



Written Testimony of Alexis Goldstein
Director of Financial Policy, Open Markets Institute

United States Congress
Joint Economic Committee

“Demystifying Crypto: Digital Assets and the Role of Government”

November 17, 2021

Chair Beyer, Ranking Member Lee, and Members of the Committee:

Thank you for inviting me to testify at this hearing. I am Director of Financial Policy at the Open Markets Institute, where my work focuses on financial regulatory policy and investor and consumer protection. Previously, I worked as a programmer at Morgan Stanley in electronic trading, and as a business analyst at Merrill Lynch and Deutsche Bank focused on equity derivatives. There, I worked primarily as a product manager for the trading and risk management software used by the global equity options flow trading desks.

I want to start by thanking the Committee for holding today’s hearing. I would like to highlight several areas that the Committee may wish to examine further, including consumer and investor protections, concentration and centralization, cyber security, and national security concerns.

Broad Investor and Consumer Protection Concerns

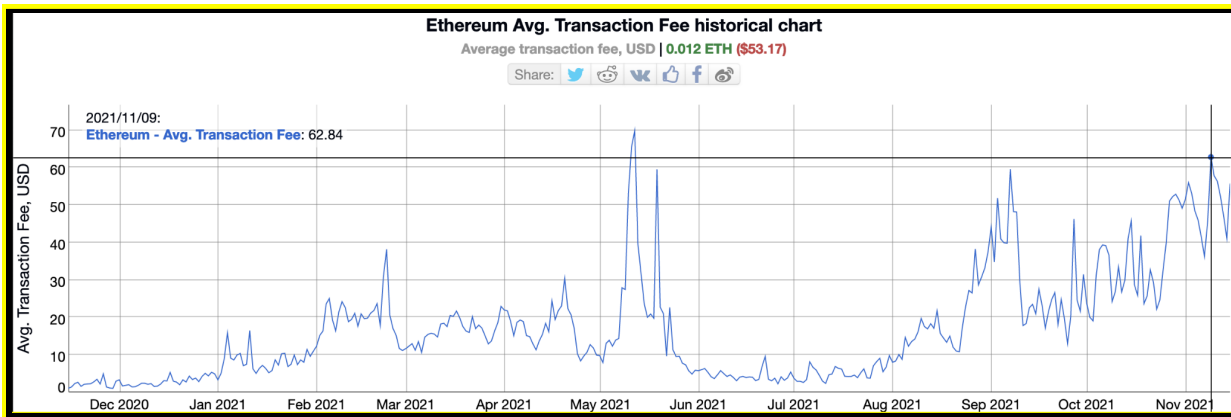
New Users with the Least Assets Often Pay Disproportionately High Fees

While crypto firms market their products as having the benefit of “democratizing” access to investments and credit, in truth, crypto markets often replicate the same problems present in traditional financial markets. For example, one of the problems with existing financial firms is that users with the least money often pay the highest proportional fees. This problem is largely replicated in the digital asset markets. For example, Coinbase has two cryptocurrency exchange platforms: Coinbase, and Coinbase Pro. Coinbase is aimed at newer users — but charges astronomically higher fees than its Coinbase Pro offering: it costs \$0.99 to purchase \$5 worth of Bitcoin on Coinbase, but only \$0.02 to do so on Coinbase Pro. Another example is that users with smaller amounts to invest may face higher fees than they could overcome with trading returns or interest income. The crypto borrowing and lending platform Aave, which allows users to deposit crypto assets and earn rewards, and use their crypto as collateral for borrowing, is explicit about this in its FAQ, writing “You can deposit any amount you want, there is no

minimum or maximum limit. Still, it's important to take into account that for really low amounts it is possible that the transaction cost of the process is higher than the expected earnings. It is recommended that you consider this when depositing very low amounts”¹

The Ethereum blockchain remains the dominant blockchain for DeFi, with an estimated 70% of all DeFi activity, according to an analysis by JPMorgan². Ethereum continues to face challenges of scalability, congestion, and extremely high fees that make DeFi transactions prohibitively expensive for users with smaller holdings.³

The average Ethereum transaction fee was \$62.84 on November 9th, 2021, according to bitinfocharts.com⁴:



Via BitInfoCharts.com, accessed November 15, 2021

Fees to merely transfer a crypto asset from one wallet to another were an estimated \$22 on November 5th, and some \$54 on November 11th.⁵

¹ <https://docs.aave.com/faq/depositing-and-earning>

²

<https://www.bloomberg.com/news/articles/2021-11-12/jpmorgan-team-suggests-crypto-s-defi-boom-slower-than-it-seems> (“The Ethereum network now has about a 70% share of DeFi activity, versus a near-total lock at the start of the year, the team added.”)

³ See: Liesl Eichholz, “Avalanche: The New DeFi Blockchain Explained”, Glassnode, February 10, 2021, <https://insights.glassnode.com/avalanche-the-new-defi-blockchain-explained/>. (“With the price of ETH on the rise, even basic token swaps on Ethereum are becoming prohibitively expensive for entry-level players, while interactions with more complex DeFi contracts can come attached with fees exceeding 0.1 ETH (over \$170 at the time of writing).”); and Nivesh Rustgi, “Ethereum Miners Earn Record \$110M Amid ETH Crash”, Crypto Briefing, May 21, 2021, <https://cryptobriefing.com/ethereum-miners-earn-record-110-million-amid-eth-crash/>. (“The gas fees essentially rendered the [Ethereum] network unusable for users with smaller holdings, while those trying to save their loans or enter new positions suffered longer wait times due to the surge in activity”).

⁴ <https://bitinfocharts.com/comparison/ethereum-transactionfees.html#1y>

⁵ <https://etherscan.io/gastracker>, accessed November 5, 2021, 6pm ET; and accessed November 11, 2021 at 9:45pm ET.

Insider Trading Concerns

A number of aspects of digital asset markets may help enable insider trading: lack of regulation and enforcement, failure to disclose potential conflicts, and pseudonymity — particularly in Decentralized Finance (“DeFi”), a term broadly used to refer to platforms that allow a user to trade, lend, or borrow cryptocurrency assets, typically without any Know Your Customer (KYC) or Anti-Money Laundering (AML) compliance.

This September, the head of Product for the largest NFT platform, OpenSea, was accused of insider trading. CNBC reported that Nate Chastain would purchase NFTs right before they were listed on the homepage.⁶ He did so from an anonymous wallet, but users/analysts happened to notice the suspicious activity.

In October, a blockchain analyst discovered that the venture capital firm Divergence Ventures extensively profitted off insider information they obtained from one of their investments, by gaming an “airdrop.” Airdrops are giveaways of newly created crypto tokens. Many projects give a portion of these airdrops to themselves and to their investors, and another portion to their historical users.⁷ Ribbon Finance told its investors that an airdrop was coming in the future. One of their investors, Divergence Ventures, set up dozens of crypto wallets so they could receive dozens of airdrops. This technique is referred to in the crypto community as “sybil farming” an airdrop.

The incident raised many questions, such as: how prevalent is this type of insider trading among venture capital investors. Divergence stated “we aren’t the only one that has tried this tactic”, and the head of research for the crypto publication *The Block* tweeted “the world suddenly discovered that basically every fund/whale Sybil farms airdrops”.

