Chainalysis

FEBRUARY 2023

The 2023 Crypto Crime Report

Everything you need to know about cryptocurrency-based crime

Table of Contents

Introduction	3
Sanctions	9
Ransomware	26
Money Laundering	41
Stolen Funds	55
Oracle Manipulation Attacks	65
Darknet Markets	70
Scams	85
Pump and Dump Tokens	104

Introduction

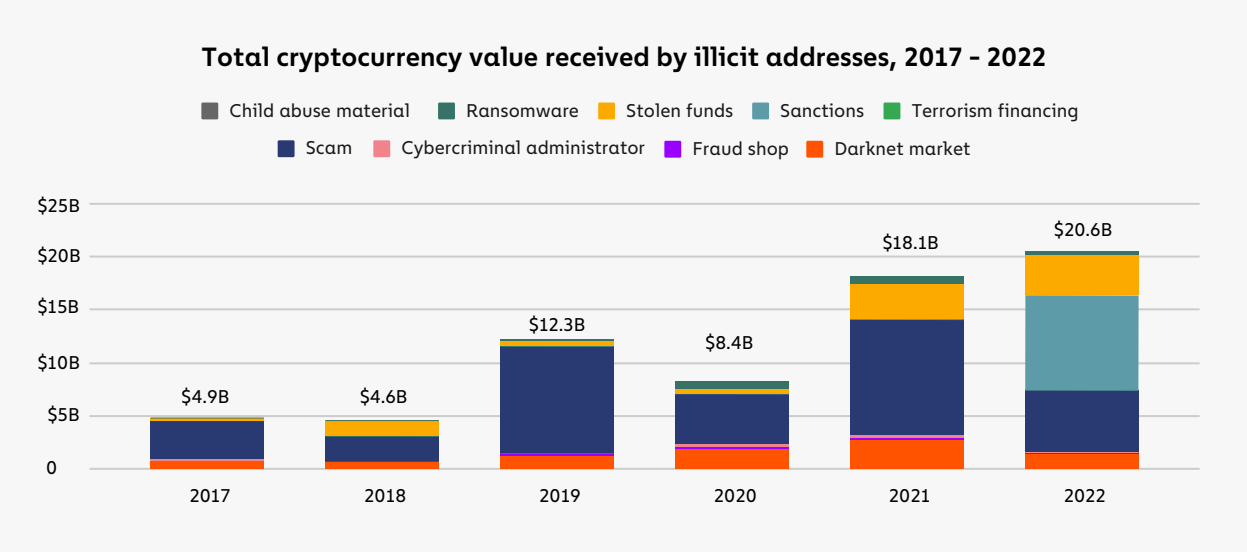
2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs Amid Surge in Sanctions Designations and Hacking

Every year, we publish our estimates of illicit cryptocurrency activity to demonstrate the power of blockchains' transparency – these kinds of estimates aren't possible in traditional finance – and to teach investigators and compliance professionals about the latest trends in cryptocurrency-related crime that they need to know about. What could those estimates look like in a year like 2022? Last year was one of the most tumultuous in cryptocurrency history, with several large firms imploding, including Celsius, Three Arrows Capital, FTX, and others — some amid allegations of fraud.

Those allegations make this year's Crypto Crime Report a bit tricky, as some feel that those businesses should be treated as criminal enterprises. Ultimately though, we don't include their transaction volumes in our measures of illicit activity because our estimates are based solely on on-chain intelligence — we don't account for instances where, for example, off-chain bookkeeping may have been fraudulent. Plus, the bankruptcy and criminal cases associated with these collapses are still ongoing, so for the time being, we'll leave questions of criminality to the legal system.

The events of this year have made clear that although blockchains are inherently transparent, the industry has room for improvement in this respect. There are opportunities to connect off-chain data on liabilities with on-chain data to provide better visibility, and transparency of DeFi, where all transactions are on-chain, is a standard that all crypto services should strive to achieve. As more and more value is transferred to the blockchain, all potential risks will become transparent, and we will have more complete visibility.

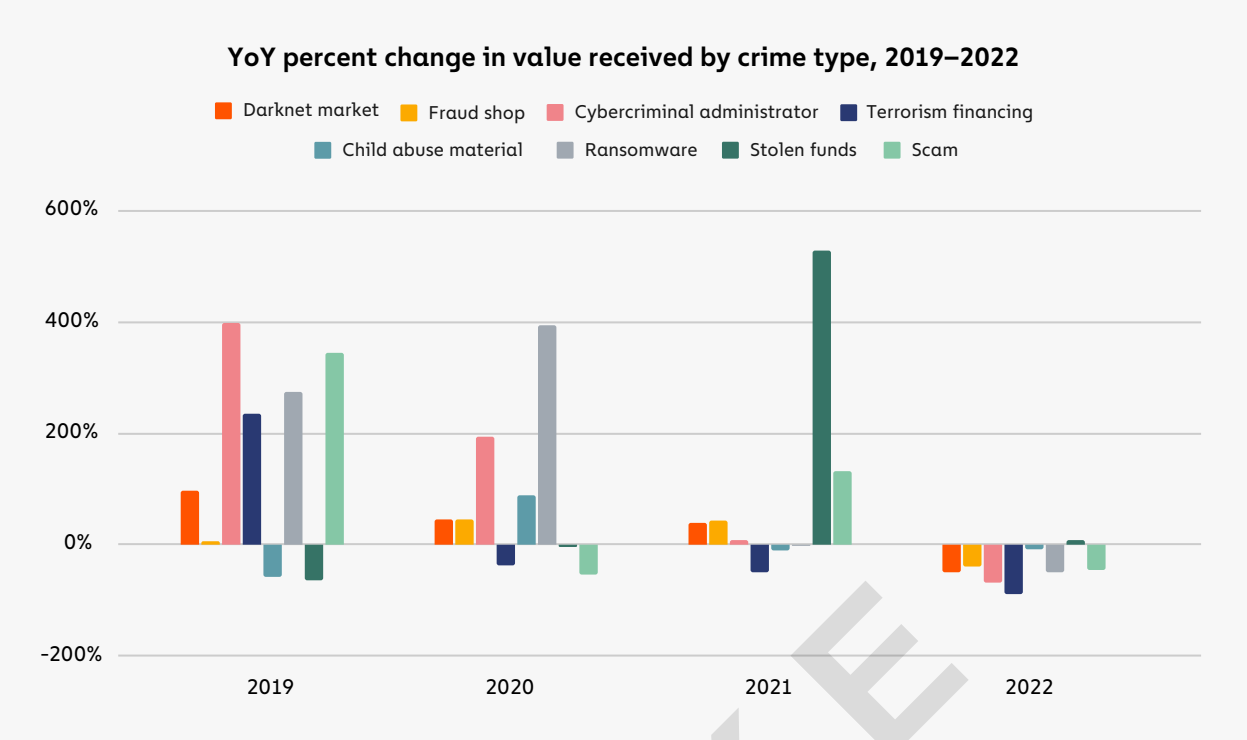
For now though, we'll continue to focus on illicit activity that can be measured on-chain. Let's look at how the market tumult of 2022 affected cryptocurrency-based crime.



See endnote [1] for notes on this chart.

Despite the market downturn, illicit transaction volume rose for the second consecutive year, hitting an all-time high of $20.6 billion. We have to stress that this is a lower bound estimate — our measure of illicit transaction volume is sure to grow over time as we identify new addresses associated with illicit activity, and we have to keep in mind that this figure doesn't capture proceeds from non-crypto native crime (e.g. conventional drug trafficking involving cryptocurrency as a mode of payment). For example, last year we published that we found $14 billion in illicit activity in 2021 — we've now raised that figure to $18 billion, mostly due to the discovery of new crypto scams.

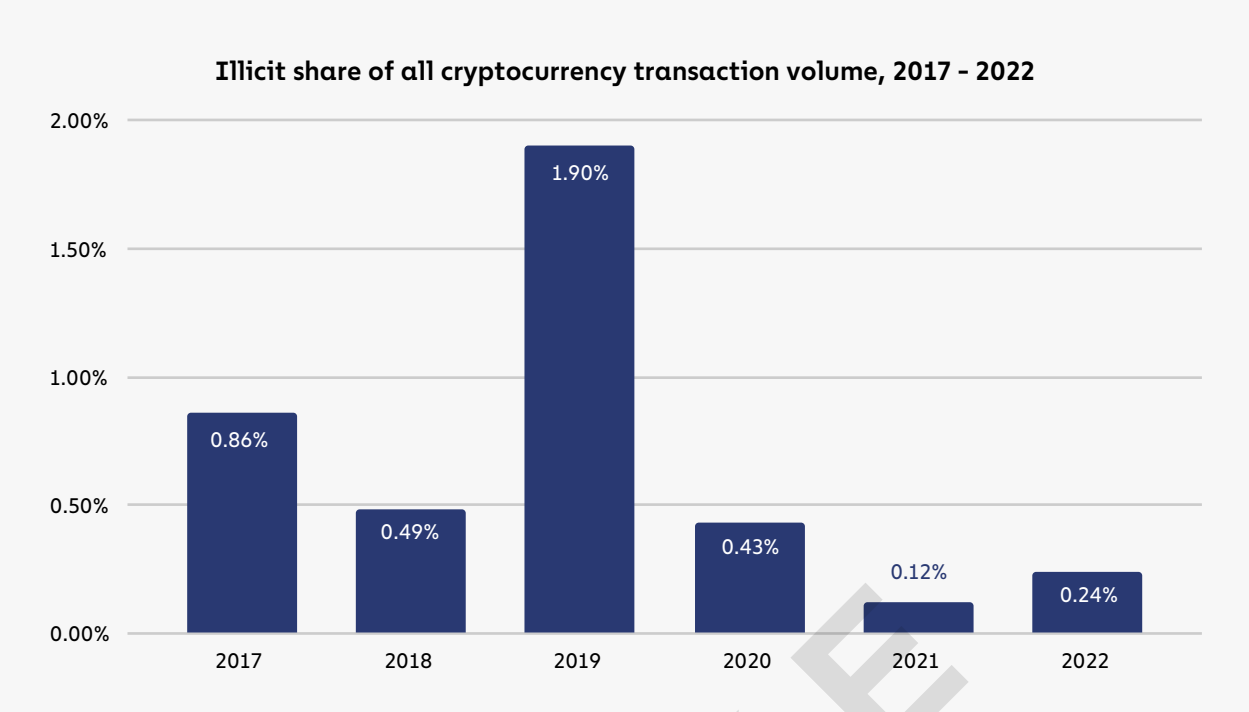
It's also worth keeping in mind that 43% of 2022's illicit transaction volume came from activity associated with sanctioned entities, in a year when OFAC launched some of its most ambitious and difficult-to-enforce crypto sanctions yet. Crypto exchange Garantex, which accounted for the majority of sanctions-related transaction volume last year, is a great example. OFAC sanctioned Garantex in April 2022, but as a Russia-based business, the exchange has been able to continue operating with impunity. Transactions associated with Garantex or any other sanctioned crypto service represent, at the very least, substantial compliance risk for businesses that are subject to U.S. jurisdiction, including fines and potential criminal charges.



