

DECODING DEFI: BREAKING DOWN
THE FUTURE OF
DECENTRALIZED FINANCE

HEARING
BEFORE THE
SUBCOMMITTEE ON DIGITAL ASSETS,
FINANCIAL TECHNOLOGY,
AND INCLUSION
OF THE
COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 10, 2024

Serial No. 118–106

Printed for the use of the Committee on Financial Services



www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

57–121 PDF

WASHINGTON : 2026

HOUSE COMMITTEE ON FINANCIAL SERVICES

PATRICK MCHENRY, North Carolina, *Chairman*

FRENCH HILL, Arkansas, <i>Vice Chairman</i>	MAXINE WATERS, California, <i>Ranking Member</i>
FRANK D. LUCAS, Oklahoma	SYLVIA R. GARCIA, Texas, <i>Vice Ranking Member</i>
PETE SESSIONS, Texas	NYDIA M. VELÁZQUEZ, New York
BILL POSEY, Florida	BRAD SHERMAN, California
BLAINE LUETKEMEYER, Missouri	GREGORY W. MEEKS, New York
BILL HUIZENGA, Michigan	DAVID SCOTT, Georgia
ANN WAGNER, Missouri	STEPHEN F. LYNCH, Massachusetts
ANDY BARR, Kentucky	AL GREEN, Texas
ROGER WILLIAMS, Texas	EMANUEL CLEAVER, Missouri
TOM EMMER, Minnesota	JAMES A. HIMES, Connecticut
BARRY LOUDERMILK, Georgia	BILL FOSTER, Illinois
ALEXANDER X. MOONEY, West Virginia	JOYCE BEATTY, Ohio
WARREN DAVIDSON, Ohio	JUAN VARGAS, California
JOHN W. ROSE, Tennessee	JOSH GOTTHEIMER, New Jersey
BRYAN STEIL, Wisconsin	VICENTE GONZALEZ, Texas
WILLIAM R. TIMMONS, IV, South Carolina	SEAN CASTEN, Illinois
RALPH NORMAN, South Carolina	AYANNA PRESSLEY, Massachusetts
DANIEL MEUSER, Pennsylvania	RASHIDA TLAIB, Michigan
SCOTT FITZGERALD, Wisconsin	RITCHIE TORRES, New York
ANDREW R. GARBARINO, New York	NIKEMA WILLIAMS, Georgia
YOUNG KIM, California	WILEY NICKEL, North Carolina
BYRON DONALDS, Florida	BRITTANY PETTERSEN, Colorado
MIKE FLOOD, Nebraska	
MICHAEL LAWLER, New York	
ZACHARY NUNN, Iowa	
MONICA DE LA CRUZ, Texas	
ERIN HOUCHIN, Indiana	
ANDREW OGLES, Tennessee	

Kim Betz, *Staff Director*

SUBCOMMITTEE ON DIGITAL ASSETS, FINANCIAL TECHNOLOGY AND INCLUSION

FRENCH HILL, Arkansas, *Chairman*

WARREN DAVIDSON, Ohio, <i>Vice Chairman</i>	STEPHEN F. LYNCH, Massachusetts, <i>Ranking Member</i>
FRANK D. LUCAS, Oklahoma	JOSH GOTTHEIMER, New Jersey, <i>Vice Ranking Member</i>
TOM EMMER, Minnesota	BILL FOSTER, Illinois
JOHN W. ROSE, Tennessee	RITCHIE TORRES, New York
BRYAN STEIL, Wisconsin	BRAD SHERMAN, California
WILLIAM R. TIMMONS, IV, South Carolina	AL GREEN, Texas
BYRON DONALDS, Florida	SEAN CASTEN, Illinois
MIKE FLOOD, Nebraska	WILEY NICKEL, North Carolina
ERIN HOUCHIN, Indiana	

C O N T E N T S

Tuesday, September 10, 2024

OPENING STATEMENTS

	Page
Hon. French Hill, Chairman of the Subcommittee on Digital Assets, Financial Technology and Inclusion, a U.S. Representative from Arkansas	1
Hon. Stephen F. Lynch, Ranking Member of the Subcommittee on Digital Assets, Financial Technology and Inclusion, a U.S. Representative from Massachusetts	3

WITNESSES

Mr. Brian Avello, Chief Legal Officer, UDHC	4
Prepared Statement	6
Ms. Rebecca Rettig, Chief Legal and Policy Officer, Polygon Labs	19
Prepared Statement	21
Ms. Amanda Tuminelli, Chief Legal Officer, DeFI Education Fund	33
Prepared Statement	35
Mr. Peter Van Valkenburgh, Director of Research, Coin Center	55
Prepared Statement	57
Mr. Mark Allen Hays, Senior Policy Analyst, Americans for Financial Reform	74
Prepared Statement	76

APPENDIX

RESPONSES TO QUESTIONS FOR THE RECORD

Written responses to questions for the record from Mr. Brian Avello	
Representative Warren Davidson	117
Representative Maxine Waters	117
Written responses to questions for the record from Ms. Rebecca Rettig	
Representative Warren Davidson	119
Representative Maxine Waters	119
Written responses to questions for the record from Ms. Amanda Tuminelli	
Representative Warren Davidson	121
Representative Maxine Waters	121
Written responses to questions for the record from Mr. Peter Van Valkenburgh	
Representative Warren Davidson	122
Representative Maxine Waters	123
Written responses to questions for the record from Mr. Mark Allen Hays	
Representative Warren Davidson	125
Representative Maxine Waters	127

LEGISLATION

H.R. ———, To require the Securities and Exchange Commission, Commodity Futures Trading Commission, and the Secretary of the Treasury to jointly carry out a study on decentralized finance	129
H.R. ———, To require the Secretary of the Treasury to report on privacy-preserving technologies	135

DECODING DEFI: BREAKING DOWN THE FUTURE OF DECENTRALIZED FINANCE

Tuesday, September 10, 2024

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON DIGITAL ASSETS, FINANCIAL
TECHNOLOGY AND INCLUSION,
COMMITTEE ON FINANCIAL SERVICES,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2128, Rayburn House Office Building, Hon. French Hill [chairman of the subcommittee] presiding.

Present: Representatives Hill, McHenry, Lucas, Davidson, Rose, Steil, Timmons, Flood, Lynch, Foster, Gottheimer, Sherman, Green, Casten, and Nickel.

Chairman HILL. Good morning. The Subcommittee on Digital Assets, Financial Technology, and Inclusion will come to order.

Without objection, the chair is authorized to declare a recess of the committee at any time.

This hearing is entitled “Decoding DeFi: Breaking Down the Future of Decentralized Finance.”

Without objection, all members will have 5 legislative days within which to submit extraneous materials to the chair for inclusion in the record.

I now recognize myself for an opening statement.

OPENING STATEMENT OF HON. FRENCH HILL, CHAIRMAN OF THE SUBCOMMITTEE ON DIGITAL ASSETS, FINANCIAL TECHNOLOGY AND INCLUSION, A U.S. REPRESENTATIVE FROM ARKANSAS

Welcome back, members and staff, to Capitol Hill following our August work period. Today we are going to discuss decentralized finance.

After the Financial Innovation and Technology for the 21st Century Act (FIT21) legislation passed with broad bipartisan support, I wanted this subcommittee to explore emerging topics like tokenization and decentralized finance (DeFi). As we consider how blockchains can be used in finances, we must continue expanding our knowledge of the possible costs and benefits as it relates to DeFi.

Decentralized finance envisions a financial system that is permissionless, transparent, efficient, and built on top of blockchain networks. It is based on the fundamental idea that indi-

viduals should have the freedom to transact without the fear of illegal financial surveillance or abuse by governments.

By substituting intermediaries for autonomous self-executing code, decentralized finance can shift the way the financial markets and transactions are currently structured and governed; a peer-to-peer future where a Canadian prime minister in the future cannot freeze your bank account just for going to a protest.

Whether it is artificial intelligence or digital assets, we cannot legislate thoughtfully or do oversight of the regulatory agencies if we do not understand it, and DeFi is not only complex but cutting edge, changing, and a completely different way of working.

At the end of the day, decentralized finance is not a person or a company. It is a technology and one that connects people together to reimagine how we transact with one another.

Today's hearing is designed to take a deep dive into some core concepts behind DeFi. I would like members on both sides of the aisle to approach it with an open mind. We will hear from our witnesses about this technology, how it works, the potential benefits and risks, the legal and regulatory implications.

It is important to remember that our regulatory and legal frameworks were designed for a financial system with centralized intermediaries. It does not contemplate the decentralized peer-to-peer ecosystem made possible with digital assets and blockchains.

That is why jurisdictions like the European Union have chosen to explicitly carve out DeFi in their digital asset legislation so they can continue to better understand it.

Rightfully, we took the same approach in drafting our FIT21 legislation here in the House, which directed the Treasury, the Securities and Exchange Commission (SEC), and the Commodity Futures Trading Commission (CFTC) to study this issue together and report back to Congress on the implications and their recommendation.

Contrast that with the Biden-Harris Administration, which uses rulemaking and enforcement actions to go after DeFi and threaten its existence and the future of its use in the United States.

Now that this committee has moved with our historic bipartisan FIT21 legislation, it is important that together we assess DeFi and study the most effective way forward. This hearing is not just about smart contracts and decentralized protocols; it is about how decentralized peer-to-peer technology can preserve individual freedom and improve our financial services for business and consumers alike.

Together we will take another step at our work on the regulatory landscape that supports transformative technology. I encourage everyone on the subcommittee to engage in an informed, open-minded dialog with our esteemed witnesses today to better understand how Congress can help Americans assess and leverage this technology in a safe and secure manner.

I am grateful to our witnesses on our panel today and sharing their wealth of knowledge, and I look forward to the discussion.

Now let me yield to the ranking member for some opening comments.

OPENING STATEMENT OF HON. STEPHEN F. LYNCH, RANKING MEMBER OF THE SUBCOMMITTEE ON DIGITAL ASSETS, FINANCIAL TECHNOLOGY AND INCLUSION, A U.S. REPRESENTATIVE FROM MASSACHUSETTS

Mr. LYNCH. Good morning. Thank you, Mr. Chairman, for hosting this hearing, and I want to thank our witnesses in advance for their willingness to help the committee with its work.

This hearing aims to explore the future of decentralized finance services, or DeFi. DeFi generally refers to virtual assets protocols and services that allow for automated peer-to-peer transactions by using blockchain technology. Unfortunately, there is no consensus definition of DeFi among regulators or industry, which makes this a difficult sector to assess.

DeFi providers claim to offer permissionless and interoperable payments, allowing for efficient and anonymity. However, it has become increasingly evident that these features have made DeFi most attractive to illicit actors who seek to conduct illegal activity. Bad actors continue to develop the techniques that conceal the origins of crypto funds, such as chain hopping and using anonymity-enhanced cryptocurrency.

A risk-assessment report recently issued by the Treasury found that cyber criminals, scammers, and ransomware actors take full advantage of DeFi vulnerabilities to launder illicit proceeds. Additionally, the lack of compliance with anti-money-laundering and terrorist financing laws by DeFi players make this space even more susceptible to illegal activity.

To be clear, we do have consensus in the need for faster payments, anonymity, and privacy. These goals can be achieved in legal and safe ways through policy change. I continue to champion the Electronic Currency and Secure Hardware (ECASH) Act, which directs the Treasury to explore privacy-preserving technology that facilitates permissionless interoperable and instant payments.

I am also encouraged by the Fed's progress in achieving a real-time payment system. I hope to see more projects that explore innovation, such as Project Hamilton, which was led by the Boston Federal Reserve System (Fed) and Massachusetts Institute of Technology (MIT).

The digital assets industry had episodes of implosion and a continuous stream of enforcement actions and a drumbeat of reports of scams, money laundering, demonstrating why it will only survive through proper legislation.

The crypto lobby continues its pursuit of becoming exempt from basic investor and consumer protections and national securities laws. The growing presence of the digital assets industry in this election cycle speaks to its growing desperation to remain unregulated.

This committee should have explored digital asset topics, such as DeFi and tokenization, long before legislation was introduced. The FIT Act, which I strongly opposed, excluded DeFi services, and I urge this committee to refrain from moving forward with similar legislation that would invite the same consumer and investor protection risks by legitimizing this industry.

The DeFi and digital assets industry has proved that it cannot be trusted to offer what it claims. Instead, we should be exploring

policy changes that modernize our payments and banking system and encourage safe innovation.

I want to thank the witnesses for their willingness to appear and help the committee with its work. I look forward to our exchange of ideas.

I yield back.

Chairman HILL. The gentleman yields back.

Today we welcome the testimony of Brian Avello: Mr. Avello is the chief legal officer of Universal DeFi Holding Company (UDHC), an investment fund focused on DeFi's ecosystem; Rebecca Retting: Ms. Retting is the chief legal and policy officer of Polygon Labs; Amanda Tuminelli: Ms. Tuminelli is the chief legal officer of the DeFi Education Fund, an advocacy and educational organization focused on DeFi policy; Peter Van Valkenburgh: Mr. Van Valkenburgh is the director of research at Coin Center, a research and advocacy group focused on the public policy issues facing digital asset technologies and; Mark Hays: Mark Hays is a senior policy analyst on financial technology (Fintech) with Americans for Financial Reform.

Each of you will have 5 minutes for your oral remarks. Your whole statements will be put in the record.

Mr. Avello, we recognize you for 5 minutes.

STATEMENT OF BRIAN AVELLO, CHIEF LEGAL OFFICER, UDHC

Mr. AVELLO. Before I begin, a brief disclaimer.

I am here today in my personal capacity, and the views and opinions I express are my own and do not reflect the views or opinions of my employer, my colleagues, any of our portfolio companies, or any projects with which I serve as a nonexecutive director.

Thank you for the opportunity to speak today. My name is Brian C. Avello, and I am the chief legal officer for the Universal DeFi Holding Company, a principal investment firm. I have been an attorney in the cryptocurrency space since 2016, and my experiences as outside counsel and general counsel have shaped my understanding of decentralized finance, or DeFi, and its growing significance in our financial ecosystem.

DeFi has evolved rapidly since the early days of 2017 and 2018. My journey here began in earnest as the general counsel for the Maker Ecosystem Growth Foundation, a now dissolved software company that worked with its industry partners to bearing the leading credit generation platform, Maker Decentralized Autonomous Organization (DAO), known as Maker, a decentralized stablecoin, multicollateral Dai, to market in November 2019. Some would say that Maker was the world's first DeFi project.

I also have had the privilege of investing in various startups that bridged DeFi and centralized finance, or CeFi. These experiences have led me to believe that a thoughtful regulatory framework is essential for DeFi to fully integrate with traditional financial systems.

DeFi, at its heart, is an open-source technology movement that encompasses a broad spectrum of products that operate outside of centralized financial institutions. They are built on public permissionless blockchains, Ethereum, and encompass various

business models focusing primarily on borrowing and lending and decentralized exchange and now real world assets, or RWAs.

Most importantly, DeFi projects are open protocols, meaning anyone can use them to build new and innovative products, from Citibank using a lending protocol to Great Lakes expand their client accounts to a single developer building a product competitive to established financial institutions.

At present, the leading DeFi applications range from borrowing and lending protocols that allow users to lend their crypto assets in exchange for returns to decentralized exchanges that facilitate peer-to-peer trading through automated market makers.

Moreover, RWAs have recently come to the fore. These are on-chain representations of off-chain assets that provide users access to either interest-bearing opportunities or alternative assets, as well as near real-time execution and settlement and easily verifiable accounting. They can include government securities, corporate credit, and tokenized funds, and allow accredited and institutional investors to access various sources of yield on-chain.

One significant issue is the regulatory landscape surrounding DeFi. Many users are underinformed about the complexities of DeFi protocols, and the absence of traditional intermediaries complicates compliance.

For instance, most, if not all, current financial regulations assume the existence of intermediaries like banks, brokers, and investment advisors, which can be difficult to square decentralized systems built on peer-to-peer and peer-to-protocol transactions.

Addressing these challenges is hard but not impossible by focusing at first on enhancing consumer protections through mandatory disclosures. These should include clear explanations of the technology, detailed information on token distributions, and transparency regarding governance.

Please note that I do not view simple disclosure as a cure all for DeFi's issues or an end around from other ideas for regulation. Rather, I believe it is the initial step of many before we arrive at DeFi sufficiently regulated and integrated into our financial systems.

Indeed, a multiagency regulatory framework could ensure users are, one, fully informed about the protocols they access; and, two, protected from malicious actors or permitting developers and user communities to compliantly innovate and scale this promising technology here in the United States.

In sum, DeFi has shown remarkable growth and potential since its inception, and I hope that my practical experiences can contribute to a better understanding of how these markets are developing while communicating the base idea that, however lawmakers arrive at regulating DeFi, a focus on disclosure and consumer protection is paramount.

Thank you.

[The prepared statement of Mr. Avello follows:]



Testimony of Brian C. Avello

Chief Legal Officer

BEFORE THE

United States House of Representatives Committee on Financial Services

Subcommittee on Digital Assets, Financial Technology and Inclusion Subcommittee

Tuesday, September 10, 2024, 10:00 am.

I. Introduction

Thank you for the invitation to speak today. My name is Brian C. Avello, and I am the Chief Legal Officer for the Universal DeFi Holding Company, a principal investment fund focused on the divide between decentralized and centralized finance (“DeFi” and “CeFi,” respectively). I have worked as an attorney in the cryptocurrency space since 2016, counseling projects and capital on how best to comply with our ecosystem’s developing legal frameworks. Most recently, I was General Counsel for the now-dissolved Maker Ecosystem Growth Foundation (“Maker Foundation”), a software development company that worked with its industry partners to bring the leading credit generation platform, MakerDAO (“Maker”), and decentralized stablecoin, multi-collateral Dai, to market in November 2019.¹

Two experiences in my career have molded my worldview with regard to DeFi and its burgeoning place in our society. First, I was counsel to Maker while it grew from an incipient platform in 2018 to a circulating supply of approximately nine billion Dai by December 2021, so I’ve witnessed how Dai’s growth supported the development of Ethereum’s onchain economy. Part and parcel to that

¹ I also serve as a non-executive director for multiple companies and foundations in DeFi (Nayms, a decentralized insurance market), CeFi (Oasis Pro, a FINRA-registered broker dealer and alternative trading system) and the wider crypto industry (Optimism, the leading Ethereum Layer 2, and Iron Fish, a privacy-centric Layer 1).



success was launching the framework for a “fully decentralized” DAO to Maker’s long-standing community and dissolving the Maker Foundation once its useful life concluded.

Second, as a principal investor, I’ve had the privilege of supporting various real world asset (“RWA”) projects bridging or straddling DeFi and CeFi. Many of their products could become, in my opinion, ubiquitous as they augment on-chain access to treasuries and institutional lending and lower barriers to participation in global finance, creating new possibilities in and reach for finance.² I’ve also borne witness to DeFi’s evolution beyond a niche vertical on Ethereum Layer 1, to being a primary driver of growth on Ethereum Layer 2s³ and Solana, among other ecosystems.

The trials and tribulations of my time in crypto also have crafted my thinking on regulation: if DeFi is to move towards full inclusion with traditional financial rails, a common-sense regulatory apparatus that recognizes DeFi’s unique aspects and focuses foremost on compulsory disclosure is paramount to our industry’s success in the coming years.

II. Brief Primer on DeFi Business Models and Decentralized Protocols

Since ours is a highly technical space with varying definitions, I do not intend to cover all the different business models that have arisen since “DeFi Summer” in 2020, nor will I cover well-trodden topics such as DeFi technical infrastructure (*e.g.*, oracles) or centralized stablecoin models (*e.g.*, Tether

² In many ways, I believe this intersection is similar to how ChatGPT has established a new paradigm for retrieving and presenting data and information.

³ For instance, Optimism (including Base), Arbitrum and Scroll, saw total value locked (“TVL”) increase substantially due to the growth of DeFi in their respective ecosystems. See State of DeFi Q2 2024, Messari.io, available at <https://messari.io/report/state-of-defi-q2-2024> (last visited on August 27, 2024).



and USDC)⁴. Rather, I describe below several generic product categories in DeFi⁵, and briefly discuss decentralized protocols.

(a) DeFi Business Models

(i) Borrowing and Lending; Credit Creation

Multiple DeFi protocols have come to market offering users the means to lend their crypto assets to earn a fixed or variable return by depositing them in a smart contract or lending pool that simultaneously allows other participants to borrow those assets.⁶ Depositors receive a different crypto-asset, representing his or her pro rata interest in the lending pool and can be redeemed at any time for the amount of the original deposit plus the accrued interest.⁷ The above describes a “simple” borrowing and lending protocol; however, many modified versions have come to market in recent years, including protocols that permit “self-paying” loans.⁸

Credit creation is a unique twist on the traditional concept of borrowing and lending made possible by the permissionless nature of smart contracts. A well-known example of a credit creation engine is the Maker Protocol, an open-source suite of permissionless smart contracts designed to allow users to generate (*i.e.*, draw) a price-stable decentralized digital currency called Dai against their own

⁴ Stablecoins are a (if not, *the*) critical infrastructure that makes DeFi work. Notably, despite a tepid crypto market through summer 2024, the stablecoin market cap recently reached all-time highs (\$168.1b), further evidencing their positive trajectory and, I hope, foreshadowing similar growth for DeFi. See “Stablecoin Market Cap Hits New All-Time High, Beating Early 2022 Record.” The Block, *available at* theblock.co (last visited August 29, 2024).

⁵ For further reading, there are voluminous examples of succinct explanations of the varied business models in DeFi (*see e.g.*, DeFi and the Future of Finance, by Campbell R. Harvey, Ashwin Ramachandran, et al) as well as a plethora of media that covers our industry’s latest innovations (*e.g.*, Messari.io, Bankless.com and the Bell Curve Podcast).

⁶ See Final Report with Policy Recommendations for Decentralized Finance (DeFi), p. 11, The Board of the International Organization of Securities Commissions.

⁷ *Id.*

⁸ With these debt positions, users deposit their yield bearing assets (*e.g.*, staked ETH) into a smart contract and that smart contract automatically uses the yield generated by the token to pay down one’s debt. *See e.g.*, Alchemix (“self-repaying loans”), <https://alchemix.fi/>; *see also* Altitude.fi (users configure the parameters of their debt positions and the Altitude protocol “borrow[s] against it and deploys excess collateral into generating yield, which is used to pay [off one’s debt].”)



crypto-collateral.⁹ Notably, a user's collateral is segregated into the individual's personal position, called a vault, and is not pooled with the assets of any other user, a key differentiator when compared with notable lending and borrowing protocols.

(ii) Decentralized Exchange

Best described as a verb,¹⁰ *decentralized exchange* ("DEX") is the process for peer-to-peer swapping of different crypto assets on-chain. Although different models of exchange were prominent before 2018¹¹, the dominant model¹² to arise since then is the "automated market maker" ("AMM"). AMMs "are a type of [DEX] that use algorithmic mechanisms to facilitate the trading of digital assets."¹³ Unlike "traditional financial markets that rely on buyers and sellers, AMMs aim to maintain liquidity in the DeFi ecosystem through liquidity pools."¹⁴ Users supply these pools with crypto tokens, and "the prices of these tokens are determined by a constant mathematical formula."¹⁵ When a user wants to trade, they swap one token for another directly through the AMM, and this system allows the protocol to provide continuous liquidity for a wide range of assets, including less liquid

⁹ The Maker Community changed its branding and purportedly added new product offerings in August 2024 while making revisions to the current versions of Maker and Dai. See, e.g., "MakerDAO is now 'Sky' as \$7B Crypto Lender Rolls Out New Stablecoin, Governance Token." Coindesk, available at www.coindesk.com (last visited on August 28, 2024). Neither my UDHC colleagues nor I was involved in these changes as we stepped away from Maker in 2021.

¹⁰ See "There's No Such Thing as a Decentralized Exchange," Van Valkenburgh, Peter, The Block, available at <https://www.theblock.co/post/79768/theres-no-such-thing-as-a-decentralized-exchange> (last visited on September 2, 2024).

¹¹ Many early DEXes ran some variant of the "order book" model, whereby users created orders using a smart contract protocol and those orders were then matched with other buyers and sellers. Oftentimes, DEX operators incorporated an offchain order book, and incorporated the underlying Layer 1 blockchain as the settlement layer. See e.g., Final Report with Policy Recommendations for Decentralized Finance (DeFi), p. 17, The Board of the International Organization of Securities Commissions (Dec. 2023). That said, other DEXes were fully decentralized, with non-custodial and permissionless on-chain matching markets (order matching between buyers and sellers and settlement happened completely on-chain, which, with high Ethereum gas prices at the time, became cost-prohibitive in comparison with AMMs). See e.g., OasisDEX Protocol FAQs, available at <https://oasisdex.com/faq> (last visited on August 28, 2024).

¹² The leading DEXes on Ethereum and Solana use variants of the AMM model.

¹³ See "What is an Automated Market Maker?" Coinbase.com (last visited on August 28, 2024).

¹⁴ *Id.*

¹⁵ *Id.*



cryptocurrencies.¹⁶ Many users access AMMs to trade assets at spot but many markets also list an ever-growing cornucopia of leverage tokens and exotic options, like perpetual futures.¹⁷

(iii) Miscellaneous

These last categories, which overlap with the three mentioned *supra*, have seen considerable growth as of late:

- **Synthetic Assets:** these are “tokenized, blockchain-powered financial products mirroring the values and characteristics of real-world assets (RWAs),”¹⁸ and include any variety of underlying assets from commodities (*e.g.*, gold) to government bonds (*e.g.*, US treasuries) and stablecoins.
- **Aggregators:** these “provide services that offer users optionality to access trading, liquidity or yield-generating opportunities” from a variety of protocols through one easy-to-use front-end interface.

(b) Decentralized Protocols

A Decentralized Protocol is a distributed, permissionless, non-jurisdictional protocol that serves as infrastructure to manage value, help build an ecosystem and afford users autonomy.

The objective of a Decentralized Protocol is self-sovereignty. A user should have the autonomy to engage with the protocol freely on a person-to-protocol or business-to-protocol basis with little or

¹⁶ *Id.*

¹⁷ Also known as perpetual swaps, these popular futures contracts have no expiration or settlement. Rather than “expiring on a given day, a funding rate mechanism is used to tie the price to an index of the price of the underlying asset, [] and several times a day participants must pay each other based on the imbalance between mark price and index price: (i) if the mark price is over the index price, longs pay shorts or (ii) if the mark price is under the index price, shorts pay longs.” See The Quest for Perp AMMs, by Deribit, *available at* <https://medium.com/deribitofficial/the-quest-for-perp-amms-662124742dd1> (last visited on August 28, 2024).

¹⁸ See “What are Synthetic Assets in Crypto?” Unchained Crypto, *available at* <https://unchainedcrypto.com/synthetic-assets-in-crypto/> (last visited on August 28, 2024).



no intermediation. For example, Citibank should be able to use the protocol to create products and services just as easily as an entrepreneur could use it to run her business.

The arc of decentralization is how a project starts up and develops into a decentralized protocol. However, we call a project that develops this protocol within the guardrails of an evolving regulatory landscape the Compliant Arc of Decentralization.¹⁹ At the heart of it is anticipating how regulation will apply to decentralized protocols and DeFi specifically.

III. **Bridging DeFi and CeFi: Real World Assets**

Over the last two years, RWAs, on-chain representations of off-chain assets, have moved from an experimental niche in DeFi to a central ecosystem pillar offering users exposure to various yield-bearing assets and strategies. There are multiple strands of RWAs – stablecoins,²⁰ equity and debt-like instruments and tokenized versions of alternative assets – gaining considerable traction not only with retail users but also with institutions.²¹

Many RWA projects incorporate and overlap with proven DeFi business models (*e.g.*, lending and borrowing protocols) and, as such, expand upon options for yield generation that are available to users. I provide a brief review on what I see as the three prominent categories.

¹⁹ My colleagues at the UDHC have written extensively about decentralized protocols. *See e.g.*, “On Being Sufficiently Decentralized”; “On Optimal Decentralization”; “The Arc of Decentralization”; and “The Compliant Arc of Decentralization,” UDHC, *available at* <https://www.udhc.com/writing> (last visited September 2, 2024).

²⁰ As mentioned *supra*, stablecoins were the first RWAs providing synthetic exposure to the US dollar. Given the enormity of that topic, in addition to widespread familiarity with stablecoins, I focus more on recent developments in the wider market.

²¹ Notably, RWA protocols have returned to the fore as the crypto market entered a more bullish phase in Spring 2024, with the total value locked (“TVL”) “growing from \$2 billion to \$8 billion since Q1 2023, excluding traditional stablecoins.” *See* “Welcome to the Real World,” Messari.io, *available at* messari.io/reports/welcome-to-the-real-world (last visited on August 20, 2024).



(a) Yield-Bearing Assets

Over the last eighteen months, many new RWA protocols have offered users exposure to Treasury-backed yield-bearing assets in DeFi, including the stability of government-issued securities with the accessibility and programmability of blockchain technology. Typically, platforms tokenize US Treasury bills or similar government debt to back dollar-denominated stablecoins that earn yields comparable to traditional Treasury securities.²² These tokens can automatically distribute interest to holders, providing returns while also permitting holders to use these fungible assets to pursue other opportunities in DeFi.²³ Notably, they tend to be offered only to organizations and individual purchasers outside the United States.

(b) Alternative Assets

Notably, some borrowing and lending protocols have pivoted from purely crypto-asset plays such as BTC or altcoin lending to corporate credit, overcollateralized lending and receivables financing and have incorporated more stringent borrowing standards and formal lending desks to professionalize their operations.²⁴ In many ways, these teams represent an actual bridge between DeFi and CeFi: institutions and accredited investors can lend their assets and get the benefits of using permissionless, smart contract-based lending while being serviced by an institutional grade team that screens, verifies, and manages borrowers.

In addition, some physical commodity-backed tokens, such as Tether Gold, have come to the market, though it's unclear whether there is significant demand on par with stablecoins. Other parties have attempted to launch other precious metals-backed tokens in the past but

²² See e.g., Ondo Finance's USDY, <https://ondo.finance/usdy>; see also Mountain Protocol's USDM, <https://mountainprotocol.com/>.

²³ *Id.*

²⁴ See Maple Finance, <https://maple.finance/>.



failed.²⁵ It remains to be seen whether there is robust demand for these sorts of items though it's reasonable that they could grow in popularity for investors who are comfortable maintaining portions of their wealth on-chain.

(c) Tokenized Funds

Tokenized funds typically provide exposure to traditional assets, such as US Treasuries, while issuing digital tokens that represent shares in the fund.²⁶ By tokenizing fund shares, investors can benefit from the efficiency and flexibility of blockchain-based transactions, including daily liquidity and the ability to use the tokens in DeFi applications. For example, some projects allow qualified purchasers to buy or redeem shares using USDC or USD, with the fund's net asset value ("NAV") updated daily, and integrate with oracle networks like Chainlink to bring critical data NAV on-chain. These steps allow for real-time pricing information and even use the tokenized shares as collateral in DeFi, further melding DeFi and CeFi. Perhaps one day we may see these RWAs issued, living and operating onchain, rather than simply creating token representations of custodied assets.

²⁵ Many such projects launched in the early days of DeFi but failed to take hold. See "More Than 77 Crypto Projects Claim to Be Backed by Physical Gold – After 30 Failed," Bitcoin.com (last visited on August 31, 2024).

²⁶ See e.g., Superstate's USTB (<https://superstate.co/ustb>) (last visited on August 30, 2024). Projects such as Blackrock's BUIDL have seen tremendous growth in less than six months on the market. See BlackRock Tokenized Treasury Fund BUIDL Reaches \$500M," Cointelegraph.com (last visited on August 29, 2024).



IV. Regulatory Challenges and Potential Considerations

Permissionless, genuinely decentralized (tech, social, and governance) technology poses perplexing questions for regulators accustomed to intermediary touchpoints for market insight and enforcement. Tomes have been written on the issues that arise from DeFi²⁷, but from my perspective, boiling down the challenges to their essence helps when considering potential solutions.

(a) Challenges

(i) Under-Informed Users

DeFi presents considerable *initial* barriers to entry for nascent users unfamiliar with its underpinning technology or significant jargon. What's more, projects often fail to present fulsome information on topics like token distributions and unlock schedules, in addition to simple-to-follow documentation on how the protocols work and summaries and annotations of important parts of the applicable code. It's a common criticism but one that, when combined with the cumbersome UX for new participants²⁸, rings true. How can we expect DeFi to truly be inviting when much of what users or investors would expect – who are the largest token holders and what are the lockup schedules, for instance – must be ferreted out and reported on by third parties.²⁹

²⁷ See generally, "Decentralized Finance: Report of the Subcommittee on Digital Assets and Blockchain Technology, Technology Advisory Committee (TAC) of the US Commodities Futures Trading Commission.

²⁸ This point – criticism about the difficulty for new users to easily understand and access cold storage and hot wallet software – is a tired trope in my opinion, and industry leaders like Coinbase are releasing the UI/UXs for onboarding the next ten million users. See e.g., Introducing Base (Coinbase's L2), available at <https://www.coinbase.com/blog/introducing-base> (last visited on August 29, 2024).

²⁹ While this statement is still true and has been since DeFi's early days, market standards in the industry have rapidly matured. In my experience, common business practice dictates that many teams and DAOs publish detailed breakdowns on token issuances and token distributions, while making available information to their communities regarding large token sales or movements from their respective treasuries. Moreover, details on token distributions



(ii) A (Sometimes Futile) Search for Intermediaries

Our regulatory financial apparatus generally assumes the existence of intermediaries that interact with user funds at different points in a given transaction and places the onus for compliance on said intermediaries (be they firms or individuals).³⁰ But that need becomes problematic when there is no one playing a traditional intermediary role in a permissionless, non-custodial protocol and where users always maintain total, independent control of their assets, rather than placing them with a third-party custodian. Finding the right regulatory touchpoint for DeFi protocols then becomes a novel task with commentators suggesting that responsibility may sit with protocol founders,³¹ development teams,³² validators, miners, node operators and/or front-end operators. Regardless of the approach, identifying and addressing gaps and the regulatory perimeter around DeFi places authorities in the difficult and unenviable position of searching DeFi “projects, enterprises and ecosystems” to identify responsible actors for “regulatory compliance and the imposition of systems, processes and controls ... both consistent with [] objectives and robust to changing circumstances.”

and related transactions are synthesized by web3 reporting companies like Messari, Token Flow and Dune Analytics.

³⁰ See generally, the Bank Secrecy Act, Know-Your-Client record collection obligations sit with custodial service providers and the Commodities Exchange Act requires registration for individuals or firms acting “on behalf of another person in connection with trading futures, swaps, or options.”

³¹ See generally, “Decentralized Finance: Report of the Subcommittee on Digital Assets and Blockchain Technology,” p. 55, fn. 67, Technical Advisory Committee (TAC) of the US Commodity Futures Trading Commission.

³² See Walch, Angela, In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains, p.19 (June 27, 2018). Chapter in *Regulating Blockchain. Techno-Social and Legal Challenges*, edited by Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos & Stefan Eich, Oxford University Press, 2019.



(b) Considerations

(i) Disclosure Regimes and Consumer Protections

Before approaching thornier questions about decentralization, I believe it's essential to address DeFi's lowest-hanging fruit: enhancing customer protection by mandating information disclosures. For instance, a notice and disclosure regime³³ may suffice to ensure that users are fully informed about the tooling they use. The breadth of information I'd expect to see should include (1) plain English descriptions of the protocol and its component pieces; (2) annotated copies of the code highlighting what material lines of code enable what functions for the protocol's smart contract architecture; (3) detailed information regarding token distribution to investors and insiders; (4) information on individuals, firms or both holding a certain percentage of tokens (*e.g.*, 10%); and (5) dates and amounts applicable to investor and insider token unlocks.³⁴

Admittedly, information disclosure regarding DeFi tokens and governance appears to tread closely to what could arguably be expected from traditional disclosures required by financial regulators, such as the Securities and Exchange Commission,³⁵ though many commentators have noted why current disclosure regimes do not suffice for crypto.³⁶ From my

³³ I do not suggest efficiency or effectiveness will be found in a restrictive licensure regime whereby any potential DeFi project must apply and be approved for a license. Quite conversely, such an approach appears to be motivated by eliminating DeFi in the US, rather than creating appropriate guardrails for its growth and maturity.