Honeypots and Rug Pulls

Crypto firms purport to be on the cutting edge of technology, however a lack of regulatory oversight and legal accountability often leads to worse cybersecurity and data privacy outcomes for users of trading platforms. There is an attitude in crypto markets that some refer to as “do your own research” (often referred to by an acronym, “DYOR”) where users who are duped are often treated as if they should have known better. This deflects responsibility from the platforms who may have failed to adhere to regulatory protections.⁸

⁶ <https://www.cnn.com/2021/09/15/opensea-insider-trading-rumors-are-true.html>

⁷ One example of an historical airdrop is the one that the Uniswap platform did September 2020. They created, and then gave away, 1 billion UNI tokens to investors, the core development team, a newly-formed “Treasury”, and historical users.

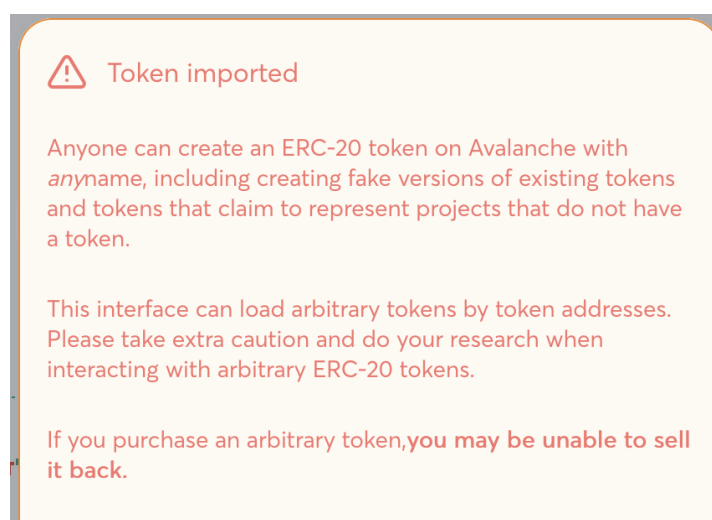
Of the 1 billion tokens, 100,613,600 of them were sent to 251,534 crypto wallets that used Uniswap prior to September 1, 2020. Each of these wallets received 400 UNI each, worth approximately \$1,400 at the time.

⁸ As the Binance Academy explains in its entry on DYOR, “Shilling is a common practice in cryptocurrency where people tend to advertise the coins that they own in hopes of positively affecting the price. Quite often, it can be difficult to distinguish the difference between a shill or an unbiased post...People with malicious intent can quickly create multiple fake accounts, attempting to trick investors

There are certain basic assumptions in traditional financial markets, including that, barring a serious liquidity crisis, you will be able to sell back a product that you buy. But in digital asset markets, malicious actors can design tokens that can be bought, but not sold. Such actors can then use DeFi platforms like Uniswap, SpookySwap, and Trader Joe to create a new “liquidity pool”: a pair of two tokens locked in a “smart contract”: these are digital contracts stored on a blockchain that automatically execute once certain conditions are met⁹. The liquidity pool is then used to facilitate trades between the two tokens on a decentralized exchange¹⁰. Once a liquidity pool exists, the makers of the so-called “honeypot” tokens¹¹ can attract new buyers, and once enough have purchased the token, the scammer pulls out all the liquidity, crashing the token price and making off with the money.

One recent example of this phenomenon is the Squid Game token, which was a token that could be purchased but not sold, but gained considerable popularity following a series of uncritical headlines in the financial press, touting its 83,000% gains, all before the anonymous development team pulled all the liquidity out of the project -- causing the price of Squid Coin to plummet to zero (a technique known as a “rug pull”).¹²

Scams are prevalent enough that some DeFi websites include an explicit warning on their website if you attempt to import a custom token (by searching for the token by its alpha-numeric address). For example, the Avalanche blockchain-based exchange Trader Joe displays the following warning when you import a custom token¹³:



into purchasing a cryptocurrency based on a ‘popular’ post within a social media platform.”

<https://academy.binance.com/en/glossary/do-your-own-research>

⁹ <https://www.ibm.com/topics/smart-contracts>

¹⁰ <https://www.gemini.com/cryptopedia/what-is-a-liquidity-pool-crypto-market-liquidity>

¹¹

<https://techcrunch.com/2018/02/16/clever-ethereum-honeypot-lets-coins-come-in-but-wont-let-them-back-out/>

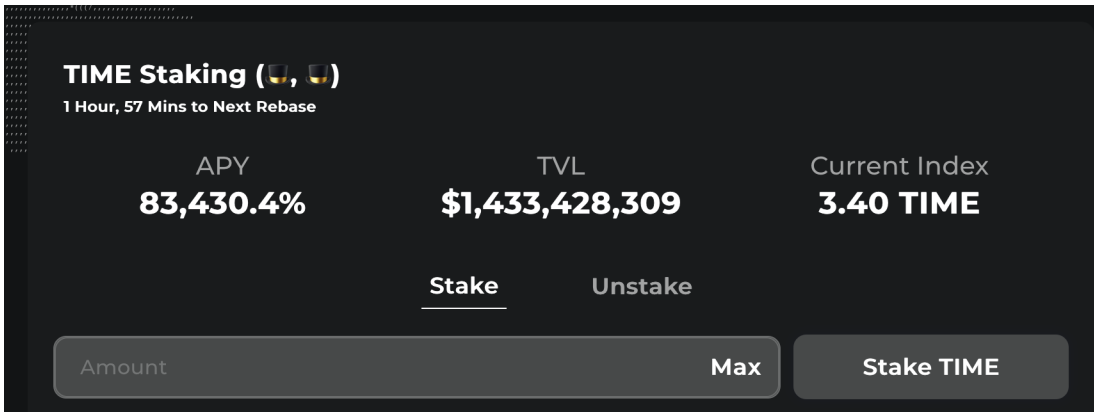
¹² <https://gizmodo.com/squid-game-cryptocurrency-scammers-make-off-with-2-1-m-1847972824>

¹³ TraderJoe.xyz, accessed November 15, 2021.

Fast-moving APRs with unclear terms

Many DeFi applications offer rewards to users if they lock (i.e., temporarily removing your ability to trade or move them) a single crypto asset, or a pair of assets, on the platform.¹⁴ These rewards are billed as interest and listed with Annual Percentage Rates (APRs) or Annual Percentage Yields (APYs), and are sometimes paid in the same crypto you've locked, but may also be paid in another cryptocurrency entirely. According to self-reported industry data, these arrangements are increasingly popular: as of November 15, 2021, there was \$111.93 billion locked into DeFi,¹⁵ an over 130% growth from less than five months ago.¹⁶

One DeFi platform called Wonderland.Money, which is a fork of the Ethereum-based OlympusDAO project,¹⁷ offers eye-popping, six-figure APRs in exchange for locking a crypto token called TIME into the platform:



Screenshot from Wonderland.Money (<https://app.wonderland.money/#/stake>), displaying a 83,430% APY for staking the crypto asset TIME, accessed November 15, 2021.