Note: Sanctions-related transaction volume rose 152,844% from 2021 to 2022 – we do not include that on the graph above due to the scale issues it would create.

Transaction volumes fell across all of the other, more conventional categories of cryptocurrency-related crime, with the exception of stolen funds, which rose 7% year-over-year. The market downturn may be one reason for this. We've found in the past that crypto scams, for instance, take in less revenue during bear markets, likely because users are more pessimistic and less likely to believe a scam's promises of high returns at times when asset prices are declining. In general, less money in crypto overall tends to correlate with less money associated with crypto crime.

Overall, the share of all cryptocurrency activity associated with illicit activity has risen for the first time since 2019, from 0.12% in 2021 to 0.24% in 2022. [2]



This shouldn't come as a huge surprise. As one might expect, total transaction volume fell with the onset of the bear market, and as we showed above, illicit transaction volume grew slightly. In fact, we first spotted this trend back in August, when we noted that legitimate transaction volumes were declining faster than illicit volumes.

Overall, illicit activity in cryptocurrency remains a small share of total volume at less than 1%. It's also worth keeping in mind that despite this year's jump, crime as a share of all crypto activity is still trending downwards. Keep reading, and we'll dig into the details of the criminal activity behind that 0.24%, as well as what our on-chain analysis reveals about the market failures of the last year.

Endnotes:

[1] Notes on our illicit transaction volume chart:

- These are lower bound estimates that will likely rise over time as additional illicit activity is discovered.
- This does not include off-chain criminal activity where proceeds may have been moved into crypto for laundering, though that activity can still be traced.
- This does not include volumes associated with centralized services that collapsed in 2022, some of which are facing charges of fraud, given lack of off-chain insights.
- Funds received by sanctioned entity Garantex accounts for much of 2022's illicit volume. While most of that activity is likely Russian users using a Russian exchange, most compliance professionals treat this as illicit activity.

[2] For those keeping a close eye on our annual analyses, you may be surprised to find that our estimate for the illicit share of all cryptocurrency transaction volume for 2021 actually decreased from the number we published in last year's report – 0.15% to 0.12%. Don't these estimates usually increase over time, as mentioned above? In this case, our denominator – total volume analyzed – increased as we added mature support for additional blockchains.

Sanctions

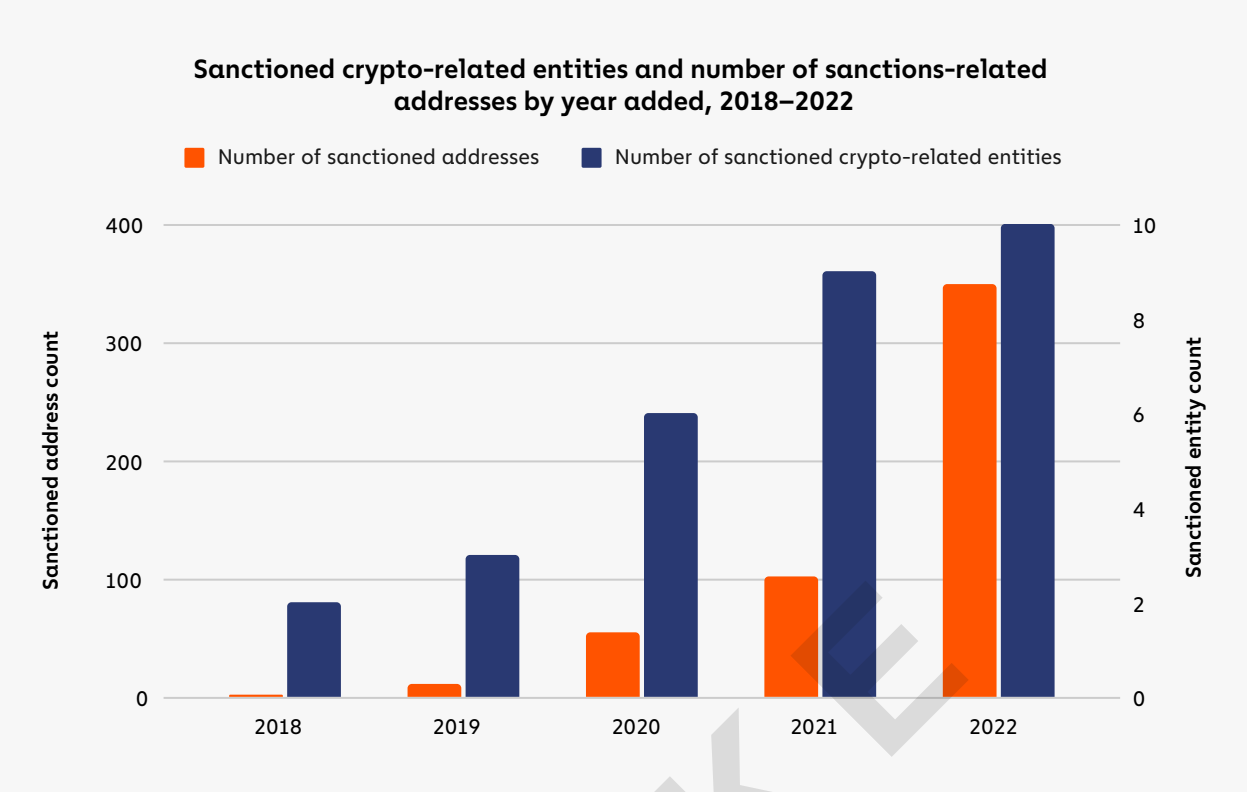
How 2022's Biggest Cryptocurrency Sanctions Designations Affected Crypto Crime

Agencies like the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and its equivalents in other countries implement sanctions through the targeting of countries, regimes, individuals, and entities that are considered threats to national security and foreign policy. Traditionally, sanctions enforcement relies on the cooperation of mainstream financial institutions, but some bad actors have turned to cryptocurrency to circumvent these third party intermediaries, giving policymakers and sanctioning bodies new challenges with which to grapple. However, cryptocurrency's inherent transparency, along with the willingness of compliant cryptocurrency services — in particular, the many centralized exchanges that function as the link between crypto and fiat — have demonstrated that sanctions enforcement is possible in the crypto world.

In this section, we'll look at how the U.S. government's crypto-related sanctions strategy has evolved over time, examine the types of entities that it has sanctioned so far, and analyze the impact of those sanctions on the entities themselves and the wider crypto crime ecosystem.

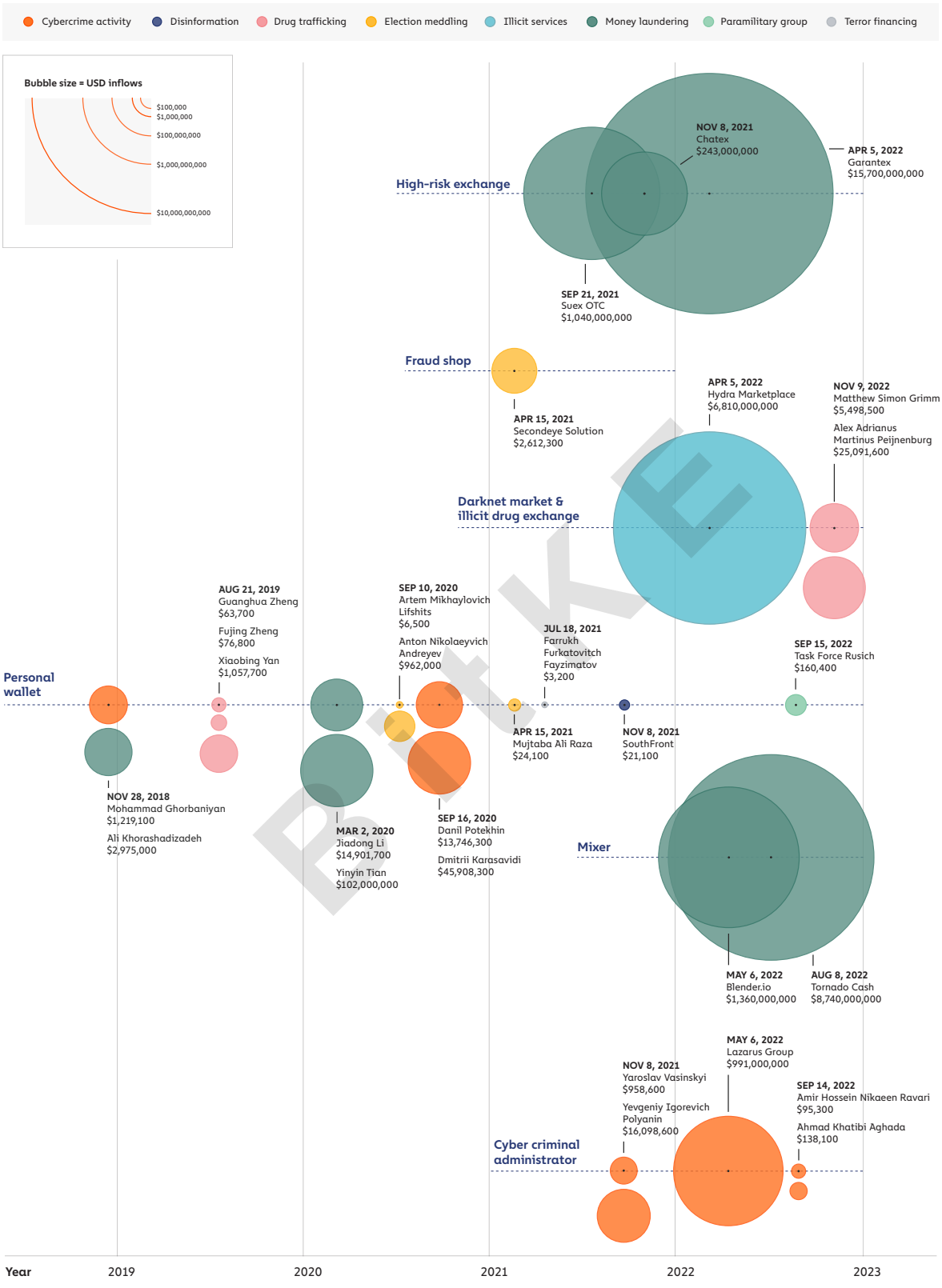
OFAC's cryptocurrency-related sanctions are on the rise since 2021

