Written Testimony of Jonathan Levin
Co-Founder and Chief Strategy Officer
Chainalysis Inc.

Before the
House Agriculture Committee
Commodity Exchanges, Energy and Credit Subcommittee

Hearing on
Future of Digital Asset Regulation

June 23, 2022

Chairman Maloney, Ranking Member Fischbach, and distinguished members of the Committee. Thank you for inviting me to testify before you today on this important topic. I appreciate that this Committee is looking at how to approach market regulation of digital assets. The topic of market regulation is important for safeguarding digital assets, but also the financial system more generally.

My name is Jonathan Levin and I co-founded Chainalysis Inc. with Michael Gronager, CEO of Chainalysis, in 2014. I currently serve as Chief Strategy Officer. I began studying cryptocurrencies ten years ago through my research as an economist. I was interested in the way that the Internet could create accessibility to markets and impact developing economies. While the Internet brought citizens of the world closer together in terms of global connectivity, it did not give people the economic opportunities that were promised. The cryptocurrency industry provides a new way to conduct global commerce, creating economic opportunities for people across the world. The entrepreneurial dynamism that cryptocurrencies present allows for innovators and builders to create universal access to financial products that serve individuals and their data. This technology has the potential to be significant in global competition over coming decades.

An important point I want to make to the members of this Committee, is that the transparency of blockchains enhances the ability of policymakers and government agencies to detect, disrupt and, ultimately, deter illicit activity in cryptocurrency markets. By examining a cryptocurrency payment made to a scammer, government agencies unlock immediate insight into the network of wallet addresses and services (e.g., exchanges, mixers, etc.) that have a relationship with this entity. In contrast, in a traditional criminal financial investigation, a similar tip, linking an illicit actor to a bank account, is just the beginning of a long, extensive process to request and subpoena records that are manually reviewed and reconciled to generate a comparable amount of insight. Despite the success of many of these investigations, the significant time investment that is required may create opportunities for illicit actors to evade justice vs. the real-time monitoring capabilities of blockchain intelligence.

As with any new technology, cryptocurrency can be used by both good and bad actors. As such, preventing cryptocurrency from being abused for illicit purposes is intricately connected to our ability to unlock its profound potential for the world. We are in a unique position to help this industry mitigate risks and, in turn, increase the potential for a vibrant economy to be built on this new infrastructure. The transparency provided by the blockchain enables unique insights into cryptocurrency markets, including an understanding of market risks, that can enable surveillance. There is a great deal of data and information available to government agencies looking to understand this space that is available for analysis. Whereas blockchain analytics companies like Chainalysis survey and glean insights from transactions settled on the blockchain, off-chain analytics companies offer trading insights into cryptocurrency firms' order books, and alert on typologies related to market price/volume manipulation. Off-chain analytics and market surveillance companies that we integrate with, provide alert capabilities to such typologies as pump and dumps, rugpulls, flash attack loans, spoofing, circular wash-trading as well as insider/employee trading. Where these datasets are found to be insufficient for market oversight, regulators may look to have a more complete understanding by combining on-chain data with off-chain data from other sources, or requiring additional reporting.

American markets are the world's largest, most developed, and most influential. Many of the world's most important agricultural, mineral, and energy commodities are priced in U.S. dollars in the U.S. derivatives markets. Dollar pricing of the world's commodities provides a tremendous advantage to American producers in global commerce, an advantage well-recognized by competing economies abroad. There is a key opportunity for the United States to have the regulator that establishes the world's prices for cryptocurrencies.

American markets are the best regulated in the world. The Commodity Futures Trading Commission (CFTC) has provided oversight of the U.S. exchange-traded derivatives markets for over 40 years. The CFTC is recognized for its principles-based regulatory framework and econometrically driven analysis. It also is recognized around the world for its level of expertise and breadth of capability. This combination of regulatory expertise and competency is one of the reasons why U.S. markets continue to serve participants' needs around the globe to hedge price and supply risk safely and efficiently. It is why well-regulated U.S. markets continue to serve a vital national interest – U.S. dollar pricing of important global commodities.

If America wants to lead in this sector, we must lead cryptocurrency market regulation. The clarification of cryptocurrency market regulator responsibilities would be a very important step for this market and would help to lend a greater degree of order. We should aim to create a stable, regulated market whereby the world looks to the United States for established asset-reference cryptocurrency prices, just as they do for many types of commodities.

I would also like to highlight that the cryptocurrency industry is working hard to ensure that there are the right protections for investors in this space. Two ways this is happening is through work conducted by trade associations made of cryptocurrency industry members,

as well as initiatives like the Crypto Market Integrity Coalition, a group of cryptocurrency industry members who have taken a pledge to focus on cultivating a fair digital asset marketplace to combat market abuse and manipulation and promote public and regulatory confidence in the new asset class. The cryptocurrency industry has made enormous strides to improve market integrity in the past few years. At the same time, cryptocurrency businesses are keenly aware of the concerns that still need to be addressed, and are committed to engaging with regulators to advance solutions to cryptocurrency's unique challenges.

In my testimony, I provide background on Chainalysis, outline how blockchain analysis can be leveraged by government agencies to provide greater insight into the cryptocurrency ecosystem, and describe risks we see to consumers, including contagion risks, scams, thefts, and manipulation in the cryptocurrency space and how they can be identified and mitigated using blockchain data. I also provide recommendations for how the government agencies, like the CFTC, can address potential risks in the market.

Background on Chainalysis

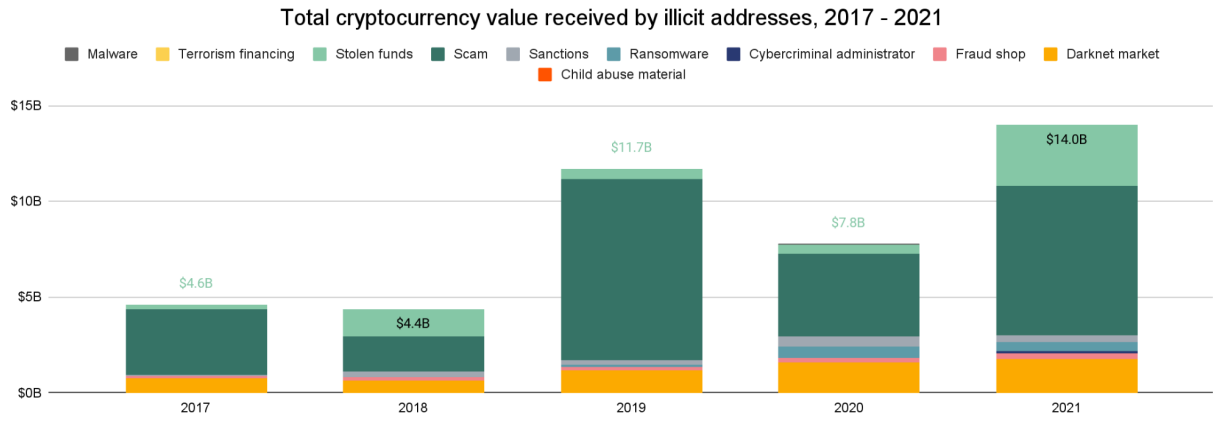
Chainalysis is the blockchain data platform. We provide data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies. Chainalysis has over 750 customers in 70 countries. Our data platform powers investigations, compliance, and risk-management tools that have been used to solve many of the world's most high-profile cyber-crime cases and grow consumer access to cryptocurrency safely. We have worked closely with law enforcement and regulators as they have worked to disrupt and deter illicit uses of cryptocurrency.

Chainalysis's partnerships with law enforcement and regulators are consistent with our corporate mission: to build trust in blockchains. Fundamentally, we believe in the potential of open, decentralized blockchain networks to drive new efficiencies, reduce barriers for innovators to create new financial and commercial products, encourage innovation, enhance financial inclusion, and unlock competitive forces across financial services and other markets. Our goal is to contribute our data, tools and expertise to drive illicit finance and other risks out of the cryptocurrency ecosystem, enabling the realization of the technology's potential.

Chainalysis's data powers both investigative and compliance tools. Our investigative tool, Reactor, enables government agencies and investigative teams to trace the illicit uses of cryptocurrency, including money laundering, theft, scams, and other criminal activities. Our compliance tool, KYT (Know Your Transaction), provides cryptocurrency businesses and financial institutions the ability to screen their clients transactions and ensure that they are not attempting to interact with illicit entities. This transaction monitoring tool provides ongoing insights for cryptocurrency businesses so that they can protect their businesses and clients and ensure regulatory compliance.

Another tool, Chainalysis Market Intel, provides the unique insights needed to conduct cryptocurrency research and make investment decisions. Chainalysis traces the funds flowing on the blockchain and tracks the cryptocurrency activity of over 3,300 businesses. This translates into intelligence on over 95% of the cryptocurrencies traded on the market. As all transfers are recorded on the blockchain in real-time, on-chain data, once mapped to real-world entities, this is a powerful dataset. It is a complete and real-time description of how cryptocurrency is being used and held. This means our metrics describe tangible, real-world activity rather than technical blockchain metrics. This offers new ways to value cryptocurrencies, and understand the market and the broader crypto-economy, as we can see how assets move in response, or to cause, events.

Chainalysis also leverages our data to conduct research into the cryptocurrency ecosystem, including the illicit use of cryptocurrency. We publish a number of reports, including our annual Crypto Crime Report. Based on this research, we reported in our 2022 Crypto Crime Report that cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020. Top categories include scams, stolen funds, darknet markets, and – pertinent to this hearing – ransomware.



Despite this large increase in illicit transaction volume, illicit activity as a percentage of total volume has actually fallen dramatically since 2019. In 2019, the illicit share was about 3%, in 2020 it was just over 0.5%, and in 2021 it was 0.15%. The reason for this is that cryptocurrency usage is growing faster than ever before, so while cryptocurrency-related crime is definitely increasing, the legitimate use of cryptocurrency is far outpacing its use by illicit actors. This is good news for the cryptocurrency ecosystem, but the government and industry are still faced with putting in place and implementing the appropriate controls to mitigate risks in the system.