Wonderland runs on the Avalanche blockchain, and claims that its TIME token is backed by “a basket of assets” including the stablecoin “Magic Internet Money”, and promises this gives it “an intrinsic value it cannot fall below”, although it is unclear how the platform can make such a promise, nor do they disclose precisely what the level it cannot fall below.¹⁸

¹⁴ <https://www.coindesk.com/defi-yield-farming-comp-token-explained>

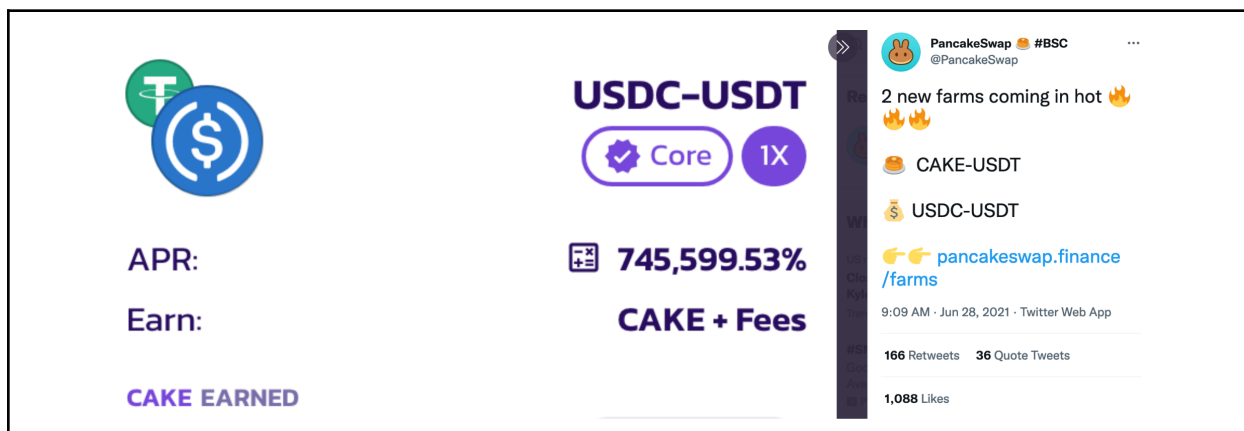
¹⁵ <https://defipulse.com/>, accessed November 15, 2021.

¹⁶ Alexis Goldstein, Written Testimony, “America on “FIRE”: Will the Crypto Frenzy Lead to Financial Independence and Early Retirement or Financial Ruin?”, U.S. House of Representatives Committee on Financial Services Subcommittee on Oversight and Investigations, June 30, 2021, <https://financialservices.house.gov/uploadedfiles/hhrg-117-ba09-wstate-goldsteina-20210630-u1.pdf> (“According to DeFi Pulse, as of June 28th there are \$48.23 billion in crypto assets locked in DeFi.”)

¹⁷ <https://www.yahoo.com/now/olympusdao-success-inspires-dozens-forks-171914320.html> (“In the case of OlympusDAO, Daniele Sesta, who co-founded Wonderland, as well as the collateralized debt position protocol Abracadabra, told his 101,000 Twitter followers that he has plans to differentiate the forked product.”)

¹⁸ <https://docs.wonderland.money/> (“Wonderland is the first decentralized reserve currency protocol available on the Avalanche Network based on the TIME token. Each TIME token is backed by a basket of

Other DeFi projects have shown these wild APRs to be either deeply misleading and/or extremely fleeting. For example, on June 28th at 9:09am ET, the Pancake Swap Twitter account tweeted a screenshot of an available 745,000% APR¹⁹ if a user locked in a pair of stablecoins: US Dollar Coin²⁰ and Tether²¹. (Tether and the company that runs it, Bitfinex, have been barred from doing business in New York state under the terms of a settlement reached with Attorney General Letitia James;²² Tether and Bitfinex also paid \$42.5 million in October to settle charges with the Commodity Futures Trading Commission of making untrue or misleading statements and omissions of material fact in connection with the Tether stablecoin²³)



Pancake Swap’s Twitter account advertising an 745,000% APR if a user locked in a pair of stablecoins: US Dollar Coin and Tether, June 28th, 2021 at 9:09am ET.

Twitter users noted in the replies that when they visited the PancakeSwap website to try and obtain the staggeringly high APR, it was nowhere close to being in the same order of magnitude, but rather in the 30-38% APR range.²⁴ When I visited PancakeSwap’s “Farms” page at 9:50am, less than an hour after the tweet was posted, I saw an APR of 15.77% for the USDC-USDT pair.

While PancakeSwap offers a rudimentary explanation of how these interest rates work in its documentation section,²⁵ this information is not presented on or linked to the main Farms page,

assets (e.g., MIM, TIME-AVAX LP Tokens etc etc) in the Wonderland treasury, giving it an intrinsic value that it cannot fall below.”)

¹⁹ <https://twitter.com/PancakeSwap/status/1409499271519297545>

²⁰ USDC is a stablecoin jointly run by the cryptocurrency exchange Coinbase and the startup Circle. <https://blog.coinbase.com/coinbase-and-circle-announce-the-launch-of-usdc-a-digital-dollar-2cd6548d23>.

²¹ Tether is a stablecoin run by Finex Inc., which operates the cryptocurrency exchange Bitfinex.

²²

<https://www.nbcnewyork.com/news/business/ny-bans-tether-bitfinex-over-false-statements-about-dollar-banking-and-losses/2904206/>; and

https://ag.ny.gov/sites/default/files/2021.02.17_-_settlement_agreement_-_execution_version.b-t_signed-c2_oag_signed.pdf.

²³ <https://www.cftc.gov/PressRoom/PressReleases/8450-21>

²⁴ See, e.g.: “Down 745 to 30% apr in 30 min.”

<https://twitter.com/TomGuerrier/status/1409505537138565122>;

²⁵ (“Yield Farm APR calculation includes both the rewards earned through providing liquidity and rewards earned staking LP [liquidity provider] Tokens in the Farm. Previously, rewards earned by LP

nor does it present the user with any terms or conditions to evaluate. While other platforms offer better explanations of how and why the APR offered by liquidity providers in yield farms might fluctuate, even with considerable explanation it may not be clear to users just how highly variable the interest rates are.²⁶

Prevalence of Forced Arbitration Clauses and Class Action Bans

In traditional financial markets, consumers and investors are often subject to forced arbitration clauses and bans on class action lawsuits. These forced arbitration clauses prevent users from suing financial firms in a court of law, instead conducting dispute resolution in private arbitration, where the outcomes are typically secret and there is no right to appeal. Curiously, many crypto websites, including DeFi sites, require users to sign forced arbitration agreements while also claiming to be decentralized autonomous organizations (DAOs) with no responsibility for conduct occurring on the platform. A review of 12 major cryptocurrency platforms showed forced arbitration and class action bans present in every single one’s terms of service:

Platform	Category	Link to Terms	Forced Arbitration?	Class Action Ban?
Binance.US	Exchange	https://www.binance.us/en/terms-of-use	yes	yes
Coinbase	Exchange	https://www.coinbase.com/legal/user_agreement/united_states	yes	yes
FTX.us	Exchange	https://ftx.us/TermsOfService.pdf	yes	yes
Kraken	Exchange	https://www.kraken.com/en-us/legal	yes	yes
Maker (via Oasis.app)	Borrowing/Lending	https://oasis.app/terms	yes	yes
Curve Finance	Borrowing/Lending	https://gov.curve.fi/tos	yes	yes
Aave	Borrowing/Lending	https://aave.com/term-of-use/	yes	yes
yearn.finance	Asset Aggregator	https://gov.yearn.finance/tos	yes	yes
Rari Capital	Asset Aggregator	https://rari.capital/terms-conditions.html	yes	yes
Fei Protocol	Asset Aggregator	https://assets.feimoney.com/docs/fei_terms_of_service_03_18_21.pdf	yes	yes
Uniswap	Exchange (DeFi)	https://uniswap.org/terms-of-service/	yes	yes
dydx	Derivatives Exchange (DeFi)	https://dydx.exchange/terms	yes	yes

Token-holders generated from trading fees were not included in Farm APR calculations. APR calculations now include these rewards, and better reflect the expected APR for Farm pairs.”)

