combined with the use of social media, also makes them vulnerable to so-called *"pump and dump" schemes*. Meanwhile, the reliance on oracles for key real world inputs that support the execution of smart contracts render the digital asset markets based on these contracts vulnerable to *oracle exploitations*. By facilitating artificial price manipulation within digital asset markets, these trading and other strategies can harm investors, undermine market confidence, and impede the continued growth of DeFi. As with risks presented to consumers, the *lack of clear lines of responsibility* further complicates the ability to emplace mechanisms to address these risks, as one would be able to do in TradFi. The absence of sufficient governance systems, backstopped by regulation and accountability, inhibits the systems' abilities to respond to unexpected events and to foster trust.

[51] Billions of dollars per year have been lost in hacks targeting DeFi platforms. *See* TRM Labs, "DeFi, Cross-Chain Bridge Attacks Drive Record Haul from Cryptocurrency Hacks and Exploits" (December 16, 2022); and Chainalysis, *2023 Crypto Crime Report* (2023).

- **For DeFi projects, enterprises, and ecosystems**. The technological architecture of DeFi also poses a number of risks for DeFi projects, enterprises, and ecosystems themselves. As a preliminary matter, the use of open source software, combined with pseudo-anonymous participation in decentralized networks, create opportunities for *malicious actors* to manipulate consensus protocols, gain control of a network, access the private keys of other network users, or view their personal information. In addition to harming investors, consumers, and other stakeholders, these malicious attacks can undermine confidence in, and the stability of, DeFi projects, enterprises, and ecosystems.[52] Open source software may or may not be inherently more secure than closed source software; the security of the platform relies heavily upon the quality, timeliness, and effectiveness of the community of contributors that can identify and address vulnerabilities.[53] Especially in instances of open source software, the public nature of the code directly exposes the platform to intense scrutiny from actors seeking to exploit weaknesses. For DeFi activities that are inherently financial and present as potential high value targets, it can be extremely difficult to design code for the underlying blockchain and applications that can stand up to persistent targeting by cybercriminals, including state actors and advanced persistent threats.

  The use of smart contracts—self-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. Where this is the case, the resulting smart contracts—like their real-world counterparts—will invariably be *incomplete*. This incompleteness is most likely to reveal itself, and inflict the most harm, during periods of acute market, institutional, or network stress, leading to potential operational failures, preventing contractual performance, and undermining trust and confidence in DeFi projects, enterprises, and ecosystems. Where DeFi projects, enterprises, and ecosystems are characterized by decentralized development, this can also make it more difficult to implement necessary changes and updates in a timely manner to address this incompleteness and respond to any unfolding crises.

  The problem of contractual incompleteness is compounded by the inherently self-executing nature of smart contracts. Specifically, where self-executing software provides the impetus for actions in the real world—*e.g.,* by entering a buy or sell order on a DEX, or automatically liquidating the collateral posted with a DeFi lending protocol—any incompleteness in the relevant smart contracts can generate significant, and potentially destabilizing, unintended consequences. The market disruption unleashed by Knight Capital in August 2012 offers an illuminating example from the world of TradFi. Knight Capital was engaged in high frequency trading: a strategy that involved using sophisticated algorithms to rapidly execute buy and sell orders for U.S. equity securities. As a result of a coding error, over a 45-minute span Knight's algorithms inadvertently executed trades involving more than 397 million shares, acquiring approximately $7 billion in unwanted positions, and eventually resulting in a loss of over $460 million. The high volume of trading activity over such a short period of time also caused a major disruption on the New York Stock Exchange. In theory, these types of *hard-wired algorithmic failures* may be an even bigger risk in the DeFi world, where highly complex compositions, along with the absence of centralized intermediaries and governance mechanisms, may make it more difficult to intervene at an early stage to arrest these failures and their unintended consequences.

  Lastly, DeFi projects, enterprises, and ecosystems frequently rely on more centralized network nodes for the delivery of critical inputs. Prominent examples include stablecoins, oracles, cross-chain bridges, and AI and cloud computing services. In the same vein, most DeFi applications are currently built on a single distributed ledger: the Ethereum blockchain. Industry reliance on a small number of providers for the delivery of these inputs can result in network congestion and outages. Reliance on centralized nodes also exposes DeFi

[52] *See* Metrika, "Understanding and Managing Blockchain Risk", 16 Journal of Risk Management in Financial Institutions (2023).

[53] *See* Ashely Schuett, Alison Parker, and Alex Long, "Open Source Software and Cybersecurity: How Unique is This Problem?" Wilson Center (November 10, 2022).

projects, enterprises, and ecosystems to operational, technological, and security risks. In effect, these nodes represent a single point of failure, making them targets for malicious actors and exposing the DeFi networks that rely on them to the risk of interruption, corruption, and the resulting inability to provide financial products and services to their own investors and consumers.

- **For financial stability**. At present, DeFi projects, enterprises, and ecosystems are nowhere near large, critical, or interconnected enough to pose a clear and present danger to U.S. or global financial stability. Nevertheless, as the scale, scope, and importance of DeFi continues to grow, it may eventually create new sources of systemic risk. Despite its underlying transparency, 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. The continued reliance on a small number of distributed ledgers or centralized network nodes would lead to *concentration risk*: the risk that any interruption to the products and services they provide could spill over into the wider DeFi ecosystem, creating instability and—depending on the circumstances—perhaps even into the TradFi system and real economy. In addition to these concentration risks, the composability of DeFi supports the development of multi-functional platforms that combine digital asset trading, lending, investment advice, custody, payments, and other financial products and services. This combination of products and services can create *conflicts of interest* and exacerbate the risks posed by *excessive leverage* and *liquidity mismatches*[54] Lastly, the highly automated nature of many DeFi projects, enterprises, and ecosystems introduces the possibility of *hardwired procyclicality*. Perhaps most obviously, the highly correlated and automated liquidation of collateral by DEXs or DeFi lending protocols could trigger downward pressure on prices within digital asset markets, triggering additional automated liquidations, and further reinforcing the downward spiral in prices. This rigidity of smart contract-operated financial systems could prevent critical interventions needed in cases of crises to prevent great harms like runs and fire sales.[55]

- **For combatting illicit finance, protecting national security, and maintaining U.S. leadership**. The emergence and growth of DeFi poses several challenges to the ability of the U.S. to effectively combat illicit financing, protect its national security, and maintain its global leadership in finance and technology. As a starting point, the pseudo-anonymity facilitated by DeFi payment networks, the ability to "wrap" stablecoins and other digital assets in order to move them across chains, and the option to conduct off-chain transactions, can make it harder to identify money laundering and terrorist financing and trace the flow of illicit funds, especially when compounded by the inherent speed of value transfer permitted by these technologies. By the same token, fully decentralized payment networks pose new challenges for the design and implementation of the compliance frameworks through which anti-money laundering and terrorism financing laws are monitored and enforced.[56] Perhaps most importantly, whereas the conventional approach toward compliance with these laws allocates front-line responsibility for identifying and reporting suspicious transactions to banks and other financial intermediaries, the decentralized nature of these networks demands that policymakers rethink who should ultimately bear this responsibility, along with the regulatory and technological tools necessary to ensure effective compliance.

  Combatting illicit financing is critical to U.S. national security. So too is the ability to effectively target and enforce economic sanctions, pursue international criminal and civil enforcement actions, and project economic strength abroad. Importantly, the ability of the U.S. to wield this geopolitical power and influence is highly dependent on the central role of U.S. markets and institutions in global finance, along with the dominant role

[54] *See* Financial Stability Board (FSB), "The Financial Stability Implications of Multifunction Crypto-asset Intermediaries" (November 28, 2023).

[55] *See* Hilary J. Allen, "DeFi: Shadow Banking 2.0?", 64 William and Mary Law Review 919 (2023).

[56] *See* FinCEN, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019); U.S. Treasury, "Illicit Finance Risk Assessment of Decentralized Finance" (April 2023).

of the U.S. dollar as a global reserve currency and in international trade and investment. Ultimately, it is the threat of being cut off from access to these markets, institutions, and international payment networks that make these sanctions and other enforcement mechanisms effective economic weapons and deterrents.

Experts have long discussed risks that ongoing development of financial projects, enterprises, and ecosystems outside of the United States may in the long term open the door for its geopolitical competitors to challenge U.S. leadership in these realms.[57] In the event that these challenges were successful, the likelihood and contributing factors for which require extensive study,[58] one of the effects could be to reduce U.S. financial surveillance capabilities, thereby undermining its ability to effectively combat illicit financing or wield economic sanctions, and heightening the risks to national security. While these challenges transcend DeFi, further transitioning offshore of significant financial projects, enterprises, and ecosystems—including those related to DeFi— and failing to support their responsible development through effective regulation and enforcement could potentially compound these challenges in the long term.

These risks share a common theme. Simply ignoring the emergence, development, and adoption of DeFi, or failing to fully engage with broader international efforts to build and regulate DeFi projects, enterprises, and ecosystems, poses potential risk of longer-term erosion of U.S. economic power and influence.

- **For the climate.** The creation, trading, clearing, and settlement of digital assets within DeFi ecosystems—especially those based on cryptographic tools built on proof of work—can require significant electricity consumption, thereby contributing to greenhouse emissions and creating pollution, noise, and other environmental impacts in the communities near mining facilities.[59]

As with any technological or financial system, it is critical to underscore that one DeFi project, enterprise, or ecosystem is not necessarily like another—the potential impact of these risks and mitigations can be significantly shaped by the specific design choices and implementations along technological, functional, and operational dimensions. For example, whether a distributed ledger is permissioned or permissionless will inevitably affect the nature and sources of the relevant risks. Permissionless systems that permit anyone access without built-in controls to detect or root out bad actors may present heightened risk of illicit financing, countermeasures against which are generally reliant on understanding a certain amount of information about customers and counterparties. However, the greater level of decentralization and redundancy generally associated with permissionless versus permissioned systems may better withstand network disruptions, which could present lower risks for operational resilience and cybersecurity.