2018 saw OFAC's first crypto-related sanctions, when it designated two Iranian nationals associated with the SamSam ransomware strain and included Bitcoin addresses linked to the individuals as identifiers on their Specially Designated Nationals And Blocked Persons (SDN) List entries. For the next two years, virtually all cryptocurrency addresses included as sanctions identifiers were personal wallet addresses controlled by individuals, with an average of two addresses per crypto-related designation in 2018, four in 2019, and nine in 2020.



That changed starting in 2021 though, when OFAC began to designate entire crypto services as opposed to just individual bad actors — overall, the average number of addresses per sanctioned entity reached 35 by 2022, with some designations containing over 100 cryptocurrency addresses as identifiers. As seen below with the expanding funnel of sanctioning activity, OFAC's efforts have increased across three dimensions, targeting larger entities and services, more diverse service types, and doing so for a wider array of reasons.

Timeline of OFAC crypto-related sanctions designations, 2018–2022



2022 has seen some of OFAC's biggest cryptocurrency service designations to date. Three in particular are notable not just due to their size, but also in how each highlights unique challenges in enforcing sanctions against different types of crypto entities: darknet market Hydra, decentralized mixer Tornado Cash, and Russia-based cryptocurrency exchange Garantex. But before we get into those, we'll provide an overview of all crypto-related sanctions designations over the last year.

Sanctioned crypto-linked entities in 2022: Who they are and what they do

Here's the breakdown of the individuals and entities with cryptocurrency nexuses sanctioned in the U.S. in 2022, along with the reason OFAC sanctioned them.

Name	Reason for sanction
Lazarus Group	Hacking and crypto theft on behalf of North Korean government
Ahmad Khatibi Aghada	Ransomware
Amir Hossein Nikaeen Ravari	Ransomware
Alex Adrianus Martinus Peijnenburg	Drug trafficking
Matthew Simon Grimm	Drug trafficking
Hydra Marketplace	Darknet market and money laundering
Garantex	Money laundering
Blender.io	Money laundering
Tornado Cash	Money laundering
Task Force Rusich	Russian paramilitary group in Ukraine

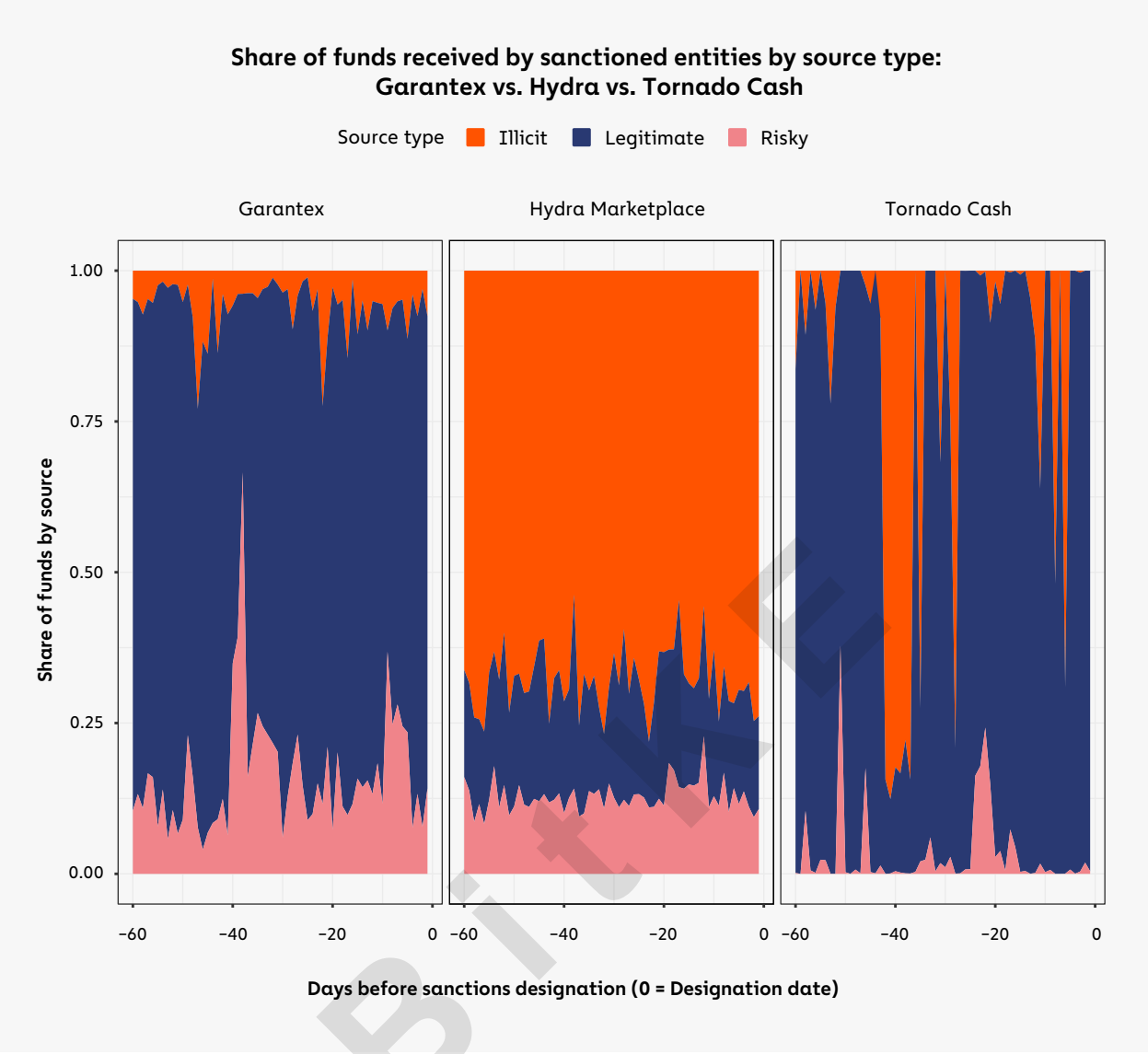
OFAC sanctioned a relatively even mix of individuals and different types of entities in 2022, citing activity such as cybercrime (including ransomware), drug trafficking, money laundering, and in the case of Task Force Rusich, participation in Russia's invasion of Ukraine. Again, this diversity of entities represents a huge change compared to OFAC's pre-2021 designations, which were all against individuals and, at the blockchain level, comprised of only a relatively small number of personal wallets.

Exploring pre and post-designation activity for three of 2022's most notable sanctioned entities: Hydra, Garantex, and Tornado Cash

In order to examine the effects of sanctions on illicit cryptocurrency activity, let's look at how a few of 2022's most notable sanctioned entities behaved before and after their OFAC designations. We'll analyze three services: Hydra, Garantex, and Tornado Cash. First, some brief background on each:

- Hydra was the largest darknet market in the world until its servers were seized by German police, concurrent with its designation by OFAC in April 2022, effectively shutting down the marketplace. Based in Russia, Hydra not only facilitated drug sales, but also offered money laundering services to cybercriminals, including ransomware attackers.
- Garantex is a high-risk crypto exchange based in Russia and was sanctioned at the same time as Hydra for similar money laundering activity. Unlike Hydra, Garantex continues to operate following its designation.
- Tornado Cash is a decentralized mixing service on the Ethereum blockchain that was sanctioned in August 2022 (and again in November) for facilitating money laundering, primarily in relation to funds stolen in cryptocurrency hacks by cybercriminals associated with North Korea. Tornado Cash is currently the only DeFi protocol to have been sanctioned by OFAC — all other designations have been centralized services or personal wallets. As a DeFi protocol, no person or organization can "pull the plug" as easily on Tornado Cash as they could with a centralized service, which has led to questions around the feasibility of sanctioning the service and who, if anyone, can be held responsible for criminal activity it facilitates.

On-chain data can tell us more about the types of entities transacting with these services prior to their sanctions designations.