<https://docs.pancakeswap.finance/products/yield-farming>

²⁶ More thorough explanations of the variability of rates offered in yield farming are documented on other websites, such as Uniswap’s explanation of liquidity providers and impermanent loss <https://uniswap.org/docs/v2/advanced-topics/understanding-returns/>; as well as curve.finance’s liquidity pools explanation <https://resources.curve.fi/base-features/understanding-curve>.

Users self-manage counterparty risk and the risk of hacks and scams.

There are a long list of potential scams and hacks that digital asset users can fall prey to. As Bobby Ong, co-founder of cryptocurrency data provider Coin Gecko tweeted, “Crypto is a very dangerous and adversarial place”.²⁷ Many users report having their crypto stolen when an attacker gains access to the private keys in their self-hosted wallet²⁸. There are many attempts by scammers to pose as customer support for these wallets²⁹, or as admins in chat rooms³⁰ for particular cryptocurrency projects, in order to gain the trust of a potential victim, and convince them to click malicious links or take other steps to reveal their private keys.

Scams and hacks are prevalent enough that there are websites³¹, guides³², and services devoted to identifying them. These include suggestions that users read the “smart contract” code of any cryptocurrency token they wish to purchase, looking out for common pitfalls—a fairly high bar for non-programmers.³³ New tokens will often partner with firms that offer audits of their code to signal that the product is valid and safe.³⁴

In the last four months alone, digital assets markets have been hit with over \$1 billion in hacks, exploits, and erroneous payments:

- The cryptocurrency protocol **bZx** had its private key compromised due to a phishing scam targeted at a member of its development team.³⁵ As of this writing, \$55 million in crypto assets have been lost, with the potential of more losses to come. (November 2021)
- The Ethereum based DeFi platform **Cream Finance** lost \$130 million due to a flash loan exploit. This is the third hack suffered by the platform.³⁶ (October 2021)
- A bug in an upgrade to the borrowing and lending platform **Compound** put \$147 million worth of the platform’s funds at risk.³⁷ (October 2021)
- The Ethereum blockchain-based **Indexed Finance** lost \$16 million in a smart contract exploit. The platform believed they identified the hacker, but the hacker refused to return the funds.³⁸ (October 2021)

²⁷ <https://twitter.com/bobbyong/status/1403881080902471680?s=21>

²⁸ Examples: <https://twitter.com/0xflim/status/1459673602874249216>; and XX.

²⁹ <https://coingeek.com/beware-of-latest-scam-metamask-warns-of-new-phishing-bot/>

³⁰ <https://usa.kaspersky.com/blog/cryptoscam-in-discord/24193/> (“Scammers are luring Discord users to a fake cryptocurrency exchange with the promise of free Bitcoin or Ethereum”)

³¹ See, e.g. <https://tokensniffer.com/>.

³² See, e.g. <https://coinmarketcap.com/alexandria/article/how-to-identify-and-avoid-uniswap-scams> and <https://www.cylynx.io/blog/the-rise-of-cryptocurrency-exit-scams-and-defi-rug-pulls/>.

³³ See, e.g.: <https://twitter.com/ahmedismail/status/1426141622287298569?s=21>.

³⁴ “DeFi Audit Firms Seeing ‘Overwhelming Demand’ Even Amid Token Price Slump”, Coin Desk, Oct 15, 2020, <https://www.coindesk.com/defi-audit-firms-swamped>. (“The separation between audited projects and non-audited projects became palpable over DeFi’s boom months – often referred to as “DeFi Summer” – as code flaws in some projects led to contracts being exploited by hackers.”)

³⁵ <https://rekt.news/bzx-rekt/>

³⁶ <https://decrypt.co/84590/cream-finance-suffers-third-hack-losing-over-130-million>

³⁷ <https://rekt.news/compound-rekt/>

³⁸ <https://beincrypto.com/indexed-finance-attacker-refuses-return-16-million-authorities/>

- The Avalanche-blockchain based platform **Vee Finance** was hacked for a total of \$35 million.³⁹ (September 2021)
- The Avalanche blockchain-based **Zabu Finance** was exploited for \$3.2 million.⁴⁰ (September 2021)
- The Binance Smart Chain-based **pNetwork** lost \$12 Million in a hack (September 2021)⁴¹
- **SushiSwap**'s token platform MISO lost \$3 million due to a hack.⁴² (September 2021)
- The cryptocurrency exchange **Bitfinex** (whose owners are also the issuers of the stablecoin Tether) paid over \$23 million in Ethereum gas fees (7,676.61 ETH) in order to move \$100,000 worth of Tether to deversifi.com⁴³, in a single transaction.⁴⁴ While the miner returned the majority of the gas fee, they appear to have kept 291 ETH – worth some \$850,000.⁴⁵ (September 2021)
- **Poly Network** initially lost \$613 million to a hacker exploiting a bug in their smart contract.⁴⁶ Many crypto market participants blacklisted the hackers address, leading to most of the funds eventually being returned.⁴⁷ (August 2021)

In a sign that exploits are increasing in severity and frequency, this is more than three times the amount lost to hackers in DeFi hacks and exploits from 2019 - April 2021.⁴⁸

By contrast, in traditional financial markets, market intermediaries like broker-dealers and exchanges are subject to a host of cybersecurity and data privacy regulations and ongoing examinations.

Concerns Surrounding Potential False Advertising or Misleading Claims

There are also false advertising concerns in the space. For example, the exchange Crypto.com tells its users that it can get "\$25 USD" if it refers a friend to its platform. But this referral bonus marketing in its mobile app makes it seem that the bonus is "\$25 USD", when it is actually \$25 in Crypto.com's own coin, CRO, and the user must meet certain criteria before accessing this CRO reward: either by signing up for the Crypto.com credit card, or purchasing a total of \$400

³⁹

<https://markets.businessinsider.com/news/currencies/avalanche-vee-finance-crypto-hack-ether-bitcoin-defi-platform-lost-2021-9>

⁴⁰ <https://www.coindesk.com/tech/2021/09/13/avalanche-based-zabu-finance-exploited-in-32m-hack/>

⁴¹ <https://decrypt.co/81301/defi-bridging-protocol-pnetwork-suffers-12-million-hack>

⁴² <https://decrypt.co/81120/sushiswaps-token-launchpad-hacked-over-3m-ethereum>

⁴³

<https://markets.businessinsider.com/news/currencies/crypto-exchange-bitfinex-ethereum-tether-transaction-fees-error-deversifi-2021-9>

⁴⁴ <https://etherscan.io/tx/0x2c9931793876db33b1a9aad123ad4921dfb9cd5e59dbb78ce78f277759587115>

⁴⁵ <https://etherscan.io/tx/0x85294effd53126b3bfa9e7f655267e00ac1ae2ef76f4569644670bf5403637d6>