Understanding the source of the risks is equally important when considering options for potential mitigations or countermeasures. Yet assessing both the source and nature of risks in DeFi is challenged by current limitations of useful, consumable, and verifiable data to support market surveillance and oversight by regulators, as well as to help regulated institutions and consumers accurately assess their exposures and changes in risk profile by engaging in certain DeFi activities.[60] This is generally derived from the current state of DeFi's extremely limited financial reporting, broad market data, and registrations and licenses of businesses in the ecosystems that would enable more information collection and oversight of both on-chain and off-chain activities supporting the financial services. While RegTech firms

[57] For example, Treasury and other experts have noted potential long term impacts that foreign central bank digital currencies and private digital assets, including stablecoins, could have on demand for U.S. dollars. *See* U.S. Treasury, Report Pursuant to Section 4(b) of Executive Order 14067, "The Future of Money and Payments" (September 2022); U.S. Treasury, "Remarks by Under Secretary for Domestic Finance Nellie Liang During Workshop on 'Next Steps to the Future of Money and Payments'" (March 1, 2023); and Daniel McDowell, "Bucking the Buck: U.S. Financial Sanctions and the International Backlash against the Dollar" (2023).

[58] *See* Atlantic Council, "Dollar Dominance Monitor" (2023).

[59] *See* White House, "Fact Sheet: Climate and Energy Implications of Crypto-Assets in the United States" (September 8, 2022).

[60] *See* IOSCO Consultation Report, "Policy Recommendations for Decentralized Finance (DeFi)" (2023).

have arisen in DeFi, there are still not sufficient data providers in this highly specialized and fragmented domain. Limited or no access to underlying data to assess the validity of these vendors' data sets and analytic conclusions also presents risks for regulators to trust third party assessments and an inability to investigate or query the outputs or determinations, just as the limitations of the regulators themselves in capacity to consume and leverage available data presents risks for ensuring effective oversight. Ultimately, this issue of information gaps presents a cross-cutting issue across all risk areas outlined that can limit policymakers and engineers alike from developing a sophisticated understanding of the type, nature, sources, probability, and potential impact of identified risks to tailor their approaches to technical solutions and regulatory expectations across the DeFi spectrum.

IV. Issues for DeFi Policymakers and Industry

Having identified the opportunities and risks presented by DeFi, it is possible to distill several key issues for both policymakers and industry. Both the public and private sectors hold critical and unique roles, responsibilities, and capabilities for designing and implementing policy frameworks governing financial markets, institutions, and systems—neither side can do it alone. Unconstrainted technological development can be harmful and destabilizing. Yet policy frameworks designed to prevent or minimize these harmful and destabilizing effects are of limited value unless they are driven by political will, supported by sufficient resources, grounded in technical expertise, and actually capable of implementation by both regulators and industry players. Accordingly, both policymakers and industry should devote effort to dissecting these key issues, especially with an eye toward identifying those that are most tractable, prioritizing near- and long-term regulatory, development, and engagement efforts, and evaluating their own needs for internal resourcing and capacity building.

(A) Issues for Policymakers

Policymakers bear ultimate responsibility for articulating, monitoring, and enforcing compliance with legal frameworks that advance the many and important objectives of financial policy and regulation. These frameworks can be highly complex, ranging from regulatory requirements for industry bodies and individual citizens, to investigative and enforcement capabilities of supervisory and law enforcement authorities, to positive incentives to promote market and consumer behavior, all of which should work in harmony to pursue policy goals. Yet mapping these complex frameworks and objectives onto equally complex and rapidly evolving DeFi projects, enterprises, and ecosystems can be incredibly difficult.

Compounding this challenge, some of the more novel features of these projects, enterprises, and ecosystems may also demand that policymakers fundamentally rethink or reframe their current regulatory frameworks, along with their approaches to supervision and enforcement. It may involve changing strategies for many long-understood and examined financial activities when the existing approach does

ISSUES FOR POLICYMAKERS

Policymakers bear great responsibility and authority for shaping the responsible development of DeFi. To successfully develop and implement regulatory strategies in a space with very complex business models and technologies, as well as a challenging environment for dialogue, policymakers will have to address several core issues:

- Determining whether and how DeFi systems fall within the existing regulatory perimeter
- Identifying whether, where, and how the regulatory perimeter might need to be expanded
- Crafting the appropriate regulatory response
- Allocating responsibility and accountability for regulatory compliance in a world of decentralized governance
- Mapping counterparty exposures in a world of decentralized balance sheets
- Mapping key service providers and services in a world of decentralized operations
- Oversight of new and rapidly evolving technology
- Ensuring DeFi lives up to critical policy objectives of expanded financial access, transparency, and responsible governance
- Mitigating the unique threats DeFi poses
- Identifying the best role for policymakers in building DeFi (standards, research, identity)
- Fostering a robust and constructive dialogue with industry

not appropriately or easily apply or achieve the desired end-state of previously-established approaches. And even where policymakers are willing to rethink these frameworks and approaches, they must still overcome the technocratic challenges of design and implementation and the practical challenges of ensuring sufficient engagement and buy-in from regulated industries and actors. Making forward progress on engagement will be complex in identifying the right levers and roles to foster identified and needed market evolutions, and addressing real or perceived hostilities across stakeholders in this space. Addressing these challenges requires capability, capacity, and political will, backed with resourcing and prioritization.

The core issues that policymakers should address in connection with the rise of DeFi include:

- **Determining whether and how DeFi projects, enterprises, and ecosystems fall within the existing regulatory perimeter.** Policymakers should start by evaluating whether and how the current universe of DeFi projects, enterprises, and ecosystems fall within the perimeter of existing regulatory frameworks and corresponding obligations. This includes an evaluation of whether they fall within both the *subject matter* and *geographic* jurisdiction of U.S. regulators and law enforcement. This assessment will help regulators clearly delineate for themselves, other authorities like law enforcement, and for industry where the bounds of responsibility and permissible activity for those regulated entities lay within DeFi.

  Assessing jurisdiction can be challenging, though. Evaluating subject matter jurisdiction requires a complex understanding of elements like actors, components, and economic functions of the systems; potentially where key points of control and sufficient influence exist; and if a regime is technology-specific,[61] what the state and features are of the technologies involved to see if they fall under established policy.[62] In addition to complex and distributed business models and technologies, regulators will have to determine whether or not having one or multiple parties conduct parts of regulated functions or activities, but not all of them, would trigger the application of regulatory frameworks. DeFi's highly dispersed business operations and activities over cross-border digital networks that, while conducted by entities and over networks that rely on physical infrastructure, can also present difficulties in discerning locations of system components and actors.[63] It is likely that at least some portion of most DeFi systems fall under existing regulatory authorities, whether simply individuals involved and users that fall under obligations like taxation or sanctions restrictions, or where there are activities and/or involved persons that are generally functioning as intermediaries in regulated activities such as money transmission or trading in securities or commodities.

  Where these projects, enterprises, and ecosystems do fall within the existing regulatory perimeter, policymakers can then shift focus to regulatory implementation and enforcement, including evaluating whether current regulatory frameworks effectively address the unique risks posed by DeFi. Even where these projects, enterprises, and ecosystems only partially fall within the regulatory perimeter, this will still provide a platform for further risk assessment, industry engagement and, where necessary, enforcement action. Once regulators assess the existing DeFi and regulatory landscapes, they can move forward with determining if any changes to that coverage are needed via expansion or adjustment to address risks and optimize benefits.

[61] Most of the existing U.S. regulatory framework for digital assets are technology-neutral, meaning that regulatory obligations are not triggered by the use of a certain technology—in this case distributed ledger technology and digital assets— but instead by the institutional status, functions, or activities performed by a regulated actor regardless of specific technologies used to perform these functions or activities.

[62] *See* Financial Action Task Force, "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (2021).

[63] *See* Inca Digital, "Geotagging Crypto Users on the Top Decentralized Exchanges Using NLP" (2023).

Financial policy and regulation is far from the only domain in which policymakers should evaluate whether and how DeFi elements or entire systems fall within the regulatory perimeter. For example, there are several ongoing initiatives to create regulatory frameworks for cybersecurity incident reporting for *critical infrastructure* operators[64] and imposing KYC and other requirements on *Infrastructure-as-a-Service (IaaS) providers*.[65] Depending on how these frameworks are developed and implemented, they could potentially apply to DeFi and its underlying infrastructure.

- **Identifying whether, where, and how the regulatory perimeter might need to be expanded in order to capture DeFi projects, enterprises, or ecosystems.** Having identified any gaps within the existing regulatory perimeter, policymakers should determine whether this perimeter needs to be expanded to capture DeFi projects, enterprises, and ecosystems. Policymakers should also determine whether the regulatory frameworks and approaches used within the existing perimeter, as applied to DeFi, sufficiently address the key risks posed by DeFi. Where policymakers determine that the regulatory perimeter needs to be expanded, or that applicable regulatory frameworks do not address the relevant risks, they will then need to identify what legislative and regulatory changes are necessary to bring DeFi within the perimeter and ensure that these frameworks are ultimately fit for purpose.

  Most existing regulatory frameworks target the application layer of the DeFi technology stack: where responsible actors, functions, and customer interfaces are often more readily identifiable. However, where risks are not effectively addressed at the application layer, authorities must look elsewhere within DeFi projects, enterprises, and ecosystem to identify where to locate responsibility for regulatory compliance and the imposition of systems, processes, and controls in a manner that is both consistent with regulatory objectives and robust to changing circumstances.[66]

