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 celerity 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, Ciaran. "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 pools[13] 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] Kharif, Olga. "Wash trading Is rampant on decentralized crypto exchanges." *Bloomberg*, September 12, 2023.
[16] McAughtry, 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."

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 Tornado 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 Tornado 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. "Tornado 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." *CrypoSlate*. 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 entities[26] 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 audit[38]). 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 facilities 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 FIT 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, it's 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 report[50]) 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.