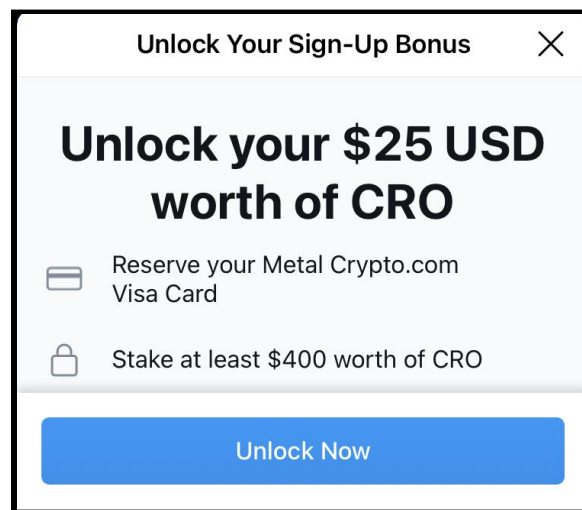
⁴⁶

<https://www.reuters.com/technology/how-hackers-stole-613-million-crypto-tokens-poly-network-2021-08-12/>

⁴⁷ <https://www.lawfareblog.com/disrupting-cryptocurrencies-2-lessons-poly-hack>

⁴⁸ <https://finance.yahoo.com/news/messari-defi-exploits-total-284-091600754.html> ("over \$284 million has been lost to hackers from decentralized finance (DeFi) hacks and exploits since 2019.")

worth of this CRO coin and “staking” it -- locking the CRO into the Crypto.com site for a certain period of time.⁴⁹



Crypto.com app, accessed November 15, 2021

Concentration and Centralization Concerns

Is Decentralized Finance Truly Decentralized?

Some DeFi proponents claim that their systems are purely [peer-to-peer](#) and operate without intermediaries.⁵⁰ However, market participants, including crypto metrics providers, have raised [questions](#) as to whether or not DeFi is truly decentralized given factors such as protocol fees, governance token control, and platform treasuries.

Most tellingly, while marketing oneself as “decentralized” may be opportune from regulatory, legal and marketing standpoints, when crises happen that warrant quick action many DeFi platforms take actions with many indicia of centralized control.

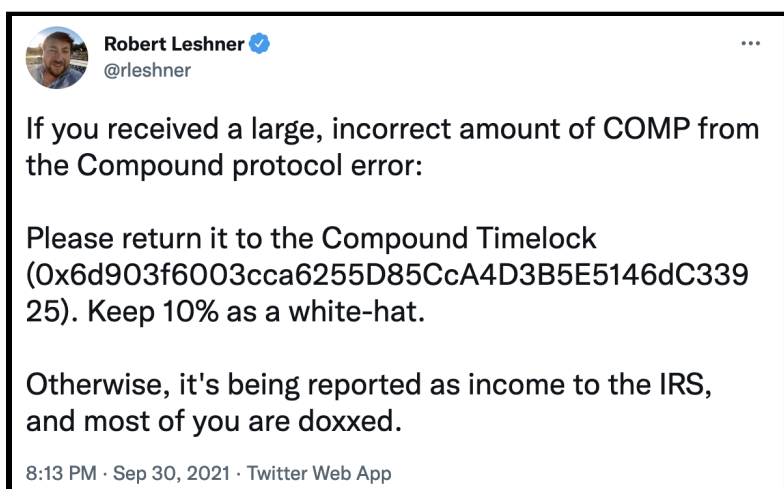
Compound threatening to report user’s income to the IRS following a bug

⁴⁹ The [actual conditions](#) (available on the website) of even accessing this \$25 in CRO coin are that the user must either stake \$400 in CRO, or sign up for the Crypto.com credit card. The only way to turn this into \$25 USD would be to meet the conditions, trade it for USD (ostensibly after paying a fee), and only if the price of CRO hasn't depreciated from the \$25 USD level after meeting the conditions. See: <https://help.crypto.com/en/articles/3124990-bg25-referral-program>.

⁵⁰ “DeFi vs. Traditional Finance”, Ethereum Foundation, <https://ethereum.org/en/defi/>. (See: “One of the best ways to see the potential of DeFi is to understand the problems that exist today...There's a premium to financial services because intermediary institutions need their cut.”)

A bug in the crypto borrowing and lending DeFi platform **Compound** led to erroneously large rewards of their crypto token COMP being distributed to certain users.⁵¹ (One user allegedly was able to claim some \$28 million worth of COMP tokens⁵²).

During the infrastructure bill negotiation, the crypto industry was adamant that they didn't possess the technological capability to ensure tax reporting among its users. However, in response to this bug in their protocol's code, the CEO of Compound Robert Leshner demanded that users who received large sums of COMP tokens return them. He said they could keep 10% should they return them -- but if they didn't return the rest, he threatened that they would be reported to the IRS:



This stands in stark contrast to claims that tax reporting in DeFi wasn't possible. Indeed, it is clearly viewed as possible when such tax reporting can be viewed as a coercive attempt to have users self-correct bugs in Compound's code. This makes it clear that the lack of tax reporting is a design decision, not a technical limitation.⁵³

Curve Finance Shutting Down a Competitors' Presence on their System via an "Emergency DAO"

Curve Finance is a major crypto borrowing and lending platform. Like many DeFi protocols, Curve uses a decentralized autonomous organization (DAO), to govern the project and allow users to vote on its future. Part of the motivation of creating DAOs is to argue that decision-making is not controlled by a single institution.⁵⁴ But recent events have called into question just how "decentralized" Curve truly is.

⁵¹ Andrew Ross Sorkin, Jason Karaian, Sarah Kessler, Stephen Gandel, Michael J. de la Merced, Lauren Hirsch and Ephrat Livni, "The limits of decentralization", NYTimes Dealbook, Oct. 26, 2021, <https://www.nytimes.com/2021/10/04/business/dealbook/facebook-whistleblower-frances-haugen.html#link-1567b404>.

⁵² <https://etherscan.io/tx/0xf4bfef1655f2092cf062c008153a5be66069b2b1fedcacbf4037c1f3cc8a9f45>

⁵³ <https://www.bloomberg.com/opinion/articles/2021-08-26/crypto-doesn-t-have-to-enable-tax-cheats>

⁵⁴ <https://www.investopedia.com/tech/what-dao/>

Curve allows external projects to add their own liquidity pools, and attempt to lure in more users to the liquidity pool by offering better rewards than competitors. Recently, a new project called Mochi Finance created a new liquidity pool on Curve, and through exploiting a series of loopholes, was able to amass a huge amount of voting power in Curve’s governance system.