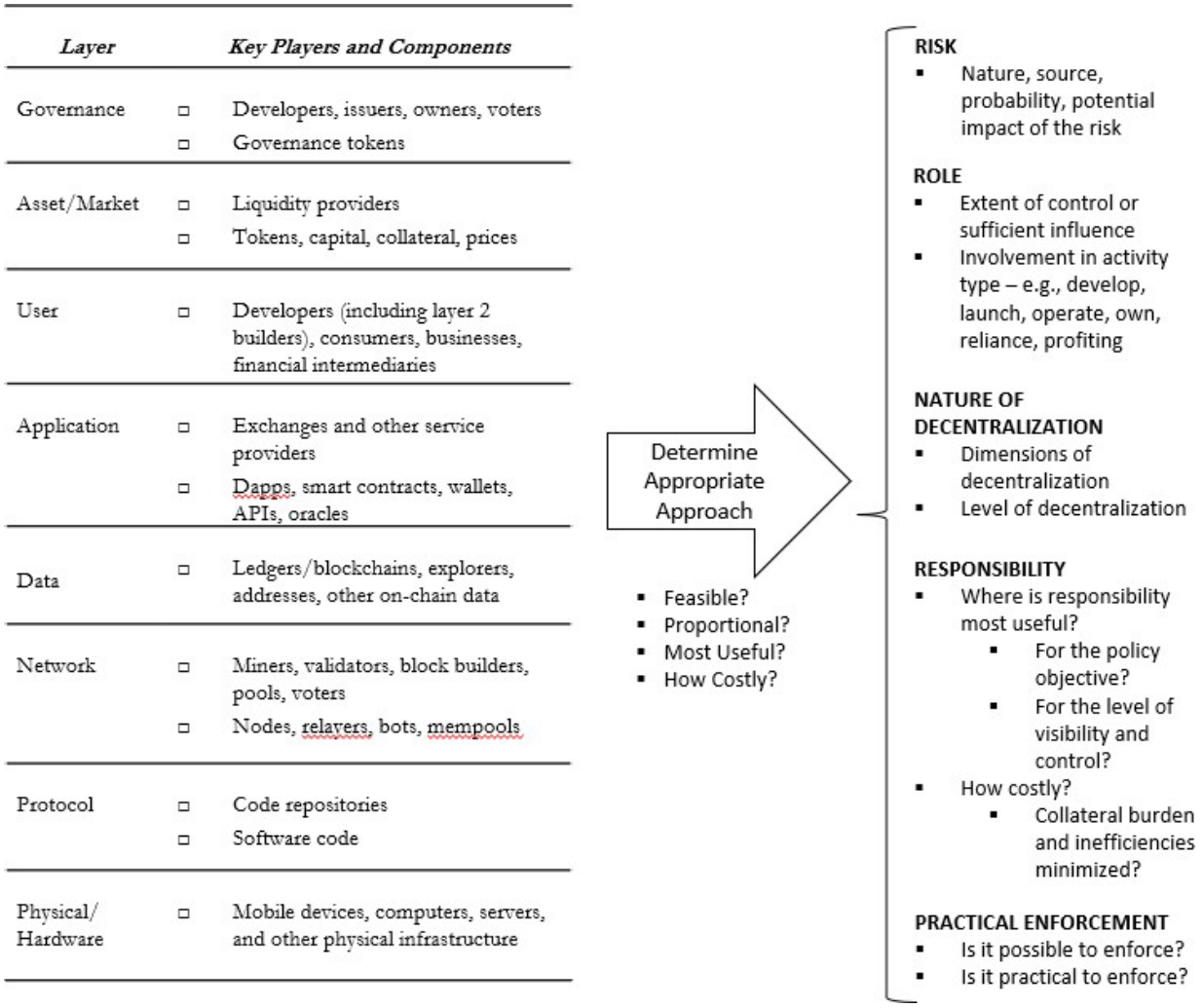
  Along the same vein, any expansion in the regulatory perimeter may demand new thinking about the types of institutions, functions, or activities that can and should be subject to some form of regulatory oversight. In assessing what options are available and optimal, it can be helpful to consider the key players and components within each layer of the DeFi technology stack. Specifically, policymakers should examine what makes an expansion in the regulatory perimeter appropriate: including whether it is *feasible* or accomplishable; whether it is *proportional* in consideration of the nature of the risk and of the burden imposed; whether it is as *useful* in advancing desired policy objectives and benefits; and *how costly* it is as a way to advance these objectives.

[64] *See* the Cyber Incident Reporting for Critical Infrastructure Act of 2022.

[65] *See* Department of Commerce, 86 FR 53018, Advanced Notice of Proposed Rulemaking, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities" (September 24, 2021); and President Biden's Executive Order 14110, "Executive Order on the Safe, Secure, Trustworthy Development and Use of Artificial Intelligence" (2023).

[66] This is consistent with a concept dubbed by Dr. Dan Awrey as the "first law of regulation," adapted from the first law of thermodynamics, indicating that the general amount or mass of regulation and regulatory functioning can neither be destroyed or created, only transformed in shape and form, including through dispersal across government regulators, self-regulatory bodies, and regulated entities. *See* Dan Awrey, Presentation to the CFTC TAC, "Stability and Security Challenges and Regulatory Implications for Crypto" (July 18, 2023).

FIGURE 8: EVALUATING THE APPROPRIATE REGULATORY APPROACH TO ACCOUNTABILITY IN DEFI



Generally, this examination will involve identifying and evaluating the nature and sources of the relevant risk, the key players within the project, enterprise, or ecosystem, and the critical roles these players perform (*see* Figure 8). Based on this examination, policymakers should then determine the most appropriate target and form of regulatory intervention. For example, actors at the network, protocol, and governance layers will often possess more detailed and timely information about network and market functioning. They will also often wield significant power over network functionality, along with an understanding of how the positive or negative consequences of that functionality are distributed across the network. These attributes may make these actors effective targets for regulatory intervention. They may also be the actors most willing and able to work with policymakers to mitigate risks that cannot be effectively addressed at the application layer.[67]

[67] It is also possible that entities operating at layers like the network, protocol, and governance layers may already be subject to certain regulatory expectations in jurisdictions like the United States. For example, the U.S. Treasury Office of Foreign Assets Control (OFAC) referenced U.S. person digital asset administrators and miners as members of the virtual currency industry "responsible for ensuring they do not engage in unauthorized transactions or dealings with sanctioned persons or jurisdictions." *See* U.S. Treasury Office of Foreign Assets Control (OFAC), "Sanctions Compliance Guidance for the Virtual Currency Industry" (September 21, 2021).

When identifying potential targets for regulatory intervention, policymakers will need to consider where this intervention is likely to impose the lowest costs and otherwise generate the fewest unintended consequences, resulting in an appropriate balance of cost and benefit. For example, the imposition of broad reporting requirements can impose significant costs on both government agencies—which must collect and maintain the relevant data—and citizens and businesses—which must share their data in compliance with these requirements. More broadly, poorly targeted or overly burdensome regulation poses risk to U.S. competitiveness and innovation, along with its leadership in the realms of both finance and technology. Finally, policymakers will have to confront the major issue of enforceability. Considering where enforcement of obligations that could be imposed as both *possible* and *practical*, and what that enforcement may need to look like in scale, form, and timeliness, is ultimately where authorities will ensure their expansion or adjustment of regulatory perimeter is grounded in a practical reality.

- **Crafting the appropriate regulatory response.** Having determined the most appropriate targets for regulation, policymakers should subsequently identify the regulatory strategies best suited to addressing the attendant risks. Depending on the circumstances, these potential regulatory strategies include:

    - **Disclosure.** Disclosure requirements are designed to ensure collection and dissemination of certain material information to investors, consumers, regulators, and other stakeholders. The purpose of these requirements is typically to ensure that these stakeholders have sufficient information about the disclosing party to make informed decisions about doing business with them. Examples could include disclosure requirements in connection with cyber incidents and data breaches, as well as of conflicts of interest and material incentives to counterparties.

    - **Reporting.** Reporting requirements provide regulators with information necessary to evaluate and monitor the safety and soundness, operational resilience, legal compliance and risk-taking within financial markets, institutions, and systems. It is also used as a surveillance tool: helping regulators detect fraud, market manipulation, and potential systemic instability. Examples include bank call reports and suspicious activity reports (SARs).

    - **Third party auditing.** Third party auditing involves delegating the verification and certification of information that must be disclosed pursuant to periodic disclosure requirements to a trusted party that is independent from the party subject to the disclosure obligation. Examples include the requirement imposed on public companies to produce audited financial statements.

    - **Entry restrictions.** Entry restrictions prohibit firms or individuals from engaging in specific types of businesses or activities without prior regulatory authorization. Examples include bank licensing requirements and qualifying examinations for individuals selling commodities, securities, or providing financial advice.

    - **Regulatory supervision.** Supervision can involve more distanced oversight and monitoring as well as conducting onsite examination of financial institutions to ensure compliance with policies and regulations. The functions of supervision range depending on the context and include ensuring compliance with relevant law and regulation and providing guidance to regulated institutions about how to effectively manage the risks associated with their business and activities. Examples include bank supervision, market supervision, and stress testing.

    - **Governance regulation.** Governance regulation targets the mechanisms by which organizations and their stakeholders make decisions about risk and how it is allocated and managed. Examples

include rules dictating board structure and composition, executive compensation arrangements, or the allocation of liability between various stakeholders.

- **Conduct regulation.** Conduct regulation targets unacceptable risk-taking or other behavior that is inconsistent with the pursuit of the objectives of financial policy and regulation. Examples of conduct regulation include the prohibitions on market manipulation and on unfair, deceptive, or abusive acts or practices.

- **Product regulation.** Product regulation targets the processes governing the design and marketing of financial products and services, specifies the contractual terms or other features of these products and services, or restricts access to these products and services for certain types of investors or consumers. Examples of product regulation include the rules governing investment fund marketing materials, imposing interest rate caps on payday lending products, and preventing retail investors from trading in complex derivatives unless on a regulated exchange.

- **Balance sheet regulation.** Balance sheet regulation targets the assets or liabilities of a financial institution, typically in order to limit the risks associated with credit, liquidity, or maturity mismatches. Examples of asset-side balance sheet regulation include the imposition of portfolio constraints on money transmitters. Examples of liability-side balance sheet regulation include bank capital and liquidity requirements.

- **Activity restrictions.** Activity restrictions target the nature, scope, and combination of the functions or activities that can be performed within the same financial institution or group of financial institutions. Examples of activity restrictions include rules prohibiting banks and bank holding companies from engaging in activities that are not financial in nature.

- **Structural regulation.** Structural regulation is a type of activity restriction that is specifically designed to concentrate risk within, or disperse it from, systemically important financial institutions. Examples of structural regulation include the legally mandated separation of investment from commercial banking, along with mandatory central clearing for standardized derivatives.

- **Resolution planning.** Resolution planning involves contingency planning for the orderly recapitalization, reorganization, or liquidation of a financial institution that is experiencing financial or economic distress, along with the execution of these resolution plans. Examples of resolution planning include living wills for systemically important financial institutions and processes governing the purchase and assumption of the assets and liabilities of failed banks.

In determining which of these regulatory strategies to employ, policymakers should consider how to best leverage the technological features of DeFi to inject regulatory compliance directly into DeFi projects, enterprises, and ecosystems. This is not to suggest that all regulatory frameworks or strategies should be fully automated, with compliance personnel replaced by bots and oracles. Instead, it simply acknowledges that business models build on smart contracts, automation, programmability, and composability open the door to integrating these risk monitoring and mitigation capabilities directly into the technological architecture.