³⁴ Notable crypto-focused academics have made similar suggestions. *See e.g.*, Center, C. B., Agnes N. Williams Professor of Law at Georgetown University Law. (2022). *Disclosure, Dapps and DeFi*. Stanford Journal of Blockchain Law & Policy.

³⁵ *See generally*, "The Current SEC Disclosure Framework Is Unfit for Crypto," Paradigm, available at <https://policy.paradigm.xyz/writing/secs-path-to-registration-part-iii> (last visited on August 28, 2024).

³⁶ *Id.* at 4-5 (noting, for example, several difficulties in applying current SEC disclosure to crypto, including (a) that "[m]ost crypto assets do not provide legal rights against an identifiable issuer..." and (b) "[c]rypto assets can exist independent of the existence of an 'issuer'.").



vantage point, modified disclosure forms, along the lines of what Commissioner Mark Uyeda recently suggested for a “Crypto S-1”, could be a good start.³⁷

Nevertheless, without delving into the token classification debate, there is still room to ensure that projects publish material disclosures required by educated consumers and face enforcement, private litigation or both should they publish false, misleading or incomplete information.

(ii) Controlling Teams and Centralized User Interfaces

This is a complicated area where, admittedly, no easy answer exists. From my perspective, while finding the right framework for building a regulatory structure for DeFi is paramount, it also is imperative to continue ensuring that software developers writing code for DeFi protocols do not unwittingly become responsible for the control and compliance of what they launch but do not operate.³⁸ Moreover, putting the onus for compliance with money transmissions laws, or the like, on parties like validators or node operators seems counterintuitive as those infrastructure-supporting actors are (i) functionally similar to Amazon Web Services and not Stripe, and (ii) may arguably fall outside the definition of money transmitter (and within the Network Services Exemption).³⁹

On the other hand, most end-user interactions with DeFi protocols occur through graphical user interfaces and other “off-chain” components. These tools are often hosted on centralized servers and rely on traditional internet infrastructure to enable users easy access to

³⁷ See “SEC Commissioner Mark Uyeda Calls for S-1 Form Tailored for Digital Assets,” Coindesk, available at coindesk.com (last visited on September 5, 2024).

³⁸ See FIN-2019-G001, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies” May 9, 2019 (“FinCEN May 2019 Guidance”), §5.2.2 Status of a DApp Developer (“[T]he developer of a DApp is not a money transmitter for the mere act of creating the application...”).

³⁹ 31 CFR § 1010.100(ff)(5)(ii)(A).



DeFi through websites or mobile apps. Some interfaces even extract various fees from users, for instance, by charging a “swap fee” when a user makes a trade. At times, founding developer teams both launch their protocols with one hand and operate with the other businesses that channel users to their protocols. That situation, with one team centrally controlling the decentralized application’s entire tech stack (through governance of the protocol plus ownership of more than 10% of the governance token and with fee extraction from a market-dominant user interface), would be a logical focus for regulatory application. And which regulatory regime and regulator depends on the service or activity permitted through the interface.

V. Conclusion

DeFi has shown incredible traction since 2017 and 2018, when many of the current blue chip projects (Maker, Aave (f/k/a EthLend), Uniswap and Compound) came to the fore. My hope in testifying today is that my practical experiences through the years of attempting to address DeFi’s complicated legal questions as outside counsel and a General Counsel may benefit the Committee not only with its understanding of this technology but also with possible ways to begin considering its regulation.

Chairman HILL. Thank you, sir.

Ms. Rettig, you are recognized for 5 minutes. Thank you.

STATEMENT OF REBECCA RETTIG, CHIEF LEGAL AND POLICY OFFICER, POLYGON LABS

Ms. RETTIG. Good morning, Chairman Hill, Ranking Member Lynch, Chair McHenry, and members of the subcommittee. Thank you for the opportunity to testify.

I have spent the last 7-plus years of my legal career representing software developers building novel blockchain-based technology, including DeFi applications. I brought to this work years of experience at a large New York law firm where I represented Fortune 500 companies and traditional financial services firms with securities and other regulatory matters and where I experienced the intersection of law and technology firsthand in one of the early peer-to-peer file-sharing cases.

Currently, I am the chief legal and policy officer of Polygon Labs, an international software development company building blockchain technology.

Today I will discuss how the unique mechanics of DeFi have informed the global regulatory response to this technology and briefly touch on a policy proposal to treat DeFi's critical infrastructure and maximize user and market protection.

Decentralized finance refers to a software system that allows users to engage independently in financial transactions. It is part of the larger web3 movement that returns the internet to individuals, a response to consumer demand for peer-to-peer transparent networks, for increased competition, and for control over one's own data. This means no Big Tech company and no big finance firm sits in the middle of any DeFi transaction.

The hallmark of DeFi is that users retain custody and control over their assets and their data at all times. DeFi protocols are a set of automated code-based rules that allow for financial transactions when users provide the instructions. These are similar to the software protocols, like Transmission Control Protocol/Internet Protocol (TCP/IP), that underlie our internet today.

Code for DeFi protocols is open, can be reviewed in real time, and audited by anyone. There is no proprietary black box, as in the traditional financial world. This increases predictability for users, and these open systems increase competition to build better user experiences.

DeFi protocols are built on public infrastructure, namely, blockchain networks. DeFi transactions are cryptographically settled on these networks via automated consensus of thousands of computers, which creates a transparent record of transaction data. Like the internet itself, this infrastructure can be accessed and utilized by anyone with an internet connection.

The term "infrastructure" usually evokes the idea of roads and bridges. Today, it is also the technological system that underpin many industries, from aviation to farming to financial services. In the United States, that infrastructure is overseen by CISA, the Cybersecurity and Information Security Agency, as critical infrastructure in collaboration with various other agencies, including the

Treasury Department and law enforcement. DeFi can, likewise, fall under their purview.

Today, DeFi allows users to exchange one crypto asset for another, provide crypto asset liquidity for borrowing, or engage in novel trading strategies. Yet DeFi remains nascent. The first DeFi protocol is approximately 7 years old, and today, DeFi holds around \$78.9 billion of crypto asset value. This is only 3.9 percent of total crypto value and .07 percent of global Gross Domestic Product (GDP).

Because DeFi systems are neutral technology, regulators have recognized that we cannot perfectly map traditional financial laws onto intermediary-less systems. The International Monetary Fund (IMF) and the financial stability board recognize that, quote, in the case of DeFi, the lack of intermediaries means that the traditional approach to regulation cannot be applied.

The U.K.'s (Her Majesty) HM Treasury agreed, stating that regulation of DeFi, if any, would occur after any centralized crypto regulation.

The same is true for EU, Japanese, Singaporean, and UAE regulators, all of whom have implemented centralized crypto regulation but not DeFi regulation to date. In fact, it used markets and crypto asset regulation, specifically exempt services performed in a fully decentralized manner without intermediaries, and requires a study of DeFi.

Other regulators around the globe have devoted time and resources to analyzing novel DeFi use cases, including the Bank of International Settlements, various central banks, and the Singapore Monetary Authority, who have all experimented themselves with DeFi technology.

DeFi addresses many of the core policy considerations of traditional financial services in a different way through automation, transparency, and user control over assets and data, and many of the risks in DeFi can be addressed by treating it as critical infrastructure.

This is the topic of a recent paper I coauthored examining how CISA, in collaboration with OCCIP, Treasury's Office of Cybersecurity and Critical Infrastructure Protection, can work to mitigate cyber and system management risk to bring about policies that protect both users and markets, a mission fundamental to the long-term growth of DeFi.

I am appreciative of the subcommittee's efforts to understand this technology, and I look forward to your questions.

[The prepared statement of Ms. Rettig follows:]

**Written Testimony of
Rebecca Rettig
Chief Legal & Policy Officer of Polygon Labs**

“Decoding DeFi: Breaking Down the Future of Decentralized Finance”

**Before the U.S. House Financial Services Committee Subcommittee on
Digital Assets, Financial Technology, and Inclusion**

September 10, 2024

Bio

I am the Chief Legal Officer of Polygon Labs, an international software development company building blockchain scaling infrastructure and an aggregated blockchain network. I spent the early part of my legal career at a large New York law firm litigating and defending cases relating to, among other things, traditional financial services and regulations as well as early peer-to-peer file sharing technology.

In the last seven-plus years of my legal career, I have focused on advising companies building novel applications in the blockchain space, including in decentralized finance (“DeFi”), as well as how to implement risk mitigation mechanisms that achieve regulatory goals that underlie many of our traditional systems today.

Prior to joining Polygon Labs, I was General Counsel at a UK-based software company that developed one of the most well-known DeFi protocols and created other blockchain-based user applications. As part of my work there, I began engaging with regulators and policymakers in the U.S. and abroad to meet requests for greater education about DeFi and its underlying technology, benefits, and risks as well as the ways to achieve regulatory goals within this system. I have continued that work to the present.

Recently, I co-authored a paper entitled “Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance,” published in January 2024, which sets forth a three-part proposal to effectively detect, document and deter the proliferation of illicit activity in DeFi — to bring traditional financial integrity standards into the system without classifying pure technology as financial institutions — while preserving the technology as permissionless, neutral infrastructure.¹

¹ Rebecca Rettig, Michael Mosier, and Katja Gilman, *Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance*, SSRN (Jan. 29, 2024), <https://ssrn.com/abstract=4607332> [hereinafter *Genuine DeFi as Critical Infrastructure*].

Chairman Hill, Ranking Member Lynch and members of the Subcommittee, thank you for inviting me to speak today on the topic of decentralized finance.

DeFi is part of the larger web3 movement of decentralized applications built upon open networks — a movement that seeks to return the Internet to individuals and move away from the centralization and ownership of large tech companies and financial institutions. It's a movement arising from consumer demand for peer-to-peer transparent networks, for increased competition, and for control over one's own data.

DeFi is an innovative technological system that allows for novel ways of transacting (*see* Part I), brings new and different benefits from the traditional financial system (*see* Part II) and thus, has received different regulatory treatment from policymakers around the globe (*see* Part III).

I. Decentralized Finance Explained

A. Defining DeFi

The first blockchain network — Bitcoin — enabled peer to peer transfers of value; DeFi is Bitcoin's successor, allowing financial transactions through technological systems where no intermediaries are necessary.

Although there is no widely agreed-upon definition of DeFi,² I generally define it as a blockchain-based, software-based system that empowers users to engage in economic transactions without the need for intermediaries.

Certain hallmarks of DeFi distinguish it both from other blockchain-based software applications that allow for financial transactions and from the traditional financial system:

- it's non-custodial, *i.e.*, there is no identifiable entity or person who holds or otherwise can control cryptoassets on behalf of others: in DeFi systems, users maintain custody and control of their assets at all times;
- all transactions are user-directed and user-controlled, *i.e.*, there is no third party entity or person needed to effect any transaction; and
- the code is open source or source available, which allows users, developers and other third parties to verify functionality, and gain certainty over transactions.

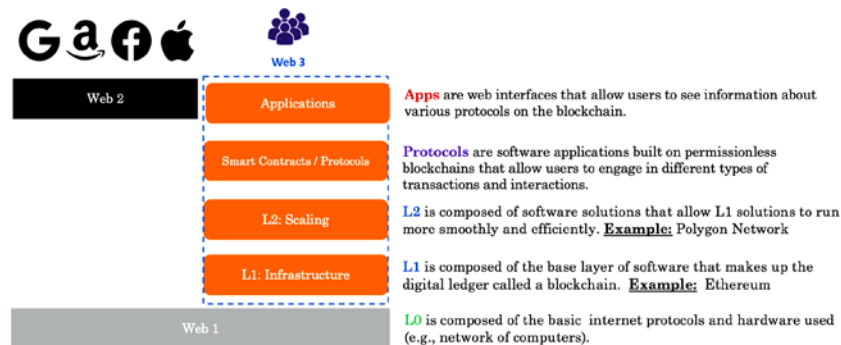
² See, e.g., Mariana de la Roche W. & Mirko Zichichi, *Bringing Clarity to the DeFi Sector: A Cross-Sector Proposal for a Unified DeFi Definition*, IOTA Foundation (Aug. 8, 2023), https://files.iota.org/comms/Bringing_clarity_to_the_DeFi_sector.pdf; Katrin Schuler, Ann Sophie Cloots & Fabian Schar, *On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance*, 2 (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4422473; U.S. Dep't of the Treas., *Illicit Finance Risk Assessment of Decentralized Finance*, 1 (2023), <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>; The Bd. of the Int'l Org. of Sec. Comm'ns, *Consultation Report: Policy Recommendations for Decentralized Finance (DeFi)*, 1 n.3 (2023), <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD744.pdf>.

“Smart contracts” — automated software that executes particular logic and functions in a conditional manner — comprise DeFi protocols. With this software, if a certain condition occurs under particular circumstances, then a specific action will automatically follow. A “smart contract” is not an actual legal contract between parties: “smart” refers to the fact that the code is autonomous and self-executing; “contract” refers to the fact that a transaction occurs automatically when predetermined conditions are met.

DeFi protocols are built on public infrastructure — namely blockchain networks. Like the Internet itself, this infrastructure can be accessed and operated by anyone with an Internet connection. The graphic below shows the technology stack upon which these protocols are built and the ways in which they can be accessed, including through user interfaces (discussed in Part I.B below). Leveraging public infrastructure means that information about DeFi transactions is recorded in real time and is viewable by anyone with an Internet connection.

The layers of Web3

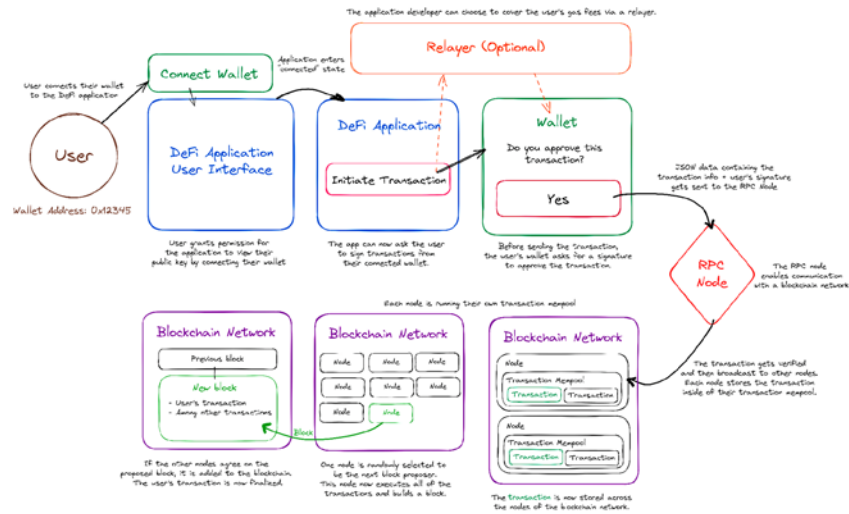
Web3 builds on the foundations of the Internet we know today.



B. DeFi Software

DeFi allows users to communicate and execute financial transactions that are settled on permissionless blockchains. The below graphic shows the progression of DeFi transactions through the various software components comprising DeFi systems. The top half of the graphic depicts the DeFi software system; the bottom, the way in which base layer blockchain networks settle those transactions and record them on a blockchain.

Notably, this transaction flow is the same as for non-financial, blockchain-based applications, as well, such as blockchain-based social media applications, gaming, consumer loyalty programs and the like.



The following are descriptions of the software involved in communicating a DeFi transaction:

- Wallets:** A wallet is software comprising two unique numbers, each called keys: one public key, which is an identifier that lets users receive cryptocurrencies — similar to an email address; and one private key, which allows the user to access and send the cryptocurrencies associated with the paired public key — similar to a password.³ Together, these keys allow individuals to utilize their wallet to interact or communicate with a blockchain network. Wallets — also called “externally owned accounts” — can either be downloadable software stored locally on a user’s computer or smart contract-based accounts stored directly on a blockchain network. In DeFi, wallets are typically self-hosted — that is, downloaded, owned and controlled by the user, without an external third party providing custody. As a general rule, wallet software developers who create and make them available for download do not have any ongoing involvement with the wallet software’s operation

³ See Brief for DeFi Education Fund as Amici Curiae Supporting Respondents, Coinbase Inc. and Coinbase Global Inc.’s Motion for Judgment on the Pleadings, SEC v. Coinbase, Inc. et al., No. 23 Civ. 4738 (S.D.N.Y. 2023), 4; see also Fin. Crimes Enforcement Network, FIN-2019-G001, Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies, 16 (2019), <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf> (“Unhosted wallets are software hosted on a person’s computer, phone, or other device that allow the person to store and conduct transactions in CVC. Unhosted wallets do not require an additional third party to conduct transactions. In the case of unhosted, single-signature wallets, (a) the value (by definition) is the property of the owner and is stored in a wallet, while (b) the owner interacts with the payment system directly and has total independent control over the value.”).

by users. When users engage in transactions with their self-hosted wallets, they maintain independent control over their cryptocurrency.

- **User Interfaces / Front Ends:** User interfaces — sometimes referred to as front ends — are websites or applications that run on a person’s full service computer, phone, or other mobile device.

All Internet interactive sites or applications require front ends and back ends. The front end is a visual interface of a software system with which a user interacts. They are the part of a computer system or application that a user can see and with which a user interacts — usually to more easily access information and services available on the Internet. Back ends are the structure, system, data and logic underlying the user-facing application — that is, the aspects of a system or software program that a user does not see or interact with directly.

A user provides inputs through a front end, and the back end of the system processes the inputs. The back end may read, analyze and write data that it then provides as an output to the user, through the front-end user interface. For example, www.x.com is a front end that allows a user to access X’s social media software algorithm and data, with the algorithm and data being the back end.

User interfaces relating to DeFi Systems can take a number of forms: (1) some only provide information about one or more DeFi protocols, such as potential transactions available through those protocols and related pricing and terms, without taking a fee; (2) others provide information and functionality to allow a user to connect their self-hosted wallet and then provide information about a transaction through their wallet directly to a protocol independent of the front end, with some of the providers of these interfaces taking a fee; and (3) a third type that provides some off-chain configuration (*e.g.*, a matching engine or order book hosted on a private server) where a user’s transaction is reliant on the host of the off-chain server or service provider to match orders or otherwise to take steps towards completion of transactions, regardless of whether they take a fee. Although many users employ user interfaces, they are *not a necessary prerequisite* for either initiation or completion of a genuine DeFi transaction; users are able to engage in transactions on genuine DeFi protocols by accessing the smart contracts directly on a blockchain network. User interfaces, however, make these interactions less technically demanding.

When users view interfaces to DeFi protocols, they have the same visual experience as when they interact with more traditional, web2 user interfaces. The most notable difference is that users interact with the Internet protocols in DeFi via software that allows them to retain control over their data and their assets, while in web2, all user information and assets are handled via intermediaries – whether it be large tech companies or big financial firms.

- **Protocol:** “Protocol” refers to a set of smart contracts that work together to allow users to communicate transaction instructions through a series of communications providers to a

blockchain network for processing and execution. “Protocol” generally refers to a set of rules or procedures for a certain system; in DeFi protocols, the interaction among smart contracts sets the rules. These protocols may also be referred to as “dApps” — decentralized applications. As neutral technological infrastructure, DeFi protocols are akin to early Internet protocols such as HTTP, which allows for websites to exchange data and information, and SMTP, the underlying infrastructure for email.

- **Relayers:** Relayers are software that sends a user’s transaction instruction to a protocol⁴ by accepting a user’s communication from a DeFi protocol and sending it to the next step in the transaction flow, such as a node for remote procedure calls (“RPCs”) or a blockchain network node. Relayers do not take custody of or exercise independent control over user assets at any time — they relay communications, often about transactions. Users or application developers may compensate parties who run relayers, or the developer of a software application may subsidize third party relayers’ gas fees.⁵ Relayers are optional, at the discretion of each individual user for any transaction and for any protocol. Transactions can be fully accomplished and completed without relayers.
- **Nodes for Remote Procedure Calls:** Remote Procedure Call (“RPC”) is a widely used software communication protocol that one software program can use to request a service from another software program that is running on a separate computer or network.⁶ RPC is not specific to blockchains but rather relates to technology network systems more generally and has been employed for decades. In the blockchain context, RPC nodes are computers that run blockchain client software (*e.g.*, an Ethereum node). RPC nodes receive communications from wallets about users’ transactions and then transmit those communications to be included in a block that will ultimately be validated and finalized on a blockchain network.⁷

Individuals can maintain their own RPC node to communicate their own transactions. Some companies also provide RPC-node-as-a-service offerings, through which they host RPC nodes that individuals can use instead of running or hosting their own node. RPC-node-as-a-service providers generally charge fees for their services, usually paid by the developers of a DeFi application or by other third parties (*e.g.*, foundations) but typically *not* paid by users. Many RPC-node-as-a-service providers conduct some form of due

⁴ See Antier Solutions, *The Role of Blockchain Relay in Transforming Financial Systems*, Medium (Jul. 19, 2023), <https://antiersolutions.medium.com/the-role-of-blockchain-relayer-in-transforming-financial-systems-ca2776dd761f> [hereinafter *Role of Relayers*] (“Blockchain relayers are third-party services that facilitate the communication and transaction of data between different blockchain networks.”); see also Benjamin Gruenstein, Evan Norris & Daniel Barabander, *Secret Notes And Anonymous Coins: Examining FinCEN’s 2019 Guidance On Money Transmitters In The Context Of The Tornado Cash Indictment*, Int. Acad. Fin. Crime Litig., 10 (2023), <https://edit.financialcrimeliterators.org/api/assets/b9fa10a1-5e91-4473-96f6-c240f0761eb.pdf>.

⁵ See *Role of Relayers*, *supra* note 4.

⁶ John Barkley, U.S. Dep’t of Com., NISTIR 5277, *Comparing Remote Procedure Calls*, (1993), <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir5277.pdf> (“The Remote Procedure Call (RPC) concept is a simple and useful technique for developing applications where communication between cooperating processes on networked systems is required”).

⁷ Relayers can also be — and frequently are — RPC node providers, whether as individuals or as RPC-node-as-a-service providers.

diligence and/or sanctions screening on their direct customers (those that pay fees), akin to the type of due diligence and screening Amazon Web Services (“AWS”) conducts when a customer seeks to open a new server. It is important to note that AWS does not conduct the same due diligence or screening on users of a website hosted on an AWS server.

C. DeFi Use Cases

DeFi remains nascent: the oldest DeFi protocol is approximately seven years old, and DeFi did not gain meaningful traction until the summer of 2020. As of the end of August 2024,⁸ DeFi protocols held approximately \$82.68 billion of cryptoasset value locked. This is only 3.9% of the global cryptocurrency market cap and 0.08% of global GDP.⁹ Compare this to the \$17.6 trillion in commercial bank deposits accumulating over the past five decades¹⁰

DeFi applications have grown from simple exchanging, liquidity and borrowing protocols to robust software systems allowing for more complex transactions. Foundational use cases such as swapping through decentralized exchanges (“DEXs”) as well as providing and borrowing liquidity comprise almost 60% of the TVL across all DeFi protocols.¹¹ Developers have expanded the scope of DeFi to include novel applications such as investing through tokenized real world assets, a use case that has gained traction via large institutions like BlackRock and Franklin Templeton. These use cases – and numerous non-financial use cases – are chronicled in The Value Prop, an open database compiling blockchain-based applications.¹²

One of the first and now most well-established DeFi use cases are decentralized exchanges, which allow users to exchange one cryptoasset for another. In the most well-known type of DEX — the automated market maker — users create pools of cryptoasset pairs (“liquidity pools”), which then allows users to exchange one cryptoasset for another in the pool. In this way, exchanging is peer-to-protocol rather than peer-to-peer. In contrast to traditional trading venues, DEXs operate 24/7/365, run autonomously (no intermediary), and eliminate counterparty risk (peer-to-software).

DEXs have gained such popularity that they rival centralized exchanges (“CEXs”). The Uniswap protocol, the most prominent DEX holding \$4.6 billion of total cryptoasset value,¹³ has surpassed volume on Coinbase, one of the most prominent U.S.-based CEXs, in daily and quarterly

⁸ “Overview,” DeFiLlama, <https://defillama.com/> (last visited July 19, 2024) (estimating \$97.589B in total value locked in DeFi protocols).

⁹ “Total Crypto Market Cap Chart,” CoinGecko, <https://www.coingecko.com/en/global-charts> (last visited Sep. 5, 2024) (estimating 2.124T for global cryptocurrency market cap); “Global gross domestic product (GDP) at current prices from 1985 to 2029,” Statista, <https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/> (last visited Sep. 5, 2024) (estimating \$109,529.22B for global GDP in 2024).

¹⁰ “Deposits, All Commercial Banks,” FRED, <https://fred.stlouisfed.org/series/DPSACBW027SBOG> (last visited Aug. 20, 2024).

¹¹ “Dexes TVL Rankings,” DeFiLlama, <https://defillama.com/protocols/Dexes> (last visited Aug. 20, 2024) (\$17.101B TVL for DEXs); “Lending TVL Rankings,” DeFiLlama, <https://defillama.com/protocols/Lending> (last visited Aug. 20, 2024) (\$31.411B TVL for lending protocols).

¹² <https://thevalueprop.io/>.

¹³ “Uniswap,” DeFiLlama, <https://defillama.com/protocol/uniswap#information> (last visited Aug. 20, 2024).

spot volume on a number of occasions.¹⁴ Today, DEXs hold \$17.1 billion in TVL, with more than 1,300 DEX protocols deployed.¹⁵

This popularity has spurred another use case – the DEX aggregator, which are protocols and interfaces that pull data from multiple sources to allow users to access the best liquidity and price for a particular trade through a single transaction.

Liquidity protocols — which allow users to supply and borrow cryptoassets — also provide core DeFi functionality.¹⁶ Protocols such as MakerDAO, Aave and Compound, among others, allow users to supply and borrow crypto-assets in an over-collateralized manner. Like DEXs, users create liquidity pools through the supply function and can borrow against assets supplied, according to an algorithmically set collateralization ratio. Users earn fees — also through algorithmic code — where the amount earned is proportional to the amount of assets borrowed. The over-collateralization acts as a proxy for creditworthiness, ensuring that users return borrowed cryptoassets to access the greater value of their supplied cryptoassets.

Beyond exchanging and liquidity provision, users also engage in DeFi to participate in Ethereum staking and validation through a collective liquidity pool, which allows them to earn proportional validator rewards.

Developers have also created decentralized, autonomous protocols that allow for trading of crypto-derivatives (outside of the U.S.), as well as automated asset allocation and management, protocols that provide for “backstops” or “insurance” in the case of unanticipated events and even decentralized prediction markets (also outside the U.S.).

Although much of the types of activities described above harken to traditional regulated financial activity, the manner in which they occur is fundamentally different and thus, require different regulatory guardrails, as discussed in Section III below.

II. The Benefits of DeFi

DeFi offers unique benefits to users and participants in the system.

First, DeFi offers increased transparency. With open source licensing for DeFi protocols and related software, the rules of the code are open for all to see, audit and verify at all times such that users can know what will occur prior to engaging in any transaction. With protocols deployed on permissionless blockchains, all DeFi transactions are recorded publicly on blockchain ledgers in real time. The visibility of all transactions reduces information asymmetries and allows for

¹⁴ Samuel Haig, *Uniswap Spot Volume Surpassed Coinbase In 2023*, The Defiant (Aug. 25, 2024), <https://thedefiant.io/news/defi/uniswap-spot-volume-surpassed-coinbase-in-2023>.

¹⁵ “Protocol Categories,” DefiLlama, <https://defillama.com/categories> (last visited Aug. 20, 2024).

¹⁶ DeFi liquidity protocols hold approximately \$31.4 billion in TVL. See Lending TVL Rankings, *supra* note 11.

verification of financial and economic data for users and protocols alike. This transparency can also allow for enhanced or new types of risk mitigation mechanisms.

Second, DeFi will improve the operational resiliency of the financial system (assuming the risks associated with DeFi are addressed appropriately). Notwithstanding certain seismic events from centralized players in the digital asset ecosystem in the last half of 2022, DeFi protocols withstood significant volatility, functioning as anticipated whereas the centralized crypto system experienced seismic shifts that caused user harm.¹⁷ By further understanding why and how decentralized, software-based financial systems can withstand market volatility, we may be able to provide more robust underpinnings for our financial system that are not subject to failures or extreme volatility from large players in the system (*e.g.*, the 2008 financial crisis).

Third, DeFi can provide for expanded access to financial services by lowering barriers to entry, reducing prohibitive fees, and eliminating the types of discriminatory practices that can afflict the traditional financial system. While DeFi has not accomplished this feat at scale yet, given its innate characteristics of transparency and permissionlessness, it has the promise to do so. The permissionless nature allows anyone to build new applications at any time, and eliminates unknown or unaccounted for counterparty risk.

Fourth, DeFi brings increased efficiency to financial services in a number of ways:¹⁸ whereas opening bank accounts can take days or weeks, a user can download a wallet and engage in a DeFi transaction within hours; capital is aggregated within and among DeFi protocols allowing for enhanced liquidity, which allows users to engage in all manners of financial transactions at their election; DeFi protocols operate 24/7/365, allowing for instantaneous settlement and immediate access to liquidity. “Inherently international markets have access to a larger pool of liquidity, significantly reducing transaction costs for all market participants.”¹⁹

This does not mean that DeFi is without its own risks; however, the sources of those risks differ significantly from those in the traditional financial system. In fully decentralized systems, risk to users and to market integrity is borne primarily from technology risk and cyber risk, or from integration with centralized systems. By contrast, risk in the traditional financial system is borne primarily from concentration of data or information, centralized sources of failure (as witnessed with the CrowdStrike failure this past July), or errors in human or subjective judgment.

These benefits and the fundamental differences between DeFi and traditional financial services necessitates careful analysis when it comes to creating evergreen regulatory guardrails.

¹⁷ See *e.g.*, Gino Matos, *DeFi protocols show resilience despite this week's macro crash: IntoTheBlock*, Crypto Briefing (Aug. 9, 2024) <https://cryptobriefing.com/defi-market-resilience-tested/>.

¹⁸ Hilary Schmidt, *DeFi: A Cutting Edge Technology That Continues to Upend Traditional Financial Models*, Int'l Banker (Apr. 22, 2024), <https://internationalbanker.com/finance/defi-a-cutting-edge-technology-that-continues-to-upend-traditional-finance-models/>.

¹⁹ Marvin Ammori, *Decentralized Finance: What It Is, Why It Matters* (Jun. 15, 2021) <https://a16zcrypto.com/posts/article/what-is-decentralized-finance/>.

III. Global Regulatory Approaches to DeFi

Global regulators have recognized the challenge in considering regulation of DeFi: the U.K.’s HM Treasury stated that “DeFi presents complex and unique challenges for policy makers and regulators”.²⁰ This is consistent with the statement from the International Monetary Fund (“IMF”) that “DeFi calls for creative risk mitigation” in any regulatory response,²¹ and the Bank for International Settlements (“BIS”) stating that “traditional regulatory approaches and tools may not be effective, implementable or enforceable for DeFi.”²²

Traditional laws attach to intermediaries: most financial laws in the U.S. are directed to “persons,” which are defined as entities or natural persons who act affirmatively or must be regulated to do so in a way that brings integrity, fairness and transparency to the system. These current laws are not amenable to intermediary-less systems like DeFi. Global regulators have recognized the need for regulatory equivalence rather than imposing a “same risk, same regulation” framework.

To that end, DeFi has been excluded from any crypto-specific regulation to date. Recital 22 in the EU’s Markets in Cryptoasset regulation (“MiCA”) excludes financial services performed in a “fully decentralized manner without any intermediary,” and the UK’s HM Treasury stated that it would consider any regulation of DeFi at a much latter stage of any regulatory process. Japan — which enacted strict laws relating to crypto-asset exchanges and stablecoins — has not imposed any regulation of DeFi nor have Singapore, Hong Kong, or the UAE, all of which have licensing regimes relating to centralized cryptoasset activity.

The most critical challenge in regulating DeFi is to ensure that any regulation does *not* force centralization into the system where it otherwise does not exist, as certain global regulators have suggested. There are ways to ensure the regulatory goals of protecting users, enhancing market integrity and combating illicit finance in DeFi systems that differ from regulation of the traditional financial system today.

Framing DeFi as purely financial services overlooks the realities of DeFi and critical tools that the government already has in ensuring the safety and security of the technological infrastructure underlying our current financial system. Grounding DeFi in its technological reality as a communications protocol, opens up new ways of thinking about achieving policy goals such as by classifying DeFi as “critical infrastructure,”²³ a concept that dates back to 1998 and that would put DeFi under the oversight of Cybersecurity and Infrastructure Security Agency, a standalone federal agency that is part of the Department of Homeland Security, which ensures that

²⁰ HM Treasury, *Future financial services regulatory regime for cryptoassets* (2023) <https://www.gov.uk/government/consultations/future-financial-services-regulatory-regime-for-cryptoassets>, at 66.

²¹ IMF, *Elements of Effective Policies for Cryptoassets*, Policy Paper (Feb. 2023), at ¶ 59.

²² Bank for Int’l Settlements, *Crypto, tokens and DeFi: navigating the regulatory Landscape* (2023), <https://www.bis.org/lsi/publ/insights49.pdf>, at 36.

²³ See Genuine DeFi as Critical Infrastructure, *supra* note 1.

the regulators are able to bring about appropriate rules and regulations in compliance with best practices for the protection of cyber systems. This is the topic of a recent paper I co-authored that describes when, why and how different parts of DeFi systems should be viewed as critical infrastructure and *not* financial services — and how doing so can achieve favorable policies that protect users.

IV. Conclusion

I appreciate the Committee's continued interest in the digital asset space generally and the efforts to understand this technology specifically. I look forward to your questions.

Chairman HILL. Thank you for your testimony.

Ms. Tuminelli, you are recognized for 5 minutes to give your oral remarks.

**STATEMENT OF AMANDA TUMINELLI, CHIEF LEGAL OFFICER,
DEFI EDUCATION FUND**

Ms. TUMINELLI. Thank you to the subcommittee for holding this hearing.

My name is Amanda Tuminelli, and I am the chief legal officer at the DeFi Education Fund, a nonprofit, nonpartisan group that educates lawmakers and the public about decentralized finance and advocates for sound DeFi policy.

We believe that DeFi is the path to a more equitable and more efficient financial system, one in which people have access to finance regardless of where in the world they live and regardless of the merits of their application.

I will leave you with two points today. First, DeFi is different from and an improvement upon traditional finance because it does not rely on intermediaries. Second, the existing approach of demanding that DeFi look like, function like, or be treated like traditional finance has not and will not work.

So what is DeFi, and how is it different? As others have said today, DeFi enables peer-to-peer transactions in which user self-custody their assets, just like with cash. Using DeFi, a person can trade assets, make and take loans, or earn interest.

It is an improvement on the current system in a number of ways. For example, traditional finance (TradFi) relies on intermediaries that often serve as gatekeepers to finance. Traditional financial institutions like big banks can and do deny access to the system for discriminatory reasons or no reasons, but DeFi has open access. Anyone with an internet connection has access to a DeFi protocol, and that is the epitome of financial inclusion.

TradFi is expensive to access and slow to use. Even the simple act of sending money usually requires paying fees to third-parties and waiting days for a transaction to be approved or processed, but using DeFi, I can send money or execute far more complicated transactions anywhere in the world, 24/7, with nearly instant settlement.

As one last example, DeFi is better because it is self-custodial. As this committee knows, when TradFi services fail, customers lose access to their assets but, in DeFi, there is no fear of losing access to your money in a bank crisis because assets in your self-hosted wallet are always available to you.

So that brings me to my second point. The existing approach of trying to apply rules for TradFi to DeFi will not work. The traditional financial system requires intermediaries to function. Brokers affect stock trades and clearinghouses settle transactions, and that means that we need to trust intermediaries to do their jobs reliably and honestly and the existing rules evolve to prevent the abuse of our trust.

DeFi does not use intermediaries. If I want to swap two digital assets using a DeFi protocol, there is no broker, and there is no clearinghouse. DeFi's existence, the very reason that this technology was developed was to eliminate the need to rely on inter-

mediaries and empower people to transacting directly with their peers.

Existing law assumes that there is some identifiable entity that can take possession of my funds, collect information about my transaction, and even block a trade, but that entity does not exist in DeFi.

The untenable position between the law as it stands and the reality of DeFi technology has led to an increasing amount of regulatory uncertainty. Seasoned lawyers with decades of regulatory experience cannot give their clients advice with certainty about whether their projects comply with the law.

That is why judges in multiple district courts across this country have called on Congress to make new rules regarding digital assets, and this Chamber has supported bipartisan efforts and signaled that the status quo is not working for DeFi and digital assets.