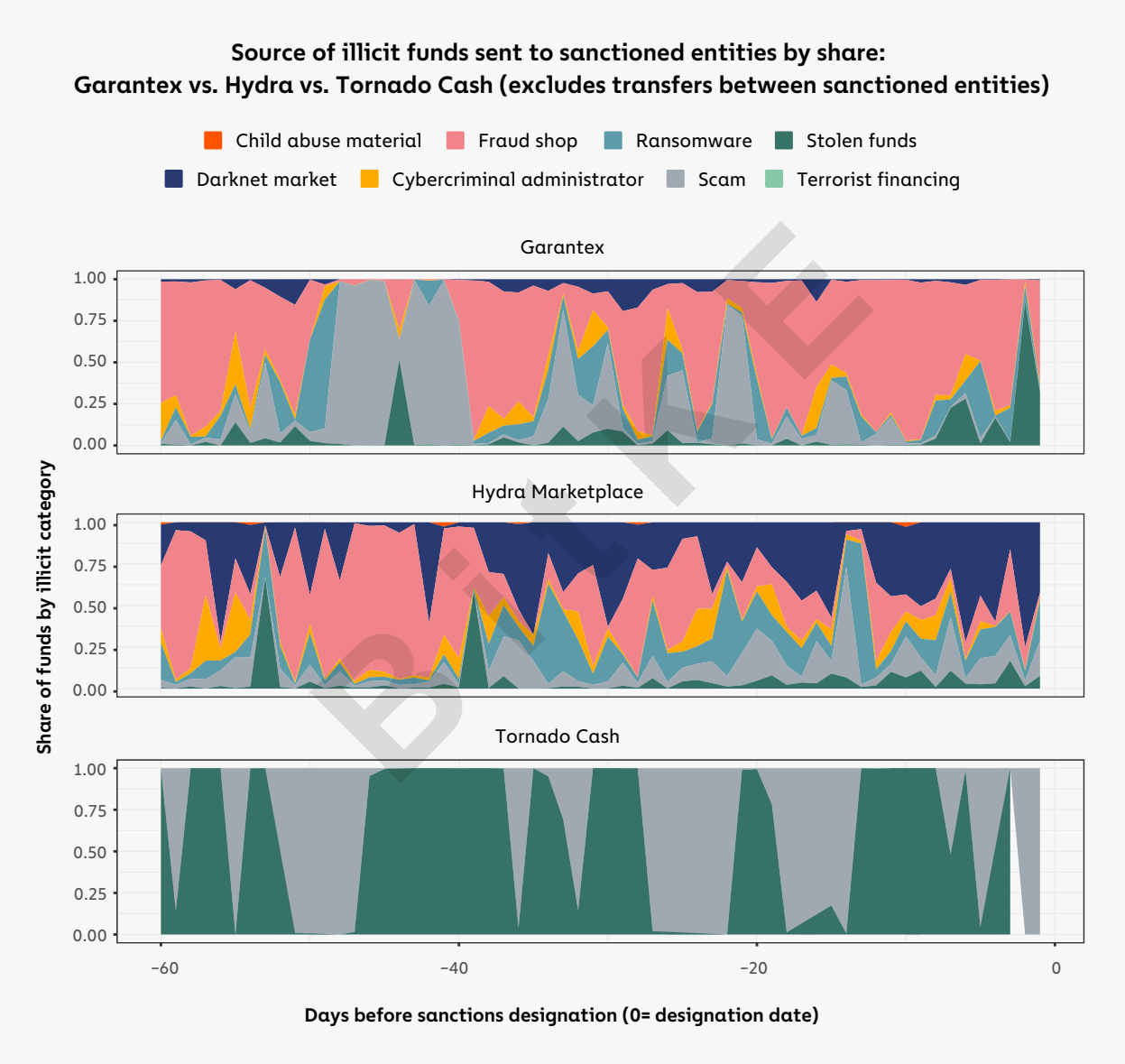
Note: Illicit transaction activity refers to transactions in which one or more counterparty addresses are associated with an illicit entity, such as a darknet market or ransomware attacker. Risky activity refers to transactions in which one or more counterparty addresses are associated with a risky entity, such as a high-risk exchange or gambling service. Legitimate activity refers to transactions in which one or more counterparty addresses are associated with entities that are not inherently criminal or risky, such as personal wallets or exchanges.

- The chart above shows the breakdown of each sanctioned entities' source of incoming funds in the 60 days prior to their designations based on whether the sending wallets were associated with legitimate, illicit, or risky activity. A few things stand out:
- Hydra had by far the most criminal activity of the three services, with 68.2% of all incoming funds coming from illicit addresses, and 12.6% coming from risky addresses.
- Garantex, on the other hand, saw 6.1% of its inflows come from illicit sources and 16.1% from risky sources. 6.1% may sound like a small share of inflows, but it actually puts Garantex firmly

on the riskier end of the spectrum for exchanges — over the same 60-day period, centralized exchanges as a whole received on average just 0.3% of funds from illicit addresses.

- 34% of all funds sent to Tornado Cash came from illicit sources, but this number fluctuated greatly depending on the day, with most illicit funds coming in brief spikes

Let's dig deeper into the specific types of illicit entities that sent funds to each of these sanctioned services.

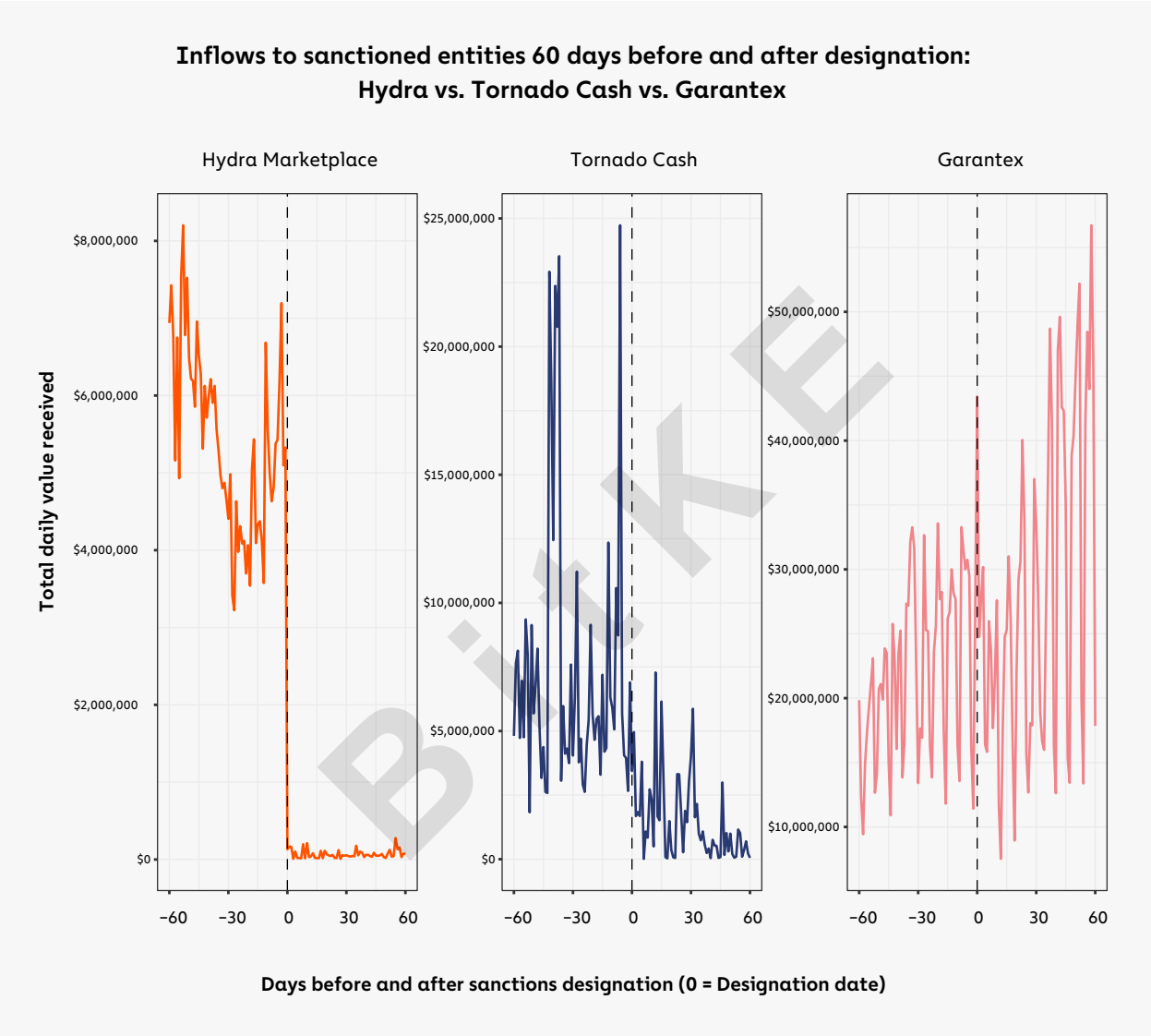


Garantex and Hydra both received funds from a wide array of illicit actors in the 60 days leading up to their sanctions designations, including fraud shops, scams, and most notably, ransomware. During this time period, Hydra received roughly $176,000 worth of cryptocurrency from ransomware addresses, representing 2.2% of all funds sent by any ransomware address. Garantex was even worse, taking in $931,000 from ransomware addresses, or 11.6% of all funds sent by ransomware addresses. The numbers underscore how crucial these services — especially Garantex — have been to enabling ransomware attacks. We must also note that these dollar figures may grow as we continuously identify more ransomware-related wallets over time.

Tornado Cash's illicit activity was concentrated to just two forms of cybercrime: Crypto hacks and scams. While not apparent from the graph above, we should note that stolen funds make up nearly all of that total, at 99.7% of all illicit funds received during the entire 60-day time period. The inflows of stolen funds come in periodic spikes, which in turn drive the spikes in overall illicit inflows to Tornado Cash that we saw in the previous graph. The Harmony Bridge hack, which occurred in June 2022, roughly 45 days before Tornado Cash's sanctions designation, accounted for 65.7% of the mixer's total stolen fund inflows during this period. This pattern of isolated, unique events, contrasts with the more constant flow of illicit activity from services such as darknet markets, which produce a steady stream of funds.

How did sanctioned entities behave post-designation? It depends.

On-chain data shows that each of the three sanctioned services were affected differently by their designations. The charts below show cryptocurrency inflows for Garantex, Hydra, and Tornado Cash in the 60 days before and after they were sanctioned.



On one end of the spectrum, we have Hydra. Its inflows dropped to zero as soon as it was sanctioned because the service was also seized in a coordinated law enforcement action at the same time.