Figure 9 illustrates how various technological features can support regulatory compliance and security controls throughout a DeFi system. This list is not exhaustive or comprehensive, nor does it envision that a risk-based approach would entail implementing all controls at every level of the tech stack. Instead, Figure 9 provides a helpful demonstration of the spectrum of capabilities that could theoretically be implemented across DeFi systems to support compliance across regulatory domains.

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)

An important consideration for policymakers as they identify where to draw this new regulatory perimeter is what an *optimal level of decentralization* may be for a particular category of DeFi project, enterprise, or ecosystem. As discussed above, centralization and decentralization in financial systems do not often fall to either extreme. This is true in the case of both DeFi and more conventional financial networks: where, for example, a combination of bilateral (decentralized) and centrally-cleared (centralized) network structures have long been a feature of many payment systems, money markets, and derivatives markets. Nevertheless in at least some cases, it may be possible for policymakers to determine the optimal nature, level, and location of decentralization, making it possible for them to design regulatory interventions designed to influence or dictate the structure of DeFi projects, enterprises, and ecosystems.

Additionally, given the fundamentally hybrid nature of DeFi's underlying infrastructure and technologies, regulators may want to consider whether all the institutional and technological building blocks of DeFi projects, enterprises and ecosystems are inherently financial in nature. Where one or more dimensions are not inherently financial, policymakers might then consider whether the applicable legal and regulatory frameworks governing the internet or other digital infrastructure represent an effective complement to, or substitute for, the application of financial policy and regulation.

- **Allocating responsibility and accountability for regulatory compliance in a world of decentralized governance.** One of the most challenging issues for policymakers to address in DeFi is also the most critical: how to identify *responsibility* and ensure *accountability* across decentralized systems for their high risk, highly sensitive activities. In particular, decentralization and automation challenge the ability of policymakers to effectively target regulation, apply conventional regulatory strategies and levers, and take regulatory or enforcement action when a project, enterprise, or ecosystem fails or poses a significant risk to investors or consumers, market integrity, financial stability, or national security. As discussed above, decentralization is often an illusion,[68] or used as a catch-all term that captures a wide spectrum of business models and technologies, some of which may not be decentralized across any meaningful dimension. However, even in instances where there is some modest level of centralization, identifying responsible actors within a widely dispersed group of constantly changing participants can be challenging and resource intensive. Compounding matters, bringing successful enforcement actions against these actors can demand novel, sophisticated and well-grounded legal analyses not yet widely tested in the courts.

  Locating and enforcing responsibility in DeFi ecosystems requires policymakers to address a number of other complex and novel issues including:

  - *Regulation involving software code and First Amendment arguments.* Some proponents of DeFi argue that many DeFi projects, enterprises, and ecosystems are simply automated, self-executing code, not susceptible to influence or control by any person or group, or subject to regulation or enforcement. Based on this and other reasoning, these proponents have argued that the regulation of these projects, enterprises, and ecosystems would be unconstitutional in the United States as a violation of the First Amendment's protections on freedom of expression. Arguments based on First Amendment grounds have not generally thus far appeared to deter regulators, which have observed that most if not all current DeFi projects, enterprises, and ecosystems exhibit significant levels of centralization and control.[69] And while First Amendment issues in relation to open source software are growing in attention well beyond DeFi, courts have thus far signaled that there are likely greater complexities and potential limitations when transactions are involved.[70] As increasing digitization drives more critical functions online, including via DeFi networks and other infrastructure, questions around how regulation can and should apply to software code will likely remain a live issue, demanding that policymakers consider them when designing their approaches toward the regulation of DeFi.[71]

  - *Determining entities and "personhood."* Most regulatory frameworks rely on being able to identify persons or legal entities that control the business and affairs of a regulated actor. These persons or

[68] *See* Sirio Aramonte, Wenqian Huang, and Andreas Schrimpf, BIS Quarterly Review, "DeFi Risks and the Decentralization Illusion" (December 6, 2021).

[69] *See* Securities and Exchange Commission (SEC), RIN 3235-AM45, "Supplemental Information and Reopening of Comment Period for Amendments Regarding the Definition of 'Exchange'" (May 5, 2023); U.S. Treasury, "Illicit Finance Risk Assessment of Decentralized Finance" (April 2023).

[70] *See* United States District Court, W.D. Texas, Austin Division, 1:23-CV-312-RP, *JOSEPH VAN LOON, et al., Plaintiffs, v. DEPARTMENT OF TREASURY, et al., Defendants* (2023).

[71] In addition to First Amendment issues, these questions may also implicate issues under the Fourth and Fifth Amendments; *see* Laura K. Donahue, "The Fourth Amendment in a Digital World", 71 NYU Annual Survey of American Law 533 (2017).

entities then provide the locus for the imposition of regulatory obligations, along with a corresponding target for enforcement actions stemming from the failure to comply with these obligations. Some DeFi projects, enterprises, and ecosystems have explicitly attempted to use decentralization as a veil for avoiding these obligations and related enforcement action. However, most regulatory frameworks adopt an extremely expansive definition of persons and entities: giving regulators and law enforcement officials a great deal of flexibility when wielding their authority, yet also raising potential questions about the nature and level centralization necessary to trigger regulatory obligations. Given the high value and sensitivity of financial activities, along with the importance of effective regulation and enforcement, policymakers are justified in seeking to identify the persons and entities behind DeFi projects, enterprises, and ecosystems. Indeed, the alternative—a future financial system in which no persons or entities are held responsible for their actions—is neither feasible nor desirable. As DeFi becomes more decentralized, policymakers will need to consider what approach toward identifying responsible persons will be most effective in advancing the objectives of financial policy and regulation.

- **Mapping counterparty exposures in a world of decentralized balance sheets.** Policymakers will need to consider how to identify and monitor critical interdependencies across DeFi balance sheets, along with the potential channels they create for the spread of contagion and cross-sectoral systemic risks. This includes counterparty exposures and interdependencies between DeFi projects, enterprises, and ecosystems and conventional TradFi intermediaries and financial market infrastructure. Identifying and accurately measuring these exposures can be challenging given the varied and often lax financial reporting standards employed within DeFi.[72] This challenge is further compounded by the highly complex and pseudo-anonymous nature of DeFi, along with the sheer number of balance sheets relative to the structure of conventional "hub-and- spoke" financial networks dominated by a small number of large counterparties. Effectively addressing this challenge will likely require a shift in regulatory approach reflecting the number of counterparties, the matrix of exposures and interdependencies between them, and how quickly these exposures and interdependencies can change within DeFi networks.

- **Mapping key service providers and services in a world of decentralized operations.** As discussed above, even highly decentralized systems often involve a small group of core developers and other key service providers. Policymakers need to consider how best to identify these key service providers and map their roles within DeFi projects, enterprises, and ecosystems. This exercise is necessary to both identify key centers of gravity among the upstream and downstream service providers and then implement any regulatory strategies designed to mitigate the attendant risks. In building an understanding of where these key points of influence and control for financial services reside, regulators can then observe the market and technological functionalities to improve their visibility of risk indicators like anomalies and increasing points of concentrated influence. This could be critical for detecting the actions of malevolent actors or potential threats to network stability.

- **Oversight of new and rapidly evolving technology.** The exponential pace of technological innovation[73] brings with it significant implications for the ability of policymakers to mount timely and effective policy responses, enforcement actions, and other regulatory interventions. Relative to TradFi, the transparency associated with many DeFi projects, enterprises, and ecosystems offers the possibility of significantly

[72] *See* European Systemic Risk Board (ESRB), Task Force on Crypto-Assets and Decentralized Finance, Crypto- Assets and Decentralized Finance, "Systemic Implications and Policy Options" (2023).

[73] *See* Gordon Moore, "Cramming More Components onto Integrated Circuits" (1965).

increasing the amount and quality of information available to regulators. As described above, for the first time, it also offers the ability to integrate regulatory compliance features and security controls directly into the technological architecture of financial markets, institutions, and products. Yet in reality, this potential will never be fully realized without regulators gaining greater confidence in their understanding of this technology, and that this technology will actually work as intended in times of crisis.

The state of the market, including in development of RegTech and monitoring tools needed to measure and oversee complex varieties of risks and attributes across markets including constantly evolving interconnections and dependencies, has not yet matured sufficiently to give regulators assurance in their and regulated institutions' abilities to accurately assess their risk exposures. Though DeFi has been developing and growing over the past fifteen years, experimentation and use cases are still nascent, as are efforts across the sector to attempt to derive and coalesce around industry standards and best practices, which would typically form a basis for regulators to look toward as they consider their expectations of responsible participation in financial markets. Policymakers should consider mechanisms for promoting responsible innovation and market evolutions in RegTech and DeFi compliance and generation of best practices.

Authorities should also address their own capabilities and capacity to oversee the space. Human capacity can also easily become the delimiting factor to ingest and leverage information within the bounds of the investigative, regulatory, and enforcement structures. The risks stemming from asymmetric information[74] described previously do not just point to issues with DeFi systems' typically very complex information, but also implicate technical literacy of regulators or consumers in leveraging information that may be even more readily discoverable or available than in TradFi but not (yet) easily understood based on the current state of RegTech solutions and regulator capacity.

- **Ensuring that DeFi lives up to critical policy objectives like expanded access to safe and affordable financial services, necessary transparency, and responsible governance**.[75] Next comes the key issue of defending against simply building and disguising a "new" financial system that just imports all of the problems of centralization, exclusion, and poor visibility and security from earlier iterations of finance and the internet. Ensuring that major DeFi implementations actually achieve the goals of expanding access and inclusion to financial services, providing sufficient transparency for consumers and government authorities, and maintaining responsible governance to defend against system vulnerabilities and exploitation requires a balance of "stick" and "carrot" approaches—specifically, enforcement and key partnerships with industry.

  Policymakers will likely continue to grapple with the difficulties of scaling practical application of regulation and enforcement in order to shape a sector into compliant and responsible behavior. Scaling both amount and timeliness of enforcement is already difficult for authorities even in TradFi spaces,[76] where many business models and operations have been understood for years and typically there are regulatory and investigative capacity and frameworks in other jurisdictions to support investigations on transnational financial activities and exploits. It is an even greater challenge in DeFi due to factors like highly dispersed and complex business operations, as well as insufficient regulation and capacity internationally. Implementation of even the first clearly established international standards on virtual assets, specifically the FATF's standards adopted in 2019, still significantly lags across at least 75% of jurisdictions.[77] It takes years to emplace even just the policy

[74] *See* IOSCO Consultation Report, "Policy Recommendations for Decentralized Finance (DeFi)" (September 2023).