How Blockchain Data Can be Leveraged to Gain Insights into the Cryptocurrency Ecosystem

It is a common misconception that cryptocurrency is completely anonymous and untraceable. In fact, the transparency provided by many cryptocurrencies' public ledgers is much greater than that of other traditional forms of value transfer. Cryptocurrencies like Bitcoin operate on public, immutable ledgers known as blockchains. Anyone with an Internet connection can look up the entire history of transactions on these blockchains. The ledger shows a string of numbers and letters that transact with another string of numbers and letters. Chainalysis maps these numbers and letters – or cryptocurrency addresses – to their real-world entities. For example, in Chainalysis products, we are able to see that a given transaction was between a customer at a specific exchange, with a customer at another exchange, between a customer at an exchange and a sanctioned entity, or any other illicit or legitimate service using cryptocurrency. Our data set and investigative tools are invaluable in empowering government and private sector investigators to trace cryptocurrency transactions, identify patterns, and, crucially, see where cryptocurrency users are exchanging cryptocurrency for fiat currency.

Using blockchain analysis tools, law enforcement can trace cryptocurrency addresses to identify the origination and/or cash-out points at cryptocurrency exchanges. Law enforcement can serve subpoenas to these cryptocurrency exchanges, which are required to register as money services businesses (MSBs) here in the United States and collect know-your-customer (KYC) information from their customers. In response to a subpoena, the exchange will provide law enforcement with any identifying information that it has related to the cryptocurrency transaction(s) in question, such as name, address, and government identification documentation, allowing the authorities to further their investigation.

Blockchain analytics and market surveillance are two pillars for effective crypto risk monitoring and compliance programs. Chainalysis KYT addresses the need for insights across blockchain-based transactions and anti-money laundering (AML) compliance, while market surveillance tools detect manipulative trading behavior across order books and venues. Combined, these capabilities give exchanges, brokerages, regulators and other market participants a powerful view across both the external and internal risk landscapes of crypto trading. This takes market integrity to the next level, bringing us closer to addressing regulatory concerns associated with consumer and investor protections, for example.

There are many private sector tools that enable oversight of the cryptocurrency markets and detecting market abuse and manipulation in cryptocurrency trading. Our tools can be paired with these tools, including those focused on analysis of orderbook data, to enable broader insight into the ecosystem. We are working with regulatory agencies to incorporate our on-chain data alongside off-chain data from other sources in order to allow for better market surveillance. This will better enable agencies to identify market manipulation and malicious activity on the blockchain, including front and back running, rug pulls, and initial coin offering (ICO) scams, among other things.

The amount of transparency that exists in the market enables an understanding of the systemic risks that can be used to provide appropriate oversight of this space. There is a

great deal of data and information that are readily available for analysis. Agencies can identify where there may be information gaps and implement additional reporting requirements or additional data sources to gain a more complete picture.

Risks in the Digital Asset Space

While Chainalysis tracks the illicit use of cryptocurrency in a number of different categories, for the purposes of this committee and the agencies over which they have jurisdiction, I will focus on scams, thefts, and manipulation in this testimony. Here I will explain what we see in each of these categories.

Contagion Risks

One risk that has been highlighted by recent cryptocurrency news is the potential broader contagion of risks in this market. We are currently in a bear market across financial assets, including cryptocurrency. In fact, cryptocurrency prices are now more correlated to tech stocks than ever before. This means, when the broader financial markets slump, cryptocurrency prices do as well.

But there's one important difference between cryptocurrency and traditional finance: transparency. Due to the open nature of decentralized finance (DeFi) protocols, the market can often see where large, well-known players placed their bets and if those positions are facing liquidation. Furthermore, market participants can use this transparency to assess the stability of the core protocols that power the DeFi ecosystem. However, this transparency has not stopped large, centralized companies from making bets on the price of various cryptocurrencies, both using open DeFi protocols and by lending funds to one another. This creates potential contagion risks, as various centralized market participants are financially exposed to one another. While the transparent DeFi protocols continue to function as designed because they are simply code running on the blockchain, some highly leveraged businesses have struggled to unwind complex financial positions in a hostile macroeconomic environment.

This transparency and the fall in cryptocurrency prices is also exposing projects with fundamental design flaws or unsustainable economic models. Some projects that were hastily built or didn't properly manage risk will fail, and that's a natural process for any new technology or industry. This is an opportunity for the industry to leverage blockchains' transparency to analyze systemic risk and build better systems and design better rules for the next bull market.

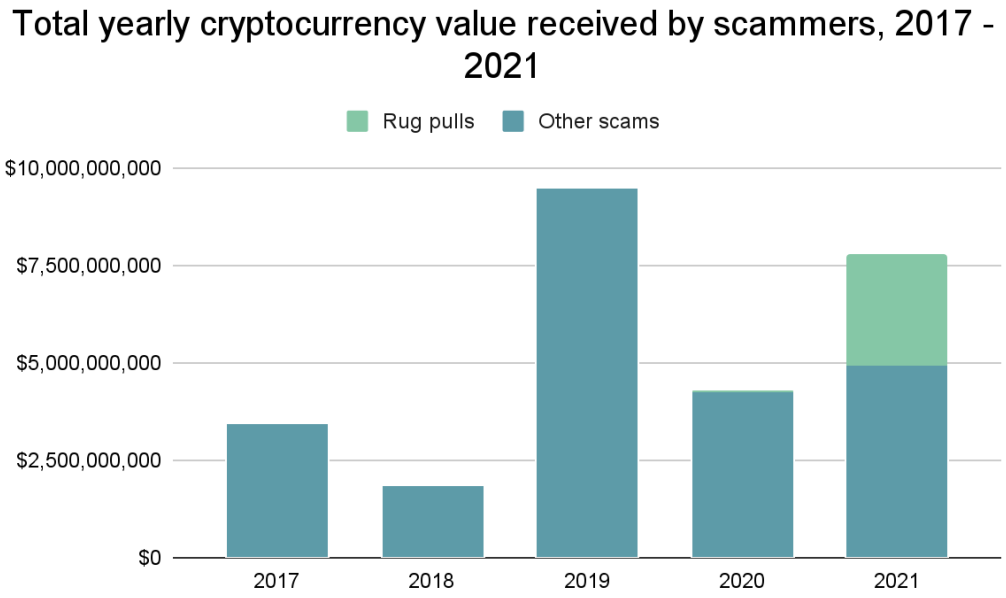
It is important for regulators to understand both the decentralized and centralized parts of the cryptocurrency market and how they may impact each other. For example, centralized players investing in decentralized finance may find themselves over-leveraged if they have not appropriately calculated the risks, in particular in a bear market. The decentralized projects in which centralized entities have invested may also fall victim to code exploits or

hacks and lose their value precipitously. Being able to adequately oversee centralized players will require understanding the entire ecosystem.

Scams

There has been an evolution of scamming activity in the cryptocurrency space over the past few years. Several years ago, scams mostly presented themselves as centralized platforms where you could invest in new cryptocurrencies. OneCoin is an example of this type of scam. As law enforcement has become better at identifying and investigating these sorts of scams, and as consumers have become wise to them, we are seeing a new trend in this space, where scammers will impersonate high-profile people and make claims such as offering to double any cryptocurrency sent to them. Others will impersonate legitimate cryptocurrency projects on social media platforms like Telegram, Discord, or Twitter in order to trick would-be investors into sending the scammers their funds, rather than sending them to the real platform. We also see an increase in romance scams, where the scammer develops a relationship with a victim over time and convinces them to invest in a scam website, or send them funds directly. This type of scam is also conducted using other financial assets, but it's becoming prevalent in the cryptocurrency space, with a focus on elderly individuals. Another type of scam we now increasingly see are rug pulls. As is the case with much of the emerging terminology in cryptocurrency, the definition of “rug pull” isn’t set in stone, but we generally use it to refer to cases in which developers build out what appear to be legitimate cryptocurrency projects, for example create “legitimate” ERC-20 tokens or non-fungible tokens (NFTs) that work technically on-chain. However, the real intention of the project is to accumulate as much funds as possible and disappear abruptly. Usually they try to drum up as much hype as possible (potentially hiring celebrities to endorse the product) before taking investors’ money and disappearing.

In 2021, scams were once again the largest form of cryptocurrency-based crime by transaction volume, with over $7.7 billion worth of cryptocurrency taken from victims worldwide.



That represents a rise of 81% compared to 2020, a year in which scamming activity dropped significantly compared to 2019, in large part due to the absence of any large-scale Ponzi schemes. That changed in 2021 with Finiko, a Ponzi scheme primarily targeting Russian speakers throughout Eastern Europe, netting more than $1.1 billion from victims.

Another change that contributed to 2021's increase in scam revenue: the emergence of rug pulls, a relatively new scam type particularly common in the DeFi[1] ecosystem, in which the developers of a cryptocurrency project — typically a new token — abandon it unexpectedly, taking users' funds with them. We'll look at both rug pulls and the Finiko Ponzi scheme in more detail later in this testimony.

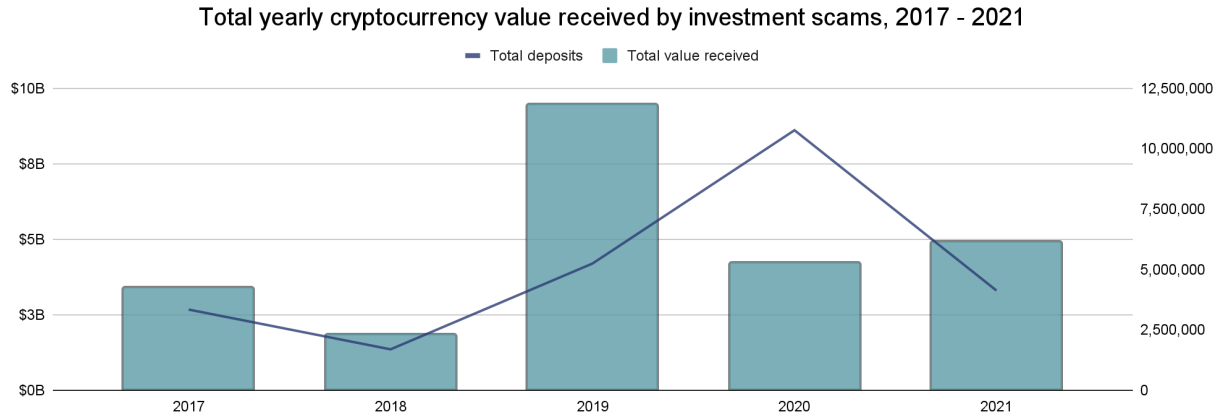
As the largest form of cryptocurrency-based crime and one uniquely targeted toward new users, scamming poses one of the biggest threats to cryptocurrency's continued adoption. However, cryptocurrency businesses are taking innovative steps to leverage blockchain data to protect their users and nip scams in the bud before potential victims make deposits.