The existing approach of trying and failing to apply existing rules to this technology has led to so much hostility to innovation that American jobs and businesses have been heading overseas but the vast majority of DeFi developers are smart, creative people with a vision of building a better financial system, and they want to do that legally. So the U.S. can be at the forefront of that and create a clear path to building here, or we can let other countries pass us on the path toward our digital financial future.

If you care about national security and you care about economic development, then you want this industry here on U.S. soil.

We appreciate the efforts of Members of Congress, such as those on this committee, who have engaged with us on the reality of the technology and engaged with us on a path forward.

Thank you.

[The prepared statement of Ms. Tuminelli follows:]



WRITTEN TESTIMONY OF
Amanda Tuminelli
Chief Legal Officer
DeFi Education Fund

BEFORE THE
United States House of Representatives
Committee on Financial Services
Subcommittee on Digital Assets, Financial Technology and Inclusion

IN A HEARING ENTITLED
Decoding DeFi: Breaking Down the Future of Decentralized Finance

September 10, 2024

Chairman Hill, Ranking Member Lynch, and Members of the Subcommittee:

Thank you for having me before the Subcommittee to speak about the importance and value of decentralized finance (DeFi). My name is Amanda Tuminelli and I am the Chief Legal Officer at the DeFi Education Fund, a nonpartisan nonprofit advocacy group that educates lawmakers and the public about sound policy for DeFi.

I am often asked why I left my job working as a litigator in private practice to join the digital asset industry. The answer is simple: the future of finance is on blockchains. The best financial system is one in which individual people are able to access finance regardless of where in the world they sit or the subjective merits of an individual's application. DeFi is the path to that more secure, efficient, and transparent financial system.

I am honored to have the opportunity to discuss a topic that I am passionate about: why policymaking pertaining to digital assets must account for the realities of DeFi technology. The exponentially increasing amount of regulatory enforcement actions in recent years—which pay no mind to the details of the technology they presume to center on—have not accomplished any policy objectives or resulted in any kind of clarity for the industry. There has also been a growing number of criminal actions against software developers that evidence a lack of understanding of the technology at issue. The net result of the current legal landscape for digital assets and DeFi has driven American developers and businesses to relocate to friendlier jurisdictions. But it is not too late. The U.S. can continue its long tradition of being a leader in innovation by taking the time to learn about new technology and create rules that make sense with its functionality.

The message I hope to leave you with is this: DeFi technology is vastly different from anything in existence in traditional finance and the existing rules have not and will not work with DeFi. We are grateful that the Subcommittee is taking the time to learn about DeFi and we hope to continue to work together in the future.

1. Overview of DeFi

DeFi is an umbrella term generally used to describe blockchain-based software protocols that allow people to engage in economic activities online on a peer-to-peer basis and allow people to self-custody their assets (See Appendix A for detailed examples of DeFi transactions).¹ To do so, DeFi builds on the innovations of public blockchains, which are the software protocols that first enabled people to engage in peer-to-peer value transfer over the internet.² Because there is no need for a central server in a peer-to-peer network, no single entity has control over

¹ DeFi is a nascent technology, having existed for only five years, and is rapidly evolving.

² Peter Van Valkenburgh, *Open Matters: Why Permissionless Blockchains Are Essential to the Future of the Internet*, Coin Center (Dec. 2016), <https://www.coincenter.org/open-matters-why-permissionless-blockchains-are-essential-to-the-future-of-the-internet>.

the data stored on a public blockchain. Instead, all computers (nodes) participating in a peer-to-peer blockchain network (1) hold a record of the history of data stored on the network; and (2) reach consensus as to the validity of that data. No single entity participating in the network has control over, or can alter, the data record.

○ **What is a “wallet” and how is it related to self-custody?**

Users interact with public blockchains using a “wallet.”³ Crypto wallets are devices or software applications that store DeFi users’ private keys and generate a digital signature when required. A “private key” is nothing more than a randomly selected string of numbers known only to an individual user. A “public key” is a cryptographically-generated string of letters and numbers associated with a private key, but it is public-facing. People colloquially refer to a shorter, user-friendly derivative of the public key as the wallet’s “address.” To send tokens or interact with a DeFi protocol from a specific address, DeFi users produce a digital signature, which cryptographically proves that they know the private key associated with a wallet without revealing the key to anyone else.⁴

Wallets that are “unhosted” by a third-party enable individuals to directly control and custody their own digital assets without the involvement of any third-party, which is often referred to as “self-custody.” A custodial arrangement, on the other hand, refers to situations in which a person uses the services of a third-party to store the person’s digital assets or the keys to their wallet on their behalf. Using a basic analogy, cash in a person’s bi-fold wallet is “self-custodied” while a person’s cash held by a bank on their behalf is “custodied” by a

³ Broadly, there are two types of crypto wallets: hardware wallets and software wallets. A software wallet stores users’ private keys in a software file on a computer or mobile device, such as in an app on your phone or connected to your web browser. A hardware wallet stores users’ private keys in a secure element isolated from the internet and users’ personal devices, such as those created by Ledger or Trezor. Users unlock their hardware wallets by entering a password or pin code directly on the device, and then connect it to their computer, typically via a USB connection or Bluetooth. While there are numerous software programs that assist a user in creating a wallet and executing transactions associated with a wallet, no third party is needed to create or use a wallet. Digital assets are not actually stored “in” a wallet because they are simply digital representations of ownership on a ledger. In reality, only the user’s keys that grant access to their assets make up a wallet.

⁴ Asymmetric cryptography is an encrypted method of communication using two keys: a public and a private key. The public key is used to encrypt messages (transactions), while the private key is used to decrypt them; both of which belong to the user receiving the message and are mathematically related to each other. For example: Alice sends Bob a message using his public key to encrypt it so Bob can be the only one to open the message. Bob then uses his private key to decrypt the message. Asymmetric cryptography is also used in authenticating the sender’s information by producing a digital signature with the sender’s private key, which is then verified by the recipient using the sender’s public key, as well as the network when validating the transaction. A private key mathematically generates a public key, which then mathematically generates a blockchain address; a public key is used to encrypt and a blockchain address is an identifier for sending and receiving.

third-party. In both instances, the cash belongs to the person; the differentiation lies in whether the owner of the cash has free access to and independent control over it.⁵

○ DeFi vs. CeFi

Centralized finance (CeFi) typically refers to digital asset businesses that are run by an identifiable, “centralized” individual or group of individuals that maintain control over a blockchain-based software system and the digital assets of its users. An important aspect of this is that the centralized business custodies a person’s digital assets or their keys to access their digital assets. Because of the unique position that such a centralized business is in, they are able to collect personally identifiable customer information (Know Your Customer or “KYC”) as well as information about each transaction that occurs in their system. CeFi exchanges are often the only way to exchange digital assets for fiat currency, which is why they are referred to as “on and off ramps” to digital assets.

CeFi, in turn, can be differentiated from traditional finance (TradFi) by the fact that CeFi businesses provide their customers with digital asset-related services while TradFi refers to businesses that provide their customers with traditional financial services. While DeFi can be distinguished from TradFi and CeFi in several ways, it bears emphasizing that when using DeFi protocols, a person retains and exercises total possession and control over their assets. In DeFi, there is no third-party that stores a person’s digital assets or controls their means of accessing their digital assets.

For an easy-to-follow chart outlining the differences between DeFi, CeFi, and TradFi, see Appendix B.

○ DeFi Front Ends

When seeking to conduct a DeFi transaction, the vast majority of DeFi users interact with a “front end,” which is an interface that makes it easier to interact with the relevant smart contracts. Smart contracts are simply software programs that run on a blockchain and automatically execute a function when certain conditions are met. Smart contracts are analogous to a vending machine that automatically releases a bag of chips on the condition that it receives \$2: the user relies on the machine to operate according to the “code” in place and

⁵ FinCEN, *Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019) (hereinafter, “FinCEN 2019 Guidance”), <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>; see also Barabander et al., *Secret Notes And Anonymous Coins: Examining FinCEN’s 2019 Guidance On Money Transmitters In The Context Of The Tornado Cash Indictment*, The International Academy of Financial Crime Litigators (Sep. 2023), <https://www.cravath.com/a/web/qyCBWVBLEMsqxPHtd9ykoc/87ntut/the-international-academy-of-financial-crime-litigators.pdf>.

dispense an item once the user has inserted \$2. Smart contracts deployed on a blockchain are transparent and immutable, and anyone can deploy a smart contract to a blockchain.⁶

Front ends are composed not only of visual elements (i.e., a website) but also of the code that powers interactive features like forms and buttons. A DeFi front end typically serves two roles: as a browser and as a data object generator. In its browser role, a front end shows the user information about the state of the blockchain relating to a set of DeFi smart contracts and provides an intuitive visual interface for users to indicate what actions they would like to perform (a user's "input") through the smart contracts. In its data object generator role, a front end "translates" a user's input into a data object, i.e., a set of data with the necessary information to submit a transaction for inclusion on-chain. Typically, DeFi front ends with data object generators include a "connect wallet" button, which, when selected, establishes a secure connection between the front end and the user's crypto wallet. The data object generator uses that connection to send the data object to the user's wallet, which a user may or may not cryptographically pair with their private key and then submit their transaction through their wallet for inclusion on-chain.

Crucially, a front end solely generates a data object based on people's interactions with the front end, and therefore, users have total discretion over whether to complete their transaction. Any deployment of a data object to the blockchain is done by the user through the user's wallet and without a front end's involvement whatsoever. Front ends only generate and display information in response to a user's actions, providing an informational service like Google, Yahoo! Finance, or Wikipedia.

2. Value and Benefits of DeFi

DeFi technology was developed in response to the many challenges and risks inherent in the structure of intermediated financial services, be it CeFi or TradFi — including limited and unequal access, slow settlement cycles, inefficient price discovery, liquidity challenges, a lack of assurance around underlying assets, opaqueness, broker risk, and uptime issues.

TradFi intermediaries establish trust between transacting counterparties—the knowledge that a transaction will occur as both parties expect—by acting as a middleman between them. For example, making a payment with a credit card involves a minimum of four separate financial intermediaries in addition to the two parties to a transaction. However, instead of relying on specialized intermediaries to establish trust between counterparties, blockchains establish trust via rules-based, encoded software protocols. These novel features enable people to use public blockchains to engage in digital transactions and economic activities without reliance on third-party intermediaries. Users of DeFi protocols have open, transparent

⁶ While smart contracts are immutable once they are deployed, users may create intermediary or proxy contracts that redirect calls and transactions to a modified contract as a way of updating an earlier contract.

access to systems that allow people to conduct various types of financial activities without requiring specialized intermediaries or institutions.

Moreover, by allowing people to transact directly with their peer utilizing open-source software, all while maintaining custody over their own funds, DeFi protocols provide the following benefits to consumers:⁷

- **Increased transparency and integrity:** DeFi protocols increase transparency about the mechanics of market infrastructures and associated fees by using open-source software, meaning the code for each protocol is transparent and auditable.⁸ Open-source software provides “security through transparency” rather than “security through obscurity.” The latter is the norm for proprietary and opaque TradFi systems and has been firmly rejected by cybersecurity experts.⁹ Transactions using DeFi protocols are also recorded on immutable public blockchains, the records of which live forever and cannot be manipulated or amended, offering greater certainty to users.
- **Equitable access and inclusion:** DeFi protocols are open and available to anyone in the world with an internet connection, significantly expanding global access to financial services.¹⁰ That access empowers people from all backgrounds and in varying circumstances to use financial services without having to go through

⁷ See generally Caitlin Ostroff & Jared Malsin, *Turks Pile Into Bitcoin and Tether to Escape Plunging Lira*, Wall St. J. (Jan. 12, 2022), <https://www.wsj.com/articles/turks-pile-into-bitcoin-and-tether-to-escape-plunging-lira-11641982077>; Roger Huang, *Dissidents Are Turning to Cryptocurrency As Protests Mount Around The World*, Forbes (Oct. 19, 2020) <https://www.forbes.com/sites/rogerhuang/2020/10/19/dissidents-are-turning-to-cryptocurrency-as-protests-mount-around-the-world/>; Timour Azhari, *Young Lebanese driving crypto 'revolution' after banks go bust*, Reuters (Sept. 20, 2021), <https://www.reuters.com/article/lebanon-crypto-currency-youth/feature-young-lebanese-driving-crypto-revolution-after-banks-go-bust-idUSL8N2QH1MW/>; Carlos Hernández, *Bitcoin Has Saved My Family*, N.Y. Times (Feb. 23, 2019), <https://www.nytimes.com/2019/02/23/opinion/sunday/venezuela-bitcoin-inflation-cryptocurrencies.html>; Jillian Deutsch & Aaron Eglitis, *Putin's Crackdown Pushes Independent Russian Media Into Crypto*, Bloomberg (May 10, 2022), <https://www.bloomberg.com/news/articles/2022-05-10/putin-s-crackdown-pushes-independent-russian-media-into-crypto>; Cristina Criddle & Joshua Oliver, *How Ukraine Embraced Cryptocurrencies in Response to War*, Financial Times (Mar. 19, 2022), <https://www.ft.com/content/f3778d00-4c9b-40bb-b91c-84b60dd09698>.

⁸ *Decentralized Finance: Innovations and Challenges*, Bank of Canada (Oct. 2023), <https://www.bankofcanada.ca/2023/10/staff-analytical-note-2023-15/>.

⁹ Okta, *Security Through Obscurity: History, Criticism & Risks* (Aug. 30, 2024), <https://www.okta.com/identity-101/security-through-obscurity/>.

¹⁰ See, e.g., Bitange Ndumo, *The role of cryptocurrencies in sub-Saharan Africa*, Brookings Inst. (Mar. 16, 2022), <https://www.brookings.edu/blog/africa-in-focus/2022/03/16/the-role-of-cryptocurrencies-in-sub-saharan-africa> (describing how cryptocurrency platforms can “help level the economic playing field and expand finance options to underserved customer markets”).

intermediaries, who often gatekeep participation through unfair or discriminatory treatment, absolute prohibitions, or excessive pricing.¹¹ It also means that people have access to finance even in challenging conditions, such as in countries where “local currencies are collapsing, broken, or cut off from the outside world,” “legacy financial systems falter[.],” or “the horrors of monetary colonialism, misogynist financial policy, frozen bank accounts, exploitative remittance companies, and an inability to connect to the global economy” are a constant reality.¹²

- **24/7/365 liquidity:** Users can access and use DeFi protocols at all times of the day without worrying about the market closing at the end of each day. Among other things, this eliminates the risk of capital dislocations due to illiquid aftermarket trading in traditional systems.¹³
- **Lower costs and faster settlement:** DeFi protocols reduce friction and transaction costs for the creation, distribution, trading, and settlement of financial assets with faster settlement times for users.¹⁴ While DeFi users may pay certain fees, such as gas fees, DeFi users do not additionally need to compensate other intermediaries such as executing brokers, prime brokers, clearing brokers, or custodians. On balance, this typically leads to DeFi protocols being available to users at lower costs than centralized exchanges and TradFi institutions.
- **Greater individual control:** The absence of intermediaries and self-custodial nature of DeFi protocols provides individual users greater control over their assets and certainty that the financial transactions they expect to happen will happen. Users do not have to trust a third-party to safely store and transact in

¹¹ *Letter in Support of Responsible Crypto Policy*, Open Letter to 117th Congressional Leadership (June 2022), <https://www.financialinclusion.tech/> (“Bitcoin provides financial inclusion and empowerment because it is open and permissionless. Anyone on earth can use it. Bitcoin and stablecoins offer unparalleled access to the global economy for people in countries like Nigeria, Turkey, or Argentina, where local currencies are collapsing, broken, or cut off from the outside world.”); *see also* Huang, *supra*.

¹² *See Letter in Support of Responsible Crypto Policy*, *supra*; *see also* Azhari, *supra*; Hernández, *supra*.

¹³ *What is a Spot Bitcoin ETP?*, Fidelity (Jan. 10, 2024) (“Both long-term and short-term investors should note that spot bitcoin ETPs can only be bought or sold during traditional market hours. Bitcoin, however, trades 24/7.”).

¹⁴ As additional blockchains are created and new technology, such as scaling solutions, are developed, costs for transacting using DeFi protocols likely will continue to decrease. *See* Austin Adams, Mary-Catherine Lader, Gordon Liao, David Puth, & Xin Wan, *On-chain Foreign Exchange and Cross-border Payments*, UNISWAP LABS (Jan. 18, 2023), <https://uniswap.org/OnchainFX.pdf>.

digital assets. Additionally, in some instances, market participants can directly develop community governance standards.

- **Eliminate “broker risk”:** DeFi protocols have no employees to supervise, no financial risk for users from broker activity or custody, and no interaction between a broker and customers that could result in unlawful sales practices or other unfair and discriminatory dealing.¹⁵
- **Competition:** Users can easily move their assets from one DEX protocol to another at any time without significant friction on the same blockchain, which promotes competition across protocols. Sharing liquidity across traditional exchanges is near-impossible, resulting in a lack of competition.¹⁶ In addition, open-source software systems attract a vibrant ecosystem of developers focused on building better products rather than reinventing the same tools and processes dozens of times over.

3. Traditional Regulatory Approaches Will Not Work for DeFi

Because DeFi protocols are software programs whose functionality is totally different from CeFi and TradFi businesses (as discussed above and in Appendix B), public policy and regulatory approaches to DeFi should be different as well. Attempting to “shoehorn” DeFi protocols into existing public policy frameworks designed to address the risks and opportunities of TradFi and CeFi would be akin to requiring jetliners to abide by the same standards and requirements as automobiles. While both car and airline manufacturers produce vehicles for the same reason — to provide transportation — cars and airlines facilitate transportation in distinct ways. Fortunately, the requirements applicable to car manufacturers and airline manufacturers are responsive to the functional differences through which the vehicles transport people. If they were not, airplanes would never get off the ground. So too in the context of DeFi protocols.

The United States’ dynamic market economy produces all manner of novel solutions to old problems which require dynamic responses to accomplish long-standing public policy objectives.¹⁷ The United States’ economic preeminence has been built, in part, on this

¹⁵ See Azhari, *supra* (discussing Lebanon’s economic crisis and the Lebanese flight to crypto “[t]he country’s economic crisis, likely among the world’s worst since the 1850s . . . is widely blamed on systemic corruption and decades of mismanagement by a closely-knit ruling elite.”) (“[M]any entering the cryptocurrency trade in Lebanon were driven by an ideological opposition to ‘a banking system that [] no-one trusts to store their money in.’”).

¹⁶ *Around the Block #9: The Dawn of the DeFi Protocol Wars*, Coinbase <https://www.coinbase.com/learn/market-updates/around-the-block-issue-9> (last visited Sept. 5, 2024).

¹⁷ See Gary Gensler, Chair, Sec. & Exch. Comm’n, *Prepared Remarks at the Exchequer Club of Washington, D.C.: Dynamic Regulation for a Dynamic Society* (Jan. 19, 2022) (quoting Sec. & Exch. Comm’n, Report of

“flywheel” of innovation in markets and innovation in public policy. This approach has not only benefited U.S. investors and businesses, but also “contributed to America’s geopolitical standing around the globe.”¹⁸ We must not abandon it.

Failing to adjust public policy approaches in response to new technologies threatens the preeminence of the United States’ economy and establishes by law a single acceptable way of solving problems. Because regulatory frameworks cannot foresee innovations, failing to adapt them to new technology will lead to stasis, to the detriment of the United States.

DeFi protocols join the United States’ long history of innovative approaches to conducting well-established economic and financial activities. DeFi software protocols do not change the reasons why people and businesses seek financial services — to generate returns, price and hedge risks, make payments, etc. — but they have fundamentally changed how people and businesses access and conduct financial activities. According to the International Organization of Securities Commissions (IOSCO), DeFi protocols’ “peer-to-peer nature and resulting ability to create alternatives to traditional and centralized financial market infrastructures, products or services.”¹⁹ They represent “a paradigmatic shift in financial services provisioning and promises to be one of the most disruptive applications of blockchain-fuelled decentralization” and are “a novel phenomenon” the EU Blockchain Observatory and Forum

Special Study of Securities Markets of the Securities and Exchange Commission, Part 1, H.R. Doc. No. 95, pt. 1, at IV (1963)), https://www.sec.gov/news/speech/gensler-dynamic-regulation-20220119#_ftn2.

¹⁸ *Id.*

¹⁹ International Organization Of Securities Commissions, *IOSCO Decentralized Finance Report*, 2, OR01/2022 (2022), <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf>; see also International Monetary Fund, Global Financial Stability Report, *Shockwaves from the War in Ukraine Test the Financial System’s Resilience*, 73 (Apr. 2022), <https://www.imf.org/en/Publications/GFSR/Issues/2022/04/19/global-financial-stability-report-april-2022> (“Decentralized finance refers to financial applications—called “smart contracts”—processed by computer code on blockchains, with limited or no involvement of centralized intermediaries.”); European Commission, Directorate-General for Financial Stability, Financial Services and Capital Markets Union, *European Financial Stability and Integration Review 2022*, 43 (Apr. 7, 2022), https://ec.europa.eu/info/sites/default/files/european-financial-stability-and-integration-review-2022_en.pdf (“[D]ecentralised finance. . . is a newly emerging form of autonomous financial intermediation in a decentralised digital environment powered by software — ‘smart contracts’ on public blockchains.”); Organization for Economic Cooperation and Development, *Why Decentralised Finance Matters and the Policy Implications*, 15 (2022), <https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf> (“Decentralised Finance or ‘DeFi’ seeks to provide traditional financial services involving crypto-assets (i.e. mimicking the ‘CeFi’ or centralized finance market) in an open, decentralized, permissionless way.”).

concludes.²⁰ And they raise legal questions of “first impression,” a New York District Court found.²¹

○ **Example: Why CeFi Rules Related to Exchanges Don’t Work for DeFi**

Contrasting the discrete functionalities of a CeFi exchange with a DeFi exchange protocol, for example, evidences the need to think about DeFi differently. It makes sense to require custodial and centralized exchanges to comply with a regulatory regime that protects against misappropriation, negligence, errors, bankruptcy, or other failures by the centralized facility because those risks arise out of how CeFi businesses operate. However, this type of regulatory framework does not make sense in the context of DeFi protocols because those risks are not relevant to a system without a centralized market operator. It is not a matter of regulatory arbitrage – CeFi and DeFi present two very different models with different advantages and risk exposures. For example:

- **Transparency:** In a CeFi model, only the market operator has full transparency into the operation of the trading protocol, including any matching algorithm, order types, order handling, market data, or other proprietary features. With a DeFi protocol, the code governing how it operates is open-source and transactions take place on a public blockchain, which gives both regulators and market participants the ability to audit the market in real-time. No person or group of persons known to each other and acting in concert has unique visibility into trading activity or the ability to take action in connection with such activity.
- **Conflicts:** In a CeFi model, the market operator not only has access to confidential trading information but also may face conflicts of interest in the handling of that information (e.g., sharing with affiliates) or more generally through engaging in proprietary trading and other activities that might present conflicts with operation of the market. On the other hand, a DeFi protocol is neutral and functions in the same way no matter who is using it; no users have a “leg up” solely due to affiliation with the market operator.
- **Market Access:** In a CeFi model, the market operator serves as a gatekeeper and decides who can access the market and the terms for such access. DeFi protocols, in contrast, are freely accessible to anyone who can connect to the protocol.

²⁰ EU Blockchain Observatory and Forum, *Decentralised Finance (DeFi)*, 38 (2022), https://www.eublockchainforum.eu/sites/default/files/reports/DeFi%20Report%20EUBOF%20-%20Final_0.pdf.

²¹ *Risley v. Universal Navigation Inc. et al*, No. 1:2022-cv-02780, ECF No. 90 (S.D.N.Y. 2023), <https://storage.courtlistener.com/recap/gov.uscourts.nysd.577791/gov.uscourts.nysd.577791.90.0.pdf>.

- **Custody:** In a CeFi model, the market operator or another third-party holds users' assets, for purposes of safekeeping, affecting settlements and, if applicable, for margin or collateral. Assets are typically held by the centralized market operator (or a related clearing/settlement entity) in an omnibus account in its own name, directly or with a third-party. When using DeFi protocols, on the other hand, users possess and control their own assets via their private keys, eliminating the risk that users will lose funds due to custodial mismanagement or other system failures.

Regulation for CeFi businesses is premised on the existence of a central operator that has responsibility for operation of the system, oversight, conduct of participants, and government reporting. They are also responsive to a central risk exposure for a CeFi exchange's customers: the centralized exchange itself. This example evidences how public policy approaches designed with CeFi and TradFi operations in mind cannot and should not be applied to people's use of DeFi protocols to engage in economic activities with their own assets. It would be impossible for a DeFi protocol to, for example, comply with a regulatory requirement to custody users' assets with third-party financial institutions and thus eliminate or render unclear how to develop DeFi protocols compliantly in the United States. Nor would doing so provide the same benefits to market participants, as users of a decentralized exchange do not bear any risk arising from a centralized market operator.

4. Legal and Regulatory Uncertainty for Developers Is Undermining U.S. Competitiveness and Innovation

Since 2018, the U.S. has lost 14% of digital asset developer share, dropping from 40% to 26% by the end of 2023.²² The cause of this systemic collapse is no mystery: Unfortunately, to date, U.S. regulatory authorities have created legal uncertainty for software developers and other industry participants seeking to build DeFi innovations in the U.S., in part by attempting to shoehorn DeFi protocols into existing regulatory regimes designed for TradFi. For example:

- **"Am I a money transmitter?"**²³

FinCEN, the federal agency responsible for implementing and enforcing the Bank Secrecy Act (BSA), has stated that persons or businesses that "accept" and "transmit" digital assets on behalf of a third-party are money transmitters and therefore required to comply with anti-money laundering and countering the financing of terrorism (AML/CFT) obligations.²⁴ As

²² Electric Capital Partners, LLC, *Geography of Crypto Developers: 2023 Developer Report*, Developer Report (2023), <https://www.developerreport.com/developer-report-geography>.

²³ Peter Van Valkenburgh, *DOJ's New Stance on Crypto Wallets Is a Threat to Liberty and the Rule of Law*, Coin Center (Apr. 29, 2024), <https://www.coincenter.org/dojs-new-stance-on-crypto-wallets-is-a-threat-to-liberty-and-the-rule-of-law>.

²⁴ FinCEN 2019 Guidance, *supra* note 5.

relevant here, FinCEN has clarified that “the production and distribution of software, in and of itself, does not constitute acceptance and transmission of value, even if the purpose of the software is to facilitate the sale of virtual currency.”²⁵ And importantly, in its 2019 Guidance, FinCEN explained that “*partial control* over virtual currency was insufficient to classify wallet developers as money transmitters because: ‘the person participating in the transaction to provide additional validation at the request of the owner *does not have total independent control* over the value.’”²⁶ U.S. software developers working on digital assets and DeFi-related software have relied on FinCEN’s uniquely-clear delineation of when one is engaged in a regulated activity and therefore obligated to comply with BSA obligations.

Yet, in April of 2024, the Department of Justice (DOJ) took the position that FinCEN’s 2019 Guidance and its concept of money transmission under the BSA—the legislative framework FinCEN is charged with implementing—could not be relied upon. In other words, via criminal charges against developer Roman Storm, the DOJ staked out *for the first time* a position contradictory to FinCEN’s as to what constitutes money transmission. For example, in its opposition to Roman Storm’s motion to dismiss the Indictment against him, the DOJ stated that Section 1960, the section of the criminal code that makes it illegal to operate an unlicensed money transmitting business, “does not require the business to have control of the funds.”²⁷ In other words, the DOJ publicly alleged—*for the first time, in the midst of an ongoing criminal case*—that the bar for the level of control that constitutes “money transmission” is far lower than that expressed years prior in 2019 FinCEN Guidance.

So when is a U.S. developer engaging in money transmission and therefore obligated to comply with BSA obligations under the threat of criminal sanctions? It depends on which agency within the Federal government one asks at any given time.

○ **“Am I staying out of the United States?”**

Given the lack of a path to compliance under many regulatory frameworks in the U.S. for businesses and developers working in digital assets and DeFi, many seek to avoid offering products and services to U.S. persons altogether. Despite never describing what a business must do to sufficiently block U.S. persons to avoid liability under U.S. laws, regulatory agencies have brought enforcement actions against businesses for insufficiently blocking access to U.S. persons. For instance, the Commodity Futures Trading Commission (CFTC) clearly explains what

²⁵ Fin. Crimes Enf’t Network, *Application of FinCEN’s Regulations to Virtual Currency Software Development and Certain Investment Activity* (Jan. 30, 2014), <https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/application-fincens-regulations-virtual>.

²⁶ 2019 FinCEN Guidance (emphasis added).

²⁷ Br. in Opp, *U.S. v. Storm*, 23 Cr. 430, ECF No. 53 (S.D.N.Y. 2024) <https://storage.courtlistener.com/recap/gov.uscourts.nysd.604938/gov.uscourts.nysd.604938.53.0.pdf>.

blocking steps are insufficient while leaving ambiguous what steps would be sufficient. In a settlement with Opyn, the CFTC found that Opyn “took certain steps to exclude U.S. persons from accessing the Opyn Protocol, such as blocking users with U.S. internet protocol addresses, [but] those steps were not sufficient to actually block U.S. users.”²⁸ Opyn later “promptly took remedial action,” including taking “additional steps to block U.S. users.”²⁹ Those additional steps are undefined in the settlement order, and therefore, cannot serve as any form of guidance to the industry.

○ **“Am I a National Securities Exchange?”**

In January 2022, the SEC proposed a rule that would expand the regulatory definition of an “exchange” to include those persons that “make[] available” methods for trade execution or communications—rather than just those which “use” such systems.³⁰ The original proposal failed to mention digital assets at all, but a lengthy reopening of the rule discusses DeFi protocols specifically. The SEC explains that the proposed change was “intended to make clear that, in the event that a party other than the organization, association, or group of persons performs a function of the exchange, the function performed by that party would still be captured.”³¹ This flies in the face of the words of the statutory definition, which states that an “exchange” is “any organization, association, or group of persons . . . which constitutes, maintains, or provides a market place or facilities” of an exchange.³²

Altogether, the SEC’s proposed amended definition of “exchange” intentionally muddies whether developers of DeFi protocols constitute national securities exchanges under current law and regulation. To do so, the proposal vastly expands the agency’s statutory authority in an effort to ensure the SEC can selectively target any person “making available” “communication protocol systems” that allow people to express non-firm interest in trading a security, an intentionally boundless definition.

²⁸ Commodity Futures Trading Comm’n, *CFTC Issues Orders Against Operators of Three DeFi Protocols for Offering Illegal Digital Asset Derivatives Trading* (Sept. 7, 2023), <https://www.cftc.gov/PressRoom/PressReleases/8774-23>.

²⁹ *Id.*

³⁰ Amendments Regarding the Definition of Exchange and Alternative Trading Systems (ATs) That Trade U.S. Treasury and Agency Securities, 87 Fed. Reg. 15,496 (proposed Mar. 18, 2022) (to be codified at 17 C.F.R. pts. 240, 242, 249), <https://www.federalregister.gov/documents/2022/03/18/2022-01975/amendments-regarding-the-definition-of-exchange-and-alternative-trading-systems-atss-that-trade-us>.

³¹ Sec. & Exch. Comm’n, *Reopening of Comment Period for Proposed Rule on Safeguarding Advisory Client Assets* (Mar. 2023), <https://www.sec.gov/comments/s7-02-22/s70222-205079-412142.pdf>.

³² 15 U.S.C. § 78c (a)(1).

- **“Do I have liability for a third-party’s misuse of software I launch even if I have no knowledge of or ability to affect that misuse?”**

DeFi protocols, as explained above, are immutable open-source software protocols available on the internet that can be used by anyone with a wallet and digital assets. Like any tool, they can be used—or misused—without their original developers’ involvement or even knowledge. When DeFi protocols are misused, liability should fall on the person who committed a harm, not the creator of the tool itself. Holding developers liable for third-party actors’ misuse of freely available code would be “like an effort to hold a developer of self-driving cars liable for a third party’s use of the car to commit a traffic violation or to rob a bank. In those circumstances, one would not sue the car company for facilitating the wrongdoing; they would sue the individual who committed the wrong.”³³

Yet several federal agencies have done just that. They have taken the position that developers of such tools can be held liable for a third-party’s misuse, or potential misuse, of them.

United States vs. Roman Storm (S.D.N.Y.)

In August 2023, the U.S. Department of Justice (DOJ) indicted Roman Storm and Roman Semenov, the developers of the Ethereum-based smart contract protocol Tornado Cash. The DOJ alleged three wide-ranging conspiracies in the Indictment, including money laundering, operating an unlicensed money transmitting business, and violations of the International Emergency Economic Powers Act (IEEPA):

First, the indictment asserts that developers are liable for violating IEEPA³⁴ when they publish open-source software that is later used by a sanctioned entity, even if there is no allegation that they engaged with that sanctioned entity directly. Second, the indictment asserts that developers are liable for conspiracy to commit money laundering³⁵ when they publish open-source software that is later used by a third party to conduct transactions concealing the proceeds of specified unlawful activity, even if the developers did not know about or participate in those transactions. Third, the indictment asserts that developers are liable for conspiracy to operate an unregistered money transmitting business³⁶ when they publish open-source

³³ *Risley*, ECF No. 90 at 1.

³⁴ Pursuant to 50 U.S.C. § 1701 et seq.

³⁵ Pursuant to 18 U.S.C. §§ 1956(a); (h).

³⁶ Pursuant to 18 U.S.C. § 371 and §1960.

software that enables users to engage in peer-to-peer financial transactions, even if they have no ability to change the software and no control over user funds.³⁷

The DOJ's theories in this case are unprecedented and would grant the government unlimited power to prosecute any software developer who writes code that is later used by a third party for nefarious purposes, merely because the developer becomes aware of that later use. For example, the IEEPA claim hinges on expanding precedent far beyond previous sanctions cases. Based on our extensive research, previous cases of IEEPA conspiracy always included allegations that individuals purposely and knowingly transmitting money or goods to a sanctioned entity - meaning the accused directly and actively engaged with a sanctioned entity.³⁸ In none of the previous IEEPA cases did the government allege that the defendant was responsible for violating IEEPA simply because they created some tool or technology and later became aware that it was used by a sanctioned entity. But in this case, the DOJ has attempted to hold developers criminally responsible for publishing an immutable smart control protocol that was later used by a sanctioned third party bad actor.

In addition, in the DOJ's opposition to Storm's Motion to Dismiss the Indictment, the DOJ dedicated a section of its brief, "Section 1960 Does Not Require the Business to Have Control of the Funds," to the novel argument that the criminal code section pertaining to unlawful operation of an unlicensed money transmitting business is *broader* than the definitions in the Bank Secrecy Act and 2019 FinCEN Guidance and does not require the defendant to have "control" over funds being transferred.³⁹ As explained above, despite consistent industry reliance on 2019 FinCEN guidance as the most instructive government-issued guidance on what constitutes a money services business, the DOJ dismissed it. They made the unprecedented argument that "money transmission" includes every time the Tornado Cash "service" "caused cryptocurrency to pass from one place to another on the Ethereum blockchain every time a customer requested a deposit or withdrawal" *regardless of the level of control over user funds*.⁴⁰

The key point here is that the DOJ espouses brand new legal theories that are inconsistent with previous rules and do not comport with the reality of the technology — in a criminal case where individual liberty interests are at stake. This is the worst way for an

³⁷ Brief Of The DeFi Education Fund As Amicus Curiae In Support Of Defendant Roman Storm's Motion To Dismiss The Indictment, *U.S. v. Storm*, 23 Cr. 430, ECF No. 39 (S.D.N.Y. 2024).

³⁸ *Id.*

³⁹ Br. in Opp, *U.S. v. Storm*, 23 Cr. 430, ECF No. 53 (S.D.N.Y. 2024) <https://storage.courtlistener.com/recap/gov.uscourts.nysd.604938/gov.uscourts.nysd.604938.53.0.pdf>.