[75] President Biden established ensuring *responsible* development of digital assets as a national priority. *See* United States, Executive Office of the President (Joe Biden), Executive Order 14067, "Executive Order on Ensuring Responsible Development of Digital Assets" (March 9, 2022).

[76] *See* Ana Carvajal and Jennifer Elliott, IMF Working Paper, "The Challenge of Enforcement in Securities Markets: Mission Impossible?" WP/09/168 (August 2009).

[77] *See* FATF, "Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers" (June 2023).

frameworks, but less for actual enforcement capacity and prioritization across supervisors, law enforcement, and judiciary bodies. Enforcement across all financial sectors also typically takes a long time, due to longer timelines for due process and investigations as well as sometimes delayed actions by some civil or criminal authority to wait for the culmination of broader investigations and concurrent interagency action.

Timeliness of enforcement is only further complicated by the complexities of DeFi models, identifying the responsible entities, and continued growth rate of global-reaching operations. Enforcing non-compliant or criminal activities five years after they have begun, within the authority of regulators, may prove insufficient to shape a dynamic sector to develop responsibly while still in its nascent stages. And it is especially critical to shape the DeFi space early, given that the nature of its technologies and operations can make it extremely difficult practically to take down or alter upon launch and wide adoption. Additionally, novel enforcement in DeFi, which could potentially implicate actions against previously generally-unenforced actors and stakeholders—that may not be financial institutions but still hold possible regulatory obligations—could take longer times than traditional enforcement as new ground is trod in building cases. Authorities will need to consider how to sufficiently scale enforcement capabilities and strategic approaches that most effectively and timely shape the entire DeFi ecosystem to develop compliantly.

Public-private partnerships to shape responsible behavior in DeFi is another area ripe for further consideration by policymakers. The critical role of industry in implementing financial policy is acknowledged in standards evaluation regimes like the FATF as a part of a jurisdiction's assessment on the efficacy of its regulatory frameworks. Authorities need industry, and in this case can benefit especially from partnerships with DeFi and RegTech services, to work with them to effectively meet these policy objectives. Managing partnerships in implementation can be a real challenge, though. The DeFi space includes stakeholders who hold limited willingness to engage authorities and often assert a "self-reliance" ethos across DeFi communities.[78] Though some efforts have launched to enable DeFi partnerships focused on areas like cybersecurity and combating illicit finance,[79] these efforts have often relied on highly centralized parties. The desire for self-reliance and operating outside parties who acknowledge responsibility or ownership of projects—sometimes aimed specifically to avoid jurisdiction of government authority—across many DeFi players ultimately has delayed and limited efforts to organize around developing and implementing standards and partnerships to combat exploitation and mitigate key risks across the space.

Identifying the key partnerships to drive changes across an ecosystem will be critical for policymakers to address. Given challenges of scale, authorities may need to consider the types of entities and specific players that have the greatest scale of influence across the whole ecosystem. These potential partners may be those participating directly in DeFi systems, such as DEXs, miners, administrators, and other components reflected in the DeFi architecture Figure 3. They could also be players less directly involved in on-network actions but still important levers for driving change. This could include thought leaders and influencers respected across the DeFi industry, academics and researchers driving important research and development around secure and compliant technologies and models, and the highly impactful investment community that is uniquely placed to offer incentives to DeFi entrepreneurs to develop their platforms in certain ways.

[78] *See* Jonah Crane, "The DeFi World Faces a Jarring Transition", The Financial Times (May 14, 2023).

[79] For select examples, *see* Chainabuse.com; Ransomwhe.re; the Crypto-ISAC (*e.g.*, Information Sharing and Analysis Center); the Blockchain Governance Initiative (BGIN); the Joint Working Group (JWG) on interVASP Messaging Standards; and the Travel Rule Information Sharing Alliance (TRISA).

- **Mitigating the unique threats that DeFi poses to security, illicit financing, system stability, consumers and investors, market integrity, and the climate.** Policymakers should consider where the risks presented by DeFi to the outlined policy and agency regulatory objectives are truly unique, whether lesser or greater, and take mitigating steps specific to that risk. Mistakes in equivalency can be easy to make if one does not look closely enough when observing activities that look functionally similar, such as thinking about DeFi activity as either a cash transaction or as a wire transfer and therefore desiring to apply the exact approach implicated for one of these to all DeFi. In this example, DeFi enables peer-to-peer transactions without using a regulated intermediary[80] like cash and immediate, cross-border, electronic value transfer like wires. However, DeFi transactions typically publish to a public, traceable ledger—unlike cash—and transactions generally do not rely on a specific custodial money transmitter to move money nearly instantaneously with global reach—unlike wire transfers. As discussed, some of these features and correlating risks of DeFi exist within the TradFi system, but typically do not exist concurrently and in aggregate in the same asset and activity. Additionally, some of the features, like hard-wired procyclicality, are unique to DeFi. Policymakers will need to address these specific threats to ensure a properly calibrated risk-based approach for DeFi that does not inadvertently box in regulation and compliant innovation to address antiquated risks, nor permit the escalation of interconnectedness and subsequent cascading risks as DeFi grows and becomes more integrated with the broader financial system.

- **Identifying the best role for policymakers in building DeFi ecosystems, including standard setting, promoting foundational research and development (R&D), and long-term policy projects like digital identity.** Policymakers can and should play bigger roles in DeFi systems than just regulators of activities founded and operated by industry. Typically, these roles would be serving as champions for particular initiatives and ensuring appropriate prioritization, budgeting, and resourcing of personnel and tools to help build responsible DeFi ecosystems. The U.S. government has historically been a great driver of innovation shaping advancements fields like medical, information technology, communications, and manufacturing. Agencies cannot enforce alone the DeFi space into compliance. They should consider how to accelerate efforts to define and develop the building blocks necessary for a responsible future in digital payments and DeFi. Innovation in payments is happening at a great pace on a huge scale internationally,[81] and these efforts typically have long lead times for wide experimentation and subsequent innovation and system modernization. Policymakers need to be looking toward what roles they need to take in the near-term for timely intervention to shape long-term applications and infrastructure that may be the future critical infrastructure of digital economies a decade from now.

  Government bodies have long participated in standard setting efforts relating to financial regulation, market activities, financial infrastructure, as well as technology in bodies like the ISO, the IOSCO, the BIS and the FSB, the FATF, and the International Accounting Standards Board (IASB), and the International Telecommunication Union (ITU). With the growth of DeFi experimentation and applications that involve either direct integration with or serving as underlying infrastructure for other digital goods and services, such

[80] DeFi transactions are sometimes characterized as requiring no intermediary, but a more accurate characterization may be that DeFi transactions can occur without the typical type, function, or nature of control or visibility of activity that intermediaries in TradFi typically have. DeFi peer-to-peer transfers may not involve specific centralized parties taking funds or assets and transferring them to a beneficiary, but there are other (at present) typically unregulated intermediaries involved in operation of infrastructure and processes facilitating these transactions, such as miners, validators, and node operators.

[81] *See* Atlantic Council, "Central Bank Digital Currency Tracker" (2023); The World Bank, "Key Data from Regulatory Sandboxes around the Globe" (November 2020).

as the infrastructure for future smart cities,[82] policymakers should consider how and where to engage in both financial and technological standards bodies to ensure leadership of national interests and democratic principles reflected in the creation of standards pertaining to DeFi, such as for security, interoperability, network communication and messaging, and regulation and oversight. Policymakers will also need to consider where and how to convene and meet the DeFi space given that it is not traditionally a sector prone to self-organization nor significantly represented at these international bodies. The government should determine how to best position itself to help foster collaboration, debate, and eventual consensus around what standard best practices are as well as the means for implementing them.

R&D is another area that appears to present great opportunities for government involvement to support responsible DeFi. Policymakers have several levers for R&D, including through grants and challenges to promote R&D by external parties as well as internal research arms that can bring innovation and development in-house. The U.S. government has already undertaken several efforts to support greater experimentation in industry and to identify the key areas for research.[83] Authorities may need to consider what their best role would be to promote timely and consistent research, leveraging partnerships with academic institutions and federally funded research and development centers (FFRDCs). Rather than directly sponsoring R&D, there are opportunities to drive scalable and outcome-focused R&D by industry through the use of "regulatory sandbox" type authorities, such as through limited exceptive relief and "no action" letters, accompanied by regulatory guidance. As industry entities approach policymakers proposing experimentation for compliance, policymakers should consider whether using sandboxes and outcome-oriented technology sprints would help them achieve desired endstates of greater security and controls across DeFi. For both types of efforts to be fruitful, authorities would need to consider what the boundaries, criteria, and metrics for evaluation of risk mitigation are that could give DeFi efforts clear roadmaps for how to succeed toward compliance.

A focus on digital identity infrastructure and policy, which in many cases only government can effect, is foundational to ensure security, combat fraud, and enable access and better customer experiences for any future digital infrastructure. Weaknesses in identity systems result in pervasive identity fraud and exploitation that costs the economy trillions.[84] While there have been some initiatives to drive implementations of identity and verifiable credentials for decentralized ecosystems,[85] if digital identity efforts are not pursued with security or adoption of the strongest systems prioritized, DeFi could stand to import all the weaknesses of TradFi identity into their ecosystem that for now is characterized by less accountability and recourse for victims. The government has significant responsibility in fostering digital identity infrastructure. Federal and state agencies are typically the authoritative owners of and issuers of credentials, such as a driver's license or passport, attesting to one's official identity. Governments are the primary holders of critical information about individuals' identities; typically the private sector, like financial institutions, does not have access to the same information, instead has to try to verify and assess validity using

[82] *See* Mohammed S. Alnahari and Samuel T. Ariaratnam, "The Application of Blockchain Technologies to Smart Cities", 5(3) Smart Cities 979 (August 15, 2022).

[83] *See, e.g.*, White House National Science and Technology Council, Fast-Track Action Committee on Digital Assets Research and Development, Networking and Information Technology Research and Development Subcommittee, "National Objectives for Digital Assets Research and Development" (2023); and U.S. Department of Commerce, "Responsible Advancement of U.S. Competitiveness in Digital Assets" (September 2022).

[84] *See* Federal Reserve Bank of Boston, FedPayments Improvement, "Synthetic Identity Fraud Mitigation Toolkit" (2023); and Jim Gee and Mark Button, "The Financial Cost of Fraud Report" (2019).