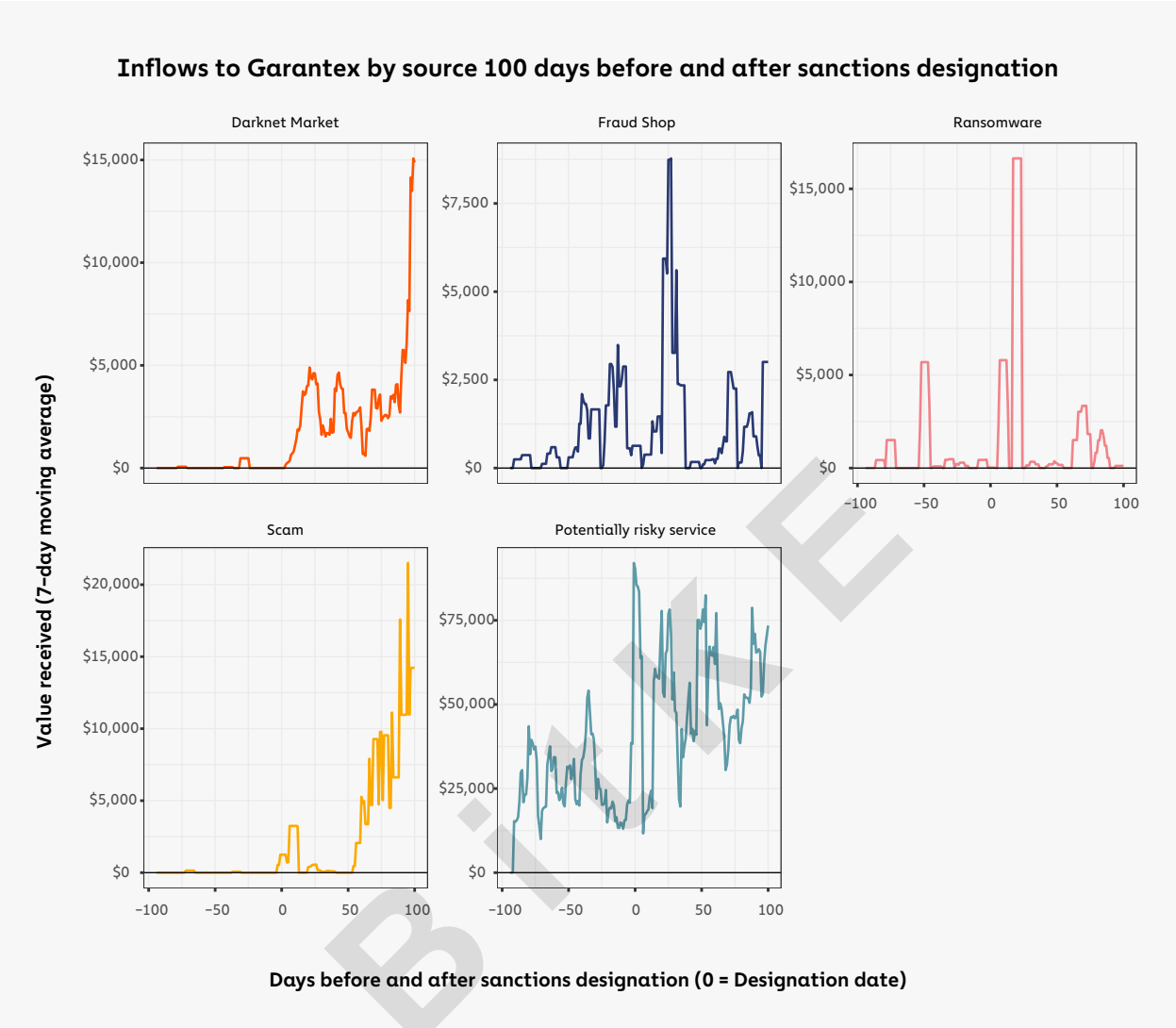
On the other end of the spectrum is Garantex, which wasn't seized upon being sanctioned, and actually saw its transaction volume steadily increase post-designation. For example, in the four

months up through April when Garantex was sanctioned, the high risk exchange had averaged $620.8 million in monthly inflows. After the sanctioning event, Garantex's inflows rose considerably, with an average of approximately $1.3 billion in monthly inflows through October. This is most likely due to the fact that Garantex and most of its users are based in Russia. The Russian government has not enforced U.S. sanctions, leaving users not subject to U.S. jurisdiction with virtually no incentive to stop using Garantex. In fact, Garantex explicitly stated its intent to continue operating in social media posts immediately following the designation.

Tornado Cash falls in the middle of the spectrum, as its activity dropped significantly after being sanctioned, but hasn't ceased completely. As we discussed previously, Tornado Cash runs on smart contracts that can't be taken offline the way a centralized service can, so there's nothing except the legal consequences of sanctions violations stopping anyone from using it. However, the Tornado Cash website that acted as a front-end for easy access to the mixing service was taken down, making it more difficult to access. And, as a global service, Tornado Cash likely had more users who could face consequences for violating U.S. sanctions, or who would be cut off from using other services if their wallets displayed exposure to Tornado Cash following its designation.

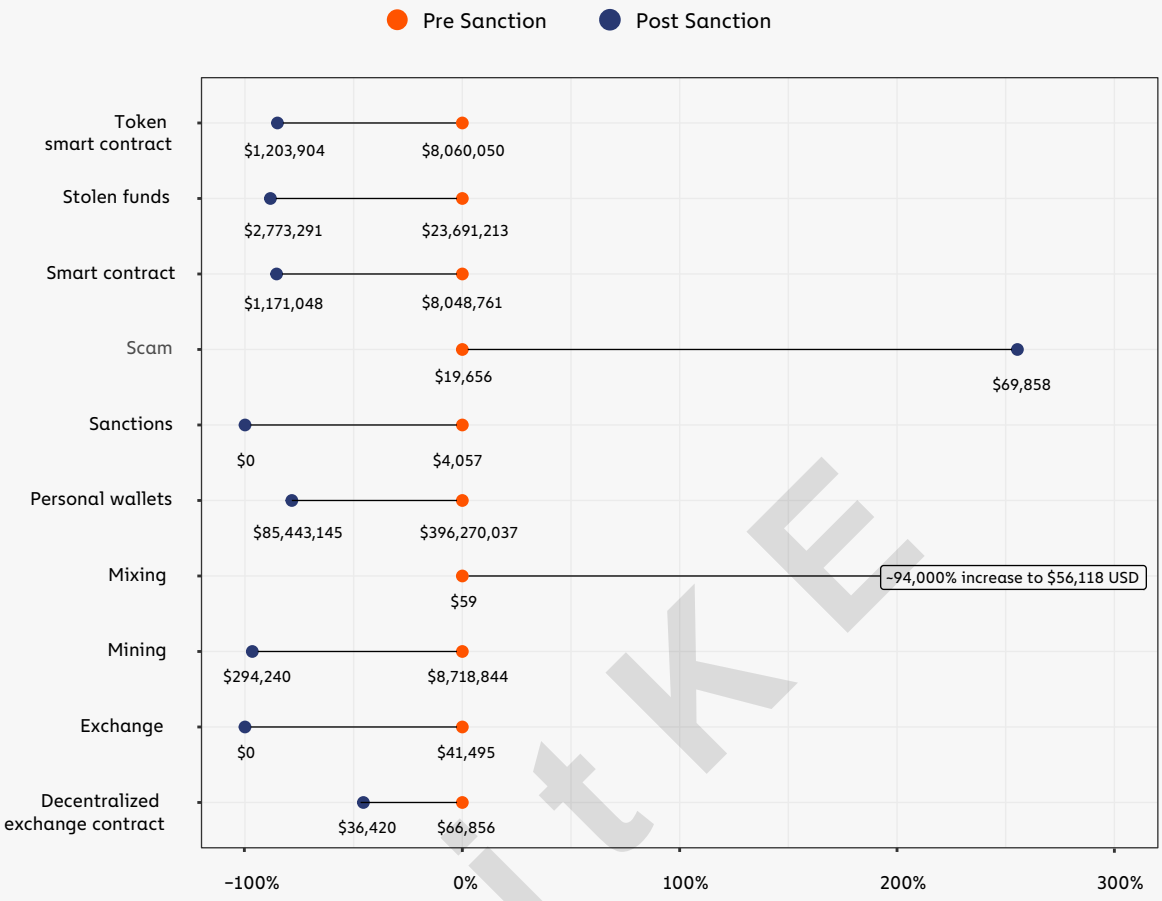
Digging deeper into these aggregate inflow patterns, we also see that different types of counterparties reacted differently to each service's sanctions designation. We'll leave Hydra out here, as we already saw above that its inflows dropped to zero due to the seizure of its darknet site infrastructure.

Here's how inflows to Garantex from different types of services and entities changed following its sanctions designation.



Most of Garantex's counterparties continued to use the service at roughly the same levels they did before the exchange was sanctioned, apparently unperturbed by the designation. In fact, darknet markets and scammers actually sent more funds to Garantex following the designation, perhaps reassured that the exchange would be unlikely to try and curb their activity.

Change in inflows to Tornado Cash post-sanctions designation by counterparty category (60-days pre/post sanction designation date)



Percent change, 60 days pre-designation vs. 60 days post-designation

Tornado Cash, on the other hand, saw drops in inflows from virtually every category, the exceptions being an increase in funds sent from scammers and mixing services. However, despite the percentage increases, neither category had sent a particularly high volume of funds to Tornado Cash before its sanctions designation anyway. And, in the case of scams, the increase was the result of a single YouTube-based liquidity bot scam that saw inflows over four deposits, and likely does not reflect a wider trend.