Investment scams in 2021: More scams, shorter lifespans

While total scam revenue increased significantly in 2021, it stayed flat if we remove rug pulls and limit our analysis to financial scams — even with the emergence of Finiko. At the same time though, the number of deposits to scam addresses fell from just under 10.7

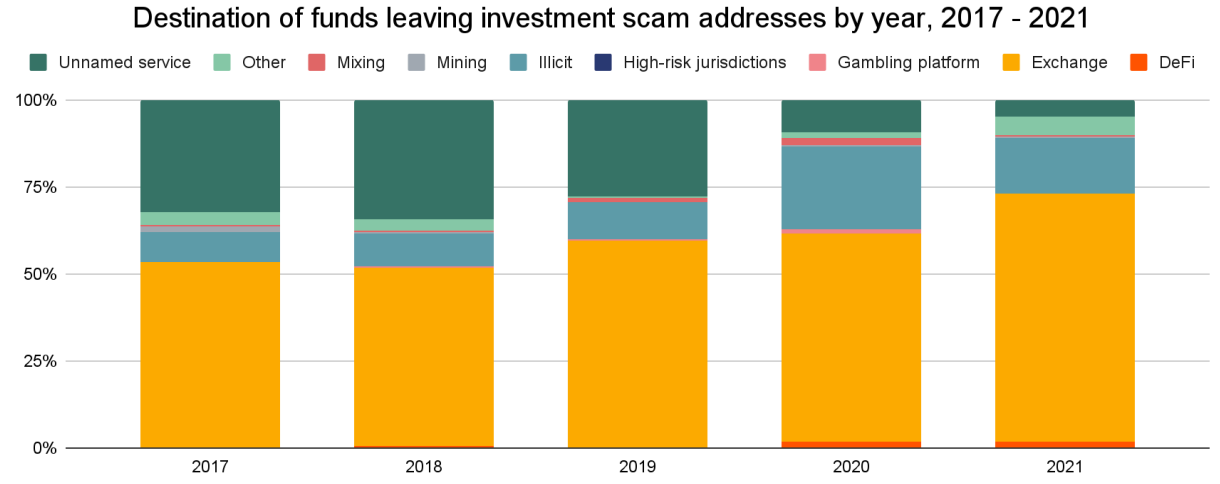
[1] Also known as decentralized finance, "DeFi" offers peer-to-peer financial services without the need of intermediaries such as banks, exchanges, or brokerages (who typically charge for their services). DeFi services are built and run on a blockchain through the use of smart contracts which defines the logic and rules for the service being used.

million to 4.1 million, which we can assume means there were fewer individual scam victims.



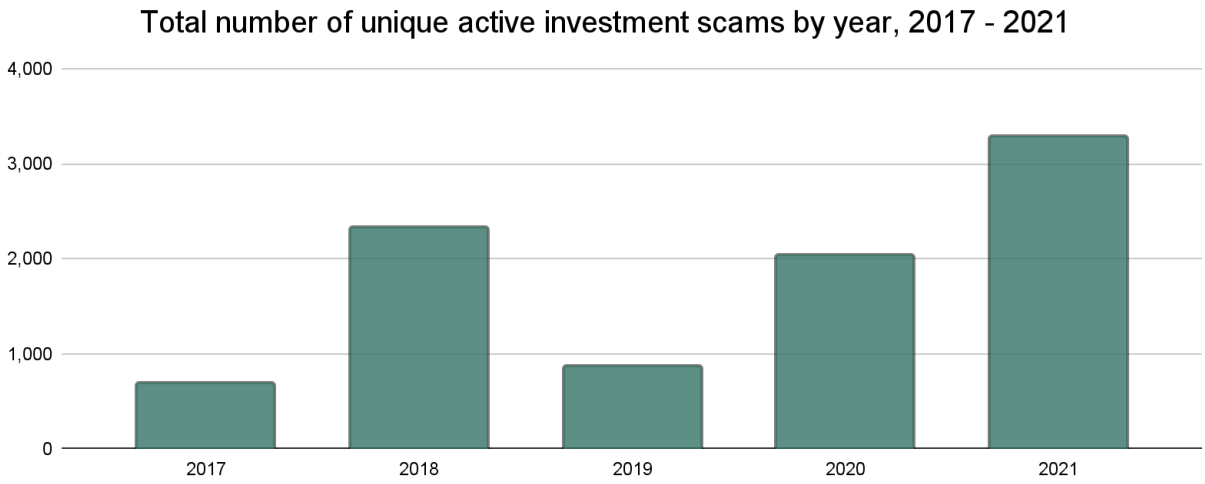
This also tells us that the average amount taken from each victim increased.

Scammers' money laundering strategies haven't changed all that much. As was the case in previous years, most cryptocurrency sent from scam wallets ended up at mainstream exchanges.

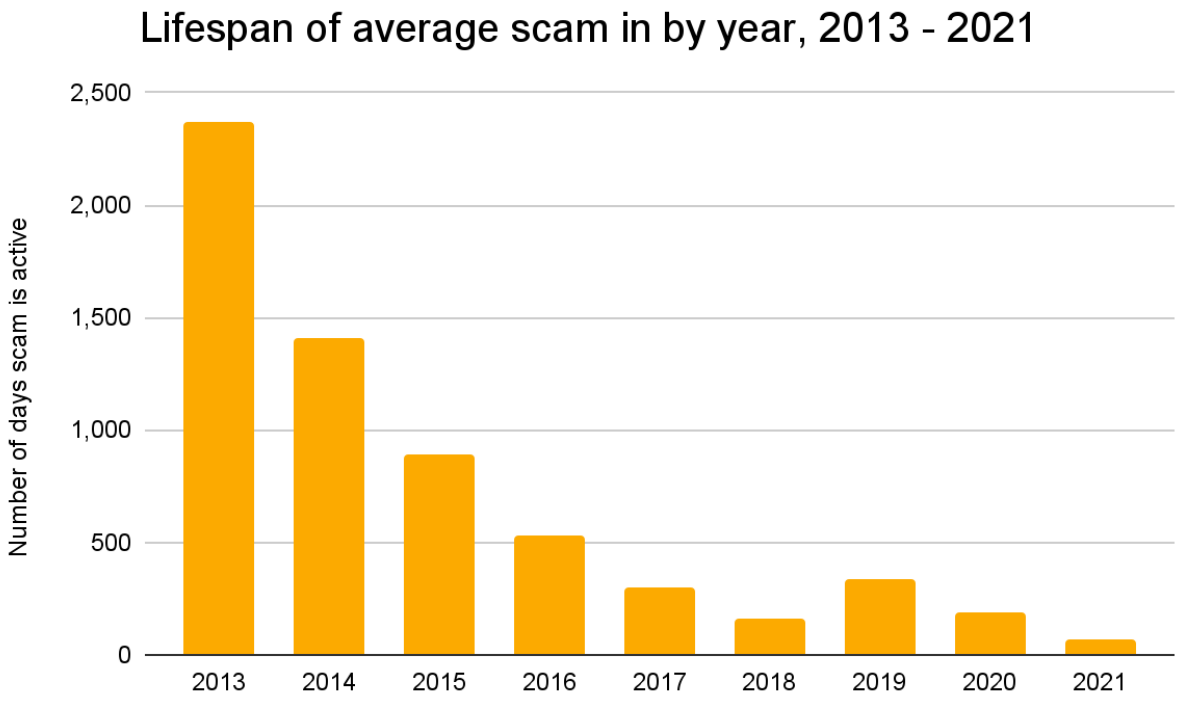


Exchanges using Chainalysis KYT for transaction monitoring and other transaction monitoring solutions can see this activity in real time, and take action to prevent scammers from cashing out.

The number of financial scams active at any point in the year — active meaning their addresses were receiving funds — also rose significantly in 2021, from 2,052 in 2020 to 3,300.



This goes hand in hand with another trend we've observed over the last few years: The average lifespan of a financial scam is getting shorter and shorter.



The average financial scam was active for just 70 days in 2021, down from 192 in 2020. Looking back further, the average cryptocurrency scam was active for 2,369 days, and the figure has trended steadily downwards since then.

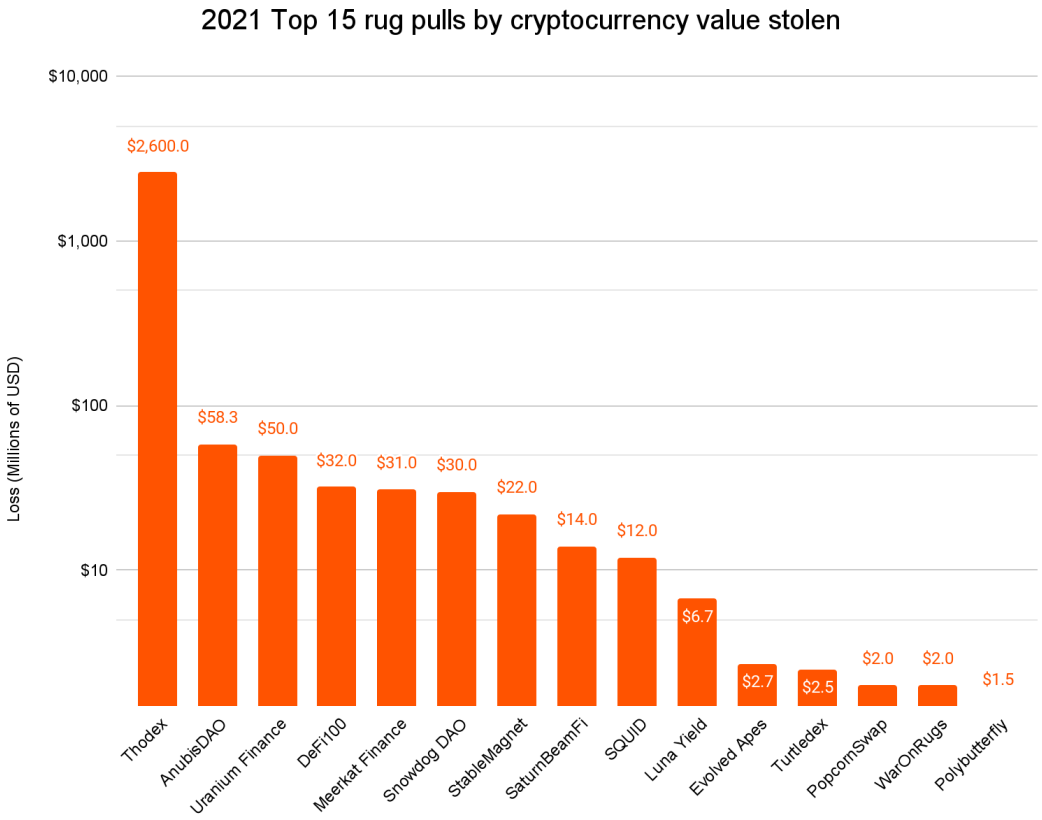
One reason for this could be that investigators are getting better at investigating and prosecuting scams. For instance, in September 2021, the CFTC filed charges against 14 investment scams touting themselves as providing compliant cryptocurrency derivative trading services — a common scam typology in the space — whereas in reality they had failed to register with the CFTC as futures commission merchants. In October 2021, the CFTC charged an El Paso resident and his firm in ongoing $3.9 million forex and cryptocurrency fraud and misappropriation scheme. In March 2022, the CFTC charged four people with fraud for operating Ponzi schemes involving bitcoin. In April 2022, the CFTC settled a case against Florida-based companies and their owner for fraudulently soliciting customers to purchase a digital asset they falsely promised would allow customers to gain access to a proprietary foreign currency (forex) trading algorithm.

