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., S*ecret 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 Ndemo, *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 power 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 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 (ATSs) 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 IEEPA[34] 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 laundering[35] 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 business[36] 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