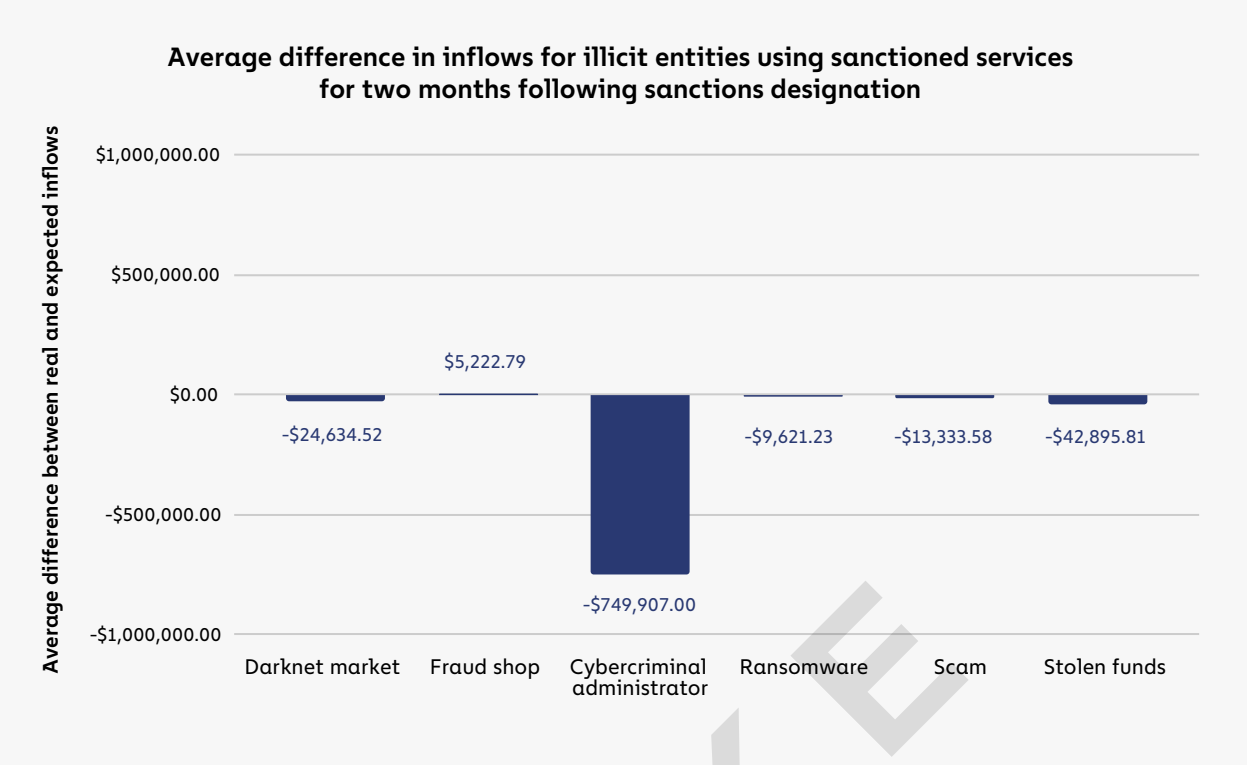
Did sanctions affect criminal users of designated services?

Four of the entities sanctioned in 2022 were designated at least in part due to their provision of money laundering services to other criminals, such as ransomware attackers, scammers, and hackers. Those services were:

- Hydra
- Garantex
- Tornado Cash
- Blender.io (another mixer)

It follows that one goal of those sanctions would be to disrupt the criminals who relied on those services for money laundering. Did this end up happening in practice? **Or, put another way, if I was a crypto criminal who relied on one (or more) of these money laundering services, did I see less revenue than expected after that service was sanctioned?**

We attempt to answer this question below by quantifying the average difference between actual inflows and expected inflows for illicit entities who used the money laundering services listed above prior to their designations. In order to calculate expected inflows, we used inflows to other illicit services in the same criminal categories who did not use those sanctioned money laundering services as a control group. These other illicit services help to establish a revenue baseline for the two months following each money laundering service's sanctions designation. [1] We found that illicit entities who used sanctioned services saw significant lost potential revenue across nearly every crypto crime category in the two months following the sanctioning event — for example, the average darknet market who had previously sent funds to one of the sanctioned services saw an estimated $25,000 less revenue in the two months following that service's designation than they likely would have had the service not been designated.



The most-affected category were cybercriminal administrators, who on average saw an estimated $750,000 decrease in revenue due to the sanctioning of money laundering services they had previously used. The one exception to this trend was fraud shops, who on average saw nearly $5,000 more revenue than we would estimate absent the sanctioning of a money laundering service counterparty.

It's important to keep in mind that the graph above shows only the average estimated change in revenue for counterparties of sanctioned money laundering services. With several distinct entities in each category who had previously used those money laundering services, the estimated total losses by category are much higher.

Illicit category	Number of entities	Average inflows change	Total revenue change for category
Darknet market	11	-$24,634.52	-$270,979.67
Fraud shop	10	$5,222.79	$52,227.91
Cybercriminal administrator	20	-$749,907.00	-$14,998,139.98
Ransomware	6	-$9,621.23	-$57,727.38
Scam	23	-$13,333.58	-$306,672.24
Stolen funds	42	-$42,895.81	-$1,801,624.08

We should caveat these findings by noting that, while we've taken steps to control for other factors and analyze only the revenue changes brought on by the sanctioning of their money laundering services, there could be other reasons these dependent entities' revenue might have changed following the sanctions designations. We should also emphasize that we're only looking at changes to revenue in the two months following the money laundering services' designations — it's entirely possible and even likely that any revenue hits to illicit entities will be temporary, and that they'll soon find alternative money laundering services that haven't been sanctioned. Nonetheless, our findings suggest that sanctions against money laundering services did in fact disrupt the illicit entities who relied on those services, at least temporarily, and impacted their bottom line.

Key takeaways: Impact of crypto sanctions depends on jurisdiction and technical constraints

New technologies and forms of value transfer change the landscape of financial crime enforcement. OFAC is learning this first-hand, and has broken new ground in the last two years with its efforts to move beyond individuals and designate cryptocurrency services that facilitate money laundering and other harmful forms of crypto-based activity. The three examples we focused on above show how different variables impact agencies' ability to levy sanctions against those services.

First, the case of Hydra teaches us that sanctions can be extremely effective against entities with key operations in cooperative jurisdictions. Hydra's servers were located in Germany — German law enforcement coordinated with U.S. agencies, and moved to seize Hydra's servers, striking a fatal blow to the organization, in addition to the sanctions levied by OFAC on the darknet market.

Second, the case of Garantex shows what happens when there is an absence of international cooperation. While Garantex has been largely cut off from the compliant exchange ecosystem, Russia has declined to enforce sanctions against the service, so it continues to operate mostly unencumbered. This case shows that it is difficult to effectively sanction entities whose home jurisdictions have no formal cooperation channels with OFAC.

Finally, the case of a decentralized service like Tornado Cash is more complicated. While its front-end website was taken down, its smart contracts can run indefinitely, meaning anyone can still technically use it at any time. That suggests sanctions against decentralized services act more as a tool to disincentivize the service's use rather than cut off usage completely. In the case of Tornado Cash, those incentives appear to have been powerful, as its inflows fell 68% in the 30 days following its designation. That's especially important here given that Tornado Cash is a mixer, and mixers become less effective for money laundering the less funds they receive overall.

These case studies provide a model of how OFAC and its international equivalents can approach sanctions designations against different kinds of crypto-related entities. It will be interesting to see how these patterns develop as sanctioning bodies continue to improve their ability to effectively target sanctions against different kinds of illicit cryptocurrency services, in partnership with other agencies in the U.S. and internationally.

Endnotes:

[1] Interventions always need to factor in what would otherwise have been. In this case, we used data on the non-counterparties of sanctioned services to estimate what total on-chain aggregate revenue inflows for counterparties might have looked like absent a sanctioning event. Non-counterparties are those entities that sent no funds to sanctioned entities in the two months before they were sanctioned. Counterparties are those entities that did send funds to sanctioned entities prior to the sanctioning event (over a two-month window).

We assume that, within a given category of illicit activity (say, darknet markets), counterparties are roughly comparable to non-counterparties, and differ largely in their counterparty status.

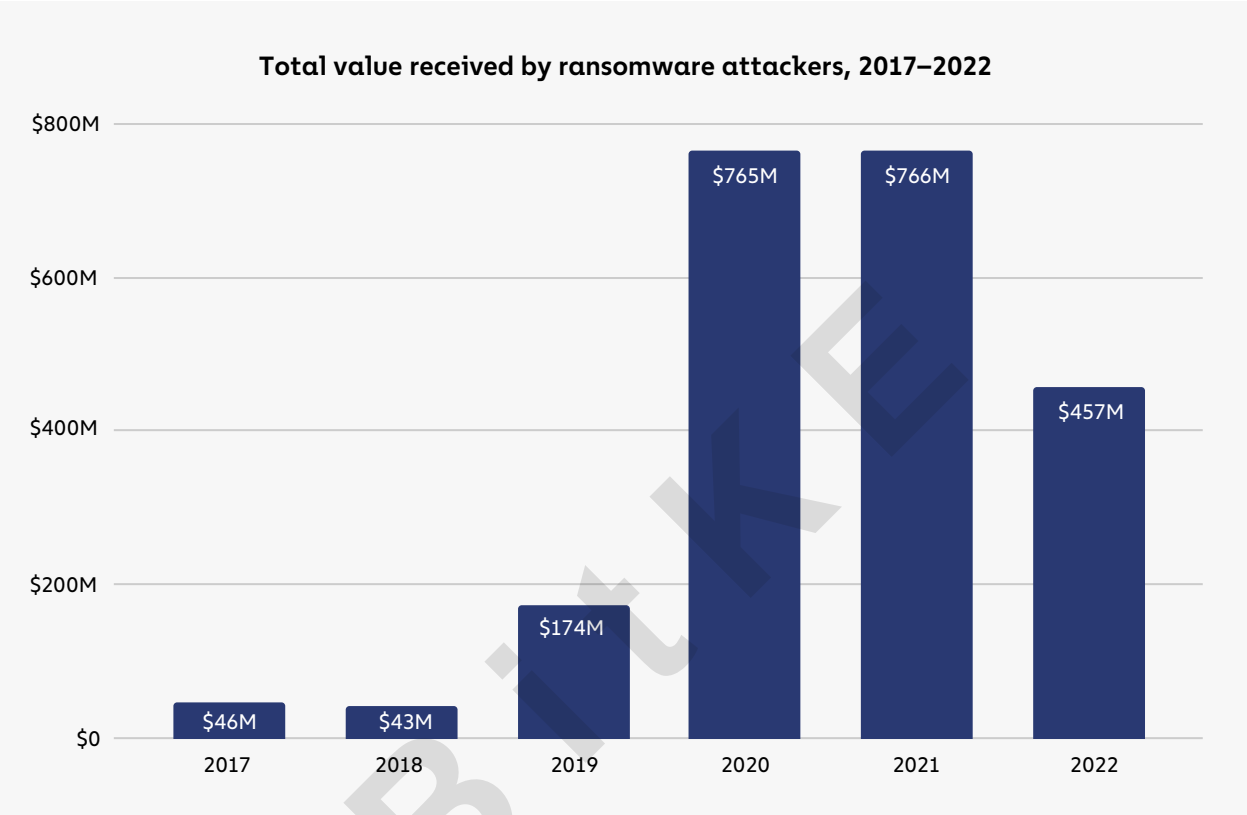
This assumption lets us compare the inflows (which we can think of as akin to revenue for a criminal enterprise or actor) of counterparties relative to the performance of non-counterparties in the months following a sanctioning event, and reveal how counterparties may have performed had their service not been sanctioned. For example, if a counterparty of a sanctioned service received 10% more aggregate revenue inflows after a sanctioning event, that can look like the sanctions had a counterproductive effect. However, if entities of a similar type that were not counterparties to the sanctioned service grew by 50%, then we have reason to suspect that the 10% growth seen by counterparties was actually less than it would have been if sanctions had not been used.