Curve accused them of taking advantage of their governance system,⁵⁵ called the incentives that Mochi offered “bribes”, and raised “serious security and decentralization” concerns.⁵⁶ As a result, Curve called a meeting of what they called its “Emergency DAO” and shut down Mochi’s liquidity pool entirely.⁵⁷ The move received criticism⁵⁸ for being against the ethos of decentralization.⁵⁹

Major Cryptomarket Players control key Sushi Swap Wallet

Certain platforms have “Development Funds” that are meant to further the growth of the platform’s ecosystem; typically, users who hold governance tokens in the platforms can vote on how to spend these funds. However, some of these Development Funds are controlled by a core group of people, via multi-signatures (“multi-sig”) wallets—cryptocurrency wallets that require two or more people to digitally “sign” and execute a particular transaction. SushiSwap is a DeFi platform whose Development Fund is controlled by a multi-sig wallet, which includes some very prominent crypto market actors as signers, including⁶⁰:

- Sam Bankman-Fried: CEO of FTX and co-founder of Alameda Research, a crypto proprietary trading fund;
- Robert Leshner: The CEO of the crypto lending and borrowing DeFi firm, Compound Labs;
- CMS Holdings: a proprietary cryptocurrency investment firm co-founded by former executives from Circle and crypto trading firm DRW/Cumberland (Daniel Matuszewski, Julien Collard-Seguin, and Bobby Cho); and
- Matthew Graham (Sino Global Capital)

Concentration

⁵⁵ <https://cryptobriefing.com/curve-blocks-mochi-after-alleged-attempted-governance-attack/>

⁵⁶ <https://gov.curve.fi/t/the-curve-emergency-dao-has-killed-the-usdm-gauge/2307>

⁵⁷ Andrew Thurman, “‘Curve Wars’ Heat Up: Emergency DAO Invoked After ‘Clear Governance’, Attack”, Nov 11, 2021, <https://www.coindesk.com/business/2021/11/11/curve-wars-heat-up-emergency-dao-invoked-after-clear-governance-attack/>.

⁵⁸ <https://twitter.com/mewn21/status/1458771401381486600> (“im saying its a bad precedent to discriminate against a user, any user, who accrued voting rights over your protocol without exploiting or breaking a mechanism. either ur mechanism is broken or its not defi”)

⁵⁹ *Id.* (“the decision from the decentralized autonomous organization, or DAO, has prompted much community debate, as some have argued that the protocol should not single out any one user and that blacklisting another protocol runs against DeFi’s open, permissionless ethos.”)

⁶⁰ <https://docs.sushi.com/governance/current-governance-model>

While cryptocurrency industry insiders promote the “democratized” benefits of digital assets, in truth, crypto concentrations of money and power match or surpass those in traditional financial markets.

The concentration of particular cryptocurrency assets into a small handful of addresses raise concerns about power concentrations. A paper by Igor Makarov and Antoinette Schoar found that, in the last five years, the top 10% of Bitcoin miners controlled 90% of all mining capacity, while 0.1% of miners (about 50 of them) controlled close to 50% of mining capacity.⁶¹ In addition, many of the so-called “governance tokens”, which provide holders the ability to vote on proposals affecting the future of certain cryptocurrency projects, are owned by a very small portion of token holders. According to the crypto metrics provider Glassnode, as of November 15, 2021:

- Over 98% of the governance tokens (COMP) for the crypto lending and borrowing platform Compound are on by the top 1% of token holders⁶² — Glassnode specifies that “Exchange addresses, smart contract addresses, and other special asset-specific addresses (e.g. team fund addresses) are excluded”.⁶³
- Over 96% of the governance tokens (UNI) for the exchange Uniswap are held by the top 1% of token holders.⁶⁴

Venture Capitalists and other private investors are a significant presence in cryptocurrency markets, and appear to hold considerable market power—and their investment in the space is growing fast. Venture Capital firms invested \$17 billion in digital asset firms in the first six months of 2021, more than three times what they invested in all of 2020.⁶⁵

⁶¹ Igor Makarov and Antoinette Schoar, “BLOCKCHAIN ANALYSIS OF THE BITCOIN MARKET”, NATIONAL BUREAU OF ECONOMIC RESEARCH, October 2021, https://www.nber.org/system/files/working_papers/w29396/w29396.pdf.

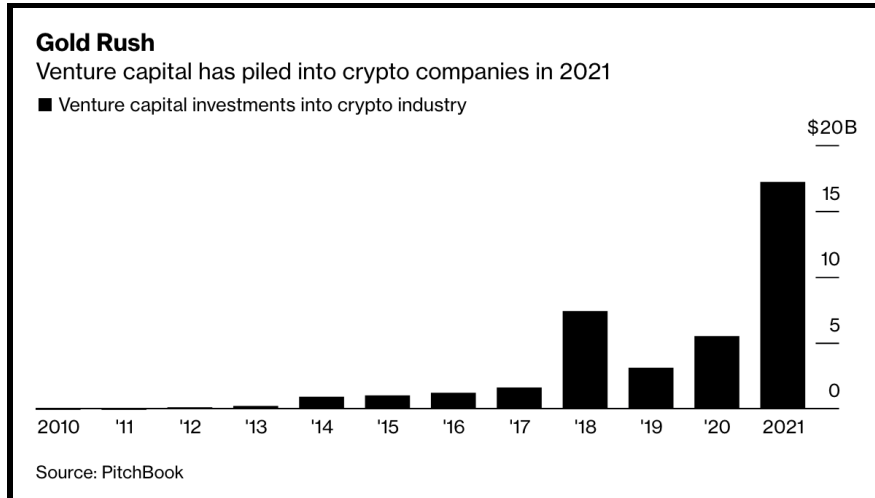
⁶² Glassnode, metrics for Compound’s COMP token: Percent of Supply Held by Top 1% Addresses, <https://studio.glassnode.com/metrics?a=COMP&category=&m=distribution.Balance1PctHolders&modal=logi>

⁶³ <https://docs.glassnode.com/api/distribution#supply-of-top-1-addresses>

⁶⁴ Glassnode, metrics for Uniswap’s UNI token: Percent of Supply Held by Top 1% Addresses, <https://studio.glassnode.com/metrics?a=UNI&category=&m=distribution.Balance1PctHolders&modal=logi>

⁶⁵

<https://www.bloomberg.com/news/articles/2021-06-18/venture-capital-makes-a-record-17-billion-bet-on-crypto-world>



This summer, PayPal co-founder and billionaire venture capitalist Peter Thiel, along with Galaxy Digital CEO Mike Novogratz, and billionaire hedge fund manager Alan Howard led a \$10 billion investment in a new crypto exchange called “Bullish” that will utilize the EOS blockchain.⁶⁶

Some venture capital firms may be using retail investors as “exit liquidity” — investors to sell their tokens to once they’re ready to exit. The *NYTimes* reported on one such potential offloading by insiders onto retail in a report about the collapse of the Internet Computer (ICP) token. According to the *NYTimes*, a number of wallet addresses presumed to be insiders “deposited 10 million ICP tokens worth more than \$2 billion to exchanges after the initial coin offering, giving the impression they were transferred for trading, not safeguarding. These transfers coincided with significant drops in the price of ICP, the report said. Small investors, left out of the process, were stuck.”⁶⁷ Among Internet Computers large investors were the venture capital firm Andreessen Horowitz (a16z).