⁴⁰ *Id.*; *Founders and Ceo of Cryptocurrency Mixing Service Arrested and Charged With Money Laundering and Unlicensed Money Transmitting Offenses*, DOJ 24-146, <https://www.justice.gov/usao-sdny/pr/founders-and-ceo-cryptocurrency-mixing-service-arrested-and-charged-money-laundering>.

individual to find out they purportedly violated the law: post hoc and as they are facing indictment. With no limiting principle in place, the government's theory would expose all developers who create open-source software to criminal liability for activity outside of their control, years or decades later. The surface area for selective prosecution would be incalculable, as the government would be free to target software developers aligned with politically disfavored causes and industries, who would have little in the way of defense or recourse. Put simply, validating the Indictment's theories of liability would mean rejecting core principles of due process and the rule of law.⁴¹

In the Matter of Uniswap Labs

In an enforcement action settled just last week, Uniswap Labs agreed to pay a fine to the CFTC for purportedly violating the Commodity Exchange Act by making certain leveraged tokens available to U.S. retail persons on its front end. Without admitting or denying the allegations, Uniswap Labs agreed to take remedial action and pay a fine.⁴² However, prior to the settlement, Uniswap Labs already "took proactive measures, attempting to block trading of leveraged tokens. In fact, Uniswap [Labs] blocked the particular tokens at issue in this settlement after the Commission's settlement in a previous 'DeFi Sweep' involving those same tokens."⁴³

Two CFTC commissioners dissented, faulting the CFTC for bringing the action based on an unclear statutory basis and for failing to provide DeFi market participants a path to compliance under the current CEA framework. Commissioner Caroline Pham found that "there is no evidence in the administrative record that describes the specific terms and/or characteristics of the" assets at issue, rendering it impossible to "determine whether they are a CFTC-jurisdictional product, and, therefore, whether the CFTC has the authority to bring this enforcement action in the first place." She wrote, "This DeFi case may very well be a regulatory allergic reaction to new technology. But this reaction is not realistic or sustainable.... Emerging technologies like the blockchain and decentralized protocols that enable the direct peer-to-peer connection that underpins the consumer-driven shifts already underway in sectors such as retail, entertainment, and financial services, have the potential to write a brand-new chapter in our Nation's rich history of ingenuity and opportunity—the embodiment of the American Dream," Commissioner Pham said.

Commissioner Summer Mersinger stated that "the [CFTC] appears to be taking the position that any DeFi platform could be liable for any and all conduct occurring on its protocol.

⁴¹ Brief Of The DeFi Education Fund As Amicus Curiae In Support Of Defendant Roman Storm's Motion To Dismiss The Indictment, *U.S. v. Storm*, 23 Cr. 430, ECF No. 39 (S.D.N.Y. 2024).

⁴² *CFTC Issues Orders Against Uniswap Labs for Offering Illegal Digital Asset Derivative Training*, CFTC, No. 8961-24 (2024), <https://www.cftc.gov/PressRoom/PressReleases/8961-24>.

⁴³ *See Dissenting Statement of Commissioner Mersinger Regarding Settlement with Uniswap Labs*, CFTC, No. 8961-24 (2024), <https://www.cftc.gov/PressRoom/SpeechesTestimony/mersingerstatement090424>.

The practical effect of this approach is to severely chill the launching of any DeFi protocol within the United States and to significantly increase the odds that all DeFi innovation and economic activity will occur elsewhere. This theory of liability also raises a broader question about whether the Commission is fulfilling its responsibility under the CEA to promote ‘responsible innovation’ (not stifle it), which Congress included as a central tenet of the CFTC’s mission... imagine if J. Edgar Hoover had charged Henry Ford with liability for the crimes of John Dillinger and Bonny and Clyde because the Ford V8 was central to their ability to commit crimes. This result is the natural endpoint of the Commission’s logic that is at play in this settlement.”⁴⁴

5. Conclusion

The U.S.’s current approach to DeFi is manifestly untenable. I find it hard to believe that there have been many other industries in history that have so consistently and intently sought clearer laws than the digital asset industry. Contrary to the belief of certain detractors, the DeFi industry is not simply trying to avoid application of any laws or rules, but is actively seeking a clear path forward to existing in the U.S.

We can acknowledge there are areas where DeFi technology is still actively being developed. However, just because we have not reached our destination does not mean the journey is not worth pursuing. But in order to arrive, we as an industry need to be able to innovate without existential fear.

What we are asking for is simple: lawmakers should learn about and understand this technology before engaging in careful rulemaking that is cognizant of the realities of the technology and does not intentionally or unintentionally ban innovation and development.

We truly appreciate the opportunity to discuss DeFi with this Committee and hope to continue to engage with its Members in the future.

⁴⁴ *Id.*

Appendix A: DeFi Examples

1. Liquidity provision

Liquidity provision is a foundational component of many DeFi smart contracts: liquidity providers contribute tokens to a smart contract, which other users can interact with in various ways (such as engaging in token swaps or token borrowings). In exchange for their contribution, liquidity providers receive transferrable tokens that can be redeemed for a portion of the assets held in the smart contract.

This section illustrates how liquidity provision works in the context of automated market makers (“AMMs”), borrowing protocols, and liquid staking protocols.

2. Automated market makers

An AMM is a suite of smart contracts that facilitate token swaps. Typically, each smart contract handles one token pair (e.g., ETH-USDC, ETH-DAI, CRV-USDT, etc.). A liquidity provider can contribute equal values of each token within a pair to the related smart contract in exchange for a so-called liquidity pool token (“LP token”).

A smart contract in a “simple” AMM executes token swaps with users at prices determined algorithmically based on the relative amount of each token the smart contract holds, and charges the same percentage fee for each trade. Liquidity providers can redeem their LP tokens at any time for a proportionate share of whatever is in the smart contract at that time. The smart contract’s transaction fees are set by the contract deployer.

The simple AMM model distributes liquidity evenly across the theoretical range of a token pair’s relative prices. In a more complex AMM, liquidity providers can select the price range to which they wish to add liquidity (e.g., from [1 ETH = 1600 USDC] to [1 ETH = 1800 USDC]), and can redeem their LP tokens only for a proportionate share of whatever is in the smart contract within that price range at that time.⁴⁵ They also typically can set their own fees, so that traders potentially bear different fees within different price ranges.

3. Borrowing protocols

A DeFi borrowing protocol is a suite of smart contracts that facilitate overcollateralized token “borrowings.”⁴⁶ Users who contribute tokens to a smart contract can “borrow” other

⁴⁵ Because LP tokens for complex AMMs are fungible only with other LP tokens that have the same parameters, they typically are represented as NFTs (i.e., ERC-721 tokens on Ethereum).

⁴⁶ Borrowing protocols are sometimes referred to as “lending protocols,” but the transactions that they enable do not involve “lending” or “loans” in a traditional sense and do not give rise to debt for U.S. tax purposes. *See, e.g.,* Jake Chervinsky, *DeFi Protocols Don’t Do ‘Lending,’* Bankless, available at <https://www.bankless.com/defi-lending-doesnt-exist-yet> (Sep. 3, 2020).

tokens from the smart contract up to a percentage of the value of the tokens they contributed, and can reacquire tokens identical to the ones they contributed by replacing the borrowed tokens and paying a time-based usage fee.

Each user who contributes tokens to a DeFi borrowing protocol is not just a potential borrower, but also a liquidity provider, because the tokens they contribute can be borrowed by other users. When a user contributes tokens to the protocol, they receive a fungible token that is redeemable for (1) their contribution and (2) any usage fees accrued in respect of that contribution.⁴⁷

4. Liquid staking protocols

Liquid staking protocols are designed to socialize the costs, risks, and rewards of running Ethereum validator software. Very generally, non-validators contribute their ETH into a smart contract in exchange for fungible tokens redeemable for a portion of the assets within the smart contract. Based on the pre-defined logic of the smart contract, users' contributed ETH is allocated among participating validators to ensure that each has the minimum stake required by Ethereum's consensus mechanism.⁴⁸ A portion of validator rewards are credited to participating validators as a fee; the remainder accrue inside the smart contract or are credited on a current basis to the non-validators.

⁴⁷ Alternatively, usage fees might be credited on a current basis to liquidity providers.

⁴⁸ Validators might be required to contribute some value as "collateral" to the smart contract.

Appendix B: DeFi v. CeFi v. TradFi

	TradFi	CeFi	DeFi
DEFINITION	Traditional finance ("TradFi") is the system of legacy institutions (e.g., banks, exchanges, etc.) that provide financial services to our economy today. TradFi companies typically take custody of customer assets to perform such services. They typically collect fees for their services.	Centralized crypto finance ("CeFi") comprise companies that perform certain financial services akin to those in TradFi, but with and/or for cryptoassets. These companies act as an intermediary. CeFi companies typically take custody of cryptoassets to perform such services, and/or act as (and are regulated as) money transmitters or money services businesses. They also collect fees for their services.	Decentralized finance ("DeFi") is a software-based system that allows users to engage in economic activities at their own direction, and without intermediaries. A software development company or an individual builds a DeFi protocol. Once a protocol is fully decentralized, the software developer has no control over the technology or user assets. DeFi is non-custodial. The software does not take custody. No company/individual takes custody in a DeFi transaction. The users retain control over their own assets. The software development company does not take fees in a true DeFi transaction.
PLAYERS	• Banks • Nat'l securities exchanges • Broker-dealers • Designated contract market • Swap execution facility • Payment providers	• Cryptoasset exchanges • Cryptoasset custodians • Cryptoasset lenders • Fiat-backed stablecoin issuers	• Software developer • User of DeFi software • Participant in decentralized governance (e.g., decentralized autonomous organizations ("DAOs"))
EXAMPLES			

polygons

Chairman HILL. Thank you very much.
Mr. Van Valkenburgh, you are recognized for 5 minutes.

**STATEMENT OF PETER VAN VALKENBURGH, DIRECTOR OF
RESEARCH, COIN CENTER**

Mr. VAN VALKENBURGH. Chairman Hill, Ranking Member Lynch, Chair McHenry, members of the subcommittee, thank you for this opportunity to testify at today's hearing.

In the 1940s, there were 350,000 telephone switchboard operators in the United States. Privacy-conscious Americans worried that operators might still be listening to their calls after connection, and their fears were not unfounded.

In the 1928 Supreme Court decision *Olmstead v. U.S.*, wiretapping was deemed not to violate the Fourth Amendment. This allowed police to listen in to calls and conversations without any proof of reasonable suspicion or judicial oversight and to use that evidence against those Americans in court.

By the end of the 20th century, two significant changes had occurred. In 1967, the court overturned *Olmstead* in the landmark decision *Katz v. U.S.*, and by the 1980s, computers and automation had largely replaced human telephone operators. By the end of the 20th century, those changes had occurred.

Today, there are around 600,000 licensed stock brokers in the U.S., fewer brokers per person than telephone operators in the 1940s. Like the operators of the past, financial middlemen can and do learn the intimate details of our lives, but in the 1976 decision *Miller vs. U.S.*, the Supreme Court ruled that Americans have no reasonable expectation of privacy in the financial records they keep with third parties.

Fortunately, now in the 21st century, two things are changing once again. First, many financial transactions no longer require a human intermediary, a concept known as DeFi. Second, the Court is poised to overrule *Miller* and vindicate privacy rights just as it did with *Olmstead*.

There is a pattern here that is hopefully clear. Initially, we have privacy in our day-to-day affairs, but we have to do things in person, a cash transaction, or a face-to-face conversation. Then technologies emerged that scale human action across vast distances, but we lose our privacy in the process: a telephone call, a bank wire.

Finally, technologies improve, restoring privacy without sacrificing scale, and the law catches up to protect citizens' expectations of privacy. We get encrypted messaging. We get Bitcoin transactions.

In the past, American dynamism and constitutional law drove these changes, but it is not inevitable that America will always lead this revolution. If we do not allow Americans to use and develop peer-to-peer financial systems, those tools will be used and developed overseas.

Insisting on re-intermediating and surveilling peer-to-peer financial transactions would make the U.S. as noncompetitive as a country still relying on human switchboard operators for telephone calls.

Nonetheless, the Internal Revenue Service (IRS) is drafting rules that would force unhosted wallet software developers to go into the business of monitoring the users of their software: re-intermediation. The Department of Justice is prosecuting mere software publishers as unlicensed money transmitters. The Office of Foreign Asset Control, OFAC, has banned Americans from using certain DeFi software tools even for entirely domestic and legitimate purposes.

The Securities Exchange Commission is using enforcement actions to fit cryptocurrency activities into traditional regulatory frameworks that require intermediaries.

These agencies pursue these regressive strategies without clear congressional direction. The IRS is contradicting the plain language of the Infrastructure Act. The Southern District of New York is offering unjustified interpretations of the Bank Secrecy Act. The SEC is stretching its jurisdiction through overzealous enforcement and an unconstitutional rulemaking.

Congress has a pivotal role to play in preserving American dynamism. Some Members have already begun to push back. The Blockchain Regulatory Certainty Act, the Keep Your Coins Act, and FIT21 would clarify the legal landscape and leave room for innovation.

My organization, Coin Center, is also dedicated to preserving American dynamism. We are here to educate Members of Congress and the executive branch about these technologies, advocate for reasonable regulation, and preserve constitutional rights as we are doing through two challenges to regulatory overreach that we have brought in the courts.

I appreciate the committee's time today, and I look forward to addressing any of your questions.

[The prepared statement of Mr. Van Valkenburgh follows:]

**TESTIMONY OF****Peter Van Valkenburgh****Research Director of Coin Center¹****BEFORE THE****Subcommittee on Digital Assets, Financial Technology and Inclusion****Decoding DeFi: Breaking Down the Future of Decentralized Finance****September 10, 2024**

In the late 1940s, there were 350,000 telephone switchboard operators in the U.S.² Privacy-conscious Americans worried that operators might still be listening to their calls after connection, and that concern wasn't unfounded. In the 1928 Supreme Court decision *Olmstead v. U.S.*, wiretapping was deemed not to violate the Fourth Amendment.³ This allowed police to listen to conversations without proof of reasonable suspicion, or judicial oversight, and use that evidence in court.

By the end of the 20th century, two significant changes occurred. In 1967, the Court overturned *Olmstead* in the landmark decision *Katz v. U.S.*⁴ By the 1980s, computers and automation had

¹ Coin Center is an independent nonprofit research and advocacy center focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. Our mission is to build a better understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using open blockchain technologies. We do this by producing and publishing policy research from respected academics and experts, educating policymakers and the media about blockchain technology, and by engaging in advocacy for sound public policy.

² Tim Taylor, *Telephone Operators: The Elimination of a Job*, *Conversable Economist* (June 21, 2021), <https://conversableeconomist.com/2021/06/21/telephone-operators-the-elimination-of-a-job/>.

³ *Olmstead v. United States*, 277 U.S. 438 (1928).

⁴ *Katz v. United States*, 389 U.S. 347 (1967).

largely replaced telephone operators, and by the 90s, strong end-to-end encryption ensured communication intermediaries were blind to message contents.⁵

Today, there are around 600,000 licensed stock brokers in the U.S.⁶—fewer brokers per person than telephone operators in the 1940s. Like the operators of the past, financial intermediaries can and do learn intimate details of your life. However, in the 1976 decision *Miller v. U.S.*, the Supreme Court ruled that Americans have no reasonable expectation of privacy in their financial records.⁷

Fortunately, in the 21st century, two things are changing once again. First, many financial transactions no longer require a human intermediary—a concept known as DeFi.⁸ Second, the Court is poised to overrule *Miller* and vindicate privacy rights, just as they did with *Olmstead*.⁹

⁵ End-to-end encryption is most visibly discussed in the context of messaging systems such as Signal Encrypted Messaging, WhatsApp, or Apple Messages, these systems reliably blind all third parties to the contents for the messages. This is not, however, a niche or exceptional development in communications. Almost all web activity today is transmitted over the Transport Layer Security (TLS) protocol (visible when you visit a website via an https: rather than http: prefix). Communication intermediaries like Verizon or Comcast cannot decode the data being exchanged between you and the host of the website you are visiting. In this way, the communications intermediary has become incapable of listening in on your activities. Many people do much of their day to day activities on major web platforms, like Meta's Facebook or Google's Workplace services and these activities can be surveilled by the maintainers of those websites but the data is still shielded from communications intermediaries and still end-to-end encrypted in the sense that the user is one end and the platform maintainer is the other end.

⁶ FINRA, *Statistics*, FINRA.org, <https://www.finra.org/media-center/statistics> (last visited Aug. 22, 2024).

⁷ *United States v. Miller*, 425 U.S. 435 (1976) (Holding that individuals do not have a reasonable expectation of privacy in their financial records held by a third party, such as a bank. This decision established what is now known as the third-party doctrine exception to the warrant requirement for search and seizure.).

⁸ Landon Zinda, *How Congress Should and Should Not Approach DeFi*, Coin Center (Mar. 2, 2023), <https://www.coincenter.org/how-congress-should-and-should-not-approach-defi/>.

⁹ See Peter Van Valkenburgh, *Electronic Cash, Decentralized Exchange, and the Constitution*, Coin Center (Nov. 2019), <https://www.coincenter.org/electronic-cash-decentralized-exchange-and-the-constitution/> ("Recently, the third-party doctrine has come under attack from justices and legal scholars who believe it is predicated on an outmoded understanding of the modern information landscape and who fear that it is today used to enable truly massive private data collection with little to no judicial process or accountability.⁸⁶ As people increasingly hand the entirety of their private correspondence and data over to cloud service providers and other online intermediaries, there grows, effectively, a gaping hole in our once comprehensive Fourth Amendment protections. As Justice Sotomayor wrote in a concurrence to the 2012 *United States v. Jones* case, 'More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.'").

The pattern is clear: initially, we have privacy in our day-to-day affairs, but we have to be in person, as in a cash payment or a face-to-face conversation. Then technologies emerge that scale human action, but we lose privacy protections: a telephone call, a bank wire. Finally, technologies improve, restoring privacy without sacrificing scale, and the law catches up to protect citizens' privacy expectations: encrypted messaging, a bitcoin transaction.

American technological dynamism and constitutional law drove these changes. It's inevitable that financial transactions will be largely disintermediated, but it's not inevitable that America will lead this revolution as it did in the past.

Peer-to-peer financial systems are crucial for the future of the U.S. economy. If we don't allow their use and development by Americans, they will be used and developed overseas. Insisting on re-intermediating and surveilling peer-to-peer financial transactions would make the U.S. as noncompetitive as a country still relying on human switchboard operators for phone calls.

Nonetheless, as we will detail exhaustively below, several executive agencies are trying to do just that. The Internal Revenue Service ("IRS") is drafting rules that would force "unhosted wallet" software developers to go into the business of monitoring the users of their software against their will. The Department of Justice ("DOJ") in the Southern District of New York ("SDNY") is prosecuting software publishers as unlicensed money transmitters because unrelated users of their software have committed financial crimes. The Office of Foreign Asset Control ("OFAC") has banned Americans from using certain DeFi software tools even for entirely domestic and legitimate purposes. The Securities and Exchange Commission ("SEC") is using enforcement actions to fit cryptocurrency activities into traditional regulatory frameworks that require intermediaries.

These agencies pursue these regressive strategies without clear congressional direction. The IRS is contradicting the plain language of the Infrastructure Act in its broker rulemaking. The DOJ is offering unjustified interpretations of the Bank Secrecy Act ("BSA"), contradicting reasonable FinCEN guidance. OFAC is offering unjustified interpretations of the International Emergency Economic Powers Act ("IEEPA"). The SEC is stretching its jurisdiction through aggressive enforcement and an unconstitutionally expansive exchange rulemaking.

To better understand these missteps in DeFi policy, let's take each example in turn. In each case we'll explain what good regulation looks like and why the current approach has gone awry.

Treasury and the IRS's Broker Rulemaking

Coin Center has long advocated for Congress and the Treasury to treat trusted intermediaries in the cryptocurrency space identically to more traditional regulated financial services companies. This advocacy has included a call for clear guidance on third-party tax reporting obligations for cryptocurrency intermediaries.¹⁰ We do not object to the imposition of third-party reporting obligations on true digital asset intermediaries so long as the imposed requirements mirror those imposed on traditional intermediaries.

A broker, as traditionally understood, is still a broker even if they are buying and selling cryptocurrencies on behalf of their customer rather than securities or more typical commodities. They are an agent of their customer in these sales or else they are a principal in a sale to the customer. Accordingly, the imposition of a recordkeeping and reporting requirement is reasonable under the relevant statute and the strictures of the United States Constitution. Therefore, we take no issue with sections of the ongoing broker rulemaking that would place true cryptocurrency intermediaries on equal footing with traditional brokerages.

However, Coin Center strongly objects to the Treasury Department's recent attempt to impose broker reporting obligations on persons who are not properly understood as brokers or middlemen and who are merely engaged in the publication or ongoing maintenance of software tools and websites or any mere relayers of cryptocurrency transaction messages.¹¹ In legal rather than technical terms, we object to the imposition of reporting obligations on any software or communications intermediaries who do not have any agency or agency-like relationship with the users of their published tools and websites, and who are in no position to know or collect personal information about those users. Indeed, we find that the extension of reporting obligations to these persons, among other legal defects, runs counter to the underlying statutory authority, the legislative history, and—most importantly—would violate the First Amendment rights of cryptocurrency software, data, and website publishers and the Fourth Amendment rights of both the publishers and the users of said software, data, and websites.

There are two areas of the proposed rulemaking that give rise to these statutory and constitutional issues: 1) the proposed new definition of “Digital Asset Middleman” and the several other new definitions providing guidance on the interpretation of that term, and 2) the

¹⁰ See, e.g., Jerry Brito, *Reps. Polis & Schweikert introduce Cryptocurrency Tax Fairness Act in Congress*, Coin Center, September 7, 2017, <https://www.coincenter.org/rep-polis-schweikert-introduce-cryptocurrency-tax-fairness-act-in-congress/> (supporting a bill introduced in 2017 that directed the IRS to issue guidance on third-party tax reporting because “clear IRS guidance and informational reporting would be a lifesaver at tax time for cryptocurrency users.”).

¹¹ See Internal Revenue Service, *Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions*, 88 F.R. 166, pgs. 59576-59659, <https://www.govinfo.gov/content/pkg/FR-2023-08-29/pdf/2023-17565.pdf>.

proposed redefinitions of the terms “effect” and “customer.” These definitions taken together ultimately determine who must do reporting.¹²

The Treasury Department is bound to enact the law as made by Congress and is not free to go beyond that authority.¹³ Broadening these definitions runs counter to the plain text of the statute as it was amended by the Infrastructure Investment and Jobs Act (hereinafter the Infrastructure Act)¹⁴ and it also runs counter to the intent of Congress as found within the legislative history of that law’s passage.

Irrespective of the statute, the Treasury Department is bound by the Constitution to ensure that its rules do not violate fundamental rights. Mandatory reporting provisions of any kind compel speech.¹⁵ Any law that compels speech faces exacting scrutiny from the courts, meaning that the rule must be narrowly tailored to address a compelling government interest.¹⁶ The proposed rule is not narrowly tailored and would subject far more persons to an onerous disclosure regime than is appropriate to ensure tax compliance. Moreover, applying a customer disclosure requirement to persons who have no customers in the traditional sense, to persons who merely publish software, websites, or other tools, compels them to write their tools in a manner that goes directly against their closely held political and social beliefs. In other words, demanding software developers to build software tools that intentionally violate the privacy of their users compels these developers not only to speak some factual disclosure about their software users but also to speak in a deeply expressive manner a viewpoint with which they do not agree.

Finally, the rule as applied to those who merely publish software, websites, or other tools, violates the Fourth Amendment rights of the persons obligated to make reports, even under the more lenient standards for warrantless administrative searches. Additionally, to the extent any obligated persons will be made to report any information about taxpayers that is not voluntarily provided by taxpayers for a legitimate business purpose, the proposed rule deputizes service

¹² For a more detailed description of the problems in the current proposed rule and our suggested alternative approach, see Coin Center, *Comment Letter on Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions* (Dep’t of the Treasury Sept. 8, 2023),

<https://www.coincenter.org/comments-to-the-department-of-treasury-on-gross-proceeds-and-basis-reporting-by-brokers-and-determination-of-amount-realized-and-basis-for-digital-asset-transactions/>.

¹³ See *Federal Election Commission v. Ted Cruz For Senate*, 142 S. Ct. 1638, 1649 (2022) (“An agency, after all, ‘literally has no power to act’—including under its regulations—unless and until Congress authorizes it to do so by statute.”).

¹⁴ See *Infrastructure Investment and Jobs Act*, Pub. L. No. 117-58 (2021) <https://www.govinfo.gov/app/details/PLAW-117publ58>.

¹⁵ *Americans for Prosperity Foundation v. Bonta*, 141 S. Ct. 2373 (2021)

¹⁶ *Id.*

providers to engage in the warrantless search and seizure of taxpayer information in violation of the Fourth Amendment.

As of this hearing, the Treasury has only partially finalized its broker rulemaking: clarifying that custodial entities in the cryptocurrency space fit the definition of broker and need to do third party reporting. We are grateful for that clarity although it is several years overdue.¹⁷ With respect to DeFI (which the IRS accurately refers to as non-custodial), the agency has further delayed offering a final rule, leaving these critical constitutional issues to another day and leaving innovators entirely uncertain about their obligations.

SDNY DOJ's Interpretation of Money Transmission

It has been the clear and consistent policy of FinCEN¹⁸ since at least 2013 that cryptocurrency wallet developers and the users of those wallets are not money transmitters. Coin Center agrees with this policy and has lauded FinCEN for its frequent guidance and further clarifications in support of clear rules that achieve meaningful deterrence of crime while preserving innovation. So it has come as quite a surprise that the DOJ is suddenly intent on charging wallet developers criminally for unlicensed money transmission even if they exercise no actual control over the assets their users choose to secure with their software. This is an insidious development that appears to be nothing less than regulation by *criminal* enforcement.

Federal prosecutors have put forward this unprecedented interpretation of money transmission law in two recent cases: the April 26th unsealed Samourai Wallet indictment¹⁹ and the DOJ's opposition to Roman Storm's motions to dismiss and suppress evidence in the Tornado Cash

¹⁷ The IRS had the authority to offer this guidance at least as early as seven years ago when Coin Center worked with Reps. Polis and Schweikert to draft bipartisan legislation calling for guidance on 3rd party tax reporting in 2017. Jerry Brito, Reps. Polis & Schweikert introduce Cryptocurrency Tax Fairness Act in Congress, Coin Center, September 7, 2017, <https://www.coincenter.org/rep-polis-schweikert-introduce-cryptocurrency-tax-fairness-act-in-congress/> (supporting a bill introduced in 2017 that directed the IRS to issue guidance on third-party tax reporting because "clear IRS guidance and informational reporting would be a lifesaver at tax time for cryptocurrency users."). And again in 2019, Coin Center and others including members of this committee urged the IRS to use existing authority to offer guidance. See Letter from Rep. Tom Emmer to IRS Commissioner Charles Rettig (Apr. 15, 2019), <https://emmer.house.gov/2019/4/emmer-leads-bipartisan-blockchain-caucus-letter-irs-ahead-tax-day-urg-ing>. See also Coin Center, *Congress Sends Letter to IRS Regarding Urgent Need for Guidance on Crypto Taxes* (Sept. 1, 2023), <https://www.coincenter.org/congress-just-sent-a-letter-to-the-irs-about-urgent-need-for-guidance-on-crypto-taxes/>.

¹⁸ FinCEN is the division of Treasury tasked with interpreting and enforcing anti-money-laundering laws for non-bank financial institutions, cryptocurrency businesses that qualify as money services businesses included.

¹⁹ *United States v. Keonne Rodriguez & William Lonergan Hill*, S2 24 Cr. 82 (S.D.N.Y. 2024).

case, which was published the same day.²⁰ It is hard to know at this point if this is a deliberate attempt to abruptly change long-established policy through criminal enforcement, or if this is a significant disconnect between the Department of Justice and FinCEN. Either way, this is a disaster for the rule of law, due process rights for the accused, and our fundamental freedoms of speech and privacy. Here's a brief review of existing money transmission policy, and a detailed summary of the recent events.

The federal laws that regulate money transmitters are anti-money laundering (AML) statutes, specifically the Bank Secrecy Act and its amendments. These laws define a category of regulated businesses as "Financial Institutions" and also empower the Secretary of the Treasury to redefine that category as he sees fit. Because of this congressionally delegated power to expand the category, it is the implementing regulations of the Bank Secrecy Act (the "regulations") that actually define the law of who must and must not register as a money transmitter or other financial institution and practice Know Your Customer (KYC) guidelines, file reports with the government, and establish other AML controls.²¹

The regulations define a money transmitter as (1) any person who offers money transmission services, which the regulations define as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means," and (2) "any other person engaged in the transfer of funds."

In the context of cryptocurrencies, that definition includes some ambiguities about whether cryptocurrency is "currency, funds, or other value that substitutes for currency." If cryptocurrency is "funds," then "any person engaged in the transfer" is a money transmitter. If, alternatively, cryptocurrency is "currency" or if it is "other value that substitutes" for currency, then any person who both "accepts" and "transmits" cryptocurrency is a money transmitter. A plain reading of the regulations suggests that cryptocurrency is a substitute for traditional currency and, therefore, a person is a money transmitter if they both accept and transmit that cryptocurrency as a business for other people. In other words, if someone has actual control over another person's cryptocurrency and uses that control to move that person's

²⁰ *United States v. Roman Storm*, 23 Cr. 430 (KPF) (S.D.N.Y. Apr. 26, 2024) (Government's Opposition to Defendant Roman Storm's Pretrial Motions) available at <https://storage.courtlistener.com/recap/gov.uscourts.nysd.604938/gov.uscourts.nysd.604938.53.0.pdf>

²¹ For a deeper analysis of the statutory authority behind anti-money laundering policies and potential constitutional separation of powers issues therein, see Peter Van Valkenburgh, *Broad, Ambiguous, or Delegated: Constitutional Infirmities of the Bank Secrecy Act 1.0*, November 2023 available at <https://www.coincenter.org/broad-ambiguous-or-delegated-constitutional-infirmities-of-the-bank-secrecy-act/>

cryptocurrency to another person or location they are a money transmitter. This has been the controlling law since before cryptocurrency existed and it has never been amended or overruled by Congress, the courts, or regulation. As we'll discuss, the minor ambiguity over whether cryptocurrency is currency, funds, or value that substitutes for currency was resolved early in the history of crypto regulation by FinCEN.

In 2013, FinCEN released its first "virtual currency" guidance.²² In it, FinCEN confirmed that cryptocurrency (virtual currency as they called it) is "value that substitutes for currency" and that it is not "funds" or "currency" itself (hence "*virtual* currency"). In a footnote it also clearly stated that it does not consider virtual currency to be "funds" because doing so would trigger prepaid access regulations that FinCEN felt were inapplicable to cryptocurrency activities:

If FinCEN had intended prepaid access to cover funds denominated in a virtual currency or something else that substitutes for real currency, it would have used language in the definition of prepaid access like that in the definition of money transmission, which expressly includes the acceptance and transmission of "other value that substitutes for currency."²³

FinCEN went on to explain that mere users of virtual currencies are not money transmitters and in a subsequent administrative ruling found that software developers are also not money transmitters: "The production and distribution of software, in and of itself, does not constitute acceptance and transmission of value, *even if the purpose of the software is to facilitate the sale of virtual currency.*" [emphases added].²⁴

Coin Center and others lauded this clear statement of policy and over the following years pushed for additional clarity on the lingering question of partial control over virtual currency,

²²Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013), <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.

²³ *Id.*

²⁴Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002 (Jan. 30, 2014), https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R002.pdf.

as exists in the case of multisig wallets and time-locked contracts like those in the Lightning Network.²⁵ In response FinCEN published additional guidance in 2019.²⁶

The 2019 Virtual Currency Guidance clearly articulated that partial control over virtual currency was insufficient to classify wallet developers as money transmitters because: “the person participating in the transaction to provide additional validation at the request of the owner *does not have total independent control over the value.*”²⁷

Coin Center once again lauded FinCEN for clearly articulating a policy that rightfully required only custodial cryptocurrency businesses to license and be subject to federal money transmission regulations.²⁸ Even if we set aside these guidance documents and administrative rulings, however, a plain reading of the underlying binding rules also shows that money transmission in cryptocurrency only happens if someone both “accepts” and “transmits” cryptocurrency on behalf of another person.²⁹ In other words, for as long as cryptocurrency has existed, the law has been unambiguous: non-custodial cryptocurrency developers are not money transmitters.

On April 26th 2024 an indictment was unsealed³⁰ that accused the developers of Samurai Wallet (a Bitcoin wallet that uses CoinJoin transactions to enhance user privacy³¹) of unlicensed money transmission among other charges. For the purpose of this discussion we will not discuss the charge of conspiracy to launder money. That charge is fact-dependent and does not necessarily rely on the developers offering a custodial rather than non-custodial wallet service. The defendants may have, as alleged, operated a centralized server to coordinate CoinJoin

²⁵ The lightning network is a scaling solution to reduce the cost of making bitcoin transactions without introducing trust or reliance on third-parties. See Coin Center, *The Lightning Network* (2023), <https://www.coincenter.org/education/key-concepts/lightning-network/>.

²⁶ Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019), <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>.

²⁷ *Id.*

²⁸ Coin Center, *FinCEN's New Cryptocurrency Guidance Matches Coin Center Recommendations* (May 9, 2019), <https://www.coincenter.org/fincens-new-cryptocurrency-guidance-matches-coin-center-recommendations/>.

²⁹ 31 C.F.R. § 1010.100(ff)(5) (2023) (“The term ‘money transmission services’ means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means.”).

³⁰ *United States v. Keonne Rodriguez & William Lonergan Hill*, S2 24 Cr. 82 (S.D.N.Y. 2024).

³¹ Coin Center, *What Are Mixers and Privacy Coins?* (2023), <https://www.coincenter.org/education/advanced-topics/what-are-mixers-and-privacy-coins/>.

transactions. However, the Samourai Wallet did not afford the developers or any other third-parties actual independent control over bitcoins secured by users of the wallet software. Under a plain reading of the regulations and especially in light of the FinCEN guidance and administrative rulings, the developers of Samourai Wallet did not have “total independent control” over any user funds and therefore were thus not money transmitters.

Also on April 26th, the prosecution in the Tornado Cash criminal case against developer Roman Storm offered a reply brief that responded to the defense’s earlier motion to dismiss. A substantial subsection of the reply is titled “Section 1960 Does Not Require the Business to Have Control of the Funds.”³² There “Section 1960” is referring to the section of the criminal code that makes it illegal to operate an unlicensed money transmitting business.³³ The brief spends pages arguing that the definition at 1960 is broader than the actual definition in the Bank Secrecy Act and the regulatory definition offered by the regulator that we discussed above. It would be a blatant violation of due process rights if you could be charged under a criminal definition of “unlicensed” conduct even if the actual regulatory definition of which conduct requires a license clearly did not include the conduct in which you engaged. Nonetheless this is what the brief argues.

The brief goes on to argue that the Tornado Cash developers are culpable because the Tornado Cash software “caused cryptocurrency to pass from one place to another on the Ethereum blockchain every time a customer requested a deposit or withdrawal.”³⁴ This is a massive overreach. By the prosecution’s absurdly broad and unsupported standard, every functioning cryptocurrency wallet and smart contract is “doing” money transmission and every developer is engaged in unlicensed money transmission.

Eventually the reply brief reaches the regulatory definition but it ignores all of the existing guidance that we outlined above and interprets the “funds” section of the definition with absurd breadth, arguing that the law simply asks if someone is “any person engaged in the transfer.” This entirely ignores the fact that FinCEN has previously articulated that virtual currency is not “funds.” To illustrate their point about “control” being non-essential, the prosecution makes a comparison to parcel delivery:

³²*United States v. Roman Storm*, 23 Cr. 430 (KPF) (S.D.N.Y. Apr. 26, 2024) (Government’s Opposition to Defendant Roman Storm’s Pretrial Motions) available at <https://storage.courtlistener.com/recap/gov.uscourts.nysd.604938/gov.uscourts.nysd.604938.53.0.pdf>

³³18 U.S.C. § 1960.