[85] *See* World Wide Web Consortium (W3C), "Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations" (July 19, 2022).

non-authoritative sources in processes like due diligence. Additionally, governments are the natural authorities to account for the safeguarding of principles like equity and appropriate privacy in digital identity systems. Both executive branch agencies as well as Congress are likely needed to support the development of digital identity that can help secure identity in DeFi.[86]

- **Fostering a robust and constructive dialogue with DeFi industry.** The nature of engagement between government and private sector on DeFi at present is not constructive. Dialogue between policymakers and DeFi industry or proponents is often characterized by vitriol and defensiveness. In the most extreme instances, opponents offer little to no acknowledgement of the dangers of ignoring timely action on payment system innovations happening worldwide nor of the potential benefits these technologies *could* manifest if managed under strong regulatory management and oversight. On the other extreme, proponents voice overly sanguine praise to an immature sector with no critical eye to obvious failures in the systems that were built with little consideration for consequences of haphazard design and launch of platforms meant to support highly sensitive and critical financial functions. This issue presents a serious problem to government authorities, which depend on engagement with industry to better understand ongoing activities as well as to drive desired outcomes.

  Tensions between the sides on DeFi debates have stalled and delayed meaningful progress on critically needed regulatory agendas as well as partnerships to foster greater responsibility in the space like standards and information sharing efforts. Addressing some of the unique and complex risks in the DeFi space, and especially in determining how and where best to allocate accountability and potentially even pursue embedded supervision of these systems, cannot be done without action and adoption of regulatory and security measures by the DeFi space. Even where existing policy frameworks are determined by regulators to sufficiently cover DeFi models, being responsive to calls for specific points of clarity on the regulatory perimeter and how to fall within it via processes like registration and licensing could create great opportunities for culminating partnerships and temper heated discourse. Policymakers, across all relevant authorities, should consider how to sponsor, tailor, and participate in robust and constructive dialogue with major stakeholders in the DeFi ecosystem to drive consequential change.

[86] *See* Better Identity Coalition, "Better Identity in America: A Blueprint for Policymakers" (2018); corresponding draft bills of the "Improving Digital Identity Act" introduced by Congressman Bill Foster (H.R. 4258) and Senator Kyrsten Sinema (S. 884).

(B) Issues for Industry

ISSUES FOR INDUSTRY

Industry players also hold distinct authority and capabilities needed in complement to policymakers to shape responsible development and outcomes in DeFi. Additionally, driving compliance and security into DeFi systems will likely enhance the sector's success with wider adoption and trust across enterprises and consumers. To achieve this trust and fulfill this role in shaping the sector, DeFi industry will have to address key issues:

- Promoting industry leadership in technical standard setting and infrastructure and solutions development
- Incorporating regulatory considerations at an early stage in DeFi development
- Building dynamic regulatory compliance into DeFi protocols and systems
- Fostering a robust and constructive dialogue with regulators and policymakers.

Government authorities are not alone responsible for shaping outcomes in DeFi. Industry, as the creators, operators, and consumers of these products, services, and infrastructure, which as part of the financial services sector would generally be considered as part of *critical infrastructure*[87] given the sensitivity and importance of their function for society, hold significant responsibility for ensuring that they contribute to a financial system that is safe, secure, stable, and defended against exploitation by illicit actors. This demands that members of industry understand the complex policy objectives and frameworks of the activities and functions that they support as they build, launch, and operate technologies and infrastructure supporting critical services. Equipped with that knowledge, builders and others in the DeFi industry must take steps to organize around development, implementation, and continuous updating of best practices in compliance and security. Integrating these practices can involve leveraging programmability and composability of these systems through directly built-in technological controls, or can be through higher-level imposed controls of governance and operations. Most importantly, this requires a willingness to accept designation and allocation of *responsibility* and *accountability* in DeFi ecosystems to mitigate critical risks across these projects and enterprises.

Future digital economies, whether built in small or large part upon decentralized networks and infrastructure, will not be systems absent of critical regulations and controls needed to defend systems and consumers from exploitation. The sector must embrace that reality and be a part of building meaningful dialogue and actual solutions in pursuit of the outlined policy objectives. For DeFi industry to achieve greater, and earlier, success in implementation, adoption, and properly calibrated risk-based regulation across jurisdictions, it must address several core issues:

- **Promoting industry leadership in technical standard setting and infrastructure and solutions development.** Industry is even better positioned and more critically required than government to drive forward progress on standard setting. Standards, even if documented and published by government bodies or non-governmental organizations, are foundationally based upon there being levels of agreement across industry based on experimentation and observations on what the standardized best practices for certain technologies and operations are. The DeFi industry has struggled to organize around efforts to *build and implement* technical standards around what security and compliance features should look like in DeFi platforms, and has even struggled to implement long-existing standards, guidelines, and practices into their applications. Industry stakeholders must consider how they can effectively convene and participate in technical standards setting efforts that can give critical roadmaps to entrepreneurs and builders as they develop new applications in DeFi. Following the development of these standards, there still remains the challenge of driving actual use and integration of these standards into technical infrastructure and solutions that get built.

[87] *See* United States, Executive Office of the President (Barack Obama), Presidential Policy Directive, "Critical Infrastructure Security and Resilience" 21 (2013).

- **Incorporating regulatory considerations at an early stage in DeFi development.** Wide adoption of DeFi will not come without building in protections and mechanisms of recourse that give confidence to a wide base of consumers. The best time to integrate features like security into software is in its development. Engineers will need to look toward policy objectives like those outlined here and specific regulatory obligations as technical requirements for DeFi projects. In taking a systems architecture view, developers and operations will need to consider where the most effective and economical application of controls and security features would best secure their system, and then determine how they can best drive the design and development of solutions to integrate these features early in the lifecycle of DeFi systems.

- **Building dynamic regulatory compliance into DeFi protocols and systems.** Compliance is not a simple nor static function. Risks and lines of business evolve and shift over time, resulting in both dynamic regulatory regimes and specific risk profiles of particular DeFi projects and activities. Even more important as automation grows throughout DeFi and the points for human or organizational intervention diminish, the ability for technical intervention and adaptation must increase in sophistication, timeliness, accuracy, and assurance. This requires DeFi developers to develop mechanisms for ensuring that protocols and other systems components can be updated to reflect future regulatory changes. Areas like illicit finance compliance and cybersecurity are ripe for this kind of near-term action by DeFi developers—while systemic protections are critical, limited present use of DeFi and integration with TradFi results in lower current risks to the broader financial system. Features to secure against illicit finance and cybercrime will need to evolve as new typologies and vulnerabilities are discovered, and could be good use cases for building in dynamic compliance.

- **Fostering a robust and constructive dialogue with regulators and policymakers.** As discussed earlier for policymakers, the present state of discourse between industry and regulators is not optimal for driving informed, timely policy and informed, compliant DeFi architecture. Narratives that point fingers at regulators while ignoring insufficiencies in compliance and self-policing by the sector, often said while calling for self-regulatory approaches, do not foster an environment of trust or diminish the skepticism with which some regulators view the DeFi sector. This perception is only exacerbated by some parties' framing of decentralization as explicitly a means of avoiding regulation, rather than as a means of positively pursuing some other objective. Dialogue around requests for clarity is usually defensive and vague, often framed in a manner that seems unaware of existing policy frameworks and requirements for similar or equivalent activities and without offering specificity of the points of clarification needed. Industry will need to consider how to pursue consistent, robust discourse that includes an honest accounting for failures and successes in the current state of the industry and prioritizes wherever possible data-driven examination and debate of specific measures to drive forward progress.

V. Recommendations

There are steps that policymakers and industry should take to better understand and mitigate the risks presented by DeFi. This Committee recommends the following framework, including key questions for further examination and specific recommendation for targeted actions to help shape the future trajectory of DeFi projects, enterprises, and ecosystems and better safeguard the financial system, consumers, and national security.

(A) Resource Assessment, Data Gathering and Mapping

The first priority for policymakers should be to increase their capacity to understand DeFi, including by identifying what they do and do not yet know about DeFi. This has two elements. First, policymakers should identify the data, expertise, and other resources they need in order to gather and analyze more comprehensive data about the size, scope, economic structure, and key technological features of DeFi today. As part of this process, policymakers should also undertake additional research and analysis into the key factors driving the emergence of DeFi: including the frictions associated with more conventional models for the delivery of financial products and services, along with whether and how DeFi presents new opportunities to reduce these frictions. Second, armed with these resources, policymakers should develop and execute a strategy for gathering this data for the purposes of constructing a more detailed map of existing DeFi projects, enterprises, and ecosystems. This 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. 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.

Recommended Actions:

- Increase capacity to understand DeFi. Comprehensively map the data, expertise, and resources needed to assess the economic structure and technological features of DeFi and to implement and enforce policy frameworks for DeFi.
- Conduct a gap analysis against current capabilities and capacity, and address critical gaps with additional funding, personnel, and tools. Consider where innovative hiring and acquisitions authorities can be used or expanded to enable timely competent resourcing, as well as where public data calls and solicitations for information could fill data gap needs.
- Research and analyze the key factors driving the emergence, evolution, and growth of DeFi projects, enterprises, and ecosystems.
- Develop and institutionalize a strategy for continuous data gathering and monitoring of the DeFi ecosystem, including major DeFi projects and enterprises, interconnections, and threats.
- Share information and strategies across regulators to identify common points of information and assessment that could be harmonized across multiple authorities.
- Scale partnerships across the regulatory community to share information, harmonize any future regulatory actions, and enhance both the effectiveness and timeliness of enforcement actions.

Key Questions:

(1) What are the types of data that are needed to fully understand the economic and technical operations of DeFi projects, enterprises, and ecosystems, along with their interconnections with conventional TradFi intermediaries and financial market infrastructure?
(2) What are the existing sources of this data, and what government and industry actors have access to them?
(3) What are the actual points of friction and problems in TradFi that specific applications of DeFi are designed to address? Are TradFi or DeFi technologies and business models better positioned to address these problems?