Previously, these scams may have been able to continue operating for longer. As scammers become aware of these actions, they may feel more pressure to close up shop before drawing the attention of regulators and law enforcement.

Rug pulls have emerged as the go-to scam of the DeFi ecosystem, accounting for 37% of all cryptocurrency scam revenue in 2021, versus just 1% in 2020. All in all, rug pulls took in more than $2.8 billion worth of cryptocurrency from victims in 2021.

Most DeFi projects entail developers creating new tokens and promoting them to investors, who purchase the new token in order to access the utility that the cryptocurrency network provides, or with the hope it will rise in value. These actions also provide liquidity to the project. In rug pulls, however, the developers eventually drain the funds from the liquidity pool, sending the token's value to zero, and disappear. Rug pulls are prevalent in DeFi because, with the right technical know-how, it's cheap and easy to create new tokens on the Ethereum blockchain or others and get them listed on decentralized exchanges (DEXes).

The chart below shows 2021's top 15 rug pulls in order of value stolen.

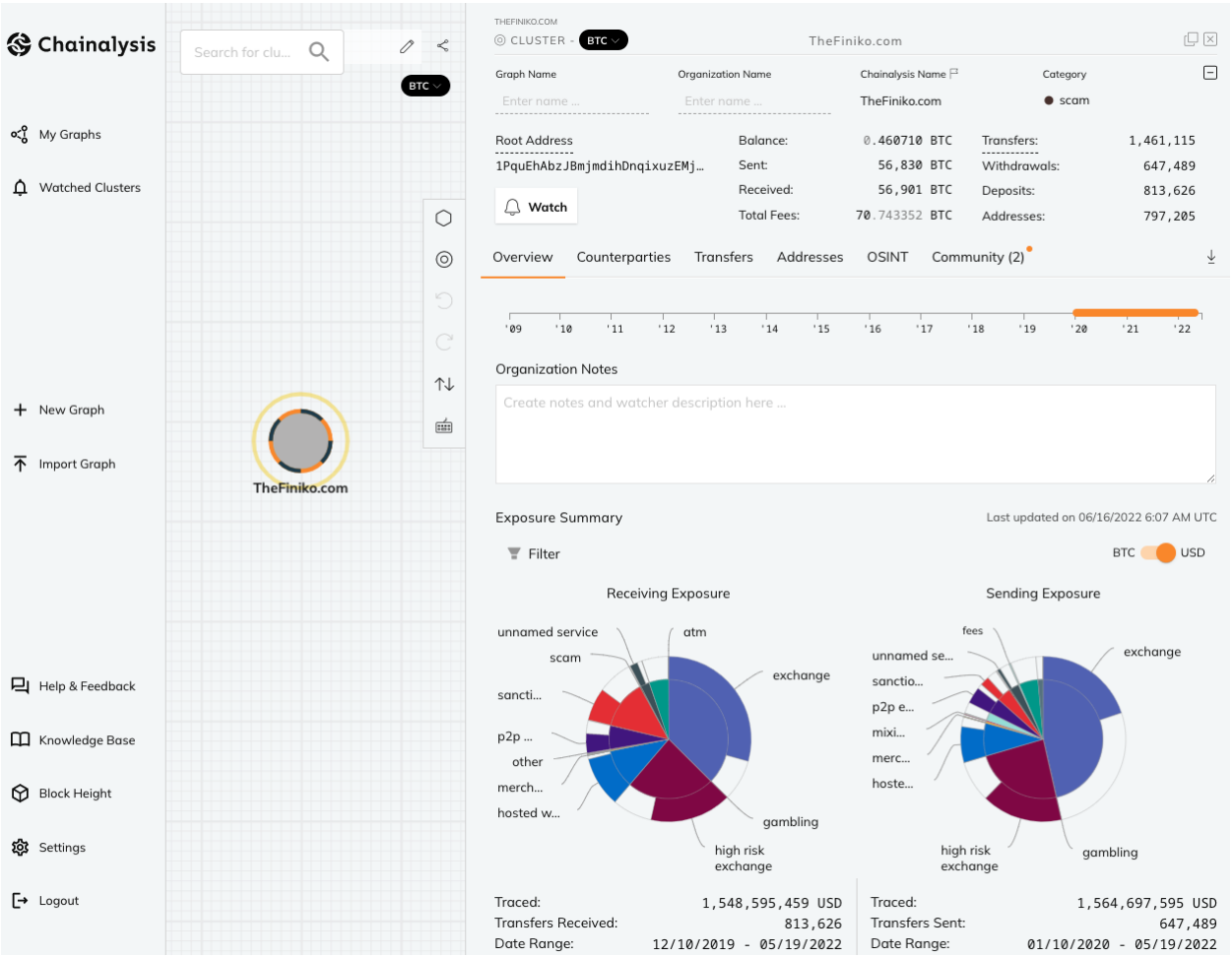


It's important to remember that not all rug pulls start as DeFi projects. In fact, the biggest rug pull of the year centered on Thodex, a large Turkish centralized exchange whose CEO disappeared soon after the exchange halted users' ability to withdraw funds. In all, users lost over $2 billion worth of cryptocurrency, which represents nearly 90% of all value stolen in rug pulls. However, all the other rug pulls in 2021 began as DeFi projects.

Finiko: 2021's billion dollar Ponzi scheme

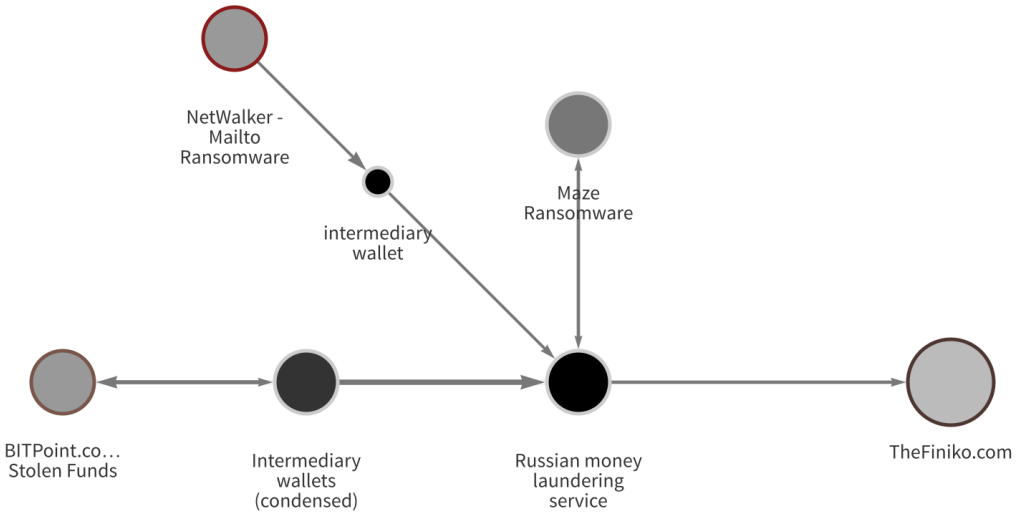
Finiko was a Russia-based Ponzi scheme that operated from December 2019 until July 2021, at which point it collapsed after users found they could no longer withdraw funds from their accounts with the company. Finiko invited users to invest with either Bitcoin or Tether, promising monthly returns of up to 30%, and eventually launched its own token that traded on several exchanges.

According to the *Moscow Times*, Finiko was headed up by Kirill Doronin, a popular Instagram influencer who has been associated with other Ponzi schemes. The article notes that Finiko was able to take advantage of difficult economic conditions in Russia exacerbated by the Covid pandemic, attracting users desperate to make extra money. Chainalysis Reactor shows us how prolific the scam was.



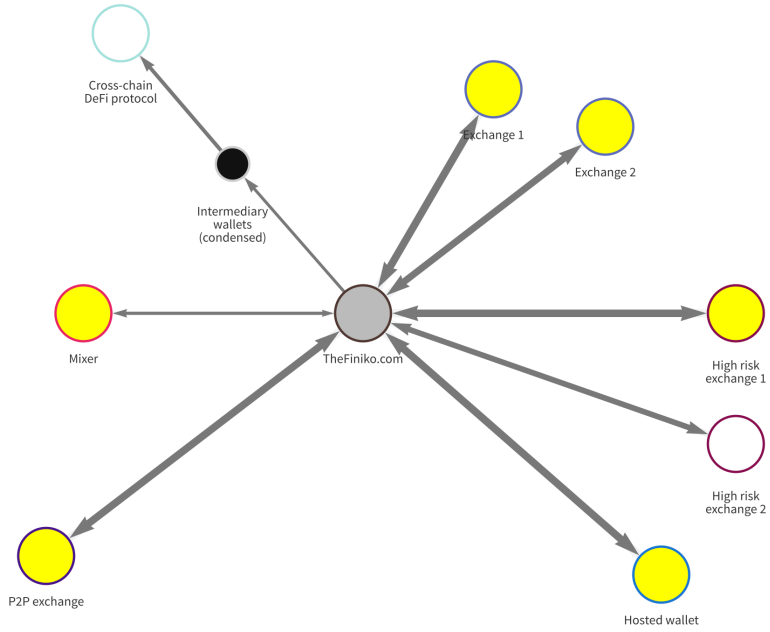
During the roughly 19 months it remained active, Finiko received over $1.5 billion worth of Bitcoin in over 800,000 separate deposits. While it's unclear how many individual victims were responsible for those deposits or how much of that $1.5 billion was paid out to investors to keep the Ponzi scheme going, it's clear that Finiko represents a massive fraud perpetrated against Eastern European cryptocurrency users, predominantly in Russia and Ukraine.