³⁴*United States v. Roman Storm*, 23 Cr. 430 (KPF) (S.D.N.Y. Apr. 26, 2024) (Government’s Opposition to Defendant Roman Storm’s Pretrial Motions) available at <https://storage.courtlistener.com/recap/gov.uscourts.nysd.604938/gov.uscourts.nysd.604938.53.0.pdf>

Consider the example of a business that accepts parcels of cash from criminals and moves the money by courier to locations overseas, perhaps the archetypal Section 1960 violation. Under the defendant's theory, such a business could escape liability by the simple expedient of only accepting cash in locked parcels, as long as its customers did not give it the keys to unlock the parcels. Then, it could claim, it never had "control" over the funds.³⁵

This brief section is indicative of the low-ball tactics being employed by the prosecution. First note the immediately prejudicial nature of the parcel service, it "accepts parcels of cash from criminals." If Tornado Cash was a parcel service it certainly didn't only accept parcels from criminals. Coin Center happily used Tornado Cash to accept legitimate donations.³⁶ Second, the comparison proves exactly the opposite of what the prosecutors want it to prove. A delivery service that cannot access the underlying contents of the parcels it delivers is *plainly and clearly not a money transmitter*. First of all, if you can't open the parcel how do you even know what is in it? Can you be guilty of unlicensed money transmission if you were told you were only moving boxes of canned Spam and had no way to open the boxes? Second, FinCEN has expressly ruled that armored car businesses that are "limited to secure transportation of currency" are *not money transmitters under their rules*.³⁷ Sadly, the prosecution may dismiss that administrative ruling just as they have dismissed the otherwise comprehensive and clear guidance that FinCEN has offered on virtual currencies.

As we have argued in our own civil lawsuit to remove the Tornado Cash smart contracts from the OFAC list³⁸ and in our amicus brief in this criminal case,³⁹ no third party including the Tornado Cash developers ever had any actual control over the cryptocurrency that users of the

³⁵ *Id.*

³⁶ See *Brief of Amicus Curiae Coin Center in Support of Defendant Roman Storm's Motion to Dismiss* at 10-11, United States v. Roman Storm, No. 23 Cr. 430 (S.D.N.Y. Apr. 5, 2024), <https://www.coincenter.org/app/uploads/2024/04/Coin-Center-Amicus-Brief-filed.pdf> ("Coin Center has used Tornado Cash to privately accept donations that support our non-profit mission. We have brought a lawsuit to have OFAC remove the Tornado Cash pool addresses from the sanctions list so that we can continue to use them for that purpose and so that other Americans can use them for any legitimate privacy purposes. We have co-plaintiffs in that lawsuit who wish to use Tornado Cash to be privately paid their salary and who have used it to privately make donations to the war effort in Ukraine without becoming targets of Russian cyber attacks.").

³⁷ Financial Crimes Enforcement Network, *Definition of Money Services Business (Money Transmitter/Currency Dealer or Exchanger)* (2004), <https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/definition-money-services-business-money>.

³⁸ Coin Center, *Coin Center Is Suing OFAC Over Its Tornado Cash Sanction* (Oct. 12, 2022), <https://www.coincenter.org/coin-center-is-suing-ofac-over-its-tornado-cash-sanction/>

³⁹ Coin Center, *Coin Center Files a Court Brief in Defense of Tornado Cash Developer* (Feb. 10, 2023), <https://www.coincenter.org/coin-center-files-a-court-brief-in-defense-of-tornado-cash-developer/>.

tool owned. Under clear and long established FinCEN guidance and under any common sense reading of the underlying law, these developers are not money transmitters. Nonetheless the prosecution persists unjustly.

We are grateful that Senators Lummis and Wyden have expressed similar concerns over these overzealous criminal prosecutions and their muddling effect on FinCEN policy. We hope members of this subcommittee will add their voices to the effort and persuade the DOJ to drop these unreasonable charges.

OFAC Privacy Tool Bans

Sanctions are an important part of our foreign policy toolset. Coin Center does not object to the use of sanctions against foreign persons who are promoting terror or international crime including if they are doing so by sending and receiving cryptocurrencies to or from cryptocurrency addresses that they control. We do not, however, support OFAC's attempt, herein described, to abuse sanctions laws in order to block ordinary Americans from using tools that protect their legitimate privacy interests.

Privacy is not the default on Ethereum or in most of DeFi generally. If you do your job using these technologies, your co-workers can see your salary. If you donate to a political cause, the opponents of your cause can see your contribution. If you are a celebrity on these networks, your fans see not just your publicized activities but also your private personal accounts and net worth. Privacy is *normal* for a salaried employee, a charitable donor, even a celebrity, but privacy is not normal if you do these things on Ethereum *unless you use a tool like Tornado Cash*. In August of 2022, the U.S. Treasury unilaterally and extralegally made it a crime for Americans to use Tornado Cash for any purpose.⁴⁰

Later that fall, Coin Center, along with a group of normal privacy-seeking American workers, donors, activists, and public figures, filed a lawsuit against the Treasury Department to keep privacy normal, to delist Tornado Cash privacy tools from sanctions, and to enjoin Treasury from enforcing against ordinary Americans exercising their self-evident and basic rights to privacy.⁴¹ Our lawsuit is currently on appeal in the 11th Circuit and oral argument is scheduled for November 18th.

⁴⁰ Complaint, Coin Center v. Yellen, No. 3:22-cv-20375 (N.D. Fla. Oct. 12, 2022), <https://www.coincenter.org/app/uploads/2022/10/1-Complaint-Coin-Center-10-12-22.pdf>.

⁴¹ *Id.*

Our lawsuit makes four claims. First, Congress gave the president *very specific* powers when it passed the International Emergency Economic Powers Act upon which Treasury's sanction rules are based: sanctions can block U.S. persons from transacting with a foreign person or majority foreign entity or the property of that person or entity. When we or our co-plaintiffs use the Tornado Cash tools, we do so as normal, privacy seeking Americans. We do not engage in any transactions with any foreign person or entity or their property. Instead, we are using immutable and widely available software on the Ethereum blockchain to move our own valuables from one place in cyberspace that is fully under our control to another place that we also control. At no point are we relying on any third party for these transactions and at no point are we transacting with a sanctioned person. Plainly, given the specific powers granted to the Treasury Department by Congress, these are not the kinds of activities that can be censored or blocked. The Tornado Cash sanction was, therefore, made in excess of statutory authority and must be set aside.⁴²

Second, even Treasury's own regulations and past executive orders limit the applicability of sanction controls to transactions with persons, entities, or their property.⁴³ The Tornado Cash sanction was made without statutory and also without regulatory authority. It was made contrary to law.

Third, in sanctioning Tornado Cash tools, the Treasury failed to consider the collateral consequences of its actions or manifest any awareness of, or justification for, their significant deviation from previous sanctions policies. Their actions were arbitrary and capricious. Since the sanction, Americans have had money trapped in a smart contract without any due process; they've been attacked by malicious continued use of the smart contract that saddles them with indefinite reporting requirements or else criminal penalties through no fault of their own. Meanwhile, the Treasury has issued statements that directly contradict their own rules, and scant public clarity has been offered in the face of real public confusion and harm.⁴⁴

Fourth, Americans have had their associational activities chilled as once private donations to political causes must now be made public on chain. Our American system relies on certain essential and self-evident rights. Among them, that you can meet with others to petition the government and contribute to groups and organizations that will further those advocacy efforts. Key to our freedom of association is the right to make these donations in private, to not be forced to disclose to the government or any third party a list of the people who believe in your cause. Coin Center, among many non-profits, relied upon Tornado Cash for private

⁴²*Id.*

⁴³*Id.*

⁴⁴*Id.*

donations. Another of our co-plaintiffs relied upon Tornado Cash to organize substantial support for the defense of Ukraine. Subjecting these transactions to public scrutiny would not only chill the protected activities of donors, it would put those donors and activists in real danger of Russian reprisals.

For all these reasons and more, Coin Center opposes Treasury's extra-legal usage of its sanctions authority to strip U.S. persons of access to software tools that are necessary to protect our basic privacy needs as we go about our lives. We hope that members of this committee will investigate Treasury's extra-legal actions and ensure both that OFAC's authority is limited to what Congress intended, and that Americans' rights are not infringed by these actions.

SEC Enforcement Actions and Exchange Rulemaking

In 2016, Coin Center was one of the first organizations to publish a detailed report on why certain so-called "initial coin offerings" ("ICOs") may be unlicensed securities issuance in contravention of the Securities laws.⁴⁵ Since 2016 we have recommended that the SEC "take action necessary to protect investors against cryptocurrencies well-fitted to the Howey test, presenting greater risks to users" such as "closed-source or low-transparency cryptocurrencies," "open but heavily marketed pre-sales or sales of pre-mined cryptocurrencies with a small and non-diverse mining and developer community" and "cryptocurrencies with permissioned ledgers or a highly centralized community of transaction validators."⁴⁶ In short, we are not in favor of and have never advocated for a fully hands-off approach to investor protection in the cryptocurrency space. We have also worked with Members of this Committee and others in Congress to draft new legislation that would impose reasonable market structure oversight on custodial cryptocurrency exchange platforms to ensure investor protection.

The SEC, however, has recently eschewed any such nuanced analysis of securities laws in favor of an imperial approach toward their jurisdiction. They have brought dubious enforcement actions and have an ongoing rulemaking that would classify mere software developers as national securities exchanges bound to registration and oversight.

The two best examples of recent inappropriate and overbroad prosecutions from the SEC are the claims against Coinbase that their noncustodial wallet product offers unlicensed brokerage services and the claims against Consensys that their metamask wallet does the same. The

⁴⁵Peter Van Valkenburgh, *Framework for Securities Regulation of Cryptocurrencies 2.0*, August 2018. (Version 1.0 of this report was published in 2016 and our in-person briefings with SEC staff covered these recommendations as early as 2015).

⁴⁶ *Id.*

Coinbase wallet claims were rightfully dismissed by Judge Failla of the Southern District of New York.⁴⁷ The Consensys claims have yet to be addressed on motion to dismiss.

The ongoing Consensys case in particular is highly fact dependent and deals with new technologies, such as liquid staking tokens, that will present various questions of first impression to judges. It's deeply unfortunate that the SEC has decided to charge into this ambiguous area with an aggressive surprise enforcement action rather than first offering clearer guidance and rulemakings that give the public and any potential defendants the benefit of due process and the rule of law. Crypto wallets like Consensys' Metamask are essentially just user interfaces; they are to blockchain networks what the desktop web browser is to the world wide web. If we'd taken the SEC's current enforcement approach back in the 1990s, federal agents would have been raiding Netscape's offices, and arresting developers because of web content their users happened to visit while using Netscape Navigator. The result would be (and is) holding the wrong people responsible for content that may not even be illegal. The result is anti-innovation and seeks centralized control over speech and discourse.

The SEC's aforementioned rulemaking is intended to expand the definition of "exchange" in order to encompass additional financial services organizations.⁴⁸ The way it does so, however, would create an inappropriately broad standard for registration that would impose an unconstitutional prior restraint on the protected speech activities of countless software developers and technologists.

The existing definition of exchange is conduct-based. One is an exchange if one engages in certain specified conduct: One "uses" methods to bring together "orders." The newly proposed definition is speech-based: One is an exchange if one publishes speech that brings other persons together and affords them a set of rules enabling them to trade, i.e. if one merely "makes available" a "communication protocol" such that other people come together and trade.

While the constitutionality of the existing regulatory definition has not been tested in court, the fact that it places a prior restraint on conduct ("using ... methods") rather than on speech ("making available ... protocols") suggests that it could survive constitutional scrutiny. Laws regulating conduct, even if it is expressive conduct (e.g. flag burning or nude dancing) and even

⁴⁷ SEC v. Coinbase, Inc., No. 1:23-cv-04738, 2024 WL 1234567 (S.D.N.Y. Mar. 27, 2024)

⁴⁸ Securities and Exchange Commission, *Amendments Regarding the Definition of 'Exchange' and Alternative Trading Systems (ATSS) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities*, 87 FR 15496, pgs. 15496-15696, March 18, 2022, <https://www.federalregister.gov/documents/2022/03/18/2022-01975/amendments-regarding-the-definition-of-exchange-and-alternative-trading-systems-atss-that-trade-us>.

if the law impacts some speech incidental to conduct (e.g. a lawyer mostly speaks but must be licensed to practice law), are judged under an intermediate scrutiny standard and are often found constitutional despite their tendency to limit otherwise protected expression. By contrast, laws regulating speech qua speech are judged under a strict scrutiny standard and are rarely found constitutional.

The Supreme Court has already ruled against similar unconstitutional overreach by the Commission in the context of the Investment Advisers Act,⁴⁹ and is primed to do so again given recent opinions dealing with data brokers and commercial speech.⁵⁰ The chilling effect inherent in imposing an overly broad standard for registration, matched with severe penalties for non-compliance, will lead many creative and inventive Americans to self-censor.

The SEC has yet to finalize this rulemaking and we hope they will abandon this unconstitutionally overbroad definition in the final rule. If this rulemaking were to move forward, Congress can exercise its appropriate oversight function to reject this rule. Congress can also provide important clarifications to securities laws, like those included in the Securities Clarity Act and FIT 21, which are already being confirmed as rational approaches under existing law in several recent court cases.⁵¹

Conclusion

Congress has a pivotal role to play in preserving American dynamism. Some members have already begun to push back against these unlawful and unconstitutional intrusions. The Blockchain Regulatory Certainty Act, the Keep Your Coins Act, FIT21, and other initiatives seek to clarify the legal landscape and leave room for innovation. If the American Constitution is to be preserved, the Court should push back. Revive our right against warrantless search by overturning *Miller*, and protect our First Amendment rights to publish software.

⁴⁹ *Lowe v. Securities & Exchange Commission*, 472 U.S. 181, 236 (1985).

⁵⁰ *Sorrell, et al. v. IMS Health Inc., et al.*, 564 U.S. 552 (2011).

⁵¹ See e.g., *SEC v. Ripple Labs, Inc.*, No. 1:20-cv-10832, 2023 WL 4508821 (S.D.N.Y. July 13, 2023). Judge Analisa Torres granted partial summary judgment in favor of Ripple, ruling that certain XRP sales did not violate securities laws, but institutional sales did. The SEC's request for \$1.07 billion in disgorgement was reduced to \$125 million in penalties during the remedies phase. See also Judge Torres's distinction between institutional and secondary market sales. See also, *SEC v. Payward Ventures, Inc. (Kraken)*, No. 3:23-cv-00634 (N.D. Cal. Aug. 23, 2023). Judge William Orrick ruled against Kraken's motion to dismiss, allowing the SEC's case regarding its staking-as-a-service program to proceed, while rejecting the SEC's claim that digital asset securities were a special form of security, and *SEC v. Binance Holdings Ltd.*, No. 1:23-cv-01599 (D.D.C. June 29, 2024). Judge Amy Berman Jackson ruled that the SEC's major charges against Binance for unregistered securities offerings and other regulatory breaches could proceed, although some claims related to secondary market activities were dismissed.

My organization Coin Center is also dedicated to preserving American dynamism. We are here to educate members of Congress and the Executive Branch about these technologies, advocate for reasonable regulations, and preserve constitutional rights, as we are doing through the two challenges to regulatory overreach that we've so far brought in the courts.

This isn't a lawless future I'm describing. It's a future where the law is not abused to force Americans to use outdated tools or ban them from building better ones. It's un-American to tell an inventor she needs state-approval before publishing words or code describing her invention. It's very American to take her to court if she lied about what the invention would do or used the invention to commit a crime. We need to focus on *ex-post* regulatory efforts, such as fraud, contracts, torts, and unfair and deceptive acts and practices prosecution. This is a significant departure from our traditional financial regulatory structure, focused as it is on *ex ante* licensing, registering, and chartering. However, it is the only regulatory structure that can be aimed at DeFi without compromising our country's technological dynamism and our Constitutional right against prior restraints on speech. I appreciate the Committee's time and look forward to addressing any questions you may have.

Chairman HILL. Thank you, sir.

Mr. Hays, you are now recognized for 5 minutes for your oral remarks.

**STATEMENT OF MARK ALLEN HAYS, SENIOR POLICY ANALYST,
AMERICANS FOR FINANCIAL REFORM**

Mr. HAYS. Thank you, subcommittee chair, Ranking Member Lynch, and members of the committee. Thank you for the opportunity to testify here today.

I am Mark Hays, a senior policy analyst with Americans for Financial Reform, which is a coalition of over 200 consumer, community, labor, civil rights, and other organizations that advocate for a financial sector that serves workers, communities, and the real economy, and provides a foundation for advancing racial and economic justice.

The cryptocurrency and decentralized finance, or DeFi industries taut themselves as alternatives to traditional finance. They use technology to side step intermediaries and offer new ways to build wealth and finance.

Unfortunately, the crypto industry is highly volatile, scam-laden, and frequently predatory, which exposes investors to substantial financial losses. In fact, yesterday, the Federal Bureau of Investigation (FBI) reported that there were 5.6 billion in losses in 2023 alone reported associated with crypto, which was 10 percent of the cases reported but 50 percent of the reported losses.

This is largely because the industry often does not comply with or is not subject to the same sorts of investor or market protections found in conventional markets. Many have lost their life savings due to industry practices, and people from communities of color and low-income neighborhoods have particularly been targeted and harmed.

Crypto and DeFi must be subject to the same kinds of investor protections and market regulations as other retail investment markets, such as those overseen by the Securities and Exchange Commission and State securities regulatory bodies. These rules promote market transparency, price discovery, and market stability, as well as protect investors from fraud and market manipulation.

Some of these risks stem from the aggressive promotion of new crypto products, DeFi or CeFi. This often includes celebrity endorsers sometimes compensated to boost investor interest in assets with little real-world tangible value. Boosters have included marquis figures like Larry David, Gisele Bündchen, and Steph Curry, among many others.

The most recent example of this type of promotion is the launch of the crypto venture World Liberty Financial, which has insinuated the involvement of public figures, such as the Trump family. Yet this does not work out well for consumers. A Harvard and Indiana University study on such promotional activity found that crypto ventures promoted by influence or tweets slid by 18 percent within 3 months.

The DeFi industry's contention that its technology democratizes finance and makes regulatory standards found in other markets less needed or unnecessary altogether does not hold water. In fact, there is considerable centralization and consolidation of the owner-

ship, control, infrastructure and economic relationships found in DeFi.

As I describe in my written submission, decentralized finance is not all that decentralized. A limited set of powerful players control crucial elements of the DeFi industry. For example, one industry study showed that just 1 percent of DeFi platform users control 90 percent of governance tokens on 10 major DAOs, or decentralized autonomous organizations.

Far from automatically creating safety, the technology used has enabled or allowed multiple scams and hacks, amounting to, by one industry estimate, 1.5 billion worth of losses in 2023 alone, which is, based on the cases used, more than one scam per day on average.

In reality, DeFi is composed of de facto crypto-based intermediaries that play similar roles and pose similar risks as traditional financial markets do but who are not covered by or abide by the protections and rules that exist in those markets. The DeFi industry is replete with these risks and harms, widespread hacks and cyberattacks, extractive and exploitive financial products and services, market manipulation, illicit finance, and more.

These problems warrant a proactive regulatory approach to protect investors, crypto markets, and the financial system, but Congress' efforts to advance crypto-related legislation, such as with FIT21, which passed the House this year, have mostly proposed creating new, lax, custom-made crypto and DeFi regulations or exempting the DeFi industry from existing regulatory oversight altogether.

Instead, Congress should work with regulators to use their existing regulatory authorities to protect investors, consumers, and communities from the risks and harms that DeFi presents and to hold crypto and DeFi actors accountable for complying with existing rules and regulations.

Studying this history may be useful, but it should not preclude action to protect consumers today.

I look forward to your questions, and thank you for your time and consideration.

[The prepared statement of Mr. Hays follows:]

Written Testimony before the House Financial Services Committee
Subcommittee on Digital Assets, Financial Technology and Inclusion

Mark Hays
Senior Policy Analyst
Americans for Financial Reform

Decoding DeFi: Breaking Down the Future of Decentralized Finance

September 10, 2024

Testimony of Mark Hays
 Senior Policy Analyst, Americans for Financial Reform
 Before the House Financial Services Committee
 Subcommittee on Digital Assets, Financial Technology and Inclusion
 Decoding DeFi: Breaking Down the Future of Decentralized Finance

September 10, 2024

Subcommittee Chair Hill, Ranking Member Lynch, and members of the Committee, thank you for the opportunity to testify today. My name is Mark Hays, I am a senior policy analyst with Americans for Financial Reform. AFR is a coalition of more than 200 consumer, community, labor, civil rights, and other organizations dedicated to advocating for policies that shape a financial sector that serves workers, communities and the real economy, and provides a foundation for advancing economic and racial justice.

Cryptocurrency and decentralized finance (DeFi) are promoted as an alternative to traditional finance that eliminates powerful intermediary gatekeepers and offers a new tool for access to finance and wealth building. Unfortunately, the crypto industry is highly volatile and riddled with scams and predatory behavior that can expose those that buy cryptocurrencies and tokens to substantial financial losses largely because the industry is not subject to, or does not comply with, the same sorts of investor protections or requirements found in conventional financial markets. Investors can lose their life savings to the rosy promises of the crypto promoters. And people from communities of color and lower income neighborhoods are particularly vulnerable to the industry's exploitative and predatory business practices.

The crypto industry, including DeFi tokens and trading platforms, must be subject to the same kinds of investor protections and market regulations as other retail investment actors, such as those found in financial markets regulated by the Securities and Exchange Commission. These rules promote market transparency, price discovery, and market stability as well as protect investors from fraud and market manipulation.

Decentralized finance is not immune from these problems or obligations merely because it contends that it has used technology to supposedly democratize investment opportunity and sidestep financial intermediaries. Indeed, these risks may be greater within DeFi markets because despite surface level appearances, there is considerable consolidation in the ownership, control, infrastructure, and economic interrelationships found within the DeFi sector that, without sound and robust regulatory oversight comparable to that which conventional financial markets are subject to, can leave smaller, retail investors more vulnerable to fraud or market manipulation.

Decentralized finance is replete with risks and practices that harm or have the potential to harm consumers, investors, and financial markets (discussed in section II). This includes the unique vulnerability of DeFi platforms and transactions to cyberattacks; the extractive and exploitative nature of the financial products and services offered on DeFi platforms; and investors' exposure to illicit finance and money laundering found on or facilitated by DeFi platforms.

The reality is that the crypto and DeFi ecosystems are quite centralized and concentrated, despite industry claims. Across various dimensions, from governance token ownership, to mining and validation, to relationships with centralized crypto exchanges and traditional finance, the available data and analysis suggests that decentralized financial exchanges and platforms are not actually decentralized (discussed in section III).

It is highly doubtful that the DeFi industry's claims of, or aspirations towards, decentralization is achievable or could provide meaningful, scalable benefits to consumers while also adequately addressing the risk to consumers, investors, communities, and financial markets. And, these levels of concentration and the

presence of dominant crypto intermediaries in DeFi spaces undermines the key industry's key contention that it offers an alternative to centralized financial intermediaries — they are just different, crypto-based intermediaries that pose the same or similar sorts of investor risks as traditional financial markets, but without the protections that exist into those markets to mitigate such risk and harm.

Finally, the demonstrated problems and risks posed by crypto and DeFi tokens and platforms warrant a robust regulatory approach to protect investors, crypto markets, and the financial system (discussed in section IV). Congress' efforts to advance legislation that would either create a new regulatory framework custom-made for crypto or DeFi, or would exempt DeFi platforms, assets, and actors from existing regulatory oversight, are premature at best and ill-advised at worst. Instead, Congress should work with regulators to use their existing regulatory authorities to protect investors, consumers and communities from the risks and harms that DeFi present and to hold the crypto and DeFi actors accountable for complying with existing rules and regulations.

I. The purported promise and real risks of decentralized finance

Decentralized finance combines cryptography and distributed ledger technology (often referred to as blockchain technology) to create a system where parties can exchange digital expressions of value without the apparent need for a central intermediary to verify or validate such transactions. This arrangement purportedly enhances people's access to finance by supplanting or reducing the need for central financial intermediaries such as banks, brokers, exchanges, or clearinghouses, allegedly reducing the concentration and control these intermediaries have over the financial system. Theoretically, the security and transparency of the blockchain ledger could also reduce the costs of finance for more people by streamlining financial transactions or increasing transaction speeds. In practice, however blockchain-based transactions can be slow, expensive, insecure, and just as reliant on intermediaries as traditional finance, and also lack comparable guardrails, investor protections, transactional security, fraud prevention and basic disclosures found in conventional financial markets.

These contentions are not unique to DeFi; they are broadly shared by much of the cryptocurrency industry. But DeFi goes beyond merely trading cryptocurrencies on crypto exchanges or platforms. The premise of DeFi is that individuals can have even greater autonomy over their transactions without needing brokers or exchanges or other intermediaries to facilitate transactions by relying on computer technology itself to execute financial activities. DeFi transactions are meant to be facilitated through the use of so-called smart contracts where blockchain platforms add a layer of code that can automatically take certain actions on behalf of DeFi users. These automated smart contracts can deliver crypto assets into a customer's wallet, execute a trade between two customers once certain conditions are reached, or direct the activities of a staking pool (a process that allows investors to accrue interest on their assets in exchange for helping validate blockchain transactions), among other actions.

Today, these smart contracts are mostly used to facilitate speculative investment, although DeFi proponents have suggested a host of pie-in-the-sky applications. DeFi proponents claim that these smart contract protocols free people from relying on financial intermediaries to facilitate or execute these transactions.

This is meant to differ from traditional finance, where intermediaries actively facilitate and secure these transactions. These centralized exchanges, thanks in large part to regulatory requirements, enhance price discovery and price transparency, bolster transactional safety by listing known instruments and securing transactions, and facilitate transactional liquidity. Federal financial market regulators like the Securities and Exchange Commission oversee exchanges and brokers to promote fair markets, provide disclosure of needed information to investors, and to prevent fraud and market manipulation. These markets have their own flaws and problems, but decades of financial regulatory safeguards have been developed and established to identify and address those problems.

DeFi platforms rely on technology to directly perform such financial transactions, sidestepping brokerage and exchange intermediaries. In theory, an investor trading crypto on a DeFi platform is not interacting directly with a broker to execute trades but is interacting directly with another trader or party through an automatic protocol. Critically, DeFi adherents believe that since this two-party transaction is different from how traditional intermediation operates, DeFi transactions should be either exempt from the kinds of safeguards and oversight on regulated exchanges or that the requirements should be substantially different for DeFi transactions. The premise is that two willing traders in a DeFi transaction should be free to buy or sell with little restrictions, or more limited guardrails than on a traditional exchange. But exchanges and especially regulated exchanges perform more functions than merely executing transactions that enhance transactional security and transparency for investors. And without more robust oversight by regulators and obligatory standards for intermediaries, individual investors are more exposed to information asymmetries, power imbalances, fraud and manipulations, and cybersecurity risks in a caveat emptor, buyer-beware free for all that can be financially perilous for retail crypto investors.

Decentralized finance platforms also lack meaningful ways to ensure their platforms are managed and governed in a transparent and accountable manner, when compared to the tools available in traditional regulated markets. A traditional exchange intermediary might be a company with a board of directors and chief executives who are responsible for the activities that occur on their exchanges and are obliged to establish rules for what can be traded, who can trade, how transactions are secured, and how they and their employees operate. They are accountable under the law for their firm or exchange's actions and are subject to penalties if they violate or fail to adhere to numerous investor protection standards. In contrast, software developers or a development company might initially create a crypto asset or token, but once these tokens are distributed on a DeFi platform and its protocols in place, DeFi developers claim that their role in governance and the management of the platform recedes, becoming merely administrative rather than managerial. Often, a decentralized autonomous organization (DAO) is created to provide platform governance through the possession of governance tokens that can be issued to investors, users, and others. Those that hold these governance tokens determine how the platform is operated and managed. Key decisions — such as whether to issue a new token or tweak an existing transaction protocol — are voted on by governance token holders.

As such, management decisions and responsibilities that would typically fall to a discrete, identifiable, and accountable group of managers in traditional finance is instead distributed to users and governance token holders of the platform. Thus, DeFi proponents argue that this democratizes DeFi platforms. And they argue that platform developers should not be held to the same level of accountability as managers in traditional finance because that role has been ceded to the DAO and its members. Nor, they argue, should individual DAO members be held to the same level of accountability because any one member lacks the degree of control that a manager might have. But the anonymity and diffusion of the DAO governance token holders greatly impedes the accountability and responsibility necessary to fulfill the fiduciary duties associated with operating a fair and fraud free exchange, maintaining a broker's best execution responsibilities, or the due diligence necessary to prevent money laundering (anti-money laundering or know-your-customer AML/KYC protocols). And, many DeFi proponents contend that fulfilling these basic market functions to the same degree as traditional financial intermediaries are unnecessary and unreasonable.

II. DeFi presents a host of risks and harms to investors.

DeFi platforms and crypto ecosystems are rife with fraud, market manipulation, deceptive marketing, and illicit finance that extract wealth from smaller retail investors, create market instability, and harm communities. DeFi proponents contend that the transparency of the distributed blockchain ledger and the use of open-source computer code creates transparency that is more sophisticated and secure than traditional finance, but traditional finance and regulators do not tolerate the volume of fraud losses that occur on DeFi platforms. Scammers have annually stolen billions of dollars from people's crypto accounts. Some of the attacks have focused on cyber vulnerabilities in the DeFi and crypto ecosystem, but the root of the fraud

problems lies not only in pitifully lax cybersecurity but in the structure and financial incentives of the platforms and crypto intermediaries that enable frauds and market manipulation that would be pursued as criminal actions in the regulated securities markets.

Market manipulation flourishes in the DeFi and crypto space because these platforms lack accurate pricing and the price discovery that is the bedrock of traditional financial markets. Many crypto platforms and their broker-dealer intermediaries are not required to provide accurate price information across exchanges. Retail investors lack consistent and accurate pricing information. Exchanges take advantage of this by front-running their own clients to pocket the margin difference between tokens bought and sold on different platforms. Market manipulators can capitalize on the opaque pricing and price variability between tokens on different platforms to perform pump-and-dump or order-spoofing schemes to rapidly move crypto token prices and fleece smaller investors.

Widespread deceptive and misleading marketing harms retail investors: The crypto industry drives interest in its products and new tokens through relentless marketing often driven by hype cycles spurred by heavy promotion of new crypto. Retail investors are vulnerable to deceptive marketing because investors are inundated with promotional material from self-interested crypto promoters but lack sufficient information to evaluate their claims. The lack of meaningful, standardized disclosure from crypto token issuers or platform developers makes it very difficult for prospective investors to evaluate the merits and risks of any specific token. The industry has also used well-financed advertising campaigns with affinity marketing with celebrity endorsers including actors, musicians, professional sports players, and others have been paid to promote crypto assets and platforms.

While some of the most prominent examples of such promotion have focused on centralized exchanges, such as FTX,¹ DeFi platforms have also promoted support from public figures. For example, Lindsay Lohan, boxer and internet personality Jake Paul, singer-songwriter Ne-Yo, and several other public figures promoted DeFi tokens associated with Tron and BitTorrent platforms.² Crypto celebrity come-ons are often poor investments that are indistinguishable from pump-and-dump marketing schemes. A 2023 paper by Harvard and Indiana University researchers studied 35,000 tweets by 180 influencers touting more than 1,600 crypto tokens and found influencer tweets drove up prices modestly (1.8 percent) the day of the mention but that celebrity tweets were associated with 19 percent losses over the next three months.³

Federal financial regulations do not prohibit such promotions, but regulators often warn investors about the risks of basing investment decisions on the endorsement of public figures. For example, SEC investor guidance has noted that, “Celebrities who endorse an investment often do not have sufficient expertise to ensure that the investment is appropriate and in compliance with federal securities laws.”⁴

Celebrity marketing schemes can violate the law when the celebrities do not disclose that they are paid endorsers. The SEC Division of Enforcement has said publicly that “any celebrity or other individual who promotes a virtual token or coin that is a security must disclose the nature, scope, and amount of compensation received in exchange for the promotion. A failure to disclose this information is a violation of the anti-touting provisions of the federal securities laws. Persons making these endorsements may also be liable for potential violations of the anti-fraud provisions of the federal securities laws, for participating in an unregistered offer and sale of securities, and for acting as unregistered brokers.”⁵ The SEC filed charges

¹ Lyons, Giaran. “[Celebs who got burned endorsing crypto and those that got away with it](#).” *CoinTelegraph*. January 4, 2023.

² *Ibid.*

³ Senz, Kristen. “[When celebrity ‘crypto influencers’ rake in cash, investors lose big](#).” *Harvard Business Week*. April 7, 2023.

⁴ Securities and Exchange Commission. [Press release]. “[SEC statement urging caution around celebrity backed ICOs](#).” November 1, 2017.

⁵ *Ibid.*

against the celebrities that touted the Tron and BitTorrent tokens without disclosing they were paid for such promotion. Lohan Paul, Ne-Yo, and most of the other figures charged in this case ultimately settled with the SEC, without admitting or denying the SEC's allegations, and agreed to pay fees and disgorgement.⁶

Hacks, Exploits, and Theft: DeFi tokens, protocols, and platforms are rife with flaws and bugs that can be and have been exploited on a large scale to steal from or defraud DeFi investors. The multiservice crypto platform De.Fi estimated that \$1.95 billion in crypto assets on DeFi platforms were lost in 2023 due to hacks, theft, or exploits based on 448 documented cases, more than a hack per day.⁷ Only about 10 percent of these losses were recovered for investors according to the report. The nearly \$2 billion in DeFi attack losses in 2023 was dwarfed by the \$47 billion in losses in 2022, just before the crypto crash, suggesting that scammers are more active and successful, and platforms are less attentive, during bull crypto markets. Already, De.Fi has reported that the \$430 million in losses in the second quarter of 2024 doubled the losses for same period in 2023.⁸ These costly attacks include common frauds (like phishing scams that trick investors into sharing account login credentials) and cyberattacks (like bridge attacks against blockchain programs that steal assets while in transit between different blockchains) as well as scams that are unique to crypto platforms.

The DeFi platforms and crypto intermediaries have done little to protect investors from these well-known vulnerabilities. The industry should be ashamed that an ecosystem packed with software and coding experts and backed by massive computational power is unwilling or unable to adequately protect investors from cyberattacks. DeFi platforms certainly need to do more to bulk up their cybersecurity, but the critical risks are based on economic (or human) vulnerabilities. These vulnerabilities are rooted in conflicts of interest and market manipulation blind spots that are built into the platforms and crypto intermediaries' financial incentives and are well known and understood in traditional financial regulatory circles. Some common attacks include:

- **Flash loan attacks:** Scammers exploit a DeFi platform's uncollateralized loans, borrowing large amounts of crypto without upfront capital they then use to manipulate market prices or exploit bugs in smart contracts that can extract wealth from the unsuspecting investors on the other side of these trades. The traditional financial system restricts or prohibits the use of uncollateralized loans to reduce the risks of market manipulation and counter-party exposure.
- **Rug-pulls:** A DeFi token developer and related insiders push false, misleading, or incomplete information about an investment opportunity to attract investors, then use their privileged access to the project to suddenly withdraw all project funding, leaving investors holding tokens with little or no value. The traditional market provides investor disclosures that delineate details on a company's management, operation, financials and value, risks, performance and more. Companies seeking investors that falsify or fail to provide appropriate information are subject to civil or criminal charges or penalties.
- **Access Control attacks:** Hackers exploit weaknesses in smart contracts', platforms' or wallets' permission or access rights to gain access to or control of investors' funds to redirect how those funds are used or distributed. Access control and phishing scams attack vulnerabilities in the custody of who possesses an investors' crypto assets at any given moment (the investor, the platform, or another entity or actor). These custodial responsibilities are more clearly delineated in traditional finance with rules determining who can hold assets on behalf of clients, how, and when.
- **Oracle Attacks:** Hackers manipulate the programs that provide DeFi platforms with external price data (known as oracles) to feed false information into smart contracts (that can self-execute at certain price

⁶ Russell, Josh. "SEC charges eight celebrities over promotion of cryptocurrency on social media." *Courthouse News Service*. March 22, 2023.

⁷ De.Fi. "De.Fi Rekt Report: Crypto losses reach \$1.95b in 2023." December 27, 2023.

⁸ De.Fi. "CEXs are under threat? Q2 2024 De.Fi hacks a report analysis." July 11, 2024.

points), which leads to erroneous executions and financial losses. These oracle schemes exploit the lack of accurate crypto pricing information to facilitate market manipulation. In traditional securities markets, market integration systems provide more accurate price discovery across exchanges and regulators police market manipulation schemes that defraud investors and destabilizes markets.