Many industry participants are deliberately aiming for monopoly-levels of power and concentration. Barry Silbert, the head of the digital assets conglomerate Digital Currency Group (which boasts dozens and dozens of crypto portfolio companies) told the *Wall Street Journal* that “the model I use as an inspiration is Standard Oil.”⁶⁸ This is a particularly troubling comment, as Standard Oil was an archetype monopoly that routinely exploited anemic legal restrictions, flagrantly engaged in law breaking activities, and implemented destructive and unfair market practices such as mergers, predatory pricing, and other coercive tactics to fortify its market dominance.⁶⁹ Stephen Stonberg, the COO of crypto exchange Bittrex, told the podcast BlockCrunch, “when I first saw crypto, I thought, this is gonna be like hedge funds were in the 1980s, you’re going to be able to charge whatever fees you want.” Stonberg went on to

⁶⁶ <https://www.pionline.com/markets/thiel-backed-blockone-injects-billions-cryptocurrency-exchange>

⁶⁷ <https://www.nytimes.com/2021/06/28/business/dealbook/icp-cryptocurrency-crash.html>

⁶⁸ <https://www.wsj.com/articles/digital-currency-group-wants-to-be-cryptos-standard-oil-11635764400>

⁶⁹ Naomi R. Lamoreaux, “The Problem of Bigness: From Standard Oil to Google,” <https://www.aeaweb.org/articles?id=10.1257/jep.33.3.94>.

describe that "there's always this period of lots of companies and then consolidation. And that's like the internet in the 90s, and now you have three companies that control the whole world."⁷⁰

Outsized Impact of Very Wealthy Crypto Users

Digital asset markets appear particularly susceptible to very large users moving their funds in and out of various projects. To take one example, prior to October, the DeFi borrowing and lending platform Aave was consistently ranked first in terms of "total value locked" – the amount of crypto assets reportedly locked into the platform.

But on October 29, 2021, a single user withdrew \$4.2 billion in crypto assets from Aave, causing lending and borrowing interest rates to spike, and their total crypto locked to plummet ~18% in a matter of hours. Aave fell from being ranked first in TVL to third. The event raised questions about whether other platforms are similarly dependent on very wealthy users, and what sorts of volatility may follow should those users decide to remove their crypto assets.

National Security Concerns

National security concerns arise when considering any transfer of money - including within the banking system. Cryptocurrency, however, raises unique concerns given the lack of illicit financing controls on many platforms, the borderless nature of transactions and the dispositional fondness for anonymity among crypto users and firms.

Ransomware attacks are increasing in number, and cryptocurrency assets are often used to layer and obscure ransomware payments. An October 2021 FinCEN report found that cryptocurrency exchanges with lax Know Your Customer/Anti-Money Laundering ("KYC/AML") compliance are the preferred cash-out points for ransomware payments.⁷¹ Case in point, a recent Department of Justice arrest of two foreign nationals over ransomware attacks⁷² included a warrant posted showing that up to \$13 million was held by one of the foreign nationals at the cryptocurrency exchange FTX.⁷³

The October FinCEN report also found that "Ransomware-related payments are being converted to other types of [cryptocurrency] through decentralized exchanges or other DeFi applications."⁷⁴

⁷⁰ The Amazon Moment for Crypto Exchanges - Stephen Stonberg, Bittrex Global, Ep. 126, <https://podcasts.apple.com/us/podcast/amazon-moment-for-crypto-exchanges-stephen-stonberg/id1350649166?i=1000504410789>

⁷¹

<https://www.fincen.gov/news/news-releases/fincen-issues-report-ransomware-trends-bank-secrecy-act-data>

⁷² <https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya>

⁷³ <https://www.justice.gov/opa/press-release/file/1447131/download>

⁷⁴

<https://www.fincen.gov/news/news-releases/fincen-issues-report-ransomware-trends-bank-secrecy-act-data> ("Ransomware-related payments are being converted to other types of [Convertible Virtual Currencies] through decentralized exchanges or other DeFi applications. Some DeFi applications allow for automated

One crypto mining pool, Marathon Digital Holdings, attempted to introduce a “sanctions-compliant” mining pool. However, many in the crypto community complained, and Marathon reversed course.⁷⁵ Marathon CEO Fred Thiel told *The Block* “you have groups in the bitcoin community who are all about maximum decentralization. They are against the whole concept of doing anything that has to do with financial regulatory compliance or government regulation.”⁷⁶

In October, the Treasury Department’s Office of Foreign Assets Control (OFAC) clarified this October that miners (and all other actors in the digital asset markets) are expected to comply with OFAC’s new guidance on sanctions compliance.⁷⁷ In the guidance, they wrote that “All companies in the virtual currency industry, including technology companies, exchangers, administrators, miners, and wallet providers, as well as more traditional financial institutions that may have exposure to virtual currencies” should consider incorporating the controls outlined in OFAC’s guidance into their sanctions compliance programs.⁷⁸

Cities that have been considering adopting city-specific crypto tokens, in partnership with the CityCoins project⁷⁹ which is built on the Stacks platform, should pay particular attention to the national security concerns of doing so. While it’s unclear if the Stacks project’s definition of “mining”⁸⁰ bears any meaningful resemblance to what is currently considered crypto mining, the publicly-available details of the project⁸¹ nevertheless raise particular national security questions, including how CityCoins plan to adhere to the new OFAC guidance, and ensure that they aren’t allowing crypto addresses on OFAC’s Specially Designated Nationals and Blocked Persons List to participate in the project.

Climate and Supply Chain Concerns

The two largest cryptocurrencies, Bitcoin and Ether, currently use a “Proof of Work” consensus mechanism to validate transactions. Proof of Work crypto mining creates a number of extensive climate harms, which include annual energy consumption akin to that of entire nations⁸², 30,700 tons of electronic waste annually, higher electricity bills for residents of states with crypto

peer-to-peer transactions without the need for an account or custodial relationship. FinCEN analysis of transactions on the BTC blockchain identified ransomware-related funds sent indirectly to addresses associated with open protocols for use on DeFi applications.”)

⁷⁵ <https://www.theblockcrypto.com/linked/106865/marathon-ofac-bitcoin-mining-pool-taproot>

⁷⁶ *Id.*

⁷⁷ <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20211015>

⁷⁸ https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf

⁷⁹ <https://www.citycoins.co/citycoins-faq>

⁸⁰ <https://github.com/citycoins/citycoin/blob/main/citycoin-prd.md#mining> (“The act of mining a CityCoin is defined by someone sending Stacks tokens (STX) to the smart contract created for the city, using the following criteria.”)

⁸¹ <https://github.com/citycoins/citycoin/blob/main/citycoin-prd.md#trading-and-open-markets> (“CityCoins is an open source project and any CityCoin can be listed and available for trading on centralized and decentralized exchanges at any time after mining has begun.”)

⁸² <https://www.bbc.com/news/technology-56012952>

mining⁸³, and quality of life issues⁸⁴. Over 70 climate, economic, racial justice, business and local organizations recently wrote to Congress, asking them to mitigate the considerable contribution portions of the cryptocurrency markets are making to climate change.

In addition, Proof of Work cryptocurrency mining has been exacerbating the shortages of semiconductors.⁸⁵ Senators Maggie Hassan and Joni Ernst recently introduced a bill calling on the Treasury Department to compile a report on how cryptocurrency mining operations are impacting semiconductor supply chains.

Systemic risk concerns

Systemic risk arises when the scope, size, scale or interconnectedness of certain activities can metastasize and spread contagion to other market participants or the broader financial system. Certain indicia of potential systemic risk - including leverage, opacity in market data, and poorly understood interlinkages between market participants - is currently present in digital asset markets.