As is the case with most scams, Finiko primarily received funds from victims' addresses at mainstream exchanges. However, we can also see that Finiko received funds from what we've identified as a Russia-based money launderer.



This launderer received millions of dollars' worth of cryptocurrency from addresses associated with ransomware, exchange hacks, and other forms of cryptocurrency-based crime. While the amount the service has sent to Finiko is quite small — under 1 Bitcoin (BTC) total — it serves as an example of how a scam can also be used to launder funds derived from other criminal schemes. It's also possible that Finiko received funds from other laundering services we've yet to identify.

Finiko sent most of its more than $1.5 billion worth of cryptocurrency to mainstream exchanges, high-risk exchanges, a hosted wallet service, and a peer-to-peer (P2P) exchange. However, we don't know what share of those transfers represent payments to victims in order to give the appearance of successful investments.



Finiko also sent $34 million to a DeFi protocol designed for cross-chain transactions via a series of intermediary wallets, where it was likely converted into ERC-20 tokens and sent elsewhere. It also sent roughly $3.9 million worth of cryptocurrency to a few popular mixing services. Most interesting of all, perhaps, is Finiko's transaction history with Suex, an over-the-counter (OTC) broker that was sanctioned by U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) for its role in laundering funds associated with scams, ransomware attacks, and other forms of cryptocurrency-based crime.

Between March and July of 2020, Finiko sent over $9 million worth of Bitcoin to an address that now appears as an identifier on Suex's entry into the Specially Designated Nationals (SDN) List. This connection underlines the prolificness of Suex as a money laundering service, as well as the crucial role of such services generally in allowing large-scale cybercriminal operations, like Finiko, to victimize cryptocurrency users.

Soon after Finiko's collapse in July 2021, Russian authorities arrested Doronin, and later also nabbed Ilgiz Shakirov, one of his key partners in running the Ponzi scheme. Both men remain in custody, and arrest warrants have reportedly been issued for the rest of Finiko's founding team.

How one cryptocurrency platform is saving users from scams

Mainstream cryptocurrency platforms, like exchanges, are in the perfect position to fight back against scams and instill more trust in cryptocurrency by warning users or even preventing them from executing those transactions. One popular platform did just that in 2021, and the results were extremely promising.

Luno is a leading cryptocurrency platform operating in over 40 countries, with an especially heavy presence in South Africa. In 2020, a major scam was targeting South African cryptocurrency users, promising outlandishly large investment returns. Knowing that its users were at risk, Luno decided to take action, in part by leveraging Chainalysis tools and services.

The first step was a warning and education campaign. Using in-app messages, help center articles, emails, webinars, social media posts, YouTube videos, and even one-on-one conversations, Luno showed users how to spot the red flags that indicate an investment opportunity is likely a scam, and taught them to avoid pitches that appear too good to be true.

Luno then went a step further and began preventing users from sending funds to addresses it knew belonged to scammers. That's where Chainalysis came in. As the leading blockchain data platform, we have an entire team dedicated to unearthing cryptocurrency scams and tagging their addresses in our compliance products. With that data, Luno was able to halt users' transfers to scams before they were processed. It was a drastic strategy in many ways — cryptocurrency has historically been built on an ethos of financial freedom, and some users were likely to chafe at a perceived limitation on their ability to transact. But thanks to Chainalysis' best in class cryptocurrency address attributions, Luno was able to establish the trust necessary to sell customers on the strategy.

Luno first began blocking scam payments for South African users only in November 2020, and then rolled the feature out worldwide in January 2021. The plan worked, and transfers from Luno wallets to scams fell drastically over the course of 2021.

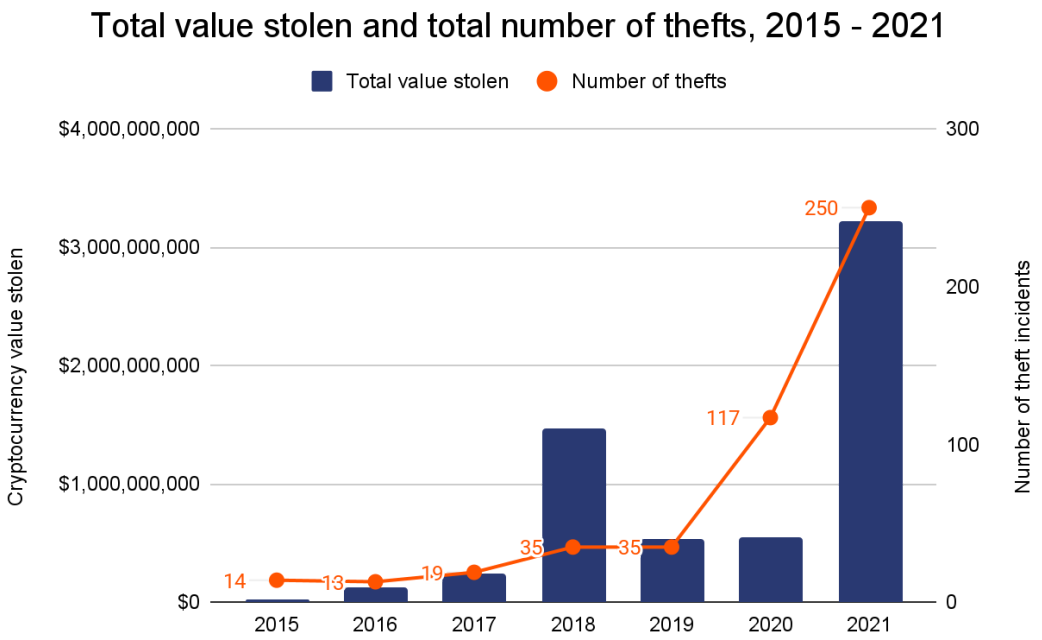
Orig Sheets link

The moving 30-day average daily transaction volume of transfers to scams fell 88% from $730,000 at its peak in September 2020, to just $90,000 by November. One customer summed up the results perfectly, saying, “Thank you, Luno. I was about to lose my pension and savings.”

Scams represent a huge barrier to successful cryptocurrency adoption, and fighting them can’t be left only to law enforcement and regulators. Cryptocurrency businesses, financial institutions, and, of course, Chainalysis have an important role to play as well. With this strategy, Luno took an important step towards establishing greater trust and safety in cryptocurrency, which we hope to continue to see grow in the industry.

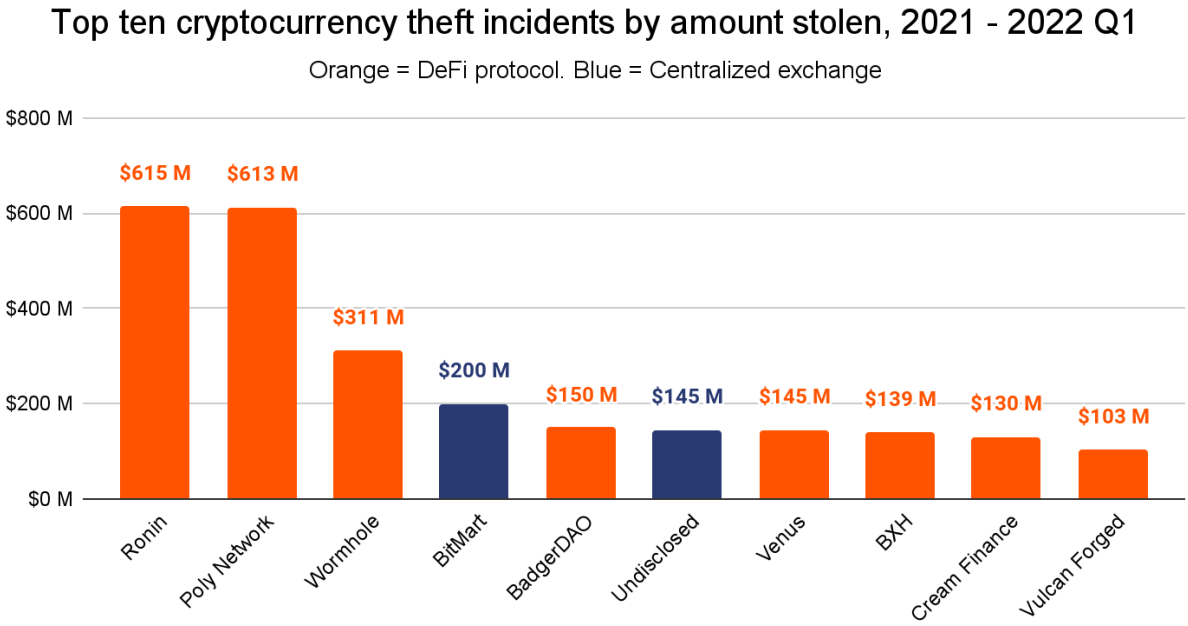
Theft

Throughout 2021, $3.2 billion in cryptocurrency was stolen from individuals and services — almost 6x the amount stolen in 2020. Approximately $2.3 billion of those funds were stolen from DeFi platforms in particular, and the value stolen from these protocols catapulted 1,330%.



This shift toward DeFi-centric attacks doesn't just sound pronounced—it looks like it, too. In every year prior to 2021, centralized exchanges lost the most cryptocurrency to theft by a large margin. But this year, DeFi platform thefts dwarfed exchange thefts.

The biggest cryptocurrency thefts of 2021



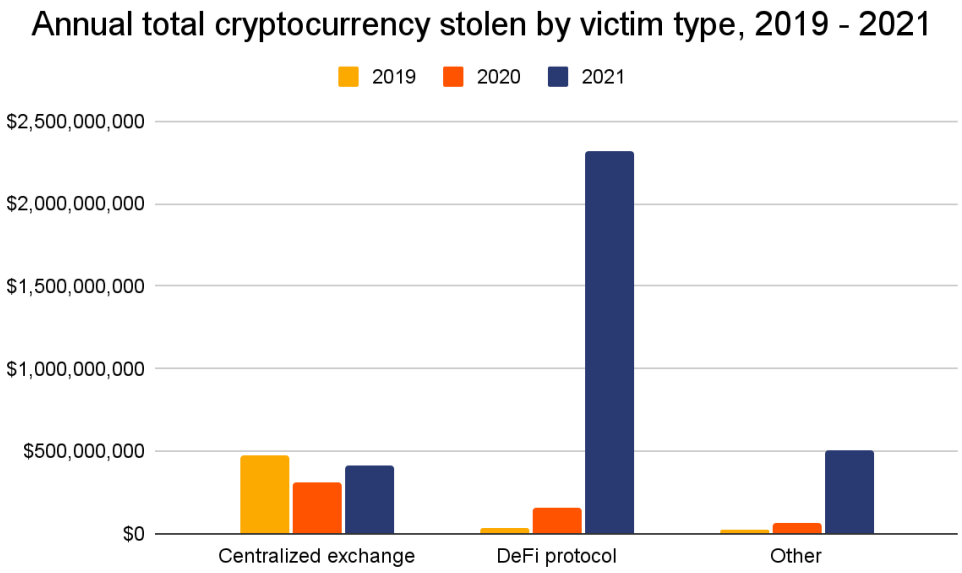
As is the case most years, the ten largest hacks of 2021 and Q1 2022 accounted for a majority of the funds stolen at $2.2 billion. Eight of these ten attacks targeted DeFi platforms in particular.