(B) Survey the Existing Regulatory Perimeter

Policymakers should use this mapping exercise as the basis for determining whether the financial products and services provided by DeFi projects, enterprises, and ecosystems, and the wide range of activities and functions they perform, currently bring them within the perimeter of U.S. financial regulation, as well as other non-financial regulatory regimes. The purpose of this exercise is to identify existing or potential future gaps in regulation that could undermine the ability of policymakers to advance the objectives of financial policy and regulation described in this report. Given the fragmented U.S. regulatory environment, policymakers should seek to promote the widest possible participation in this exercise: including by the Federal Reserve Board (FRB), Office of the Comptroller of the Currency (OCC), Securities and Exchange Commission (SEC), CFTC, Consumer Financial Protection Bureau (CFPB), and state banking, securities, and insurance regulators, along with the Department of Justice, the Department of the Treasury, to include the Office of Foreign Assets Control (OFAC) and FinCEN. To examine the non-financial regulatory perimeters, this exercise should at least include the Department of Commerce and the Department of Homeland Security (DHS).

Recommended Actions:

- On the basis of the mapping exercise, along with the range of activities and functions currently performed by DeFi projects, enterprises, and ecosystems, identify the existing U.S. state and federal regulatory frameworks to which they are currently subject.
- Assess the level of compliance by Defi projects, enterprises, and ecosystems with these regulatory frameworks.
- Identify where these regulatory frameworks would need to be expanded in order to address the risks posed by DeFi projects, enterprises, and ecosystems.
- Partner with self-regulatory organizations, like the Financial Industry Regulatory Authority (FINRA) and the National Futures Association (NFA), and state regulatory authorities to more fully assess the U.S. regulatory touchpoints of DeFi.
- Evaluate the perimeter of regulation and current compliance levels against those of international peer jurisdictions.

- Support state and international partner capacity with training and resources.

Key Questions:

(1) What are the threshold conditions for the application of various regulatory frameworks? Which DeFi projects, enterprises, or ecosystems, or the activities or functions they perform, satisfy these conditions?
(2) What are the regulatory objectives underpinning existing regulatory frameworks, and how might these objectives apply to DeFi, even if the frameworks themselves do not?
(3) What nature or degree of control and influence over a DeFi project, enterprise, or ecosystem warrants regulating it as a common entity?

(C) Risk Identification, Assessment and Prioritization

Policymakers should seek to systematically identify, define, and catalog the risks arising in connection with DeFi projects, enterprises, and ecosystems. These risks may include but are not limited to those arising from:

- Asymmetric information and conflicts of interest
- Operational, technological, and security vulnerabilities
- Liquidity and maturity mismatches
- Over-leverage
- Algorithmic discrimination
- Wash trading, front running, and other types of market manipulation
- Oracle exploitation
- Vulnerabilities in consensus protocols
- Hardwired algorithmic failures
- Reliance on key service providers and other forms of concentration risk
- The financial and technological complexity of DeFi compositions
- Hardwired procyclicality

Recommended Actions Applied to AML and Identity in DeFi

The pseudonymity and disintermediation provided in most DeFi systems presents serious concerns for policymakers focused on ensuring AML regimes, which rely upon identity, are effective and provide appropriate protections and victim recourse for consumers. Given the ongoing exploitation of DeFi systems for their absence of AML/CFT protections, we recommend policymakers apply our outlined broader holistic DeFi approach to drive specific near-term actions and address key outstanding issues to make critical progress needed on the priority issue of digital identity and AML/CFT:

Resource Assessment, Data Gathering, and Mapping

- Assess and improve policymaker and industry understanding of the policies, technologies, and functions involving the multiple dimensions of identity (*e.g.*, identity verification, authentication and credentials, federation, privacy frameworks, etc.).
- Map DeFi ecosystem players and business operations involving identity processes and data.
- Identify the identity information that currently exists at, as well as what is possible to exist or be collected at, different layers and components in DeFi systems.

Survey the Existing Regulatory Perimeter

- Assess the extent to which identity information is required to be collected at different places in DeFi systems, and identify both compliance gaps and requirement gaps.
- Compare U.S. identity-related frameworks and requirements to international standards and peer jurisdictions.

Risk Identification, Assessment, and Prioritization

- Identify the specific risks (*e.g.*, AML/CFT, consumer protection) and vulnerabilities associated with identity – both involving risks from insufficient identity solutions as well as any unintended consequences due to the collection or absence of sufficient controls like security for the sensitive information – for the DeFi systems and derive policy objectives for the identity solutions.
- Map the interconnections and interdependencies of weaknesses in identity information, credentials, and assertions across DeFi, TradFi, and non-financial entities to evaluate where fixes are needed to specific financial and non-financial infrastructure and services (*e.g.*, reliance on banking systems' identity processes as they currently operate may inadvertently import the vulnerabilities leading to trillions lost in fraud).

- Illicit finance and sanctions evasion

As part of this process, it may be desirable to identify and distinguish between different categories of DeFi projects, enterprises, or ecosystems on the basis of the types of financial products and services they provide, the activities or functions they perform, and the risks they pose. It may also be desirable to policymakers to next undertake a more detailed assessment of both the probability and potential impact of these risks across different types of DeFi projects, enterprises, and ecosystems. This assessment should reflect the many and varied interconnections between these projects, enterprises, and ecosystems, along with the potential channels for the transmission of these risks both within DeFi and between DeFi and the wider financial system. Lastly, on the basis of this risk assessment, policymakers should develop and articulate a set of policy priorities that reflect the objectives of financial law and regulation, available regulatory resources, and—as described in greater detail below—the anticipated effectiveness of the regulatory strategies and other mitigation mechanisms designed to address these risks.

Recommended Actions:

- Conduct a comprehensive assessment cataloging and mapping the players and interconnections of DeFi ecosystems and the specific risks.
- Identify the DeFi projects, enterprises, and ecosystems of greatest concern on the basis of the nature, scale, probability, and potential impact of the attendant risks.
- Identify discrete information availability and analytic gaps to comprehensively assess and understand the nature, source, and probability of certain key risks. Build capabilities internally or look to industry for acquisition or promoting development of necessary tools (*e.g.,* grant authorities, requests for information or proposals, etc.).
- Establish a prioritized list of policy goals for DeFi consistent with law and regulation. These priorities should reflect the objectives outlined in this report: customer and investor protection,

RECOMMENDED ACTIONS APPLIED TO AML AND IDENTITY IN DEFI (CONTINUED)

IDENTIFYING AND EVALUATING THE RANGE OF POTENTIAL POLICY RESPONSES

- Evaluate options for regulating and imposing requirements for identity information discoverability and verification across layers in the ecosystem.
  - Could involve regulating more centralized identity information and credential repositories and service providers, and 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. For example, less identity information may be available and required for a less consumer-facing role in the system, such as the network layer as compared with the application layer.
  - Requires examining the various types of identity information (*e.g.*, official, digital footprint, activity and behavioral) to evaluate (1) what information should (2) be discoverable to whom (3) under what conditions (*e.g.*, openly, upon completion of what stage of due process, with or without party consent, never, etc.).
  - Must account for how the assessment differs based on different functions, such as financial versus non-financial, and account for how system-wide controls may affect a risk-based approach. For example, a permissionless system may likely require more discoverability of certain identity information than a highly controlled permissioned system may.
  - Weigh the costs and benefits of which components and solutions of identity ecosystems should optimally be created and operated by government versus industry bodies.

FOSTERING GREATER ENGAGEMENT AND COLLABORATION WITH DOMESTIC AND INTERNATIONAL STANDARD SETTERS, REGULATORY EFFORTS, AND DEFI BUILDERS

- Leverage partnerships with U.S. government and industry participating in standards and technical efforts relevant to digital identity – identity management, blockchain, internet and telecommunications infrastructure, and financial experimentation like central bank digital currencies (CBDCs) – to share information and align on priorities and outcomes for digital identity solutions and infrastructure standards and development.
- Surge and align use of R&D, grant, and appropriate regulatory authorities to promote development of building blocks and integrations for traditional and web3 identity solutions and infrastructure.

promoting market integrity, financial stability and mitigating systemic risk, combating illicit finance and protecting national security, reinforcing and securing U.S. competitiveness and leadership, and expanding access to safe and affordable financial services.

Key Questions:

(1) How do risks to consumers, financial stability, market integrity, illicit finance, and U.S. leadership map on to specific DeFi projects, enterprises, and ecosystems? What are the nature, sources, probability, and potential impact of these risks?
(2) What are the specific discrete and overlapping information gaps needed to be addressed for policymakers, key industry participants (*e.g.,* regulated institutions), and consumers to make critical observations and decisions about DeFi systems based on their performance and risk profiles?
    a. What is the cause or source of the information gaps—*e.g.,* lack of transparency, absence of information reporting or aggregation streams, insufficient development of analytic and RegTech solutions to assess and use available information, etc.?
    b. Based on the source of the information gaps, what steps can government and industry players take to effectively create, make available, analyze, and distribute necessary information to specific stakeholders?

(D) Identify and Evaluate the Range of Potential Policy Responses

In conjunction with this risk assessment, policymakers should 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 connection with DeFi projects, enterprises, and ecosystems. The range of regulatory strategies and other risk mitigation mechanisms includes but is not limited to:

- Disclosure
- Regulatory reporting
- Third party auditing
- Entry restrictions
- Regulatory supervision
- Governance regulation
- Conduct regulation
- Product regulation
- Balance sheet regulation
- Activity restrictions
- Structural regulation
- Resolution planning

As part of this process, policymakers should identify key points of responsibility or control that could theoretically provide the basis for the imposition of regulatory obligations. They should also evaluate whether and how it might be possible to employ RegTech or otherwise directly embed these obligations into the technological architecture of DeFi projects, enterprises, and ecosystems. Lastly, policymakers will need to determine whether the imposition of these regulatory obligations is possible under existing law, or whether their imposition would require legislative change in order to expand the regulatory perimeter or grant regulators new legal powers.

Recommended Actions:

- Identify and inventory existing regulatory authorities to determine the range of available risk mitigation mechanisms.
- Determine which mitigation mechanisms are likely to be most effective and appropriate in addressing each of the risks posed by DeFi projects, enterprises, and ecosystems.
- Identify what additional regulatory authorities are necessary to effectively address these risks.
- Drive strategies and resourcing to scale timeliness, consistency, and effectiveness of enforcement of existing frameworks to mitigate DeFi risks.
- Pursue robust examination and debate to define information and identity availability and discovery requirements for DeFi, which will guide development of privacy enhancing technology solutions and governance architectures for DeFi systems.
- Surge policy and infrastructure development efforts for digital identity, for DeFi and more broadly.
    - Focus on policy determinations surrounding security assurance, privacy preservation and data discoverability, and accessibility expectations for government and industry providers of identity credentials, verification, and authentication solutions.
    - Define concrete near-term actions for accelerating and promoting development of secure, equitable, interoperable, fraud-resistant identity ecosystems, including through use of standards, grants, and Government credential issuing and other identity services authorities.