Leverage

While US-based exchanges have reduced the amount of leverage available to smaller investors as of this summer, DeFi platforms offer many ways for users to lever up:

Flash Loans

Flash loans are unsecured loans where capital is borrowed and repaid in a single transaction, through the use of smart contracts. As the crypto platform Monolith describes it, flash loans allow users to “potentially borrow huge sums of money at a marginal cost.”⁸⁶ They are offered by the Aave platform, and there is no upper limit to the size of the flash loan one can obtain⁸⁷: the largest flash loan processed to date was about \$200 million. Flash loans are typically used to try and take advantage of arbitrage opportunities such as discrepancies between the price of a

⁸³

<https://newsroom.haas.berkeley.edu/research/power-hungry-cryptominers-push-up-electricity-costs-for-lo-cals/>

⁸⁴

<https://www.wjhl.com/news/local/noisy-bitcoin-mines-neighbors-hope-monday-meeting-yields-answers-from-power-provider/>

⁸⁵

<https://www.economist.com/graphic-detail/2021/06/19/crypto-miners-are-probably-to-blame-for-the-graphic-chip-shortage>

⁸⁶ <https://medium.com/monolith/understanding-defi-flash-loans-explained-1a5928a4a612>

⁸⁷ *Id.* (“Unlike a regular loan, though, there’s no limit to the amount the user can borrow, and it can be taken out instantly, as long as it’s paid back in the same transaction — at a flash speed. This is made possible by smart contracts. They’re programmed to ensure that the loan is returned, otherwise the transaction gets blocked. The revolutionary part is how quickly it all happens, and the borrower only needs to shell out for a transaction fee to pay for the whole process.”)

given cryptocurrency on different exchanges.⁸⁸ However, these loans have also been increasingly used to exploit vulnerable DeFi protocols, and steal millions of dollars. As of June 2021, Aave had issued almost \$4 billion in flash loans. Flash loans that result in a profit are typically charged a mere 0.09% fee.⁸⁹

Leveraged Borrowing

Many DeFi platforms allow customers to use their crypto assets as collateral against loans denominated in other crypto assets. One example is Teddy Cash, a platform on the Avalanche blockchain, which allows users to pledge their AVAX tokens -- the native token of the Avalanche blockchain -- as collateral. Teddy Cash alleges to lend users the TSD stablecoin “interest free” (the TSD stablecoin is supposedly pegged to the U.S. dollar). In their FAQ, Teddy Cash explains how to use their website to lever up eleven times:

“Borrowers speculating on future AVAX price increases can use the protocol to leverage their AVAX positions up to 11 times, increasing their exposure to price changes. This is possible because TSD can be borrowed against AVAX, sold on the open market to purchase more AVAX — rinse and repeat.*

*Note: This is not a recommendation for how to use Teddy Cash. Leverage can be risky and should be used only by those with experience.”⁹⁰

Certain borrowing platforms, such as Aave, also fail to disclose the full terms of the loan at the time the loan is taken out. Aave’s website displays an interest rate the borrower will be charged (measured in a variable APY), and notes that there is a “health ratio” — a level of collateralization that must be maintained to avoid liquidation. But it is only in Aave’s FAQ, but at the point of the loan, are the terms of liquidation fully disclosed — including the fact that there is a variable fee (in the ~10% range) charged upon liquidation. This raises loan disclosure concerns—they may be deceiving users about the true cost of the loan by under disclosing all the fees. The FTC, for example, has taken the position that hidden disclosures are like no disclosures at all.⁹¹

Opacity

As noted by Professor Sarah Hammer of the Wharton School, there is “no official U.S. public data source for cryptocurrency prices, market size, or volatility. This lack of data is a significant problem.” This leaves regulators, lawmakers, and the public alike dependent on the self-reported data from the industry, which may be subject to double-counting, as some users

⁸⁸ <https://www.coindesk.com/learn/2021/02/17/what-is-a-flash-loan/>

⁸⁹ <https://decrypt.co/resources/what-are-flash-loans-the-defi-lending-phenomenon-explained>

⁹⁰ <https://docs.teddy.cash/borrowing>

⁹¹

<https://www.ftc.gov/news-events/press-releases/2021/07/lendingclub-agrees-pay-18-million-settle-ftc-charges>

are moving cryptoassets from one blockchain to another via “bridges”, or lending their crypto assets to others. Currently, there is no centralized data repository, reporting nomenclature or regulatory oversight into crypto metrics. This lack of data makes it difficult for users to evaluate whether to participate on a trading platform and for regulators, researchers and the public to understand wider crypto risks. Indeed, one key lesson from the 2008 financial crisis was that poor data and oversight of market participants’ positions in credit default swap markets led to the mispricing of risk and a poor understanding of counterparty exposures or risks to the broader market.

Interconnections: Family Offices, Hedge Funds, and Large Banks

While crypto proponents claim that the digital asset market is a refuge from the practices of traditional financial markets, the Too Big To Fail banks are a growing presence in the crypto currency market. Goldman Sachs plans to open a cryptocurrency trading desk,⁹² BNY Mellon allows its clients to hold Bitcoin as of February⁹³, Wells Fargo will offer professionally managed cryptocurrency funds for qualified investors.⁹⁴ Morgan Stanley’s Europe Opportunity Fund reported owning 28,298 shares of the Grayscale Bitcoin Trust,⁹⁵ according to a June 28 filing.⁹⁶ As digital assets continue to migrate into the banking perimeter, it would greatly exacerbate any future crises in digital asset markets, and could metastasize to the full economy.

Cryptocurrency exchanges and DeFi platforms alike are also trying to attract institutional business. The London-based Aave, which offers lending and borrowing of cryptocurrency,⁹⁷ is creating a private pool to allow large institutions to try out their platform.⁹⁸ Signs indicate the presence of hedge funds in cryptocurrency is growing. An Interwest survey of hedge funds managing an average of 7.2 billion showed that North American funds expect to have a 10.6% average exposure to cryptocurrency by 2026.⁹⁹ If, as the survey suggests, the majority of hedge funds with billions in assets under management hold ten percent or more of their positions in cryptocurrency, downturns in cryptocurrency markets may have spillover effects to the rest of the economy: should these hedge funds also be prime brokering with large banks, sharp swings in the volatile cryptocurrency markets could lead to forced liquidations of other assets at these private funds.

Conclusion

⁹²

<https://www.cnbc.com/2021/05/07/goldman-sachs-unveils-new-cryptocurrency-trading-team-in-employee-memo.html>

⁹³

<https://www.cnbc.com/2021/02/11/bny-mellon-to-offer-bitcoin-services-a-validation-of-crypto-from-a-key-bank-in-the-financial-system.html>

⁹⁴ <https://www.bbc.com/news/business-57147386>

⁹⁵ <https://decrypt.co/resources/gbtc-everything-you-need-to-know-about-the-grayscale-bitcoin-trust>

⁹⁶

<https://cointelegraph.com/news/morgan-stanley-equity-fund-owns-28-2k-shares-of-grayscale-bitcoin-trust-per-sec>

⁹⁷ <https://www.kraken.com/en-us/learn/what-is-aave-lend>; and <https://docs.aave.com/faq/>

⁹⁸ <https://cryptobriefing.com/aave-has-private-pool-institutions-testing-defi/>

⁹⁹ <https://www.ft.com/content/4f8044bf-8f0f-46b4-9fb7-6d0eba723017>

Congress should continue to examine if there are regulatory gaps that require new legislation to ensure consumer and investor protection in the cryptocurrency space. Congress should as ensure there are mechanisms for the regulators to have a complete picture of systemic risk in the space. Regulators should continue to monitor digital asset markets and ensure compliance with existing regulations.