Code exploits are a prominent feature in 2021's cryptocurrency theft landscape

Historically, cryptocurrency thefts have largely been the result of security breaches in which hackers gain access to victims' private keys—the crypto-equivalent of pickpocketing. These keys could be acquired through phishing, keylogging, social engineering, or other techniques. From 2019 to 2021, almost 30% of all value was stolen from just this type of hack.

With the rise of DeFi and the extensive smart contract capabilities that power those platforms, deeper vulnerabilities have begun to emerge around the software underpinning these services. While these services are decentralized, these sorts of exploits can lead to contagion in the centralized parts of the cryptocurrency market, so it is important for regulators to understand these exploits and their broader impacts.

In 2021, code exploits and flash loan attacks—a type of exploit involving price manipulation—accounted for a near-majority of total value stolen across all services, weighing in at 49.8%. And when examining only hacks on DeFi platforms, that figure increases to 69.3%.



These exploits occur for a variety of reasons. For one, in keeping with DeFi's faith in decentralization and transparency, open-source development is a staple of DeFi applications. This is an important and broadly positive trend: since many DeFi protocols move funds without human intervention, users need to be able to audit the underlying code in order to trust the platform. But this also stands to benefit cybercriminals, who can analyze the scripts for vulnerabilities and plan exploits in advance.

Another potential point of failure is DeFi platforms' reliance on price oracles. Price oracles are tasked with maintaining accurate asset pricing data for all cryptocurrencies on a platform, and the job isn't easy. Secure but slow oracles are vulnerable to arbitrage; fast but insecure oracles are vulnerable to price manipulation. The latter type often leads to flash loan attacks, which extracted a massive $364 million from DeFi platforms in 2021. In the hack of Cream Finance, for example, a series of flash loans exploiting a vulnerability in the way Cream calculated yUSD's "pricePerShare" variable enabled attackers to inflate yUSD price to double its true value, sell their shares, and make off with $130 million in just one night.

These two dangers—inaccurate oracles and exploitable code—underscore the need for the security of both. Fortunately, there are solutions. To ensure pricing accuracy, decentralized price oracles like Chainlink can protect platforms against price manipulation attacks. To ensure the security of smart contracts, code audits can steel programs against common hacks like reentrancy, unhandled exceptions, and transaction order dependency.

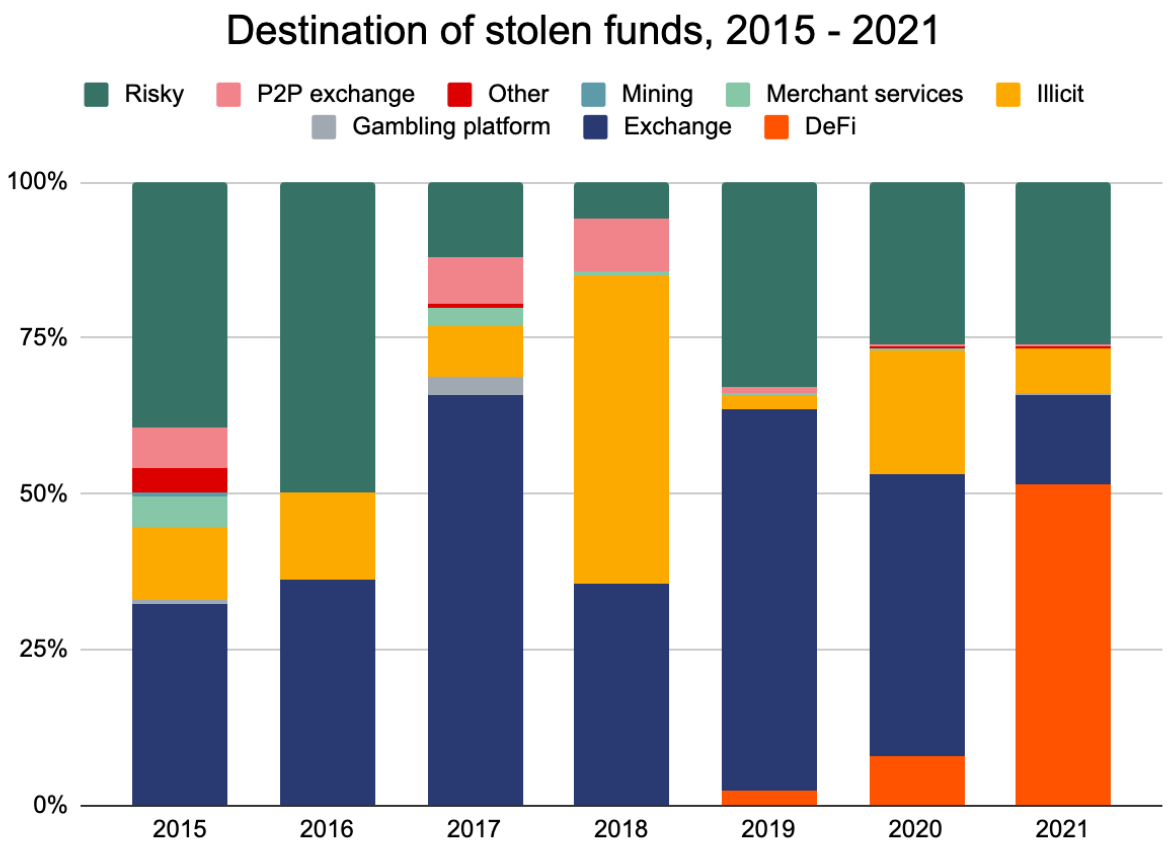
But code audits aren't infallible. Nearly 30% of code exploits occurred on platforms audited within the last year, as well as a surprising 73% of flash loan attacks. This highlights two potential shortfalls of code audits:

1. They may patch smart contract vulnerabilities *in some* cases, but not all;
2. They seldom guarantee that platforms' price oracles are tamper-proof.

So while code audits can certainly help, DeFi protocols managing millions of users and billions of dollars must adopt a more robust approach to platform security.

Following the money: the final destinations of stolen cryptocurrencies

In the aftermath of cryptocurrency thefts, more stolen funds flowed to DeFi platforms (51%) and risky services (25%) this year than ever before. Centralized exchanges, once a top destination for stolen funds, fell out of favor in 2021, receiving less than 15% of the funds. This is likely due to the embrace of AML and KYC procedures among major exchanges—an existential threat to the anonymity of cybercriminals.



Note: "Risky" refers to services like mixers, high-risk exchanges[2], and services based in high-risk jurisdictions[3].

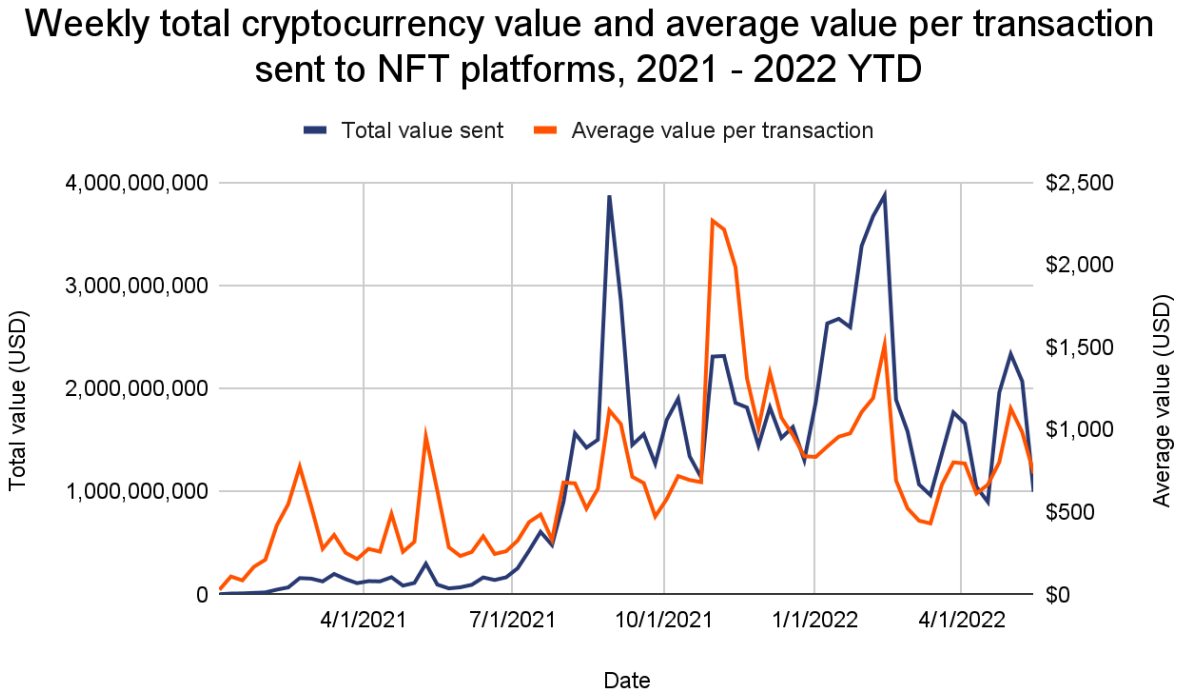
Manipulation

[2] A high risk exchange is an exchange that meets one of the following criteria:

- No KYC: The exchange requires absolutely no customer information before allowing any level of deposit or withdrawal. Or they require a name, phone number, or email address but make no attempt to verify this information.
- Criminal ties: The exchange has criminal convictions of the corporate entity in relation to AML/Combating the Financing of Terrorism (CFT) violations.
- High risky exposure: The exchange has high amounts of exposure to risky services such as darknet markets, other high risk exchanges, or mixing. We examine if the exchange's exposure to illicit activity is an outlier compared to other exchanges. A service with direct high risk exposure one standard deviation away from the average across all exchanges identified by Chainalysis over a 12 month period is considered a high risk exchange.