Key Questions:

(1) What aspects of DeFi systems should be regulated under which agency authorities? What conditions or features of maturity of systems and activities should be considered in allocating authority to government versus self-regulatory agencies?
(2) How should platforms that support significant amounts of financial *and* non-financial activity be regulated?
(3) What is the best approach to inform consumers about a highly complex and technical space to facilitate safer or at least more aware interaction with DeFi?
(4) Do approaches toward software security and accountability across different policy efforts, such as artificial intelligence, cybersecurity, internet governance, and DeFi, maintain consistency and harmony in approach?
(5) Are there lessons we can draw and put into operation for some or all DeFi systems and underlying infrastructure, such as internet multi-stakeholder governance and accountability?
(6) What is the balance of, and how do we measure, success and tradeoffs in policy objectives like innovation, economic access and inclusion, consumer and investor protection, and system security?
(7) How should independent financial regulatory agencies coordinate and account for objectives, like national security and the objectives of other agencies, in their own policy and enforcement approach?

(E) Foster Greater Engagement and Collaboration with Domestic and International Standard Setters, Regulatory Efforts, and DeFi Builders

Most DeFi projects, enterprises, and ecosystems are still at a relatively nascent stage in their development. Moving forward, the development of common industry technical standards, along with clear, consistent, and effective regulation, will be integral to their success. Policymakers should develop a strategy for fostering greater engagement and collaboration on several fronts. First, given the fragmented U.S. regulatory environment, policymakers should seek to widen and deepen the channels of communication and policy coordination within the domestic regulatory community. Second, policymakers, working with stakeholders like the National Institute of Standards and Technology, should 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. Third, reflecting the opportunities presented by DeFi, and the fact that clear and effective regulation is in the best interests of all stakeholders, policymakers should seek to foster a more constructive dialogue with the entrepreneurs, developers, and builders of Defi projects, enterprises, and

ecosystems. Lastly, policymakers should fully engage with the efforts in various international fora—including the Financial Stability Board, Bank for International Settlements, and the International Organization of Securities Commissions—to develop regulatory frameworks governing the DeFi industry and explore what future role DeFi projects, enterprises, and ecosystems might play in cross-border payments, securities clearing and settlement, trade finance, and other areas.

Recommended Actions:

- Leverage Federal Advisory Committee Act (FACA) and more open authorities for individual and joint agency advisory committees, as well as interagency fora (*e.g.,* the Financial Stability Oversight Council [FSOC], the Federal Financial Institutions Examination Council [FFIEC], etc.), to foster targeted dialogue and information gathering.
- To address cybersecurity and illicit finance risks that lend to near-term operational action and policy, scale use of the Bank Secrecy Act (BSA) Advisory Group (BSAAG)[88] and partnerships across regulators, law enforcement, and industry[89] to share real-time information about DeFi threats, exploits, critical vulnerabilities, and illicit proceeds. Where appropriate, drive and set expectations for both government and industry to take timely, lawful, operational action to interdict or otherwise disrupt illicit flows and to patch critical vulnerabilities.
- Continue to prioritize engagement with international counterparts in fora like the BIS, FATF, and IOSCO to promote U.S. leadership in DeFi policy, standards, and cross-border experimentation.
- Stand up coordinated, outcome-oriented efforts to promote research and development around the building blocks for responsible DeFi and RegTech to experiment, measure, and drive wider industry adoption of compliant and secure DeFi: including liberal and sustained use of tech sprints, partnerships with Federally Funded Research and Development Centers (FFRDCs), and exceptive relief sandboxes, all defined with a specific outcome and roadmap for potential approval or adoption.

Key Questions:

(1) What projects have requested relief from acknowledged obligations to pursue experimentation in addressing regulatory objectives in the provision of financial services? Did they propose specific controls, possible time delimitations, and measurements of efficacy?
(2) How will timelines and specific requirements for international partner regulatory frameworks affect U.S. investigations, oversight, and competitiveness?

Both government and industry have essential and unique responsibilities, vantage points, and capabilities with which to drive responsible innovation and accountability in digital assets and DeFi. Early intervention is key;

[88] The BSAAG is convened by the Secretary of the Treasury comprised of members of regulatory agencies, law enforcement, private industry, and other designees to advise financial authorities on matters pertaining to AML/CFT frameworks, enhance law enforcement use of AML data, and inform the private sector of law enforcement's use of BSA reporting. *See* FinCEN, "Charter of the Bank Secrecy Act Advisory Group."

[89] Examples include the National Cybersecurity and Forensics Training Alliance, FinCEN's Rapid Response Program, the Illicit Virtual Asset Notification (IVAN) partnership, the Financial Services and Crypto Information Sharing and Analysis Centers (ISACs), the Financial Services Sector Coordinating Council (FSSCC), and 314(b) information sharing groups.

development and especially regulatory and enforcement efforts can have extremely long lead time. Ignoring these systems that are growing in experimentations and adoption, with or without significant U.S. intervention, will only delay integration of necessary controls needed to achieve the policy objectives outlined in this report. Delay will be even more costly and time-intensive, requiring measures to redirect an already-matured sector in advancement of U.S. policy objectives, rather than taking early action to shape and guide the sector while it remains emerging. Taking timely and coordinated action across all DeFi stakeholders to understand, regulate, and develop DeFi is critical. This approach would establish frameworks that provide protections for Americans and the financial system, while also providing helpful guardrails to guide development of this nascent sector before it grows significantly.

Appendix: Additional Resources for Policymakers

Allen, Hilary, "DeFi: Shadow Banking 2.0?", 64 William and Mary Law Review 919 (2023).

Aquilina, Matteo, Jon Frost & Andreas Schrimpf, "Decentralized Finance: A Functional Approach", Centre for Economic Policy Research Discussion Paper 17810 (January 16, 2023).

Aramonte, Sirio, Wenqian Huang, and Andreas Schrimpf, "DeFi Risks and the Decentralization Illusion", Bank for International Settlements Quarterly Review (December 6, 2021).

Auer, Raphael, Bernhard Haslhofer, Stefan Kitzler, Pietro Saggese & Friedhelm Victor, "The Technology of Decentralized Finance (DeFi)", Bank for International Settlements Working Paper No. 1066 (January 2023).

Raphael, Auer, Jon Frost & Jose Maria Vidal Pastor, "Miners as Intermediaries: Extractable Value and Market Manipulation in Crpyto and DeFi", Bank for International Settlements Bulletin (June 16, 2022).

Raphael, Auer, Cyril Monnet & Hyun Song Shin, "Distributed Ledgers and the Governance of Money", Bank for International Settlements Working Paper No. 924 (January 26, 2021).

Brummer, Chris, "Disclosure, DApps and DeFi", Stanford Journal of Blockchain Law and Policy (2022).

Carter, Nick, & Linda Jeng, "DeFi Protocol Risks: The Paradox of DeFi", in Bill Coen & D.R. Maurice (eds.), Regtech, Suptech and Beyond: Innovation and Technology in Financial Services (2021).

Casey, Michael, Jonah Crane, Gary Gensler, Simon Johnson & Neha Narula (eds.), "The Impact of Blockchain Technology on Finance: A Catalyst for Change", 21 Geneva Reports on the World Economy (July 16, 2018).

European Securities and Markets Authority, "Decentralized Finance in the EU: Developments and Risks" (October 11, 2023).

Feyen, Erik, Jon Frost, Leonardo Gambacorta, Harish Natarajan & Matthew Saal, "Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy", Bank for International Settlements Paper No. 117 (July 2021).

Financial Action Task Force, "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (2021).

Financial Stability Board, "Decentralized Financial Technologies: Report on Financial Stability, Regulatory and Governance Implications" (June 6, 2019).

Financial Stability Board, "The Financial Stability Risks of Decentralized Finance" (February 16, 2023).

Financial Stability Board, "The Financial Stability Implications of Multifunction Crypto-asset Intermediaries" (November 28, 2023).

Harvey, Campbell, Ashwin Ramachandran, Joey Santoro, Vitalik Buterin & Fred Ehrsam, "DeFi and the Future of Finance" (August 2021).

International Organization for Securities Commissions, Consultation Report, "Policy Recommendations for Decentralized Finance (DeFi)" (September 2023).

Lehar, Alfred, & Christine Parlour, "Systemic Fragility in Decentralized Markets", Bank for International Settlements Working Paper No. 1062 (December 16, 2022).

Makarov, Igor, & Antoinette Schoar, "Cryptocurrencies and Decentralized Finance (DeFi)", National Bureau of Economic Research Working Paper No. 30006 (April 2022).

Metelski, Dominik, & Janusz Sobieraj, "Decentralized Finance (DeFi) Projects: A Study of Key Performance Indicators in Terms of DeFi Protocols' Valuations", 10(4) International Journal of Financial Studies 108 (November 25, 2022).

Schar, Fabian, "Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets", 103(2) Federal Reserve Bank of St. Louis Review 153 (2021).

United States, Executive Office of the President (Joe Biden), Executive Order 14067, "Executive Order on Ensuring Responsible Development of Digital Assets" (March 9, 2022).

U.S. Commerce Department, "Responsible Advancement of U.S. Competitiveness in Digital Assets" (September 2022).

U.S. Treasury Department, "Illicit Finance Risk Assessment of Decentralized Finance" (April 2023).

U.S. Treasury Department, "The Future of Money and Payments" (September 2022).

Wharton Blockchain and Digital Asset Project and World Economic Forum, "DeFi Beyond the Hype" (May 2021).

White House National Science and Technology Council, Fast-Track Action Committee on Digital Assets Research and Development, Networking and Information Technology Research and Development Subcommittee, "National Objectives for Digital Assets Research and Development" (2023).

Zetzsche, Dirk, Douglas Arner & Ross Buckley, "Decentralized Finance (DeFi)", 6 Journal of Financial Regulation 172 (2020).

DECENTRALIZED FINANCE

REPORT BY THE SUBCOMMITTEE ON DIGITAL ASSETS AND BLOCKCHAIN TECHNOLOGY,
TECHNOLOGY ADVISORY COMMITTEE (TAC) of the
U.S. COMMODITY FUTURES TRADING COMMISSION