The difference in post-sanctioning performance of counterparties and non-counterparties helps us estimate (directionally) and with modest precision the degree of under or over performance of sanctioned entity counterparties. To reach this final step, we take the difference between the average counterparty percent change in on-chain inflows by category and subtract the same measure for non-counterparties. We then use this percentage point value to weight the total amount of USD inflows to each category of sanctioned entity counterparty, ultimately providing a single best guess about the degree to which sanctioning interrelates with counterparty on chain activity.

Ransomware

Ransomware Revenue Down As More Victims Refuse to Pay

2022 was an impactful year in the fight against ransomware. Ransomware attackers extorted at least $456.8 million from victims in 2022, down from $765.6 million the year before.

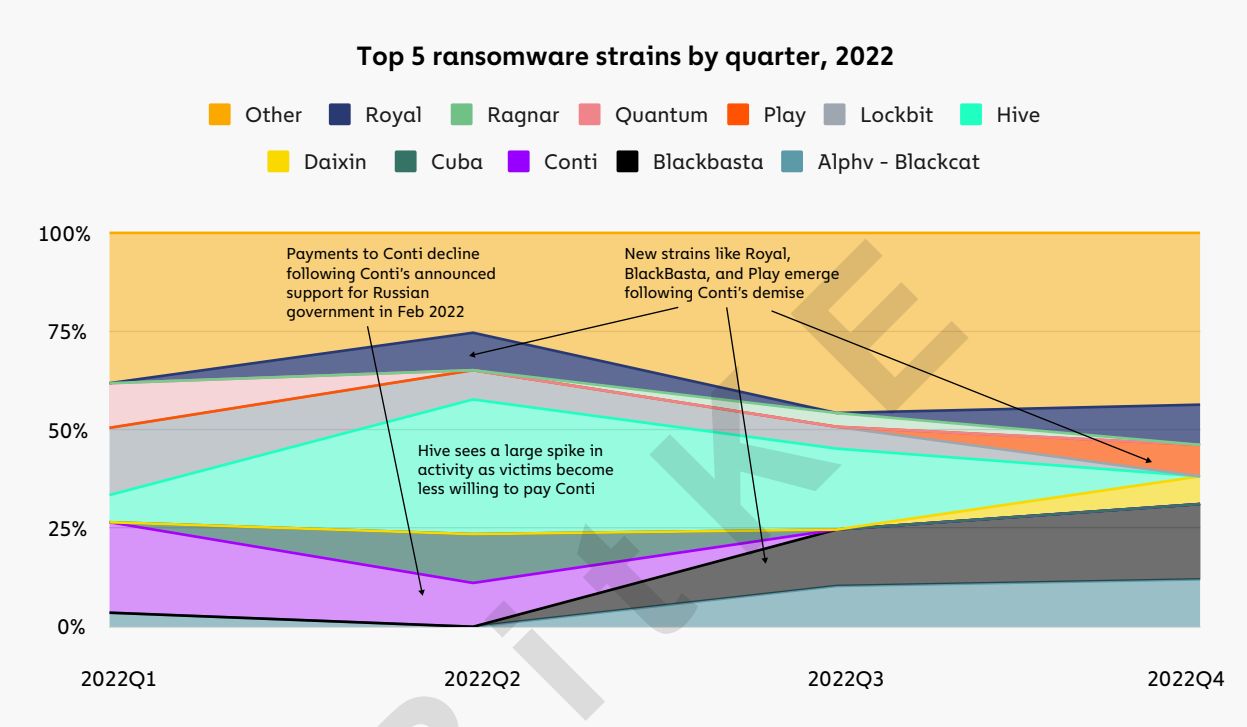


As always, we have to caveat these findings by noting that the true totals are much higher, as there are cryptocurrency addresses controlled by ransomware attackers that have yet to be identified on the blockchain and incorporated into our data. When we published last year's version of this report, for example, we had only identified $602 million in ransomware payments in 2021. Still, the trend is clear: Ransomware payments are significantly down.

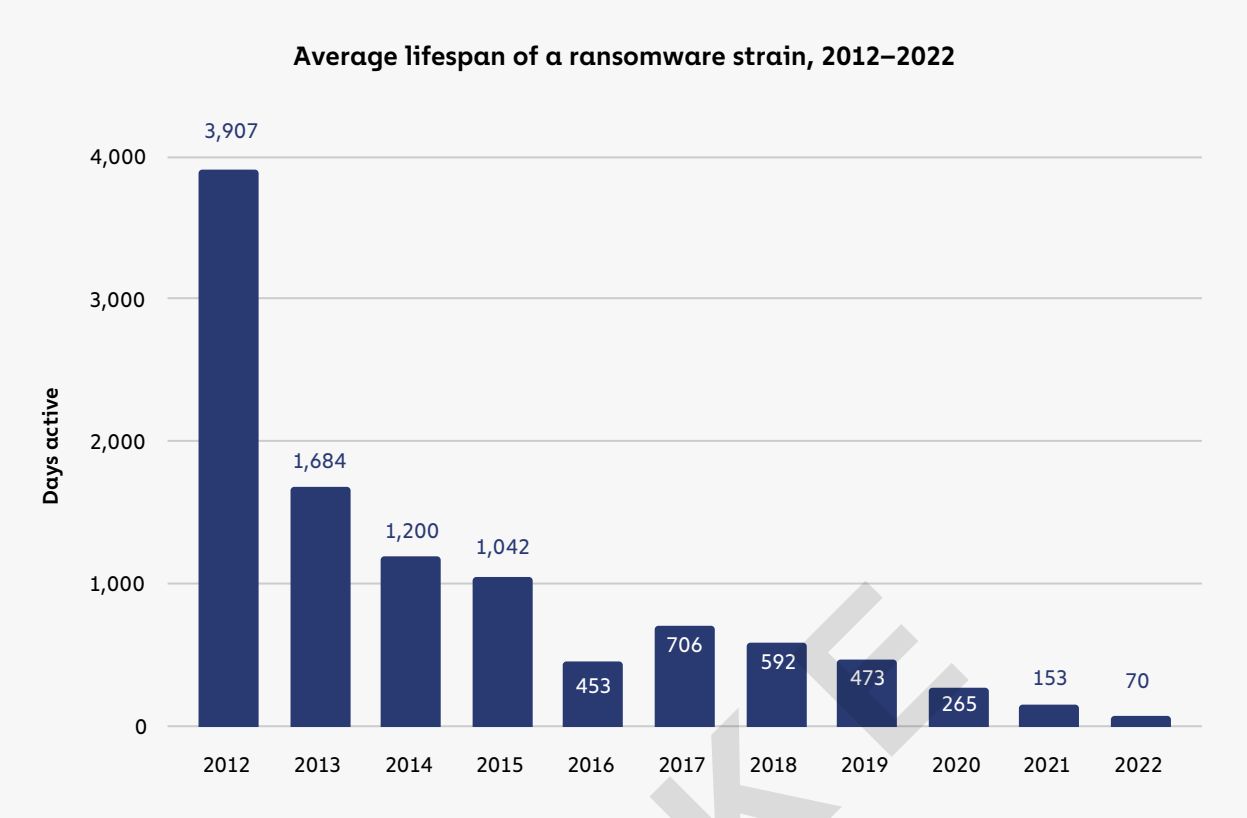
However, that doesn't mean attacks are down, or at least not as much as the drastic dropoff in payments would suggest. Instead, we believe that much of the decline is due to victim organizations increasingly refusing to pay ransomware attackers. We'll discuss this phenomenon more below, but first, let's look more at general ransomware trends in 2022.