There have been many examples of large-scale attacks and failures at DeFi exchanges. In 2023, Curve Finance, the largest decentralized exchange after Uniswap, experienced a major hack that looted between \$20 and \$40 million worth of crypto assets. Curve's native token (CRV) immediately lost about 13 percent of its value and the total value of assets locked on Curve (TVL) dropped from more than \$3 billion to about \$1.7 billion at the time of the hack.⁹ The apparent cause was a glitch in a particular version of Vyper, a programming language widely used to write DeFi smart contracts. The hackers executed a re-entrancy attack (exploiting a flaw in Vyper's re-entrancy guard code) which repeatedly withdraws funds from a smart contract and transfer them to an unauthorized contract until the funds have been exhausted.¹⁰ The hackers also exploited the Vyper vulnerability to attack other DeFi platforms, who reported losses in the tens of millions as well.¹¹

The successful hack demonstrated that DeFi self-regulation does not adequately protect investors from significant losses. This was a sophisticated cyber-attack on a protocol that had run safely for years, taking down what was considered one of the more secure actors in DeFi space. Vyper said the vulnerability was not obvious but buried in an earlier version of the program, and that it probably took a long time for the hackers to find the weakness in the code history.¹²

Market manipulation schemes like wash trading: Wash trading is a form of market manipulation where traders secretly buy and sell the same asset to themselves to artificially pump-up interest, which encourages new investors to buy the asset, boosting the asset's price and inflating the value of traders' holdings. The practice facilitates market manipulation, insider trading, money laundering, tax avoidance, and more.

Both crypto markets and DeFi markets are awash in such trading. A 2023 study by crypto market research firm Solidus Labs found that nearly 70 percent of sampled Ethereum-based decentralized exchange liquidity pools¹³ had executed wash trades that amounted to the price manipulation of nearly 20,000 crypto tokens worth \$2 billion.¹⁴ Since the study sampled only a small proportion of these DeFi liquidity pools, the true volume of these wash trades is likely to be far higher.¹⁵ More broadly, a 2022 National Bureau of Economic Research report found that illegal wash trading may account for almost three-quarters (over 70 percent) of average crypto trading volumes on unregulated exchanges.¹⁶ According to the report, "these fabricated volumes, effectively the result of firms (and exchanges) illegally trading with themselves, can amount to

⁹ Shen, Maya and Sunil Jagtiani. "Crypto token of key DeFi exchange Curve Finance sinks after exploit." *Bloomberg*. July 30, 2023.

¹⁰ White, Molly. "Bug in Vyper smart contract language enables multiple exploits on Curve and related projects." *Web3IsGoingGreat.Com*. July 30, 2023.

¹¹ Melinek, Jacquelyn. "Curve Finance's \$62M exploit exposes larger issues for DeFi ecosystem." *TechCrunch*. August 1, 2023.

¹² McGleenon, Brian. "Curve Finance exploit has 'shaken confidence in DeFi.'" *The Block*. July 31, 2023.

¹³ Crypto defi liquidity pools allow crypto investors to earn passive income on cryptocurrencies. They typically do this allowing a crypto investor to set up a DeFi platform account, connect a wallet to that account, and put two different types of crypto tokens in that platform's tool to form a trading pair. A smart contract (serving as an automated market maker) then manages the trading of those tokens on DEX, without use of a centralized order book or traditional market maker. These automated pools were set up on DeFi platforms to theoretically make trading faster and cheaper.

However, this and other factors also make it very easy to set up wash trading on DeFi platforms.

¹⁴ Solidus Labs. "DEX Liquidity Providers Have Wash Traded More Than \$2 Billion to Date." 2023.

¹⁵ Khariif, Olga. "Wash trading is rampant on decentralized crypto exchanges." *Bloomberg*, September 12, 2023.

¹⁶ McAughty, Laurie. "Illegal wash trading accounts for up to 70% of crypto volumes, finds study." *The Trade*. January 19, 2023.

trillions of dollars annually. The fraudulent practice can offer a false impression of liquidity, resulting in an improved (but inaccurate) exchange ranking, as well as temporarily distorting prices.¹⁷

Such widespread wash trading market manipulation means these markets may never operate in a sufficiently fair and transparent manner. Bigger crypto players can execute large-scale wash trades that can distort prices and causes losses for smaller investors due to market instability. The large volume and share of wash trading also undermines the industry's claims that there is broad organic demand for crypto products and services. Crypto and DeFi industry voices argue about who's responsible for detecting and preventing wash trading,¹⁷ but the Commodities Exchange Act, the Securities Act of 1933, and Securities Exchange Act of 1934 already ban, restrict, or prosecute wash trading within the markets they regulate.¹⁸

DeFi platforms facilitate illicit finance: Crypto plays an outsized role facilitating illicit finance that harms individuals and communities in the United States and around the world. The anonymity, portability, and cross-border nature of crypto transactions have been used by a range of criminal enterprises to hide and launder their illegal earnings. The link between crypto and illegal finance is well known, but DeFi platforms can play unique roles in illicit finance. DeFi platforms' cybersecurity challenges make them vulnerable to money launderers who hack into their smart protocols to launder crypto associated with illicit activities.¹⁹

The way in which decentralized crypto exchanges operate allow criminals to avoid the compliance controls and practices and administrative oversight that are typically found within traditional finance and on some, though by far not all, centralized crypto exchanges. The crypto analytics firm Elliptic stated that crypto money launders use decentralized exchanges because they "can offer criminals the advantage of bypassing compliance controls – much in the manner of dealing with non-compliant exchanges like SUEX, Chatex or BTC-e. Simultaneously offering another advantage, they lack a central administrator with active oversight of user accounts, records, identities or activities."²⁰ And decentralized crypto intermediaries and apps, like mixers that direct asset transfers between wallets to obscure transaction trails, can facilitate illicit finance as well. The Tomado Cash decentralized application that mixes transactions stemming from the Ethereum and other DeFi blockchains has been found to have facilitated money laundering, including the 2022 Ronin Bridge hack of \$540 million that was attributed to North Korea's Lazarus Group.²¹ Despite recent enforcement actions against Tomado Cash,²² the widespread instances of DeFi platforms or applications skirting or failing to adhere to anti-money laundering requirements, remain.

III. Decentralized finance isn't decentralized: highly consolidated control without safeguards poses risks for investors.

The decentralized finance model has not freed people from the shackles of financial intermediaries; it has merely created a new concentrated set of crypto financial intermediaries and infrastructure that controls the access to and governing rules of these crypto platforms. Crypto platforms, including so-called DeFi platforms, demonstrate high degrees of concentration or centralization. The emergence of centralized crypto and DeFi platforms is partially rooted in the infrastructure that undergirds blockchain platforms, but it also grew out of the trading platforms amassing market power that reinforces scale and consolidation.

¹⁷ Reguerra, Ezra. "70% of unregulated exchange transactions are wash trading: NBER study." *CoinTelegraph*. December 28, 2022.

¹⁸ Lin William Cong, et. al. National Bureau of Economic Research. "Crypto Wash Trading." Working Paper 30783. December 2022;

Dever, Joseph and John W. R. Murray. "Market Manipulation Investigations." *SEC Compliance and Enforcement Answer Book*. Chapter 16, 2021 Edition.

¹⁹ Carlisle, David. Elliptic. "Money laundering through DEXs and mixers." May 12, 2022.

²⁰ *Ibid*.

²¹ *Ibid*.

²² Khalili, Joel. "Tomado Cash developer found guilty of laundering \$1.2 billion of crypto." *Wired*. May 14, 2024.

The purported benefits of decentralization and democratization of crypto finance are not currently realized in these markets and may become more remote as platforms and emerging intermediaries with market power push out smaller rivals and new entrants and further consolidate the market. As a result, the retail crypto investors are left with all the risks of decentralization (lower transparency, imperfect price discovery, and higher risk of fraud and manipulation) but nonetheless are forced to participate in markets that are effectively consolidated, centralized, and intermediated, without the protections found in tradition finance.

There are several ways in which the concentration and consolidation present in the DeFi sector today can be identified, including: concentration of verification and validation processes; concentration of platform governance control, and economic concentration of intermediate actors. Each of these elements has the potential to introduce risks that can harm DeFi investors.

Concentration of verification and validation: Crypto assets and platforms rely on a distributed process for validating and verifying transactions, but these critical functions are already controlled by a handful of players in the most well-known and widely traded tokens and platforms. High levels of concentration can exacerbate the risks such as market manipulation, cybersecurity concerns, extractive economic models, and stability risks, just as in traditional finance.

The most widely understood consensus verification mechanism involves crypto-mining using proof-of-work verification methods. Crypto miners operating nodes amongst the distributed blockchain network compete to verify the proposed transactions on that platform by racing to solve complex mathematical problems using computational power. The mining operation that solves the problem first wins the right to verify the block and is financially rewarded with crypto assets in return. This verification process is primarily used within the Bitcoin (BTC) blockchain, which accounts for a large portion of the overall volume and market share of crypto markets. Other tokens rely on proof-of-work verification mechanism as well, including Dogecoin, Monero and ZCash.²³

DeFi platforms primarily utilize a proof-of-stake verification mechanism. Token holders' essentially put up their tokens to collateralize their stake in exchange for taking responsibility for validating and verifying a block of transactions. The DeFi platform protocols select stakers in a random process to verify a block and the stakers are financially rewarded for doing so (often by accruing some interest on their staked tokens). In practice, those who have more tokens and can stake more as collateral for verification often receive more opportunities to verify transactions and earn more yield, which leads to concentration in control of validation processes and staking pools.

These processes not only create financial incentives for individuals to participate in crypto-related activity but are meant to guard against attempts to manipulate, hijack, or misappropriate crypto transactions. Theoretically, assets based on computer code can be easily copied and shared, and these risks are higher without a central intermediary to police fraudulent transactions. Crypto and DeFi platforms seek to guard against this through the use of distributed ledger technology which provides a shared copy of the information contained on the blockchain to everyone on the network. This enables network users to spot efforts to alter information in one version of the database that was not reflected in other copies.

Additionally, these consensus-based verification mechanisms are meant to ensure one miner or a small group of validators cannot unilaterally determine which block is validated or alter the code. In theory, a miner would need to control a majority of the network nodes to take unilateral actions, and achieving such control would be costly and expensive. And since other miners are competing for the same chance to validate a transaction for economic reward, competition should ensure that no one actor achieves too much control.

²³ "PoW Cryptos: Mineable coins using the proof of work (PoW) consensus algorithm to generate new blocks on the blockchain." *CryptoSlate*. Accessed September 2024.

These theoretical safeguards against consolidation have not prevented considerable market consolidation that can pose risks to investors. The mining and validation activity that undergirds crypto tokens and transactions is highly concentrated and many of the most widely traded tokens are dominated by a handful of players. In 2023, only two mining pools controlled more than half (51 percent) of the Bitcoin networks' proof-of-work computational power (known as a hash rate) and there are similar levels of concentration on other chains.²⁴ There is also high levels of concentration in the validation of the Ethereum blockchain that is the basis for a wide range of decentralized tokens, platforms, and apps. In 2024, S&P Global analysts noted that validator concentration on the Ethereum network is already high. The three largest Ethereum validators controlled more than half of the Ethereum staking activity: Lido held 33 percent, Coinbase held 15 percent, and Binance held 4 percent.²⁵ These levels of concentration in Bitcoin and Ethereum are already high enough to facilitate market manipulation and pose risks to investors.

The concentration problem likely goes deeper. In 2022, Trail of Bits, a New York-based firm that provides security assessments and advisory services to major information technology companies, assessed the decentralization of platforms like Bitcoin and Ethereum for the Defense Advanced Research Projects Agency (DARPA).

Its report found that these two platforms were vulnerable to exploits that took advantage of their chain's other properties (including their implementation approaches, networks, and consensus protocols). These risks existed despite finding that Bitcoin and Ethereum had robust cryptographic tools used to secure blockchain's immutability (a feature which helps promote decentralization). The report determined that the number of entities²⁶ sufficient to disrupt a blockchain is relatively low: four for Bitcoin, two for Ethereum, and less than a dozen for most PoS (Proof of Stake) networks.²⁷

The report also found that a "dense, possibly non-scale free, subnetwork of Bitcoin nodes appears to be largely responsible for reaching consensus and communicating with miners — the vast majority of nodes do not meaningfully contribute to the health of the network." This means that most of the participants in the Bitcoin network aren't actively engaged in the work necessary to verify transactions, and that instead a small group of actors are effectively directing the activity of miners. To most observers, this suggests a significant degree of centralization.

Concentration of ownership and control of platforms that are purportedly decentralized: Many DeFi platforms are effectively controlled by a handful of firms or wealthy investors, not broadly governed by autonomous, democratic users. The decentralized governance of DeFi platforms are maintained and operated by decentralized autonomous organizations (DAOs). Just as distributed ledgers combined with consensus verification mechanisms are meant to ensure crypto transactions can occur without trusting an intermediary to provide transactional security, DAOs are meant to allow users to control and direct the protocols on DeFi blockchain as well as the administration and maintenance of them, without reliance on centralized oversight.

DAOs are often presented as a more equitable or democratic way of distributing governance over the financial system compared to tradition finance, where powerful banks, brokers, or exchanges control access to transactions. Theoretically, DAOs allow each user to have a say in how their platform is governed. But DAOs are largely controlled by a small number of firms or individuals that hold the governance tokens that

²⁴ Radmilac, Andjela. "The centralization of Bitcoin: Behind the two mining pools controlling 51% of the global hash rate." *CryptoSlate*. January 1, 2023.

²⁵ Reynolds, Sam. "S&P Global Just Made Ethereum's Centralization Risk a TradFi Concern." *CoinDesk*. February 22, 2024.

²⁶ Entities can be understood as firms, mining, or validator pools, as well as other conglomerate actors.

²⁷ Evan Sultanik, et. al. Trail of Bits. "Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers." June 2022.

direct the operation of DeFi platforms, including which assets are available for trade, how trades or transactions are executed, and many other aspects of the platform's administration or management.

A 2022 Chainalysis report found that less than 1 percent of platform users controlled 90 percent of the governance token voting power across ten major DAOs. In some DAOs, less than 0.2 percent of users controlled more than 90 percent of the governance tokens. The report concluded that “this has meaningful implications for DAO governance. For example, if just a fraction of the top 1% of holders coordinated, they could theoretically outvote the remaining 99% on any decision.”²⁸

A 2024 University of Pennsylvania-Boston University working paper found that voting power was highly concentrated within the DAOs for four different DeFi platforms (Uniswap, Compound, Aave and Lido). The study found that in all four platforms that voting power was so highly concentrated that “if the top three voting stakeholders agree, their preference will win out.”²⁹ The paper also documented that major venture capital firms such as a16z, Polychain, and Bain Capital were some of the largest voters in DAO decisions and controlled enough tokens to create a quorum and influence the outcome of these votes.³⁰ Many crypto enterprises, including DeFi, secure much of their initial seed money from venture capital and private equity firms, who receive large shares of tokens in return for their investments — both governance tokens as well as other assets.

The concentration of DAO governance token voting power allows the most powerful users (or investors) to control the operations and terms of the DeFi platform to their own benefit, sometimes at the expense of smaller retail investors. As in traditional finance, these firms have significant financial resources that enable them to pursue riskier investments, take on greater leverage or debt, and absorb larger losses, than retail investors. As a result, these platforms replicate a system of centralized financial intermediaries similar to what exists today and not a more democratized financial ecosystem that enables smaller investors to chart their own course to pursue wealth creation on a more level playing field.

Concentrated infrastructure impedes or even precludes real decentralization: DeFi, like the broader crypto industry, is reliant on existing digital infrastructure — both hardware and software — to maintain its operations. Since aspects of that infrastructure are highly centralized, even decentralized crypto platforms are vulnerable to operational or cybersecurity risks stemming from such centralization. The Trail of Bits report identified several such vulnerabilities, including:

- The Ethereum ecosystem has a significant amount of code reuse: 90 percent of recently deployed Ethereum smart contracts are at least 56 percent similar to each other;
- Every widely used blockchain has a privileged set of entities that can modify the semantics (e.g., software language) of a blockchain to potentially change past transactions;³¹
- Bitcoin traffic is unencrypted — any third party on the network route between nodes (e.g., ISPs, Wi-Fi access point operators, or governments) can observe and choose to drop any messages they wish; and

²⁸ Chainalysis Team. “Exploring DAOs: Uncovering Web3 Ownership Realities.” Chainalysis. June 27, 2022.

²⁹ Brett Falk, et. al. “Governance of Decentralized Autonomous Organizations: Voter characteristics, engagement and power concentration.” ArXiv:2407.10945v1 [cs.CY]. 15 July 2024; Brett Falk, et. al. “Blockchain Governance: An Empirical Analysis of User Engagement on DAOs.” ArXiv:2407.10945v1 [cs.CY]. 15 July 2024.

³⁰ *Ibid.*

³¹ Semantics here refers to the computer language of smart contracts built on top of or within blockchain platforms, as well as the common computer language used by these platforms to “talk” to one another as well as integrate data and information from the broader world wide web. This is relevant to a core theme and concern regarding crypto in general, interoperability — the extent to which blockchain based assets, programs, and actors can easily and consistently work with or across platforms.

- More than half (60 percent) of all Bitcoin traffic traverses through just three ISPs for extended periods of time.³²

These and other infrastructure-related points of concentration raise concerns about manipulation, fraud, cybersecurity, and other issues. And they are a reminder that even if decentralization within DeFi exchanges and markets might someday be achieved or clearly understood, these mechanisms are still entangled with a highly centralized set of actors and mechanisms which could undermine whatever purported benefit such decentralization proffers.

Concentration of economic actors and incentives undermines decentralization: The economic concentration, financial incentives, and interconnection with other concentrated and centralized crypto segments creates centralized conditions and intermediaries that are similar to or the same as those that exist in traditional finance. Even if DeFi platforms could demonstrate the technological capacity to create a meaningful degree of decentralization that could be sufficiently sustainable, secure and scalable to generate benefits the industry claims would arise from such decentralization, while ameliorating the technological risks, the underlying economics of DeFi platforms foster or even require concentration that makes the decentralization objective very difficult to attain.

DeFi is already significantly enmeshed with centralized crypto exchanges. A 2021 Bank of International Settlements report entitled “DeFi risks and the decentralisation illusion” notes that “DeFi has integral connections to centralised crypto-asset trading, lending and borrowing platforms, through which participants exchange crypto-assets for one another or for fiat currency, often using stablecoins.”³³ This fundamental reality undermines the contention by some DeFi promoters that these platforms stand apart from the centralized crypto exchanges (including suggesting that DeFi platforms offered a refuge from the instability of the FTX collapse that DeFi proponents blamed, in part, on centralization).

This significant interconnection between DeFi and centralized crypto exchanges was borne out by the 2022 crypto crash. Prior to the crash, major centralized platforms such as FTX and Celsius held themselves out as safe places for investors to put their money when compared to the Wild West of DeFi. They also offered their customers extremely attractive returns on their investments. Celsius promoted annual returns as high as 18 percent annually.³⁴ However, to generate these returns, both centralized trading platforms and their affiliates pursued investments — in many cases using customer funds directly or as collateral — in the DeFi space.³⁵ They did so in part to take advantage DeFi’s volatility and growth, creating the opportunity for huge returns on arbitrage, as well the fact that much of the DeFi industry was operating outside of or on the edges of existing regulatory oversight.

DeFi platforms rely on interconnected crypto assets to promote liquidity. DeFi platform users frequently use stablecoins (cryptocurrencies backed by stable assets, frequently pegged to government currencies) to facilitate trading activities on their platforms (as do centralized exchanges). Sometimes referred to as poker chips for crypto casinos, stablecoins allow crypto traders to more easily buy and sell crypto assets at stable

³² A note on Bitcoin: industry experts and observers have disagreements about whether Bitcoin and its blockchain should or should not be understood as “decentralized finance”, with some saying Bitcoin is the original version of such, and others saying it’s more complicated (leaving aside the question of to what extent Bitcoin is decentralized, full stop). The conventional way of making a distinction between the two is that Bitcoin was originally designed as an asset, or currency, while DeFi technology is more focused on programs and services built to facilitate trade in various crypto assets. That said, Bitcoin the asset and its underlying blockchain have been used as the basis for a variety of DeFi tools, synthetic assets, and other services. So, it is fair to say that there are interlinkages between Bitcoin, its network, and DeFi, even as they occupy distinct spaces within the broader crypto ecosystem.

³³ Sirio Aramonte, et. al. “DeFi risks and the decentralization illusion.” *BIS Quarterly Review*: December 2021.

³⁴ Pontem Network. “The Celsius Crash: Explained.” *Medium*. August 15, 2022.

³⁵ Hannah Lang, et. al. “Focus: How crypto lender Celsius stumbled on risky bank-like investments.” *Reuters*. June 15, 2022; Crunchbase Profile. “Alameda Research.” Accessed August 3, 2023.

prices. The DeFi industry's use of stablecoins reduces the risks associated with price volatility and makes trading much more certain and more profitable on the platform. The most prominent stablecoins are inherently centralized; there is one issuer that sells stablecoins to buyers in exchange for promising buyers that their coins are backed by collateral comprised by stable assets that they or a custodian hold on their behalf.

The assets backing stablecoins are in turn often issued by a centralized entity. The most widely used stablecoin, Tether, is likely backed by more traditional non-crypto assets (though Tether has a record of making misleading statements about its reserve assets,³⁶ failing to hold sufficient reserves,³⁷ or providing consumers with a truly independent audit³⁸). USDC, the next largest stablecoin by market share, is largely collateralized by U.S. government issued or backed assets, such as cash, repurchase agreements, or Treasury securities.³⁹

While some crypto die-hards point to stablecoins that are backed by other crypto assets or even algorithms as proof that DeFi platforms can rely on native crypto tools as collateral instead government issued assets, most of those coins have struggled or failed to maintain their price peg,⁴⁰ most infamously in the case of Terra/Luna, which was an algorithmic stablecoin used as the basis for trading on Terra's large and prominent DeFi platform.⁴¹ Even the DAI stablecoin, an algorithmic coin issued by MakerDAO, which seeks to use crypto assets and other crypto instruments to back its coin, has at various points had half or more of its reserves based on U.S. Treasuries at 50% or more at various points.⁴²

These examples show that DeFi platforms depend on centralized crypto exchanges and traditional finance for stability and for injections of investors capital, which makes them significantly interlinked with centralized exchanges and entities. In return, DeFi platforms have become yet another form of shadow banking, where investors seek liquidity and high rates of return, without pesky financial regulatory oversight meant to guard against manipulation, fraud, or instability.⁴³

Renting seeking and consolidation: DeFi transactions are far from frictionless, despite the proponents' claims that protocols and blockchain technology can replace central intermediaries to speed and simplify access to markets. DeFi transactions require intermediation, and the intermediaries involved consolidate control over these networks and profit financially from their control — which can lead to economic concentration and centralization. For example, a 2024 New York Federal Reserve Bank study examining arbitrage activity on the Ethereum network found that entities that control critical links in the network seek consolidation to maximize their own profits, which may come at the detriment of smaller retail investors.

Blockchain transactions are often not truly instantaneous; instead, transactions and other interactions are actually batched together in blocks to be validated en masse. These conditions give rise to two sets of intermediaries: block builders, who consolidate batches of transactions to be validated, and proposers (also understood as validators) who are randomly selected to propose a block be added to the chain.

³⁶ Commodity Futures Trading Commission. "[CFTC Orders Tether and Bitfinex to Pay Fines Totaling \\$42.5 Million](#)." Release Number 8450-21. October 21, 2021.

³⁷ Office of New York Attorney General Letitia James. "[Consumer Alert: Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities in New York](#)." February 23, 2021.

³⁸ Protos Staff. "[A decade without an audit, Tether says it's a new business](#)." *Protos*. April 18, 2024.

³⁹ [USDC Reserve Report](#), July 2024. Accessed September 8, 2024.

⁴⁰ Anneke Kosse, et. al. "Will the real stablecoin please stand up?" BIS Papers, No 141. November 2023.

⁴¹ Jiageng Liu, et. al. "[Anatomy of a Run: The Terra Luna Crash](#)." Harvard Law School Forum on Corporate Governance. May 22, 2023.

⁴² S&P Global Ratings. "[Stablecoin Stability Assessment: Dai](#)." Dec 12, 2023.

⁴³ Allen, Hilary J. "[DeFi: Shadow Banking 2.0?](#)" *William & Mary Law Review*, Vol. 64, No. 4. March 2023.

Conventional crypto transactions are broadcast directly to the network for other participants to see, but the Fed's study showed that traders, seeking to keep their trades private to protect their price arbitrage advantage, will send their trades directly to a builder instead, concealing the order within the bundle of other transactions. These builders are financially compensated by traders for their efforts, which creates an incentive for builders to secure more business from traders to generate more profit. On the other side of the equation, proposers/validators secure the right to validate transactions based on the number of tokens they've staked or are staked in the pools they control. More staked tokens gives them more opportunities to validate blocks and benefit financially.

The result is high degrees of concentration. The Fed report found that, "Of the 167 known block builders, over half of all builder revenue and blocks proposed is captured by three builders. Similarly, out of more than 150,000 proposers, the top five staking pools or exchanges account for more than 50 percent of proposer revenue and blocks added to the chain."⁴⁴

The main takeaway from the New York Fed report is that intermediaries are deeply embedded into DeFi platforms, and these entities often decide whose transactions get processed, when, how, and at what expense. The intermediaries are paid well for that service and end up controlling a great deal of the market activity on DeFi networks. This can create conflicts of interest, exploitation, and market instability, which is why regulated markets require intermediaries to abide by a wide range of rules and regulations to mitigate those risks and harms.

DeFi adherents contend that its technology is supposed to eliminate or greatly reduce the need for intermediation, and thus reduce the need for intervention by government regulation and oversight. Instead, the blockchain and the computer programs and protocols governing should largely suffice. But since DeFi has recreated a similar set of intermediaries, performing similar activities, with similar incentives and conflicts of interests, the same market rules and regulatory oversight should apply to DeFi.

IV. Existing financial regulatory standards can and should apply to DeFi.

DeFi platforms are already operating as financial intermediaries. Billions of dollars' worth of crypto assets are being traded and exchanged on DeFi platforms around the world. In many cases, DeFi exchanges provide services or products similar to or the same as the existing financial system — including issuing assets that are arguably securities or facilitating sale of such securities. While there is more to learn about DeFi, including the potential risks and harms this sector poses to investors and financial markets, the known harms and risks largely mirror problems in traditional finance justify regulators using their existing tools and authority to ensure entities and individuals operating within the DeFi ecosystem are complying with financial regulatory safeguards to protect investors and the market.

International regulatory bodies and experts agree this is the best course of action. BIS experts concluded in their 2021 paper on DeFi that, "Since the main challenges in DeFi resemble those in traditional finance, established regulatory principles can serve as a compass. The basic tenet, 'same risks, same rules' should apply, not least to counter regulatory arbitrage."⁴⁵ BIS recommended that policy makers apply a range of principles and approaches within existing regulatory frameworks to DeFi, including bank regulation and supervision, securities regulation with respect to funds' prudential framework, international risk management standards for payments, market integrity principles, and protocols to combat illicit finance.

The U.S. Financial Stability Board made similar a similar set of recommendations in 2023, including that regulators should enforce compliance with existing regulations because DeFi platforms present similar risks

⁴⁴ Pablo D. Azar, et. al. "[The DeFi Intermediation Chain](#)," *Liberty Street Economics*. August 5, 2024.

⁴⁵ Sirio Aramonte, et. al. "[DeFi risks and the decentralization illusion](#)," *BIS Quarterly Review*. December 2021.

and activities as traditional financial platforms and that regulators should consider developing additional regulatory requirements if and when DeFi activities are determined to fall outside of their existing scope.⁴⁶

Both institutions noted that since DeFi has not had deep interconnections with traditional finance to date, the challenges in DeFi have had limited impact on traditional finance. However, should the two spaces become more interconnected, the application of consistent regulatory standards across industries and jurisdictions would be even more important to guard against market instability and regulatory arbitrage.

Yet, there is consistent resistance from many DeFi firms and adherents to comply with existing financial regulatory law. While some of this resistance is couched in practical terms, much of it is ideological:

- Erik Voorhees, CEO of the DeFi firm Shapeshift, and seen by many as a crypto pioneer, has said that DeFi protocols do not need regulatory clarity or permission to operate and there is very little governments can do to interfere, noting that governments “can write whatever laws they want. The protocols keep working regardless... That is immensely powerful.”⁴⁷
- Puja Ohlaver, a lawyer and strategy counsel for Flashbots, a DeFi focused research and development firm, was interviewed on the Unchained podcast and said that “the whole, sort of, premise and justification for crypto is decentralization, right, it’s what protects it from being regulated by, you know, antitrust and also securities regulation.”⁴⁸
- Kain Warwick, the founder of Synthetix, a DeFi protocol that facilitates crypto derivatives trading, shared a similar view while speaking on the Bankless podcast: “When you look at what a DAO enables, you have the ability to kind of transcend any one regulatory jurisdiction or like any legal structure.”⁴⁹

Fundamentally, the crypto and DeFi ecosystems mirror the traditional financial industry. The DeFi and crypto industry offers similar services to the financial industry, have comparably high levels of concentration and intermediation, and suffer nearly identical investor protection and market manipulation problems. The DeFi industry’s argument for decentralization appears more like a rationalization for regulatory evasion than it does for democratizing or transforming finance.

Unfortunately, some Members of Congress have bought into the industry’s deregulatory strategy, by advancing legislation that would likely radically alter and weaken existing financial regulatory safeguards, based on the premise that decentralized finance — whatever it may be — is an “innovation” that merits a rewrite of decades of financial markets laws, rules and regulations. This is misguided at best, and reckless at worst.

For example, the FITT 21 Act (H.R. 4763) which the House passed this year, provides a safe harbor for various DeFi developers and intermediaries that exempts them from regulatory oversight (other than authorizing two DeFi studies). The legislation also includes a definition of a “decentralized network” that is used in part to determine both the nature of a digital asset, its issuer, and the intermediaries interacting with it — in essence using decentralization to determine which financial rules do and don’t apply to large portions of the crypto industry and which protections investors do or don’t receive. This decentralization definitional standard is worrisome. Industry, academic, and regulatory experts have failed to develop a concise definition

⁴⁶ Financial Stability Board. “[The Financial Stability Risks of Decentralised Finance](#),” 16 February 2023.

⁴⁷ Jafri, Assad. “[Crypto OG Erik Voorhees believes DeFi has already solved the regulatory clarity problem for altcoins](#),” CryptoSlate. July 1, 2023.

⁴⁸ Unchained Podcast. “[How Soulbound Tokens Could Reduce Speculation and Improve DAO Voting](#),” Episode 360. June 7, 2022.

⁴⁹ Bankless Podcast. “[How DAOs Will Change Everything](#),” August 18, 2021.

of decentralization for DeFi (as expressed in a recent CFTC Subcommittee report⁵⁰) let alone agree that the DeFi industry has achieved it. The FIT 21 definition and regulatory carve outs allow the DeFi industry to operate outside of existing financial regulatory frameworks or within friendly safe harbors despite causing clear risks and harms to investors. As Professor Hilary J. Allen, a noted expert on financial stability and fintech, and a member of the CFTC's Digital Asset Subcommittee observed, “developing accommodative, bespoke regulatory treatment like waivers and sandboxes that would effectively roll back regulations designed to protect the public from harm.”⁵¹

The DeFi ecosystem poses real risks to investors today that would be greatly reduced or largely prevented if the industry were subject to existing financial market regulations to promote fair markets and protect investors from fraud and market manipulation. We know enough about DeFi as it stands for regulators to take or continue to take action to protect investors and consumers from the risks and harms present in the sector, and to ensure actors in the DeFi industry do their part to adhere to robust and effective regulatory standards and comply with the law.

Thank you for your time and attention today. I look forward to the Committee members' questions and continued engagement on these issues.

⁵⁰ “[Decentralized Finance](#), Report of the Subcommittee on Digital Assets and Blockchain Technology, Technology Advisory Committee (TAC) of the U.S. Commodity Futures Trading Commission, January 2024.

⁵¹ Allen, Hilary J. “[TAC Meeting Statement](#),” January 8, 2024.

Chairman HILL. Thank you, Mr. Hays.

We will now turn to member questions, and I recognize myself for 5 minutes.

I spoke earlier about how our regulatory and legal frameworks were designed for a financial system with centralized entities. Because of this, it can be challenging to apply the approach of same risk, same regulation to DeFi due to its permissionless peer-to-peer nature. I think our witnesses all have done an excellent job talking about that concern or opportunity and the cost and benefits, but nothing is without risk. Current rules and regulations were established to address specific risks, and they are not the same between traditional finance and DeFi.

Ms. Tuminelli, what are the potential risks regulators should be focused on when they think about DeFi?

Ms. TUMINELLI. Thank you for that question.

As you suggested, the inherent risks in the traditional financial system are related to intermediaries. They are often opaque. We do not know what is going on, and they are often discriminatory or subject to human bias or subjective error.

In DeFi, the risks are more related to the actual technology, so like vulnerabilities in code, or consumer protection and education, making sure that people understand what a DeFi protocol does, how it is self-hosted while it works.

Of course, illicit finance is a risk in every system. It is just that the way we deal with illicit finance in DeFi has to be different than the way we address that risk.

Chairman HILL. Right. You recognize that we have to solve for that equation, which is how we do the authentication and protect against bad actors in DeFi.

Do we have the ability—when you think about it, are we not very vulnerable from a cyber point of view? I am not a big Cybersecurity and Infrastructure Security Agency (CISA) fan. I know they have that responsibility, but I think there are a lot of vulnerabilities inside our cyber system in our country, no greater risk than the U.S., which is why I do not support big—more U.S. data bases being created. They are just bigger targets.

How do you—what is the best way to do that for consumer protection from being hacked, their wallet, their protocol? I do agree that is one of most inherent risks compared to an intermediated risk of a capital failure or an error made by not doing the CrowdStrike patch in your system. We know those risks but talk about how you avoid that hack issue if you are in a decentralized finance environment.

Ms. TUMINELLI. I think, as you flagged, there is a big difference between a cybersecurity risk and a risk on the actual blockchain layer with the technology itself.

With cybersecurity risks, those are often unlocalized to one person or a small group of identifiable people, and we know what to do with cybersecurity risks. For years we have been navigating—

Chairman HILL. We are not very good at it, though, are we?

Ms. TUMINELLI. Well, the industry has created actually a number of crypto Information Sharing and Analysis Centers (ISACs) that specialize in this exactly. They jump in if there is an ongoing exploit or hack and try to assist in returning victim funds.

To get to your other point on consumer education and protection, the industry has also come up with solutions for that, and a number of front ends have actually built into the front end software fraud alerts, scam alerts so that a person can be protected on the front end.

Chairman HILL. Good.

Let me stick with our discussion but switch over to the commission now, and they proposed a new rule that broadly expands the definition of an exchange. I would like your views and Mr. Van Valkenburgh's, too, on this to capture not just decentralized digital asset platforms but also DeFi.

Pretty broad. I was telling Mr. Lynch things are not very well-defined here, and so it seems to be a pretty massive overreach, over-definition by the commission.

How should DeFi think about this exchange function? Like, one of the key functions of an exchange in an intermediate system is market making in a bond or a stock to aid in that matching for pricing purposes. I get both of your points, but I would like both of your comments on this.

The Gensler approach, what is wrong with it and what a better approach is? You have 25 seconds, I will give you 25 seconds. Go.

Ms. TUMINELLI. I would say that the very first problem is that the SEC has still never defined what a crypto asset security is, which is a precursor to this entire discussion.

With the exchange rulemaking, they have swept extremely broadly to catch developers and protocols that have no ability to comply with the rule as they have proposed.

Chairman HILL. Very helpful.

Mr. Van Valkenburgh.

Mr. VAN VALKENBURGH. The only thing I would add to that excellent answer is the SEC swept so broadly in its Exchange Act rulemaking that it has run right into the First Amendment of the Constitution, and it is not the first time. They got slapped down in SEC vs. Lowe for being overzealous in their enforcement of the Investment Advisor Act and regulating mere publishers of newsletters.

In the Exchange Act, they want to regulate people who, quote, make available a communications protocol. If making available a protocol, which is a set of rules, is not publishing speech, then I do not know what is.

Chairman HILL. Thank you, sir. My time has expired.

I turn to the ranking member for his 5 minutes of questions.

Mr. LYNCH. Thank you, Mr. Chairman.

Mr. Hays, recently the multiservice crypto platform DeFi estimated that almost \$2 billion in crypto assets on DeFi platforms were lost back in 2023 due to hacks, theft, or exploits based on they had 448 documented cases, more than a hack per day and only about 10 percent of these losses were recovered from investors, according to the report.

The nearly \$2 billion in DeFi attack losses in 2023 was dwarfed by the 47 billion that was lost in 2022. If you look at the traditional finance system, the Bank Secrecy Act, our money laundering protocols all resulted because we had crises in the industry, and we needed to take steps.