[3] High-risk jurisdictions consist of jurisdictions subject to OFAC comprehensive sanctions, which includes Iran, Cuba, Syria, North Korea, the Crimea, Donetsk, and Luhansk regions of Ukraine, as well as Venezuela due to broad government-based sanctions.

In 2021 and the first half of 2022, Chainalysis tracked a minimum $83 billion worth of cryptocurrency sent to ERC-721 and ERC-1155 contracts — the two types of Ethereum smart contracts associated with NFT marketplaces and collections — up from just $106 million in 2020.

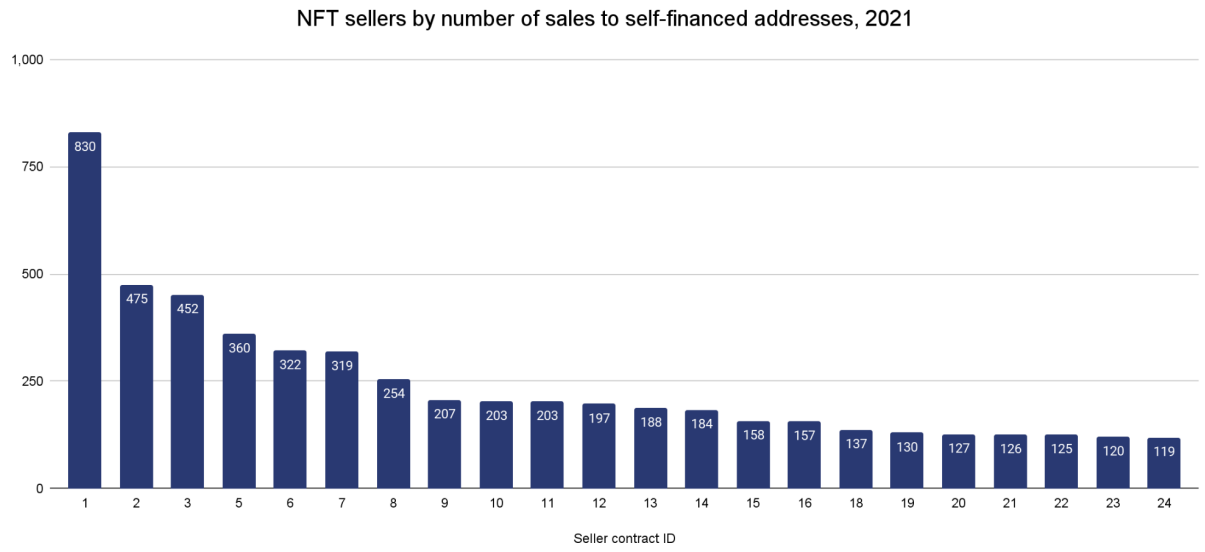


However, as is the case with any new technology, NFTs offer potential for abuse. It's important that, as our industry considers all the ways this new asset class can change how we link the blockchain to the physical world, we also build products that make NFT investment as safe and secure as possible. There have been several forms of illicit activity in NFTs: wash trading to artificially increase the value of NFTs, money laundering through the purchase of NFTs, and insider trading on NFT marketplaces. Here I will outline what we have seen in relation to wash trading.

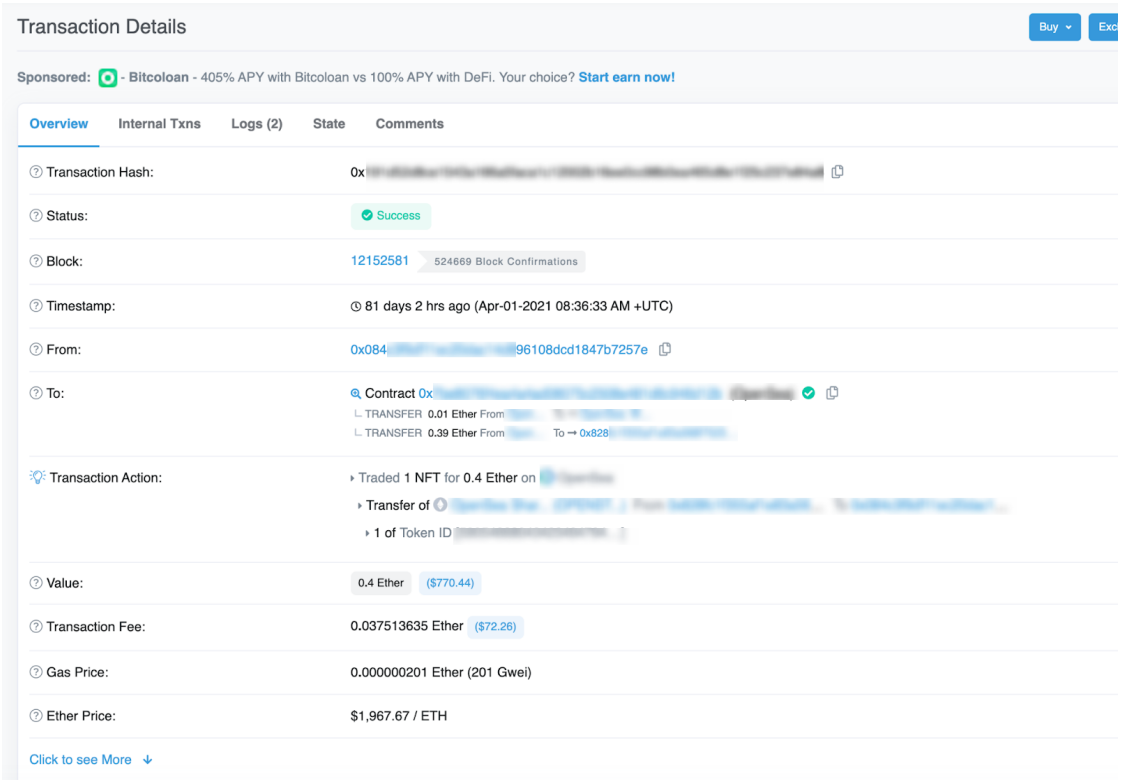
Wash trading, meaning executing a transaction in which the seller is on both sides of the trade in order to paint a misleading picture of an asset's value and liquidity, is another area of concern for NFTs. Wash trading has been a concern in the past with cryptocurrency exchanges attempting to make their trading volumes appear greater than they are. In the case of NFT wash trading, the goal would be to make one's NFT appear more valuable than it really is by "selling it" to a new wallet the original owner also controls. In theory, this would be relatively easy with NFTs, as many NFT trading platforms allow users to trade by simply connecting their wallet to the platform, with no need to identify themselves.

With blockchain analysis, however, we can track NFT wash trading by analyzing sales of NFTs to addresses that were self-financed, meaning they were funded either by the selling

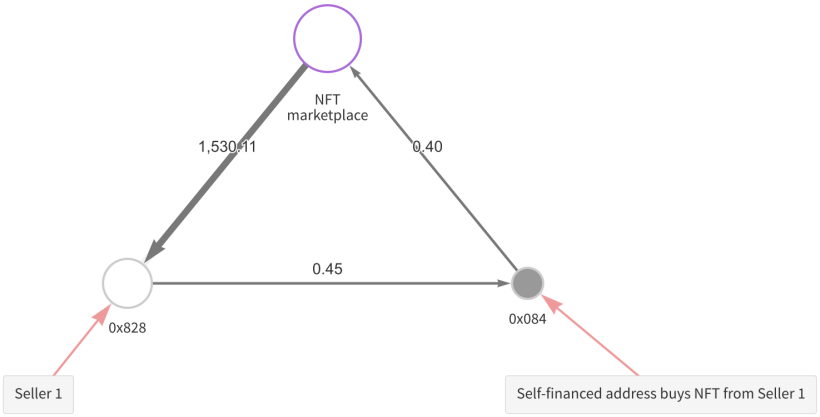
address or by the address that initially funded the selling address. Analysis of NFT sales to self-financed addresses shows that some NFT sellers have conducted hundreds of wash trades.



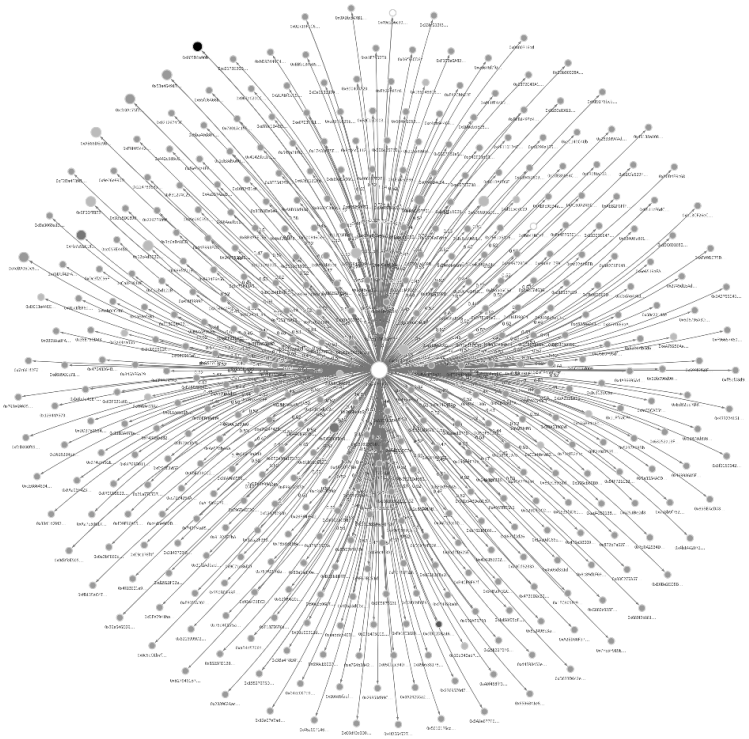
Let's look more closely at Seller 1, the most prolific NFT wash trader on the chart above, who has made 830 sales to addresses they've self-financed. The Etherscan screenshot below shows a transaction in which that seller, using the address beginning 0x828, sold an NFT to the address beginning 0x084 for 0.4 Ethereum via an NFT marketplace.



Everything looks normal at first glance. However, the Chainalysis Reactor graph below shows that address 0x828 sent 0.45 Ethereum to that address 0x084 shortly before that sale.



This activity fits a pattern for Seller 1. The Reactor graph below shows similar relationships between Seller 1 and hundreds of other addresses to which they've sold NFTs.



Seller 1 is the address in the middle. All other addresses on this graph received funds from Seller 1's main address prior to buying an NFT from that address. So far though, Seller 1 doesn't seem to have profited from their prolific wash trading. If we calculate the amount Seller 1 has made from NFT sales to addresses they themselves did not fund — whom we can assume are victims unaware that the NFTs they're buying have been wash traded — it doesn't make up for the amount they've had to spend on gas fees during wash trading transactions.