I mean, you can even look at the collapse of the banking industry during the Depression. We lost—over 1,000 banks went down. We had to come in with regulations to say, okay, we are going to have deposit insurance. We created the Federal Deposit Insurance Corporation (FDIC).

What about this argument that we do not need any intermediaries and all this theft and fraud continues to occur? What would bad actors benefit from if, per se, we do not employ Know Your Customer or anti-money-laundering protocols connected to DeFi?

Mr. HAYS. Thank you for the question, Congressman.

I think you are right to be concerned. That is a large volume of loss that is affecting consumers who are already engaging in these practices whether or not we truly understand what DeFi is or whether decentralization has been achieved.

I think the problem goes deeper, and I want to stress there is a focus on the role in which cybersecurity and the technology of these platforms facilitate some of these problems. Arguably, there is almost always a human component behind it, and the problems that arise have parallels in our current financial system and the economics of finance, which we already have addressed or at least are addressing with the regulatory structures today.

For example, many hacks are inside jobs. They are set up by the actual people involved. Rug pulls are ubiquitous, and rug pulls involve insiders that are dictating how code is written and promoting tokens or products that draw in investors with little knowledge of those products.

More disclosure, more information, such as the things found in securities regulation, would help those investors have a better understanding of who is behind the products, how they are operating them, what they are offering, what their background is but that does not exist in this space today. White papers are not standardized. People have to read code. It is a real problem.

Oracle attacks are manipulation of real-world price data. That is something that goes through DeFi interfaces, but someone designs that interface and determines how the Oracle goes in there.

With money laundering, I think the problem is there is a conundrum: If you allow DeFi to operate without the same consistent Know Your Customer (KYC) controls, money launderers look for gaps in the broader financial system. They are looking for weaknesses. They are looking for lowest common denominator spots so that they can exploit.

This committee knows full well that some of the anti-money-laundering measures that were passed in the early 2000s, or different financial professionals, were just recently, after 20 years, implemented by Treasury because of massive resistance in the industry. That was a massive gap in that framework.

So, if we allow that gap to continue in DeFi, we are essentially laying, setting a table for money launderers to continue to exploit those gaps in ways that harm lots of people. So there are ways to look at how we can tweak those things, but the bottom line is if those rules are not consistent, you are going to damage the entire approach to combating illicit finance, and that is going to harm a lot of people.

Mr. LYNCH. There is much said about the decentralization in DeFi. Is that actually the case? I mean, we have studies here that say there is a narrow group of people that actually control this and it is not—it does not have the full benefits of decentralization. Is that what you have found?

Mr. HAYS. The research we have seen suggests that, and much of that is industry research or outside observers. I think it raises a question, if decentralization cannot be defined and cannot be realized, then it cannot provide the benefits it offers.

So I think, before we rush into allowing these actors to sort of have full access to the financial system, particularly if it becomes interconnected with the broader financial system, which is starting to happen, I think we should take a precautionary approach and that includes regulators reining in some of this activity before it can cause more amplified harm.

Mr. LYNCH. Thank you.

Mr. Chairman, I yield back.

Chairman HILL. The gentleman yields back.

The gentleman from Oklahoma, Mr. Lucas, is recognized for 5 minutes.

Mr. LUCAS. Thank you, Mr. Chairman, for holding this hearing, and thank you to our witnesses for testifying today.

First, I think it would be helpful to step back and appreciate where decentralized finance fits into the larger conversation around digital assets, blockchain technology, it does not matter, the future of the internet.

Ms. Rettig, starting broadly with Web3, could you discuss how blockchain technology enables decentralized digital ownership and could you highlight some of the use cases beyond DeFi?

Ms. RETTIG. Thank you very much for your question, Congressman.

As I noted in my oral testimony, DeFi protocols are deployed onto permissionless blockchain networks. On a network like Ethereum, there are hundreds and thousands of computers that must come into consensus to settle these DeFi transactions. At the base layer, they are highly decentralized. At the DeFi application layer, they may be decentralized in a number of ways but protocols that operate without intermediaries autonomously through software are—do meet the level of decentralization.

Your second part of your question, on nonfinancial use cases, there are a number. About over a year ago, Polygon Labs launched an open-source data base of blockchain-based use cases called the value prop. Today, there are over 500 applications and 43 use cases, and the nonfinancial use cases outweigh the financial use cases.

Two that are most notable are the California DMV has digitized 42 million car titles to smooth the title transfer process. GeoNet is an application that pulls satellite data in order for farmers to have better predictability about their crops and be able to enhance predictability.

Mr. LUCAS. Mr. Valkenburgh, could you also share your perspective about the impact of decentralizing the internet?

Mr. VAN VALKENBURGH. I would be happy to. Thank you, Congressman.

So there is a paradigm shift involved with DeFi, and we keep coming back to it, which is the removal of intermediaries. The cybersecurity threats that we have discussed in the context of the larger internet are a part of that paradigm shift. Hackers today target centralized servers. Centralized servers have wealths of information and data about the users of those services.

This does not need to be the way the internet is built. Indeed, the original internet was built with individual servers run by individual internet users in mind. You would have your own blog. You would speak your own voice, and you would have censorship resistance, autonomy, and privacy, the core values of the American revolution.

We have seen a change as large companies built services, Facebook, Google on top of the internet, and created moats around their user data. DeFi, along with the nonfinancial uses that Ms. Rettig highlighted, is an alternative to that, a return really to the original view of the internet, which is that it should be an open playground for people to build what their hearts say they should build and do it themselves and own their own data in the process.

Mr. LUCAS. In the remaining time I have, I would like to focus on an issue that I put a lot of energy in on the Science, Space, and Technology Committee, and that is the future of quantum computing. Quantum computing has an enormous untapped potential to solve the world's most complex problems but also has the ability to wreak havoc in the wrong hands.

Cryptography, of course, is the backbone of blockchain networks, which is, in the near future, must withstand a post-quantum world.

Ms. Tuminelli, would you—how much attention has been given to post quantum cryptography in the context of DeFi protocols as we slide into quantum computing?

Ms. TUMINELLI. Thank you for the question.

As you suggested, cryptography is the backbone of blockchain technology, which means that it is also the backbone of DeFi technology. I think, exactly as your question said, it is key and central to the future of DeFi.

Mr. LUCAS. With the potential for quantum computing that exists, I believe, from the hearings we do on the Science Committee, the effects on these encryptions are going to be dramatic. How do we keep up? Anyone else wish to touch on that for a moment?

Mr. VAN VALKENBURGH. The one thing I would add about quantum computing is it could make a lot of our current crypto systems obsolete in a dangerous way.

Now, the interesting things about DeFi here are that we would see in real time the need to update our systems because hacks would become immediately apparent. Large centralized banks, financial services providers, and internet corporations may get hacked and may fail to rapidly disclose those vulnerabilities.

So there is something beautiful in the fact that these systems are open and that we immediately see when a vulnerability exists, and we can start to patch it. The value in these systems means there is effectively a very good bug bounty to draw people to fix these problems.

Mr. LUCAS. Thank you.

I yield back, Mr. Chair.

Chairman HILL. The gentleman yields back.

The gentleman from Illinois, Mr. Foster—Dr. Foster, I should say, is recognized for 5 minutes.

Mr. FOSTER. Thank you.

I would like to actually follow up on the chair's discussion about the need to identify bad actors. How is this actually implemented in DeFi right now? First, how do you identify them in a system where the underlying protocol is that of a permissionless, anonymous, self-hosted custody of assets? How do you identify and how do you effectively ban bad actors, or is there no such concept as bad actors in DeFi?

I will just go down the line, and if you could describe how it is implemented, if at all.

Mr. AVELLO. Sure. Happy to do that. Thank you for the question, Congressman.

Our fund, actually, has invested in a company that is building what is called zero knowledge proof protocols.

Mr. FOSTER. Yes, that is not—what is there right now? I understand. We have had hearings on homomorphic encryption. It is not ready for prime time. With the technology that exists today, how do you do it?

Mr. AVELLO. Well, this particular company has launched a product. It is actually being used in the marketplace now. It is—they have not gotten market share at this point, but they are growing significantly.

Mr. FOSTER. There is also fundamental problems with the zero knowledge, which you still need a third party to control the privacy budget on these things. I have looked at the mathematics behind there. I have programmed blockchain.

By the way, Ms. Tuminelli, I appreciate your efforts to educate Congress on this, which is a challenge. If you ever would like to learn how to program blockchain, I would be happy to teach you.

If we can go next and say, how do you implement, how do you implement identification and banning of bad actors in an anonymous self-hosted situation?

Ms. RETTIG. Thank you so much for your question, Congressman.

I think there are two primary—three primary ways that it happens today. First, there is an organization called the Security Alliance, which is an organic group that monitors and works in public-private partnership with law enforcement to watch for hacks and engage in other types of activities.

Mr. FOSTER. When you have identified a bad actor and a bad actor reappears with an anonymous self-hosted wallet, how do you identify the fact that you are a bad actor?

Ms. RETTIG. Law enforcement and blockchain analytics tools are actually able to trace a lot of this very transparently.

Mr. FOSTER. A lot is not enough. You need to be able to trace all of it, and that is I do not believe technically possible.

Ms. RETTIG. Our current system under the Bank Secrecy Act (BSA) is not 100 percent, but I think we should be aiming for that in the DeFi ecosystem, and there are a number of ways to handle that. I have actually made one such proposal in a paper that I co-authored and published in January where we identify a new cat-

egory called critical communications transmitters that will take on enhanced risk-mitigation measures for financial integrity.

Mr. FOSTER. Okay. Now, when you have identified a bad actor, how does DeFi come together to say, “This is a bad actor; we are going to ban you?” How do you even trace that person when people are operating multiple identities anonymously?

Ms. RETTIG. Sure. The critical communications transmitters will bring immediate reports to the Financial Crimes Enforcement Network (FinCEN). They will not look identical to Suspicious Activity Reports (SARs), but they will have the type of information that will allow FinCEN and other law enforcement to be able to trace both the immediate wallet you are talking about and anything that emanates out from that as well.

Mr. FOSTER. How do you trace all users of anonymous wallets? If one person is operating 12 anonymous wallets, how is that dealt with in this system?

Ms. RETTIG. I can say that, through public-private partnerships and working with the FBI and the Department of Justice (DOJ), on a number of these matters, they are actually able to trace wallets very quickly and much more quickly than the decades that it has taken to trace illicit funds in the traditional financial world.

Mr. FOSTER. Does that not apply to the most deliberately anonymous financial products that have been made, which are made, by design, very hard? This rapidly gets into classified stuff, and so, if you cannot talk about that, that is all right.

Ms. RETTIG. I cannot talk to you deeply about it, but I will say that funds from some of the worst actors are frozen today and unable to be moved given the immediate identification that has happened both with industry and law enforcement working together on these issues.

Mr. FOSTER. When you freeze someone’s funds, do you freeze their activities in every one of the anonymous wallets that they control?

Ms. RETTIG. You certainly freeze the illicit activities, the illicit funds that you have identified.

Mr. FOSTER. That you have identified. Okay. So there is no way to ban a bad actor. They just pop up in some other guise with some other set of self-hosted wallet?

Ms. RETTIG. That may be but—

Mr. FOSTER. Okay. Thank you.

There are also questions of governance here. Mr. Hays, there is a fundamental guarantee that people who are investing in anything in the regulated markets in the U.S. at least that, when you invest into something, there is not a cabal of people secretly controlling what you have just invested in that are going to rip you off.

It seems to me that also cannot really be a guarantee in a situation where people have anonymous self-hosted wallets that control the voting. How do you view this as a problem, and are there any ways to fix it?

Mr. HAYS. Well, briefly, I think it is a problem. You see concentration of ownership of governance tokens across platforms, particularly with venture capital funds, who arguably are dictating

how these programs are run and that is for their benefit, not necessarily other retail investors.

Mr. FOSTER. Thank you.

My time is up. I yield back.

Chairman HILL. Mr. Rose of Tennessee, you are recognized for 5 minutes.

Mr. ROSE. Thank you, Chairman Hill and Ranking Member Lynch, for holding this hearing today.

Thank you to our witnesses for your time and being present today.

I am proud to say that my home State of Tennessee is a leader in blockchain investment thanks to the forward-thinking approach we have taken to regulation. Limited—one such example is our recent passage of legislation that allows limited liability companies to register as decentralized autonomous organizations, or DAOs. At the time of the passage, Tennessee was only the second State in the country to have such legislation signed into law.

Mr. Avello, could you explain what DAOs are and why they have become so popular?

Mr. AVELLO. Happy to. Thank you for the question, Congressman.

In DAOs, if you ask 30 different people, you might get 30 different answers, but the way that I like to think about it kind of starts from this primitive that there are individuals who are using blockchain technology or leveraging blockchain technology to create a governance system without a centralized management team.

What the same come aspects that kind of exist in all of these different organizations are a lack of a centralized management team. There are collective decisionmaking across the groups that are organizing natively on the internet. Typically, there is a governance token involved. That is not in every single case, but there is typically your governance token rights.

As far as why they are becoming popular, I think it is very—when there is excitement within a group of people that are interested in a different project—that can be DeFi; that can be investment clubs; that can be social groups. There is a whole host of activities that people engage in through DAOs, but I think the ease with which they are able to organize initially makes them popular.

As far as long term, they can be, depending on the services that are being offered by the DAO. They take on a variety different forms: limited liability companies, different foundations overseas, sometimes operating—there are sometimes groups that operate without entities.

So the flexibility that is offered through the DAOs and of organizations I think has given rise to its popularity.

Mr. ROSE. Thank you.

Ms. Tuminelli, last year, the Internal Revenue Service proposed a rule requiring broker reporting of sales and exchanges of digital assets. This rulemaking seemed to be contingent on the assumption that broker businesses are in the position to know a person's potential tax obligation.

Is the IRS proposal workable?

Ms. TUMINELLI. Thank you for the question.

In short, no, it is not. The proposed definition of broker is extremely broad. As you said, it puts anybody in a position to know in the place where they have to report.

For example, right now I am sure members of your office have started fantasy football. At the end of the season, the commissioner of your fantasy football league is in a position to know the winnings or loss of any person who participated. That person would be a broker under the IRS' new rule.

Mr. ROSE. What is the status of the rulemaking?

Ms. TUMINELLI. Right now, the IRS finalized the part of the rule that applies to others outside of DeFi, and we applaud them for that. They did take the right tack in trying to learn more about DeFi before they finalized the rulemaking as it applies to DeFi.

Mr. ROSE. Ms. Tuminelli, I think that my colleagues on the other side of the aisle and the Biden-Harris Administration scapegoat the digital asset industry as a mechanism to avoid tax liability. How can the DeFi industry support tax compliance?

Ms. TUMINELLI. Sure.

Obviously, the tax liability for an individual is on the individual themselves, but as an industry, of course there are software and technology solutions that make it easier for a person to assess their tax liability and pay that tax liability. Ultimately, it is their responsibility as an individual to pay their taxes.

Mr. ROSE. Thank you.

Under President Trump, the Financial Crimes and Enforcement Network released guidance in 2019 that has been one of the few regulatory actions that has provided legal clarity for DeFi developers and businesses. However, I was unsurprised to learn that the Biden-Harris Administration's Department of Justice has poured cold water on that guidance and taken a more aggressive enforcement path.

Ms. Tuminelli, could you explain what the impact or what impact that has had on the DeFi industry?

Ms. TUMINELLI. Sure. As you said, in 2019, FinCEN finalized guidance that was very helpful to the industry and explained what a money services business was in the context of providing and publishing software, and the industry followed that guidance for years. Just this year, the Department of Justice took the position that guidance is merely a suggestion and that they do not need to comply with it or listen to it, and it is really unfortunate that two entities in the same government are disagreeing on what the law is, and the consequences is a person's liberty.

Mr. ROSE. Thank you, and my time has expired. I yield back.

Chairman HILL. The gentleman yields back.

We are honored to hear from the ranking member of the full committee, Ms. Waters, for 5 minutes.

Ms. WATERS. Thank you very much.

While decentralized finance, or DeFi, aims to create greater efficiencies and transparency, it can also pose heightened risks of hacks, scams, unequal information, and conflicts of interest that can harm consumers and investors. We have seen this play out in the new DeFi venture that Eric Trump and Donald Trump, Jr., plan to launch, called World Liberty Financial.

Because of the prominence of those behind the project, bad actors took advantage of the opportunity to scam potential users. Lara Trump and Tiffany Trump's X accounts were hacked, and scammers used them to announce links to a coin falsely claiming to represent World Liberty Financial. According to the analysis, at least 200,000 people viewed the post, and approximately 2,000 people purchased \$1.8 million worth of the fake token. Lawmakers have a responsibility here, and I think the lawmakers have a responsibility to consider strong protections to prevent such scams from moving forward.

Mr. Hays, I would like to ask you a question. Opaque DeFi platforms with unclear governance and control mechanisms may create hurdles for regulators to establish responsibility and accountability for regulatory compliance. In launching actions against DeFi entities, regulators, like the Securities and Exchange Commission and the Commodity Futures Trading Commission, have had to navigate complex legal issues. We have seen these issues play out in litigation involving decentralized autonomous organizations and virtual currency mixers.

In your view, how can regulators deal with mass noncompliance by entities that claim they are decentralized to avoid regulatory compliance? What more needs to be done to ensure robust consumer and investor protections in this industry?

Mr. HAYS. Thank you, Congresswoman. The issues you have laid out here are pretty profound, and I think the simplest way to answer your question is that regulators should continue to do what they are doing. For example, the Securities and Exchange Commission's rulemaking, looking at the definition of exchange, we have heard some discussion about that today. I think there are a couple points to keep in mind.

The original law that drafted that Securities Exchange Act was meant to be expansive to cover a lot of different scenarios. Far from sort of an antiquated idea, it really was meant to be evergreen. Congress in the past has considered narrowing that definition but decided against it. So this rulemaking ironically provides a certain degree of clarity that looks at the functional nature of how exchanges operate.

What their—the proposed rulemaking has said or the rule has really explored, look, if you are matching a buyer and a seller to facilitate a trade, that is an exchange. You can be a regulated exchange under that act. You can be an ATS. You can be a DCM under the CFTC if you are not dealing with securities. There are a couple different pathways. In fact, I know they are continuing to work on that rulemaking to further clarify what kind of information applies to that.

So the SEC is already embarking upon that effort, and we should continue to support their efforts. I think the CFTC has done similar work with the Ooki DAO case, where they have identified how there are times and places where DAOs meet the facts and circumstances similar to what you might find with an unincorporated association, so, in fact, persons are responsible. I think legislation that undermines that and makes it harder for regulators to do that is misguided.

Ms. WATERS. Thank you very much. I yield back.

Chairman HILL. The gentlewoman yields back.

The gentleman from Wisconsin is recognized for 5 minutes.

Mr. STEIL. Thank you very much, Mr. Chairman. Thanks for holding today's hearing.

We were just talking about risk. I want to just dive in because I think there is some real strong counter points that we need to make sure are on the record, right. With every new technology, there are benefits, there are risks. How do you manage the benefits? How do you scale down the risks?

If I can, I want to come to you, Ms. Rebecca Rettig. DeFi shows promise. There is also some risks that needs to be addressed. DeFi's hacks cost more than \$3.6 billion in 2022, and the number has likely gone up since. Can you talk about what DeFi protocols in the broader community have done to address these risks, and what else may need to be done to target existing vulnerabilities, because I think it is really important to talk. Sure, there is risk out here, but how are we working to downsize that risk?

Ms. RETTIG. Thank you very much for your question, Congressman. I think we can all agree that any of the hacks or scams or any of the risks should be mitigated as thoroughly as possible. I would say that the three primary risks in DeFi are cyber risk, system management risk, as well as usage risk. There are current efforts to combat many of those. As I mentioned previously, the Security Alliance looks at all of those types of risks, both what is happening from the illicit finance perspective but also training developers how to build safer ecosystems in general, as well as how to put in place appropriate system management controls to ensure that there are not these centralized places of data or other areas of vulnerabilities.

So that is one of the primary places that it happens, but there is also significant public/private partnership with law enforcement going on in the industry to ensure that a lot of these risks are addressed.

Mr. STEIL. That is helpful.

Let me jump over to you, if I can, Mr. Brian Avello. In your written testimony, you noted that many DeFi participants are having trouble navigating the jargon and code associated with DeFi projects. On top of that, you argued that many projects failed to prevent fulsome information. What can market participants do to ensure counterparty communications and disclosure are better understood?

Mr. AVELLO. Sure. I think—and thank you for the question, Congressman. I think you will see a lot of the most notable projects in DeFi have developed kind of almost as custom disclosing massive amounts of information, not only on tokenomics with regard to each project but also at a very granular level discussing and explaining in plain English how these different technologies work, specifically different smart contract functions if one or more persons is interacting with a contract, exactly what you will be engaging in by interacting with those protocols.

Mr. STEIL. What should regulators be looking at in considering with respect to rules required around disclosures or other communications?

Mr. AVELLO. I think there has to be a lot of interaction with the industry, probably the most notable or largest projects that have a presence and are actually coming here to engage in Washington would be a good starting point. Then, you look at kind of—I think I highlighted in my written testimony what I as a user and an investor in this space would expect to see, and I think, frankly, it is about—it is a matter of making the information as simple and as clear as possible for the users who are using it so that you do away as best as possible with the lack of confusion.

Mr. STEIL. Thank you very much.

I am going to come back to you, if I can, Ms. Rebecca Rettig. Shifting gears here because I think it is worthwhile talking about use cases, and I know Polygon Labs maintains a data base of DeFi use cases. Commissioner Peirce wrote the following Stagnation, centralization, expatriation, and extinction are the words of this release, Today's Commission treats its basic approach to exchange regulation as something that must not—indeed cannot—be altered to allow room for new technologies or for new ways of doing business.

Strong words from a sitting SEC commissioner.

I think what Commissioner Peirce is actually touching on is a point that we have made many times in this committee that laws and regulations need to evolve to accommodate innovation safely. So we are talking about the risk upfront. We know that there is use cases out there. Can you just comment on some of the use cases that you are seeing that American families and workers would benefit from this?

Ms. RETTIG. Thank you very much for your question, Congressman, and the use case aspect is something that really brought me to Web3. I talked about some of the nonfinancial use cases, and—but others that abound in the DeFi context, as we are talking about today, is faster payments, which allow for humanitarian aid transfer from the United States to those on the front lines. In Venezuela, there are health workers there who have needed it. There has been also payments in the humanitarian aid context for the efforts for Ukraine, both from people in the United States as well as outside this country, as well. Some of the other types of efficiencies that we have seen have been for the exchanging of assets and the like.

Mr. STEIL. Thank you very much.

Thank you, all, for your testimony.

Mr. Chairman, I yield back.

Chairman HILL. The gentleman yields back.

The gentleman, Mr. Casten, is recognized for 5 minutes.

Mr. CASTEN. Thank you, Mr. Chair.

Thanks to you all for being here.

So I am—I remember when I got out of college, I was living in Boston, I was in my 20s, mostly just reading the Federalist Papers. Yes. I remember there was this great pizza restaurant over on Commonwealth Avenue by Boston University (BU) that, rather famously, was—the pizza was fantastic, to be clear—they were found to have basically retained virtually every law firm in Boston, and they would hire young lawyers to go make deposits at banks that were often just below the levels that would trigger anti-money

laundering (AML) requirements, but if they were above, the FBI office was full of pictures of young, aspiring lawyers, whose firms had all been completely conflicted out of ever working against the owners of said pizza restaurant.

Nobody would have ever argued that the beneficial use case for this particular pizza restaurant meant that we should never regulate pizza restaurants under AML protocols. I get concerned in this DeFi conversation that we are framing that as its beneficial use. It is really good. It is maybe as good as the pizza that was at this pizza joint, and therefore we should not have anti-money laundering rules. Like, that does not make any sense to me.

Mr. Hays, you had mentioned the Ooki DAO case where they—my understanding is that Ooki DAO was actually advertising that they were—that you could get around AML laws, and CFTC has come after them, had alleged that they were actually created with the explicit goal of operating an illegal trap form.

So, I guess, Mr. Van Valkenburgh and Ms. Tuminelli, I am just curious, yes or no—because I do not want to misunderstand your testimony—is it your argument that, if a DeFi protocol is found to be violating anti-money laundering rules, should there be any legal accountability to the creators, the operators, the people maintaining that services? Yes or no, should those people have any legal liability?

Mr. VAN VALKENBURGH. Those who are not decentralized, those who are custodial have AML laws that apply, and they should—

Mr. CASTEN. If it is a DeFi protocol—

Mr. VAN VALKENBURGH.—should be enforcing it.

Mr. CASTEN. If it is a DeFi protocol, are you saying that there should—you are saying it is decentralized?

Mr. VAN VALKENBURGH. An immutable smart contract that I transact with?

Mr. CASTEN. I am just asking, yes or no, should they have—

Mr. VAN VALKENBURGH. As an American transacting with an immutable smart contract, I am transacting with my own funds; I should not be subject to the Bank Secrecy Act.

Mr. CASTEN. Okay. So you think no.

Ms. Tuminelli, do you think, yes or no, should there be any liability that is there?

Ms. TUMINELLI. I think bad actors should be held liable for the bad conduct that they engage in, not the developers, not the people who created the software. It is the bad actors who actually committed the crime. We should go after them.

Mr. CASTEN. There should be no liability for the people who created the tool. So, in my—back to my pizza example, the people made the pizza joint. They used these laws. There should be no liability for them because they are just pizza producers?

Ms. TUMINELLI. If I make a neutral tool that somebody uses to commit crime, I should not be held responsible for that person's conduct.

Mr. CASTEN. Okay. Mr. Hays—that is bizarre. I mean, that is aiding and abetting commission of a felony.

Mr. Hays, who do you think should be held liable in those cases? Is it the DAO members? Is it the creators? Is it the—where should that liability lie?

Mr. HAYS. I think it is a good question. It is complex, but I think you could apply existing laws to find some answers. I think it also depends on the facts and circumstances of those cases, but I think what you are raising raises a conundrum. Developers and admins intervene in the platforms that facilitate these transactions on a fairly regular basis, either directly or indirectly through the functions of the DAO. They change—update the code. They issue assets. They help determine how the validation process works.

There are many times when interventions happen by individuals with knowledge. Those include people outside of the developer team and inside the developer team. It is tricky, because why are they intervening in those moments when not only are those about the infrastructure operation of the platform but actually what the platform does, which is to facilitate transactions and move assets? Why, then, should they not be held accountable if the transactions that they help facilitate end up facilitating illicit finance? I would argue that you have to find a way to hold developers accountable to some degree, and the question is, where do you draw that line?

Mr. CASTEN. Okay. I want to get back, because I think we talk about this technology as being unique and not recognizing that we have, to your point, we have these tools. If I buy a security on Nasdaq, I have to disclose, and Nasdaq has clearing offices, and they verify the identity.

Ms. Rettig, coming to you, following in your exchange with Mr. Foster, in the case of a Nasdaq transaction, there is a clear custody title that is clear there is no way to participate in that as an anonymous actor. Is there any reason why we could not insist on those rules for DeFi protocols? If you want to be anonymous, if you want to think you conduct rules, fine, you cannot play in this sandbox.

Ms. RETTIG. I think it goes to what—to actually what Mr. Van Valkenburgh talked about in his oral testimony, which would be importing intermediaries into disintermediated systems, which will put the U.S. at a large-scale disadvantage from a long-term perspective.

Mr. CASTEN. Well, look, I am out of time, but there is no disadvantage to the U.S. economy of not protecting the interests of child traffickers, money launderers, and the North Korean nuclear system.

Ms. RETTIG. The one point on your pizza example is that the pizza restaurant had individuals who were acting with center, and that is very different than what is going on here.

Chairman HILL. The gentleman's time has expired.

Mr. CASTEN. I yield back.

Chairman HILL. The gentleman from Nebraska, Mr. Flood, is recognized for 5 minutes.

Mr. FLOOD. Thank you, Mr. Chairman, and thank you for holding this hearing today.

I would like to maybe just explain my thinking on this topic. I know there has been some discussion of the way DeFi could change finance, but in my view the largest implications of DeFi are unrelated to the financial applications. Smart contracts could change things that have nothing to do with speculating on assets or currency. It is the technology we are talking about, not trading our wallets, that could really change the world.

This leads me to what is called Web3.0. I am fascinated by how a decentralized web could change the applications that we use every day. If we have a decentralized web, it would disempower the Big Tech intermediaries that wield so much influence today. I would like to demonstrate what I mean by an example.

If you are a creator of videos, right now you are probably using YouTube to get your videos out there. Now, if you are putting your videos on YouTube, then your income stream is beholden to the rules that YouTube has regarding how much ad revenue they share with their creators. Everything flows through a centralized intermediary between the creator and the revenue generated from the audience.

What a decentralized web would do is cut out that intermediary. The creator, as I understand it, would own what they create, and they would keep the lion's share of that value that their creation brings. That would have to be beholden to the terms of a corporate third party hosting their work. They would not have to be beholden. The infrastructure of the platform itself would guarantee they are compensated directly for the value they bring.

Ms. Rettig, I know Polygon Labs is involved with some Web3.0 projects. Could you talk a little bit about those projects and your thoughts more broadly on a decentralized web?

Ms. RETTIG. Sure. Thank you very much for the question, Congressman. Polygon Labs builds the networks on which all of these Web3 applications are built, and those types of applications abound, including both in the financial context and otherwise. One of the use cases we did not talk about but you touched upon is the idea of creation and the ability to hold your own IP, not just your own assets or your own data, although that is critically important. On those types of creator platforms, including social media, it really returns ownership back to individuals, and that is one of the great benefits of a decentralized web.

Mr. FLOOD. Just continuing with you for a second here, do you have any sense of how far along we are to a potential decentralized web, and at what point do you envision we would see decentralized web solutions more broadly offered for consumers, like consumers of social media and other applications?

Ms. RETTIG. Sure. I would say that the internet has been around for 40 or 50 years and that we are probably not even 25 percent of the way into that for Web3, but very far along and moving at an exponentially rapid pace.

Mr. FLOOD. Ms. Rettig, do you have any thoughts—I guess, I have to back up. My background is in media, and I have thought a lot about how a decentralized web could change traditional print media, broadcast media, and how we consume the news more broadly. Right now, newspapers are going out of business across the Nation, and as a result, fewer journalists are watching the school board and all these political subdivisions. Do you have any thoughts on this topic?

Ms. RETTIG. Thanks very much for your question. I do think that a decentralized web or Web3 application is changing the way that we consume information. It is coming a lot more organically from individuals who are witnessing the news in a way and able to bring it on to the web in an immutable context and also to crowd source

information in a way that traditional media may not be able to right now.

Mr. FLOOD. I appreciate that. It can be challenging, I think, to forecast what the great next innovations are going to be. I am excited about what this is. I see a world of opportunity for America. I see us as the one country that can harness this like we did the internet. With the right protections for consumers and safety and internet sex trafficking and all those things, we should lead the world in blockchain. Now, candidly, I do not know if the blockchain is the technology that is going to bring this to bear, but plenty of smart people do think blockchain is our next transformational technology.

One of the things that the chairman and I really agree on is that there is so much innovation opportunity for America if we harness this technology in the right way, protect our citizens, protect the vulnerable. I just hope that as Congress continues down this path we do not suffocate innovation in a way that lets another country or series of countries have an advantage over what should be an American opportunity.

With that, Mr. Chairman, I yield back.

Chairman HILL. The gentleman yields back.

The gentleman from North Carolina, Mr. Nickel, is recognized for 5 minutes.

Mr. NICKEL. Thank you, Chairman Hill, for holding this hearing.

Thanks to our witnesses.

Decentralized finance, or DeFi, has transformative potential. It can make our financial system more accessible, transparent, efficient, and innovative. DeFi can create a more inclusive financial system, as traditional finance just might not be for everyone. Of course, as with any new technology, there are risks. I hope we can learn more about how to mitigate those risks during today's hearing.

It is important that DeFi remains a bipartisan issue. I would urge my colleagues to find common ground in supporting both innovation and consumer protection in DeFi. Bipartisan work is absolutely crucial to creating a balanced and durable legislation that will protect consumers and keep digital innovation in the United States. Frankly, I just do not think it is an either/or. I think we can do all of these things. We can protect consumers. We can encourage digital innovation. We can embrace this amazing new, transformative technology that can improve the lives for so many Americans. We have to keep those jobs here in the United States.

Ms. Rettig, first question for you, can you talk about some of the risks with DeFi and how legislators on this committee should be thinking about how to address them?

Ms. RETTIG. Thanks very much for your question, Congressman, and for your leadership in this emerging space. I will hit on the illicit finance side of the risks, because I know that is the greatest concern and I think a place, to your point, where bipartisan and industry can all agree that we want that to stop. Not a penny should go to bad actors.

I proposed a framework along with my coauthors in a paper that came out in January that looked at how to combat illicit finance in DeFi with a three-part framework. The first was to expand on

the definition of “independent control” found in the 2019 FinCEN guidance to be able to actually identify intermediaries that exist who may actually have regulatory obligations. So it will close the gap that the DeFi Treasury Illicit Finance Risk Assessment put forward in DeFi.

The second part is what I alluded to in my testimony, which is to treat pure technology protocols as critical infrastructure, just like we do with electronic clearing systems and financial messaging systems.

The third part is to create a new category of entities that will have additional risk mitigation obligations in the financial integrity space to be able to meet the goals under the BSA of document, detection, and deterrence of bad actors.

Mr. NICKEL. Thanks so much. Same question to you again. How are other jurisdictions approaching the regulation of DeFi, and is the U.S. falling behind countries like China?

Ms. RETTIG. Thank you very much for your question. Unfortunately, we are falling far behind and putting—setting China aside, we are falling behind the rest of the world. Just from an anecdotal perspective, regulators across the world have actually been engaging with industry for, I would say, the last 5 or 6 years to talk about what to do in a collaborative way, the EU in particular, the U.K. as well, and numerous countries in Asia, Japan, Singapore, and the like.

Every single country to date has—even if they have implemented centralized crypto regulation, they have said we either need to study or explore or do further analysis of DeFi. I will say the one notable proposal is from France’s prudential regulators, which seek to think about regulating DeFi much like cyber infrastructure and imposing certain types of cybersecurity standards and audits of these DeFi protocols. So it is very different everywhere across the world than how we are handling it in the U.S., other than in some of the proposed legislation we have seen, all of which suggest studying DeFi, which is the right way forward.

Mr. NICKEL. Thanks so much. We did a bipartisan CODEL (Congressional Delegation). We traveled around the world to meet with these other markets. They are open for business. They are trying to take jobs here from the U.S., and it certainly dawned on me the importance of making sure we continue to keep up with the rest of the world, because this is a place where we continue to fall behind, unless we act here in Congress, and we have the ability to do that. I am eternally optimistic that we can get it done.

Mr. Avello, next question to you. We constantly hear that both innovators and capital are leaving the U.S. due to a lack of regulatory clarity. What human capital and financing trends are you seeing in the U.S.—as the U.S. falls behind in Web3 and DeFi?

Mr. AVELLO. I can say from wearing my investor hat and from a personal perspective, I have seen a number of incredibly qualified teams, the exact types of people I think that you have mentioned that you would want to see here, building multi—hundreds of millions of multibillion dollar companies and protocols, unfortunately having to move abroad necessarily to set up operations for their companies and basically offshoring most of their activity.

I can tell you from working with or seeing pitches from teams like this, that there is an incredible interest about staying here in the United States and running—potentially launching and operating their protocols in a compliant fashion. I think the regulatory unknowns are just too challenging on a personal level, and unfortunately have had to move abroad in order to effectuate their businesses.

Mr. NICKEL. Thanks so much. I am out of time. I yield back.

Chairman HILL. The gentleman yields back.

The distinguished gentleman from Ohio, the vice chairman of our Digital Assets Subcommittee, Mr. Davidson, is recognized for 5 minutes.

Mr. DAVIDSON. Thank you, Chairman. I thank our colleagues and the panel for your testimony today.

DeFi is an essential component for a vibrant financial sector in the United States, so we have dominated markets around the world, and it would seem particularly foolish to change course now. That is what we are at the risk of. I mean, as I listen to some of my colleagues, I was—really appreciate Mr. Nickel for highlighting that this is an issue that largely unites Republicans, and it does divide Democrats. Most of the panel, we have seen from Democrats today, though, has been insane.

I mean, we have basically—if they were applying their same logic, I guess, think how many crimes Google becomes an accomplice for because people do searches or use the Maps function to navigate to the place they are going to commit crimes. Thankfully—I mean, they are targeting speech in other ways. Thankfully, I have not seen them make that ridiculous level of an argument yet.

Mr. Van Valkenburgh, you are highlighting the code of speech, and one of the things that is at the core here is another thing: privacy. The idea of—you would think, when I hear Mr. Foster talk about the government granting permission for you to do something that the government is the granter of our rights. Thankfully, in America our Founders recognize that rights come from our creator, that among them are life, liberty, and the pursuit of happiness. The First Amendment is a limitation on the government's ability to infringe on your right to speech, and the Fourth Amendment is a limitation on the government's ability to infringe on your right to privacy.

DeFi, I think how in the world can you have decentralized finance without the decentralized part? They want a central hub that is the granter of permission, the filterer of speech, the filterer of privacy, the granter of permission. Now, you could expect that in a police state. You could expect that in an authoritarian country controlled by the Chinese Communist Party or something like that, but why in the world would we see our colleagues here in Congress where we are sworn an oath to support and defend our Constitution would you see people advocating for that?

Mr. Van Valkenburgh, could you pick up—I know you wanted to say a bit about this speech angle and perhaps more.

Mr. VAN VALKENBURGH. What Member Foster suggested where the problem with anonymity is that we do not have 100 percent identification and control over financial transactions in the econ-

omy, I do not think we will have 100 percent identity and control over DeFi transactions, and I think we will have robust anonymity, and that is an American constitutional right. So you have a constitutional right to anonymous transactions that support organizations and causes that defend against discrimination and violations of our constitutional rights. We fought about this during the civil rights movement in the 1970s.

As Thurgood Marshall said with respect to the Bank Secrecy Act, the law that actually requires financial surveillance of custodial intermediaries, though not noncustodial intermediaries, Marshall dissented from the constitutionality of even that level of surveillance. He said, "The fact that some may use negotiable instruments for illegal purposes cannot justify the government's running rough shot over the First Amendment rights of the hundreds of lawful yet controversial organizations like the American Civil Liberties Union (ACLU). Congress may well be correct in concluding that law enforcement would be facilitated by the dragnet requirements of the Bank Secrecy Act, but those who wrote our Constitution recognized more important values."

Mr. DAVIDSON. Thank you for that, and great insight. I hope we can go after that in third-party doctrine again in some other venues.

As it relates to DeFi, Ms. Rettig, you have done a great job of highlighting how privacy is an inherent part of the reason people would choose to conduct transactions. It has to be protected for it to function. The other part is, for somebody to surveil your transaction, most of these companies are charging a fee-for-service. Look, I mean, I appreciate what Visa and MasterCard and American Express—I have one of each of those, or perhaps more—they do. They check and make sure it really is me, and I am buying from somebody else and if it was not me, they would provide a hedge, and for that I know—I am kind of comforted that there is an intermediary.

Now, I will admit I am a little creeped out when the government wants to mandate that they surveil me and hand over my transaction data without a warrant or subpoena. That is a lot more government than I want but for other transactions, I still carry cash, and I like that there is no intermediary. I know that, once I gave the cash to somebody, my ability to reclaim that is more limited. It does not mean I have no recourse. How do you make DeFi function if you do not have privacy?

Ms. RETTIG. I think—thank you very much for your question, Congressman. I think DeFi, as Mr. Van Valkenburgh said, will have at least pseudonymity, right, a privacy over who you are and certain types of information in that regard. I think, to your point on Visa and MasterCard, we agree that not only the people who can access those are not the only people who should be able to access the economy, right. Goldman Sachs and those—and their clients are not the only people who can participate in the American economy, and so DeFi and the larger Web3 movement is meant to expand and democratize that even more greatly.

Mr. DAVIDSON. Thank you for that, and may God bless you all with great success in spite of some of my colleagues' efforts to undermine it. I yield back.

Chairman HILL. The gentleman yields back.

The gentleman from California, Mr. Sherman, is recognized for 5 minutes.

Mr. SHERMAN. What we have here is an effort to liberate billionaires from income taxation. Every time a billionaire successfully cheats on his taxes a member of the Freedom Caucus earns his wings. Billionaires cannot keep anonymous with \$100 bills because their pockets are not that big, and the decision our country has made not to print the \$500 bill or \$1,000 bill means that the use of cash becomes less in terms of the amount of cash in a single bill declines by 3 or 4 percentage points, 2 or 3 percentage points over the last 5 or 10 decades.

Now, we are trying to create a market here for a system that is much worse than the system we have for honest people. If you have crypto, you can go to Coinbase or a similar broker, put it up, and get a loan at margin rates that are similar to what you do if you have stocks or bonds that you are borrowing against. This system is going to be more expensive, but it is much better for drug dealers, much better for human traffickers, much better for sanctions evaders, which is why Putin and Iran have embraced crypto and unhosted wallets.

The real market here is tax evasion. Trump's IRS Commissioner testified we have \$1 trillion a year of uncollected taxes. That is \$3 trillion of unreported income every year. That is \$30 trillion of unreported assets every decade. So the question is, why would somebody use a less efficient system? The answer is, if you are a patriotic anarchist and you agree that we should have a powerful America but only wage earners should pay the income tax and it should be voluntary for those in business and investment, then you design a system in which Know Your Customer is optional and in which those who wish to cheat, whether it be because they are cheating our sanctions laws or our income tax laws, they have an efficient system to do so.

Now, the other aspect of this DeFi is whether it is a security. We applied the Howey test. Mr. Hays, if you have a system where you put your money up and you have somebody else manage it and loan it out for you and then you get a return based on the results, in effect, if you have the Howey case but, instead of oranges, you have crypto, is that a security?

Mr. HAYS. Thank you, Congressman. The Howey test is designed for—to answer the question you have just raised, and it is designed to be tested broadly to apply to lots of different facts and circumstances. I would argue it is an applicable test to the situation, and there are many instances where crypto securities, whether issued on CeFi platforms or DeFi platforms, meet that test.

To be clear, a platform does not have to be issuing or facilitating the transfer of those assets. They do not all have to be securities. There just have to be a number of them that meet the test for an exchange to meet the term, conditions and obligations of a securities exchange. I think there are many instances where the Howey test is an appropriate tool and provides a useful answer in this regard.

Mr. SHERMAN. I would just reiterate that those who talk about privacy for billionaire tax evaders are waging a war against eco-

conomic democracy in this country but also creating a corrosive system in which at the country clubs and wherever billionaires meet, it will be thought to be stupid to pay income taxes when there is a whole system of finance that allows you to hide your assets while buying your yacht.

What worries me is not just those who are the tip of the spear, who will be the first to evade our income taxes and our laws against sanctions evasion and our laws against drug dealing, but a—and I have seen this happen in a number of other countries. I have studied tax enforcement in a number of other countries. Once it becomes a feeling among a subculture or an economic class that only the suckers are paying their taxes, we create a system in which no billionaire will feel right paying their taxes. After all, nobody else in the country club does it. Wages will be taxed. You get a W-2 form, and the question is whether anybody else. You can make a lot of money by making sure billionaires do not have to pay their taxes. I yield back.

Chairman HILL. The gentleman yields back.

The gentleman from South Carolina, Mr. Timmons, is recognized for 5 minutes.

Mr. TIMMONS. Thank you, Mr. Chairman.

Thank you to all our witnesses for being here today.

Decentralized finance is an incredible advancement in financial technology. At its core, DeFi leverages blockchain technology and smart contracts to create an open, transparent, and accessible financial ecosystem. This means that anyone anywhere in the world can access services like lending, borrowing, and trading without relying on centralized authorities. However, along with the many promising use cases come many questions about the government's role in this burgeoning space. As a Congress, we have yet to fully acknowledge, understand, and address this technology causing our country to fall short of our innovative values.

Mr. Van Valkenburgh, given the unique nature of DeFi protocols, it is clear that incorporating DeFi into the U.S. regulatory perimeter is a complex endeavor. While we have already touched on some, are there other challenges the U.S. oversight mechanisms and regulatory structures face as these emerging financial systems increasingly come into orbit?

Mr. VAN VALKENBURGH. Thank you for the question, Congressman. Why do we not stay on the subject of tax, because Member Sherman brought it up? So tax evasion is a crime which should be aggressively policed. Those who do not pay their taxes should suffer consequences in this country. I do not, however, think that tax evasion and its existence warrants a 100 percent surveilled and controlled financial system. So a difficult area in the cryptocurrency space has been getting clear tax guidance from the IRS on how Americans can pay their taxes when they earn capital gains or perhaps their wages on these networks.

Mr. TIMMONS. I did not hear his question or his argument. I mean, it is an open ledger. It is publicly accessible. How would you evade something that the world can see? How can you avoid taxes on an open ledger?

Mr. VAN VALKENBURGH. It is, in fact, more difficult to evade taxes when you are using open blockchain networks than using the

legacy financial system, which is happy to open shell accounts for you all over the world. I would also add that the IRS has been very, very late in offering clear guidance, and they are the big part of the problem here. They should have offered guidance on brokers, who need to file third-party tax documentation and reports, long ago using existing congressional authority.

Coinbase is a custodial broker, if you will, of cryptocurrency for tax purposes and should be doing third-party tax reporting to ensure that Americans are paying their taxes and the IRS is getting their revenue. There was no need to change the laws to tell Coinbase that they are a broker. The IRS simply had not made that rule change. Eventually, Congress, rightly, decided to direct the IRS to change those rules with the Infrastructure Act. In that process, they explicitly said, “IRS, you need to give third-party tax reporters in the crypto space the guidance they need so that Americans will pay their taxes.”

Even after Congress directed the IRS, the IRS went on a multi-year rulemaking spree where they ultimately tried to even apply these rules to noncustodial intermediaries apart from Coinbase in an effort that will not work—

Mr. TIMMONS. We are running out of time.

Mr. VAN VALKENBURGH [continuing].—and will trample our constitutional rights.

Mr. TIMMONS. We can agree that the government is not helping this process.

One more question. While Treasury and the SEC have made a regulation by enforcement, the dominant theme of the Biden Administration’s approach to DeFi, we have seen some foreign jurisdictions, such as the EU, take a different approach to this space.

Ms. Rettig, I am curious if there are frameworks in place in other jurisdictions that United States can draw from as it contemplates how to approach establishing protections around DeFi, and what did these foreign regulatory approaches get right and what can we learn from them?

Ms. RETTIG. Thank you so much for your question, Congressman. I think the foreign jurisdictions have moved forward with centralized crypto regulation and given clear guidance to centralized actors in this space. Governments all over the world have uniformly taken the approach to study DeFi more. There are also regulators who have actually experimented with DeFi themselves and conducted transactions, and there are some regulators who themselves have looked at DeFi protocols as cyber or technology that should be reviewed from a cyber perspective in order to accomplish policy goals in that way.

Mr. TIMMONS. Thank you for that. I think we can all agree that this is the future of technology. There is going to be disruption associated with it, but we need to lead the way and not have the enormous amounts of resources invested in what is indeed the future go offshore. When the U.S. economy is no longer the best place to start a business, we will lose long term, and so I would just say that is something we need to focus on, and there is balance in this approach, but we need to be intentional about it and not fall behind.

With that, Mr. Chairman, I yield back.

Chairman HILL. The gentleman from South Carolina yields back.
I want to thank our panel for your excellent testimony today and for participating in our hearing.

Without objection, all members will have 5 legislative days within which to submit additional written questions for the witnesses to the chair, which will be forwarded to each of you for your response. I ask each of you to please respond as promptly as you are able.

[The information referred to can be found in the appendix.]

This hearing is adjourned.

[Whereupon, at 11:41 a.m., the subcommittee was adjourned.]

A P P E N D I X

September 10, 2024



September 27, 2024

Via Email - Trish.Halloran@mail.house.gov

Chairman Patrick McHenry
% Ms. Trish Halloran
United States House of Representatives
Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Re: Decoding DeFi Hearing - B. Avello Responses to Questions for the Record

Dear Chairman McHenry:

I would like to extend my thanks again to you, your staff, Representative Hill and his staff for inviting me to the Subcommittee on Digital Assets, Financial Technology and Inclusion of the House Committee on Financial Services's hearing on decentralized finance earlier this month. It was an honor to offer my testimony and thoughts, and to hear the insightful questions from several representatives. Below please find my responses to the Questions for the Record from Representatives Warren and Waters, and if you or your staff need further information from me, I am available at your convenience.

Very truly yours,


Brian C. Avello

cc: Steven D. Becker
Alan C. Sobba
John M. Yarwood

Questions for the Record

Representative Warren Davidson:

A question for Brian Avello, can DeFi work without self-custody? A response by 9/27/24 at the latest, would be greatly appreciated. Thank you.

B. Avello Answer: *Thank you for the question, Representative Davidson. In short, no. While it may be technically feasible for an individual to use a wallet hosted or controlled by a centralized exchange or entity to interact with DeFi protocols, I do not see the point. The actual value of DeFi – permissionless protocols with which anyone can engage to borrow and lend, generate credit or exchange assets, among other activities – is allowing users to engage in financial services peer-to-peer or peer-to-protocol without the need for trusted intermediaries. The central tenet of that system, and why DeFi represents a sea change from traditional finance, is the user's total and independent control over their assets while engaging in varied activities rather than relying on trusted third-party custodians and gatekeepers. DeFi without self-custody is no better than using a heavily intermediated financial service, like ETrade, and in fact, may be worse given the various security and other concerns that arise by permitting a centralized exchange to custody and control a user's assets (i.e., not your keys, not your coins).*

Representative Maxine Waters:

Mr. Brian Avello

1. Which of the following options best describes your self-identified race? (you may choose more than one)
 - a. White or Caucasian
 - b. Black or African American
 - c. Hispanic/Latinx
 - d. Asian
 - e. Middle Eastern/North African
 - f. Choose not to answer
 - g. Prefer to self-describe (please specify)

B. Avello Answer: *(a) and (c): I am a white man of Cuban extraction.*

2. Which of the following options best describes your gender identity?
 - a. Woman
 - b. Man**
 - c. Non-binary
 - d. Transgender Man
 - e. Transgender Woman
 - f. Choose not to answer
 - g. Prefer to self-describe (please specify)



30 September 2024

Trish Halloran
Legislative Clerk
Subcommittee on Digital Assets, Financial Technology and Inclusion
House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Re: Responses to Additional Questions for the Record - Rebecca Rettig

Dear Ms. Halloran,

Thank you to the Subcommittee for inviting me to appear at the hearing on September 10, 2024, entitled “Decoding DeFi: Breaking Down the Future of Decentralized Finance.” It was a rewarding experience to engage on such matters.

I appreciate the opportunity to respond to the members’ additional questions. My answers are attached for the record.

Thank you, and please do not hesitate to reach out with any additional questions.

Sincerely,

A handwritten signature in black ink, appearing to read 'Rebecca Rettig'.

Rebecca Rettig
Chief Legal & Policy Officer
Polygon Labs

Ms. Rebecca Rettig

Attachment – Additional Questions for the Record

Representative Warren Davidson

Can DeFi work without self-custody?

Simply put, DeFi cannot work without self-custody.

DeFi is an open software system that allows users to engage in economic transactions in a self-directed manner — through self-hosted wallets — and without intermediaries. One of the hallmarks of DeFi, as noted in my written testimony, is that it is non-custodial— *i.e.*, there is no identifiable entity or person who holds or otherwise can control a user's cryptoassets on behalf of others: in DeFi systems, users maintain custody and control of their assets at all times.

Although it is possible for an intermediary to take custody of a user's assets and interact with DeFi protocols on behalf of users, this is a matter of user preference and not a technological constraint of the DeFi system.

Importing traditional third party custody requirements into these software systems would change many aspects and benefits of the current operation of DeFi protocols. This would also import an intermediary into the DeFi system, which would remove another hallmark of DeFi — that no intermediary is needed to effect transactions on the DeFi protocol.

Thus, self-custody is *necessary* to ensure the continuing benefits of DeFi.

Representative Maxine Waters:

DeFi is neutral technological infrastructure — software protocols that operate much like the protocols that underlie the Internet today. DeFi systems do not require disclosure of — nor do they recognize or take account of — any personally identifiable information and thus, are able to bring greater inclusivity to economic transactions.

1. Which of the following options best describes your self-identified race? (you may choose more than one)

- a. ***White or Caucasian***
- b. Black or African American
- c. Hispanic/Latinx
- d. Asian
- e. Middle Eastern/North African

Ms. Rebecca Rettig

- f. Choose not to answer
- g. Prefer to self-describe (please specify)

2. Which of the following options best describes your gender identity?

- a. ***Woman***
- b. Man
- c. Non-binary
- d. Transgender Man
- e. Transgender Woman
- f. Choose not to answer
- g. Prefer to self-describe (please specify)



Amanda Tuminelli

Responses to Questions for the Record

“Decoding DeFi: Breaking Down the Future of Decentralized Finance”

September 26, 2024

Question from Representative Warren Davidson: “Can DeFi work, without self-custody?”

Thank you for the question. In short, no, decentralized finance (“DeFi”) cannot work without self-custody because the intermediary-less nature of DeFi requires self-custody.

DeFi is an umbrella term generally used to describe blockchain-based software protocols that enable people to engage in economic activities on a peer-to-peer basis and allow people to self-custody their assets while doing so. More specifically, DeFi transactions rely on public key encryption that allows users to securely interact with public blockchains without the involvement of or need for third-party intermediaries. People use “wallets” to store their own cryptographic keys, which allow them to access, safeguard, and use their assets themselves—akin to holding cash in a traditional wallet. In order to communicate with a smart contract in DeFi, users must use their cryptographic keys, making self-custody essential to DeFi.

Because people are able to custody their own funds and maintain control over them, DeFi is an improvement on the centralized finance (“CeFi”) and traditional finance (“TradFi”) models, where a third-party holds persons’ assets on their behalf. These intermediaries safeguard customer assets and effectuate transactions for customers as a service. For this reason, regulations concerning these models are premised on the existence of a central operator that takes responsibility for customers’ funds and are responsive to a central risk exposure for CeFi and TradFi customers: the intermediary itself. But when using DeFi protocols, users possess and control their own assets via their private keys, and therefore, the risk that users will lose funds due to a third-party’s custodial mismanagement or other system failures is eliminated.

Questions from Representative Maxine Waters:

1. “Which of the following options best describes your self-identified race?”
 - a. White or Caucasian
2. “Which of the following options best describes your gender identity?”
 - a. Woman



Peter Van Valkenburgh¹

Director of Research at Coin Center

RESPONSES TO QUESTIONS FOR THE RECORD

Subcommittee on Digital Assets, Financial Technology and Inclusion

“Decoding DeFi: Breaking Down the Future of Decentralized Finance”

September 10, 2024

Responses to Questions for the Record Submitted by Representative Warren Davidson

1. *Can DeFi work without self-custody?*

No. As you know, “DeFi” is a somewhat vague and disputed term. Nonetheless, any reasonable interpretation of “DeFi” involves technologies that enable persons to make financial transactions online without the involvement of any trusted intermediaries, just as we can do with physical cash transactions offline. Therefore, at the core of “DeFi” is the assumption that the parties involved in a DeFi transaction will be in full and unilateral control of their digital assets before sending or after receiving them, i.e. they will have “self-custody” of their assets. As you know, self-custody of digital assets is achieved by retaining control over a digital wallet that safekeeps the relevant private keys that can control the movement of digital assets on-chain.

The ability, indeed, the right to maintain direct and exclusive control over our own assets is fundamental to the future of our liberty, privacy, and autonomy. Despotism and illiberal governments across the world have already and will, as technologies become more available, increasingly funnel the financial activities of their citizens through state-run or quasi-state-run intermediaries in order to surveil and control the behavior of their citizens. That is inherently unamerican and would violate our constitutional rights. Your bill, the *Keep Your Coins Act*, rightly buttresses our constitutional safeguards with a clear prohibition against any executive action that would jeopardize our ability to self-custody our digital assets.² Coin Center thanks you for your leadership and we support your legislation.

¹ Peter is Director of Research at Coin Center, the leading independent non-profit research and advocacy group focused on the public policy issues facing cryptocurrency technologies such as Bitcoin. <http://coincenter.org>

² H.R. 4841, 118th Cong. (2023), available at <https://www.congress.gov/bills/118th-congress/house-bill/4841/text>.

Responses to Questions for the Record Submitted by Ranking Member Maxine Waters:

- 1. Which of the following options best describes your self-identified race? (you may choose more than one)*

Thank you Ranking Member Waters for your question. Of the options presented, I choose: “f. Choose not to answer.”

- 2. Which of the following options best describes your gender identity?*

Of the options presented, I choose “f. Choose not to answer.”

Once again, thank you for the opportunity to testify on these important topics.



The Honorable Patrick McHenry
Chair
House Financial Services Committee
2129 Rayburn House Office Building
Washington, DC 20515

The Honorable Maxine Waters
Ranking Member
House Financial Services Committee
4340 O'Neill House Building
Washington, DC 20515

The Honorable French Hill
Chair
Subcommittee on Digital Assets, Financial
Technology and Inclusion
1533 Longworth House Office Building
Washington, DC 20515

The Honorable Stephen Lynch
Ranking Member
Subcommittee on Digital Assets, Financial
Technology and Inclusion
2109 Rayburn House Office Building
Washington, DC 20515

September 27, 2024

Dear Chair McHenry, Ranking Member Waters, Subcommittee Chair Hill, and Ranking Member Lynch,

Thank you again for the opportunity to testify before the Subcommittee on Digital Assets, Financial Technology and Inclusion of the House Committee on Financial Services.

I have received the questions you sent me from members of the Committee in follow up to the Subcommittee's hearing on September 10, 2024. My responses are shared below. If you require any further information from me, please do not hesitate to reach out.

Best regards,

-Mark

Mark Hays
Senior Policy Analyst
Americans for Financial Reform
markhays@ourfinancialsecurity.org



Additional Questions for the Record
Subcommittee on Digital Assets, Financial Technology and Inclusion Hearing
“Decoding DeFi: Breaking Down the Future of Decentralized Finance.”
September 10, 2024

1. Regarding Congressman Davidson’s question “can DeFi work without self-custody?”

Currently, my best answer to this question is, “It’s unclear.” To elaborate:

Three fundamental – though not exclusive – features of Decentralized Finance are 1) the use of self-hosted wallets (which are meant to ensure their users retain custody of their assets, as opposed to custody being granted to a third party); 2) the use of smart contracts to facilitate financial transactions (such as staking or lending) purportedly without active facilitation by a third party, and 3) decentralized autonomous organizations (DAOs), which direct the underlying development and operation of a platform and its protocols via governance tokens and other distributed decision-making mechanisms.

Operationally, it seems reasonable, if not already in practice, that a platform could use or enable the use of the second and third feature above, while using hosted or custodial wallets instead. In this scenario, the platform may play a more active role in initiating transactions on behalf of its users, but their intervention would be limited to that role. The overall governance of the platform, including decisions about which protocols to use, what administration is needed, how validation works, etc., could remain with the platform’s DAO, and developers could continue to interact independently with the platform’s source code to create and offer protocols that facilitate different types of transactions.

I imagine purists would say that DeFi without self-custody is not DeFi at all. That said, while some industry experts see decentralization as a binary condition, others have asserted it is more fluid. To paraphrase the findings from CFTC’s Technology Advisory Committee February 2024 report on DeFi, decentralization as it exists today or may exist operates more on a spectrum or could be best understood via a complex matrix of attributes – economic, technological, operational, and more.

More practically, examples of this ‘interim’ degree of decentralization already exist on some platforms, where intermediation with wallet formats already happens. For example, as was mentioned during the Subcommittee hearing by other witnesses, some DeFi firms provide front-end web interfaces that allow consumers to interact with DeFi protocols, effectively guiding them through the process. So, while the user may technically retain possession of their tokens, they are still reliant on a third party to an extent. Additionally, a lot of DeFi activity occurs on Layer 2 blockchains, which can be highly centralized – Coinbase’s Base, for example. It’s worth asking how well one maintains custody of one’s assets with a self-hosted wallet if the transaction is ultimately executed on a blockchain effectively controlled by one entity.

And, of course, as alluded to in my original written testimony, much of the current DeFi space already exhibits high degrees of concentration or consolidation, which in addition to raising

AFR Americans for Financial Reform

concerns about lack of oversight of such intermediation, at the very least suggests that the space is already contending with DeFi as it is versus what it aspires to be.

Since one of the primary legal and regulatory challenges that the use of self-hosted wallets presents is compliance with AML/KYC legal requirements, another possibility is that industry efforts to develop technology or approaches that can achieve such compliance via an alternative route – one that retains privacy preserving features – could bear fruit. In doing so, a crypto user could continue to use their own wallet to transact on a DeFi platform and would have some degree of confidence in the privacy of their interactions while maintaining compliance with the law.

I am aware of efforts like this, the most notable being work around zero-knowledge proofs (ZKPs) – but am not aware of any such technology yet in operation, certainly not at scale, that can provide the same sort of compliance results, much less in a way that is understood as compatible with existing AML legal requirements.

Additionally, a wrinkle with this type of scenario is that effective compliance with AML/KYC begins with Customer Due Diligence (say when a “user” or “client” is onboarded) but does not end there; ongoing monitoring is a critical means of identifying and combatting illicit finance. I’m not certain whether or how ZKPs could be used for such ongoing activity, but my understanding is that that initial premise of such proofs is focused on verifying specific information about a person or a transaction at a single point in time.

All that said, if any monitoring of financial activity by DeFi platform users’ activity is viewed as anathema by the industry or other observers, then even the use of such user-blind technology might be rejected on ideological grounds.

With that in mind, I would in good faith offer an answer to slightly amended version of the original question, namely, “Should DeFi platforms be allowed to operate outside international legal frameworks meant to combat illicit finance if they or their users are unable or unwilling to comply with such frameworks?”

The data on the use offshore financial centers and networks to evade financial regulation by all manner of actors, with many harmful outcomes, is voluminous. I will not fully restate such data but will identify a few benchmarks.

International experts have extensively documented the trillions in illicit financial flows that move from both developed and developing countries into offshore financial secrecy jurisdictions. The pathways used to facilitate such flows are many and varied, from trade-based money laundering, the global gold trade, crypto, traditional finance, and more. The sources of these illicit funds vary as well. Proceeds from narcotics trafficking, human trafficking, or terrorism finance are obvious sources, but the list is long – tax evasion, human rights violations, environmental degradation, poaching, cybercrime, wage theft, forced labor, patent fraud, stolen government proceeds from corrupt government officials, funding tied to armed groups engaged in religious or ethnic cleansing, and much more.

AFR Americans for Financial Reform

What they have in common is reliance on legal structures and intermediaries that circumvent the rules of sovereign nations, including the U.S., aimed at enabling law enforcement and other authorities to combat such harms. Right now, nations have ability to act individually or collectively to curb or contain the impact such secrecy jurisdictions, and those that rely on them, have on the rule of law.

The worst-case scenario with DeFi is one where DeFi platforms are exempt from complying with basic laws combatting illicit finance, further protected by legal frameworks which limit or absolve the developers and operators of these platforms of any liability for their role in facilitating illicit finance, or that tie the hands of sovereign governments to enforce rules applied to other financial actors in a fair and consistent manner. In that scenario, the DeFi sector becomes a global, virtual offshore secrecy jurisdiction – accessible everywhere, all the time, but virtually unaccountable to democratically elected governmental authorities.

So, perhaps to avoid such an eventuality, the prudent course would be to ensure DeFi platforms, wallet providers and other intermediaries meet AML regulatory standards consistent with other financial institutions and intermediaries to the extent that they are already operating in finance, while continuing to develop alternative technological compliance solutions that might be viable and scalable at some point in the future.

2. Regarding Ranking Member Waters' Questions Re: Demographic Information

My responses are bolded below.

1. Which of the following options best describes your self-identified race? (you may choose more than one)

- a. White or Caucasian**
- b. Black or African American
- c. Hispanic/Latinx
- d. Asian
- e. Middle Eastern/North African
- f. Choose not to answer
- g. Prefer to self-describe (please specify)

2. Which of the following options best describes your gender identity?

- a. Woman
- b. Man**



- c. Non-binary
- d. Transgender Man
- e. Transgender Woman
- f. Choose not to answer
- g. Prefer to self-describe (please specify)

G:\CMTE\FS\18\SEC\DEFL_STUDY.XML

(Original Signature of Member)

118TH CONGRESS
2D SESSION

H. R. _____

To require the Securities and Exchange Commission, Commodity Futures Trading Commission, and the Secretary of the Treasury to jointly carry out a study on decentralized finance.

IN THE HOUSE OF REPRESENTATIVES

Mr. DAVIDSON introduced the following bill; which was referred to the Committee on _____

A BILL

To require the Securities and Exchange Commission, Commodity Futures Trading Commission, and the Secretary of the Treasury to jointly carry out a study on decentralized finance.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Evaluating DeFi Opportunities Act”.

1 **SEC. 2. STUDY ON DECENTRALIZED FINANCE.**

2 (a) STUDY REQUIRED.—The Secretary of the Treas-
3 ury, in coordination with the Securities and Exchange
4 Commission and Commodity Futures Trading Commis-
5 sion, shall carry out a study on decentralized finance that
6 analyzes—

7 (1) the nature, size, role, and use of decentral-
8 ized finance blockchain protocols;

9 (2) the operation of blockchain protocols that
10 comprise decentralized finance;

11 (3) the interoperability of blockchain protocols
12 and blockchain systems;

13 (4) the interoperability of blockchain protocols
14 and software-based systems, including websites and
15 wallets;

16 (5) the decentralized governance systems
17 through which blockchain protocols may be devel-
18 oped, published, constituted, administered, main-
19 tained, or otherwise distributed, including—

20 (A) whether the systems enhance or de-
21 tract from—

22 (i) the decentralization of the decen-
23 tralized finance; and

24 (ii) the inherent benefits and risks of
25 the decentralized governance system; and

1 (B) any procedures, requirements, or best
 2 practices that would mitigate the risks identi-
 3 fied in subparagraph (A)(ii);

4 (6) the benefits of decentralized finance, includ-
 5 ing—

6 (A) operational resilience and availability
 7 of blockchain systems;

8 (B) interoperability of blockchain systems;

9 (C) market competition and innovation;

10 (D) transaction efficiency;

11 (E) transparency and traceability of trans-
 12 actions;

13 (F) disintermediation;

14 (G) privacy of user data;

15 (H) security of user personally identifiable
 16 information;

17 (I) autonomy;

18 (J) accessibility by users; and

19 (K) affordability for users;

20 (7) the risks of decentralized finance, includ-
 21 ing—

22 (A) pseudonymity of users and trans-
 23 actions;

24 (B) disintermediation; and

25 (C) cybersecurity vulnerabilities;

1 (8) the extent to which decentralized finance
2 has integrated with the traditional financial markets
3 and any potential risks or improvements to the sta-
4 bility of the markets;

5 (9) how the levels of illicit activity in decentral-
6 ized finance compare with the levels of illicit activity
7 in traditional financial markets;

8 (10) methods for addressing illicit activity in
9 decentralized finance and traditional markets that
10 are tailored to the unique attributes of each;

11 (11) how decentralized finance may increase the
12 accessibility and efficiency of cross-border trans-
13 actions;

14 (12) the feasibility of embedding self-executing
15 compliance and risk controls into decentralized fi-
16 nance; and

17 (13) any businesses or service providers that
18 are necessary to the communication of user informa-
19 tion for a material portion of any decentralized fi-
20 nance transaction.

21 (b) REPORT.—Not later than 180 days after the date
22 of enactment of this Act, the Secretary of the Treasury,
23 in coordination with the Securities and Exchange Commis-
24 sion and Commodity Futures Trading Commission, shall
25 submit to the relevant congressional committees a report

G:\CMTE\FS\18\SEC\DEFL_STUDY.XML

5

1 that includes the results of the study required by sub-
2 section (a).

3 (c) GAO STUDY.—The Comptroller General of the
4 United States shall—

5 (1) carry out a study on decentralized finance
6 that analyzes the information described in para-
7 graphs (1) through (13) of subsection (a); and

8 (2) not later than 180 days after the date of
9 enactment of this Act, submit to the relevant con-
10 gressional committees a report that includes the re-
11 sults of the study required by paragraph (1).

12 (d) DEFINITIONS.—In this section:

13 (1) DECENTRALIZED FINANCE.—The term “de-
14 centralized finance” means blockchain protocols that
15 allow users to engage in financial transactions in a
16 self-directed manner so that a third-party inter-
17 mediary does not effectuate the transactions or take
18 custody of digital assets of a user during any part
19 of the transactions.

20 (2) RELEVANT CONGRESSIONAL COMMIT-
21 TEES.—The term “relevant congressional commit-
22 tees” means—

23 (A) the Committees on Financial Services
24 and Agriculture of the House of Representa-
25 tives; and

G:\CMTE\FPS\18\SEC\DEFL_STUDY.XML

6

1 (B) the Committees on Banking, Housing,
 2 and Urban Affairs and Agriculture, Nutrition,
 3 and Forestry of the Senate.

G:\CMTE\F\18\SEC\PET_AET_STUDY.XML[Discussion Draft]

[DISCUSSION DRAFT]118TH CONGRESS
2D SESSION**H. R.** _____

To require the Secretary of the Treasury to report on privacy-preserving technologies.

IN THE HOUSE OF REPRESENTATIVESM. _____ introduced the following bill; which was referred to the
Committee on __________
A BILLTo require the Secretary of the Treasury to report on
privacy-preserving technologies.1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*3 **SECTION 1. SHORT TITLE.**4 This Act may be cited as the [“_____ Act
5 of 2024”].6 **SEC. 2. REPORT ON PRIVACY-PRESERVING TECHNOLOGIES.**7 (a) IN GENERAL.—Not later than 1 year after the
8 date of enactment of this Act, the Secretary of the Treas-

1 ury shall submit to the relevant congressional committees
2 a report that contains the following:

3 (1) An analysis of the following:

4 (A) Privacy-preserving technologies used in
5 connection with digital asset transactions, in-
6 cluding the potential benefits and risks of such
7 use.

8 (B) The number of digital asset trans-
9 actions conducted using privacy-preserving tech-
10 nologies, including, with respect to the 5-year
11 period preceding the report, the total number of
12 such transactions as a subset of the total num-
13 ber of digital asset transactions.

14 (C) The nature, operation, and characteris-
15 ties of privacy-preserving technologies used in
16 connection with digital asset transactions, in-
17 cluding software-only systems that are not
18 owned and operated by a person versus systems
19 involving software that are owned or operated
20 by a person.

21 (D) The types of privacy-preserving tech-
22 nologies and the purposes of each.

23 (E) The ability or inability to trace, track,
24 or otherwise detect potential illicit finance activ-
25 ity involving the use of privacy-preserving tech-

1 nologies in connection with digital asset trans-
2 actions.

3 (F) The ability to determine the location of
4 users of privacy-preserving technologies in con-
5 nection with digital asset transactions, includ-
6 ing if it can be determined whether the location
7 is within or involves a jurisdiction outside of the
8 United States.

9 (G) Whether and how preventing the use
10 of privacy-preserving technologies in connection
11 with digital asset transactions will help or
12 hinder the national security and economic inter-
13 ests of the United States.

14 (H) The threats and vulnerabilities posed
15 to individuals who use privacy-preserving tech-
16 nologies through public blockchain networks
17 and what risk mitigation techniques are avail-
18 able to such individuals.

19 (2) An estimate of the number of illicit digital
20 asset transactions conducted through privacy-pre-
21 serving technologies.

22 (3) A comparative analysis between the accessi-
23 bility of transactional data described in paragraph
24 (2) and the accessibility of transactional data from
25 traditional financial institutions.

G:\CMTE\FIN\18\SEC\PET_AET_STUDY.XML[Discussion Draft]

4

1 (4) A description of any limitations applicable
2 to the data used in the estimate under paragraph
3 (2).

4 (5) A description of legislative and regulatory
5 approaches employed by other jurisdictions to miti-
6 gate illicit finance risk relating to privacy-preserving
7 technologies used in connection with digital asset
8 transactions.

9 (b) RELEVANT CONGRESSIONAL COMMITTEES DE-
10 FINED.—In this section, the term “relevant congressional
11 committees” means—

12 (1) the Committees Financial Services and Ag-
13 riculture of the House of Representatives; and

14 (2) the Committees on Banking, Housing, and
15 Urban Affairs and Agriculture, Nutrition, and For-
16 estry of the Senate.