Address	**Spent on gas fees in wash trading transactions**	**Revenue from sales of wash traded NFTs to victims**	**Profits**
0x828	- $35,642	$27,258	- $8,383

While wash trading is prohibited in conventional securities,futures, and other derivatives, wash trading involving NFTs has yet to be the subject of an enforcement action. Wash trading in NFTs can create an unfair marketplace for those who purchase artificially inflated tokens, and its existence can undermine trust in the NFT ecosystem, inhibiting future growth. Blockchain data and analysis makes it easy to spot users who sell NFTs to addresses they've self-financed, so marketplaces may want to consider bans or other penalties for the worst offenders.

Recommendations

Provide regulatory clarity to market participants.

While cryptocurrency businesses have been subject to anti-money laundering laws since at least 2013, there are other aspects of the market that still require additional clarification, including direction from Congress. One of these areas is the cryptocurrency spot market, over and above fraud and manipulation. While the CFTC oversees derivatives markets such as bitcoin and ether futures, and the Securities and Exchange Commission provides oversight over those tokens that are securities, cryptocurrency spot markets are largely regulated at the state-level. Clarifying these responsibilities at the federal level, likely through legislation, would bolster anti-fraud and manipulation protections. It is also important to provide clarity about different tokens - for example, which tokens fall under the securities framework and which fall under the commodities framework. Having this guidance will help to make the perimeters very clear and will also make clear what falls outside of an agency's specific jurisdiction.

Providing market clarity will also support the goals of economic growth and leadership in the U.S.. If America wants to lead in the cryptocurrency sector, we must lead cryptocurrency market regulation. Clarifying roles around cryptocurrency market regulation at the federal level would be a very important step for this market and would help to lend a greater degree of order. We should aim to create a market in which the world looks to the United States for established asset-reference cryptocurrency prices, just as they do for many types of commodities.

Ensure adequate funding, resources, and training for government agencies charged with investigating fraud, manipulation, and abusive practices in this space.

As this asset class grows and is increasingly adopted, the U.S. government must do their best to root out fraud, manipulation, and abusive practices. Governments that have already embraced blockchain analysis have seized millions of dollars in cryptocurrency and stopped a number of illicit actors exploiting cryptocurrency. Many government agencies, including the CFTC, have limited or inconsistent personnel dedicated to investigating the illicit use of cryptocurrency because of a lack of training resources and a lack of funding for new personnel, tools, and training. Allocating appropriate financial and personnel resources to these efforts would ensure that agencies can address illicit activity in this space.

Leverage the unique and transparent nature of cryptocurrency in market surveillance and in the development of policies and regulations.

The information that is available to government agencies due to the transparent nature of blockchain technology provides an opportunity for policy makers and regulators to think differently about regulatory requirements in this space. For example, regulators can leverage this data to gain insights into the ecosystem and inform where the greatest risks are as they build their capacity to provide market surveillance. This will allow them to prioritize regulatory requirements that fill in information gaps. For example, reporting requirements may be different in this space given the on-chain data made available to regulators because of the transparent nature of the technology. It may not be necessary to require the same level of reporting because of the ease of availability of that on-chain data. Instead, regulators can focus reporting requirements on the parts of the market where there may be incomplete data or other gaps.

Understand and monitor systemic risks in the cryptocurrency ecosystem.

Regulators need to understand and monitor systemic risks in the whole cryptocurrency ecosystem - not just those market participants they have oversight of - to better understand the contagion risks that may be present. For example, it is important that regulators understand DeFi and DeFi products to understand the potential contagion risks. Understanding the broader market structures will better enable market surveillance and inform regulatory decisions.

Prioritize public education to ensure consumers understand cryptocurrencies and have the information they need to make educated decisions.

As with any new asset class, there is sometimes confusion among the general public about what cryptocurrencies are and how they work. It is important that the U.S. government engage in educational efforts related to cryptocurrency to better enable consumers to understand this asset class and avoid scams and fraudulent activity in the cryptocurrency ecosystem. The CFTC and others should consider partnering with the private sector in addition to conducting agency-lead initiatives to broaden the access, breadth, and depth of public education and ensure its impact.

Leverage public-private partnerships.

It is important that the U.S. government work together with private industry to address issues related to fraud, abuse, and manipulation in the cryptocurrency ecosystem. Establishing and improving upon coordination and collaboration mechanisms between countries can help to streamline investigations and improve oversight of the markets. These partnerships can provide additional insights into what is happening in the market to better inform policy decisions and guide discussions about how best to improve regulation.

Conclusion

Cryptocurrency has a variety of applications which contribute to the public good. Of particular interest to this Committee these contributions include job creation, fast cross-border payments, global leadership opportunities, and technological innovation. The U.S. is well-positioned to bring to bear our decades of innovation in cutting-edge technologies to this fast growing industry and be a key player in regulating the industry. As regulators approach this new asset class, they can leverage its technology and transparency to glean important insights and assess risks. Congress must do its part to ensure that the government agencies charged with oversight of this space are equipped to understand and address fraud, abuse, and manipulation in cryptocurrency markets. By providing the resources necessary, the U.S. government as a whole will be better equipped to mitigate risks and investigate and disrupt illicit activity when it does occur in the cryptocurrency markets. Thank you for your time, and attention to this very important issue.

Chainalysis

Jonathan Levin

jonathan@chainalysis.com

Summary

Jonathan is the Co-Founder and Chief Strategy Officer of Chainalysis, the blockchain data company. Chainalysis develops cryptocurrency investigation and compliance software deployed by 750 customers in 70 countries across government agencies, exchanges, financial institutions, and insurance and cybersecurity companies. He is responsible for designing long-term strategic initiatives that help government agencies, cryptocurrency businesses, and financial institutions around the world to manage and assess cryptocurrency-related risks, and more effectively conduct investigations. Jonathan leads outreach efforts with legislators, policymakers, and regulators globally to provide data and information related to cryptocurrency, the illicit use of cryptocurrency, and potential policy solutions. He also advises stakeholders, including government agencies and the private sector, on blockchain analysis capabilities and how they interact with broader legislative and regulatory developments.

Experience

Co-Founder and Chief Strategy Officer | Chainalysis | May 2015 to present
Independent Consultant | Mosaic Venture Partners | February to May 2015
Independent Consultant | Western Union | September 2013
CEO and Co-Founder | Coinometrics | September 2013 to November 2014
Research Assistant | Professor Ian Goldin, University of Oxford | September 2013 to May 2014

Education

2012-2014 | Economics MPhil (Merit) | University of Oxford, St. Anthony's College | Thesis title: "Creating a decentralised payment system: A study of Bitcoin"
2009-2012 | Economics BSc (1st Class Honours) | University of Bristol | Thesis title: "Distributional Effects on Aggregate Consumption"

Other

- Testified in Jun 2017 before the US House Financial Services Committee's Subcommittee on Terrorism and Illicit Finance hearing on "Virtual Currency: Financial Innovation and National Security Implications"
- Testified in March 2022 before the US Senate Banking Committee hearing on "Understanding the Role of Digital Assets in Illicit Finance"
- Mentor for the Techstars Alchemist Blockchain accelerator

Truth in Testimony Disclosure Form

In accordance with Rule XI, clause 2(g)(5)* of the *Rules of the House of Representatives*, witnesses are asked to disclose the following information. Please complete this form electronically by filling in the provided blanks.

Committee: Agriculture

Subcommittee: Commodity Exchanges, Energy, and Credit

Hearing Date: 06/23/2022

Hearing Title :

The Future of Digital Asset Regulation

Witness Name: Jonathan Levin

Position/Title: Co-Founder and Chief Strategy Officer, Chainalysis Inc.

Witness Type: ○ Governmental ● Non-governmental

Are you representing yourself or an organization? ○ Self ● Organization

If you are representing an organization, please list what entity or entities you are representing:

Chainalysis Inc.

FOR WITNESSES APPEARING IN A NON-GOVERNMENTAL CAPACITY

Please complete the following fields. If necessary, attach additional sheet(s) to provide more information.

Are you a fiduciary—including, but not limited to, a director, officer, advisor, or resident agent—of any organization or entity that has an interest in the subject matter of the hearing? If so, please list the name of the organization(s) or entities.

Chainalysis Inc.

Please list any federal grants or contracts (including subgrants or subcontracts) related to the hearing's subject matter that you, the organization(s) you represent, or entities for which you serve as a fiduciary have received in the past thirty-six months from the date of the hearing. Include the source and amount of each grant or contract.

Chainalysis has contracts related to cryptocurrency with federal agencies, but the terms of those contracts are covered by non-disclosure obligations and as such, Chainalysis cannot disclose any additional information.

Please list any contracts, grants, or payments originating with a foreign government and related to the hearing's subject that you, the organization(s) you represent, or entities for which you serve as a fiduciary have received in the past thirty-six months from the date of the hearing. Include the amount and country of origin of each contract or payment.

Chainalysis has contracts related to cryptocurrency with foreign governments, but the terms of those contracts are covered by non-disclosure obligations and as such, Chainalysis cannot disclose any additional information.

Please complete the following fields. If necessary, attach additional sheet(s) to provide more information.

☑ I have attached a written statement of proposed testimony.

☑ I have attached my curriculum vitae or biography.

***** Rule XI, clause 2(g)(5), of the U.S. House of Representatives provides:

(5)(A) Each committee shall, to the greatest extent practicable, require witnesses who appear before it to submit in advance written statements of proposed testimony and to limit their initial presentations to the committee to brief summaries thereof.

(B) In the case of a witness appearing in a non-governmental capacity, a written statement of proposed testimony shall include— (i) a curriculum vitae; (ii) a disclosure of any Federal grants or contracts, or contracts, grants, or payments originating with a foreign government, received during the past 36 months by the witness or by an entity represented by the witness and related to the subject matter of the hearing; and (iii) a disclosure of whether the witness is a fiduciary (including, but not limited to, a director, officer, advisor, or resident agent) of any organization or entity that has an interest in the subject matter of the hearing.

(C) The disclosure referred to in subdivision (B)(iii) shall include— (i) the amount and source of each Federal grant (or subgrant thereof) or contract (or subcontract thereof) related to the subject matter of the hearing; and (ii) the amount and country of origin of any payment or contract related to the subject matter of the hearing originating with a foreign government.

(D) Such statements, with appropriate redactions to protect the privacy or security of the witness, shall be made publicly available in electronic form 24 hours before the witness appears to the extent practicable, but not later than one day after the witness appears.