2022 ransomware by the numbers

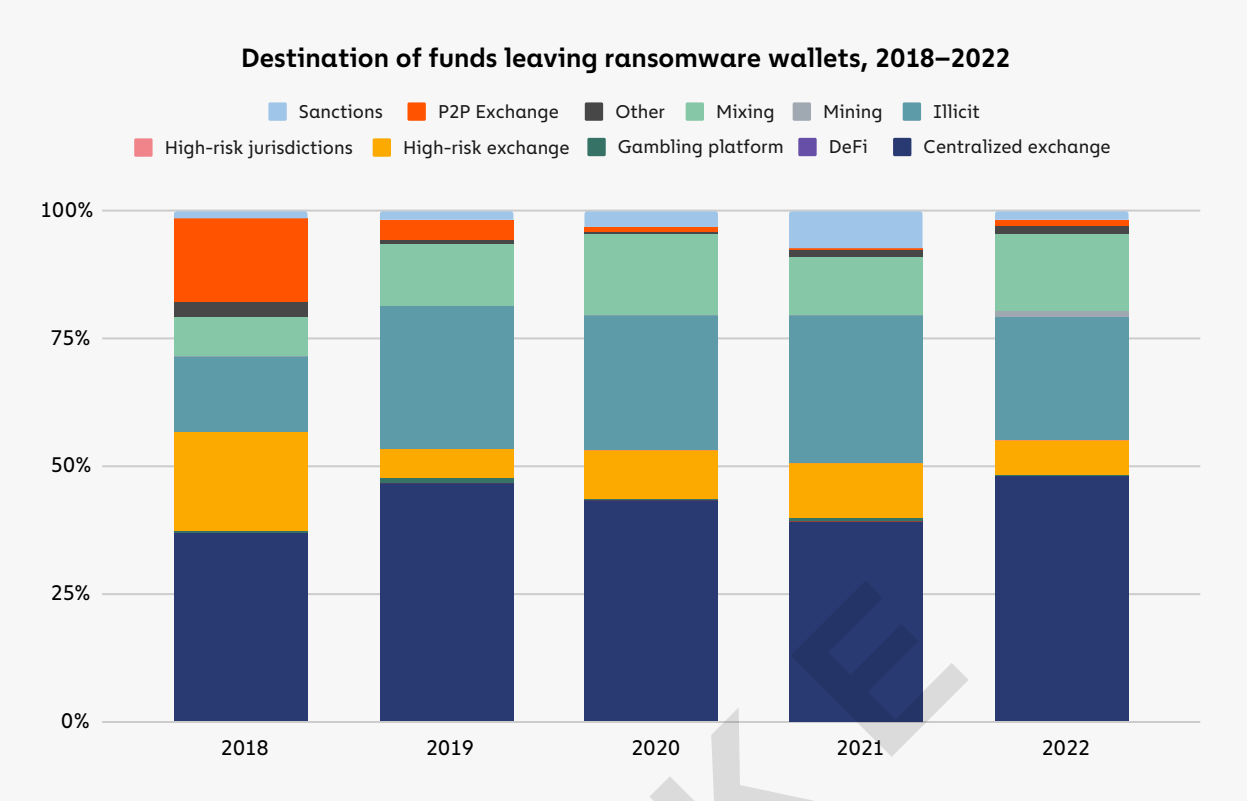
Despite the drop in revenue, the number of unique ransomware strains in operation reportedly exploded in 2022, with research from cybersecurity firm Fortinet stating that over 10,000 unique strains were active in the first half of 2022. On-chain data confirms that the number of active strains has grown significantly in recent years, but the vast majority of ransomware revenue goes to a small group of strains at any given time. We do, however, see turnover throughout the year among the top-grossing strains.



Likewise, ransomware lifespans continue to drop. In 2022, the average ransomware strain remained active for just 70 days, down from 153 in 2021 and 265 in 2020. As we'll explore below, this activity is likely related to ransomware attackers' efforts to obfuscate their activity, as many attackers are working with multiple strains.



When it comes to money laundering, the data indicates that most ransomware attackers send funds they've extorted to mainstream, centralized exchanges.



In fact, the share of ransomware funds going to mainstream exchanges grew from 39.3% in 2021 to 48.3% in 2022, while the share going to high-risk exchanges fell from 10.9% to 6.7%. Usage of illicit services such as darknet markets for ransomware money laundering also decreased, while mixer usage increased from 11.6% to 15.0%.

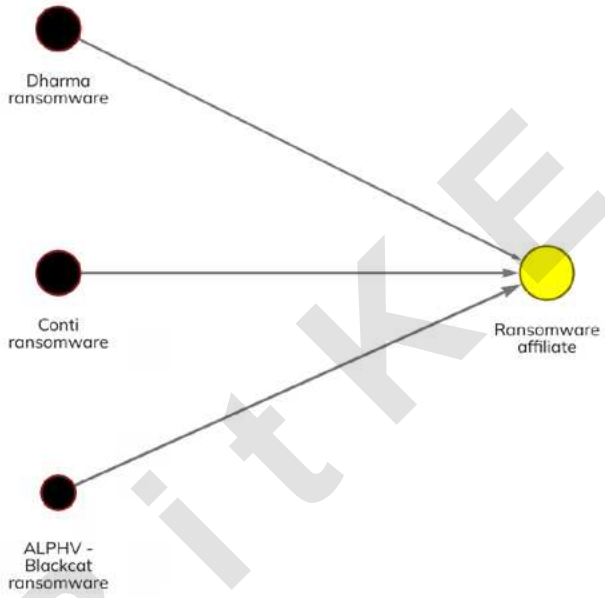
Sizing up the ransomware ecosystem

The constant turnover amongst top ransomware strains and appearance of new ones would suggest that the ransomware world is a crowded one, with a large number of criminal organizations competing with one another and new entrants constantly coming onto the scene. However, looks can be deceiving. While many strains are active throughout the year, the actual number of individuals who make up the ransomware ecosystem is likely quite small.

One place we see this is in affiliate overlap. Most ransomware strains function on the ransomware-as-a-service (RaaS) model, in which the developers of a ransomware strain allow other cybercriminals, known as affiliates, to use the administrator's malware to carry out attacks in exchange for a small, fixed cut of the proceeds. However, we've seen time and time again that many affiliates carry out attacks for several different strains. So, while dozens of ransomware strains may technically have been active throughout 2022, many of the attacks attributed to those strains were likely carried out by the same affiliates. We can think of it as the gig economy, but for ransomware.

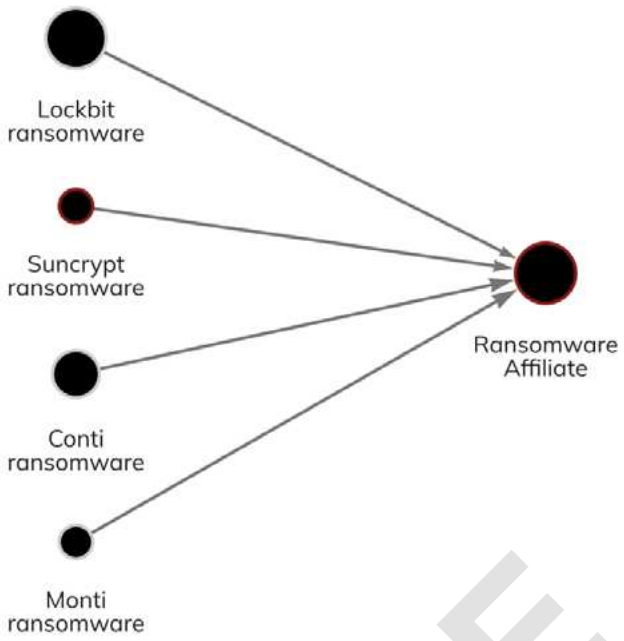
A rideshare driver may have his Uber, Lyft, and Oja apps open at once, creating the illusion of three separate drivers on the road — but in reality, it's all the same car.

Microsoft Security discussed an example of this in a blog post earlier this year discussing one prolific affiliate group, whom they've labeled DEV-0237, who has carried out attacks using the Hive, Conti, Ryuk, and BlackCat ransomware strains. Microsoft Security researchers were able to identify this example of affiliate overlap by analyzing the technical details of how the attacks were carried out, but we can also identify examples of affiliate overlap on the blockchain. On the Chainalysis Reactor graph below, we see an affiliate whose wallet has received large sums from the Dharma, Conti, and BlackCat ransomware strains at different times, which means the affiliate has carried out attacks for all three strains.



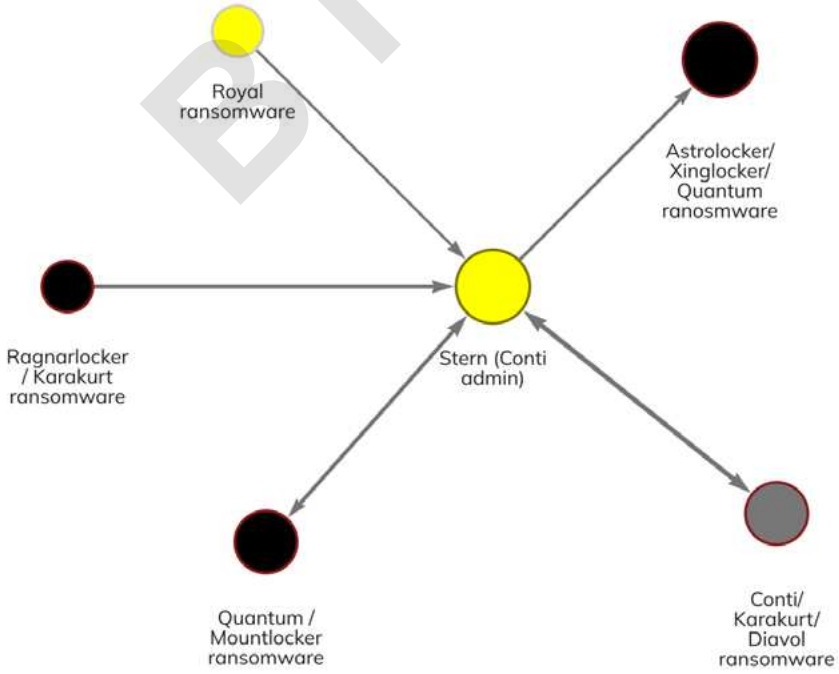
Conti is a particularly interesting case for observing how not just affiliates, but administrators as well rebrand themselves and switch between strains. Conti was a prolific ransomware strain for a few years, taking in more revenue than any other variant in 2021. But in February, immediately following Russia's invasion of Ukraine, the Conti team publicly announced its support for Vladimir Putin's government. Soon after, a cache of Conti's internal communications leaked, and indicated connections between the cybercrime organization and Russia's Federal Security Service (FSB).

For these reasons, many ransomware victims and incident response firms decided that paying Conti attackers was too risky, as the FSB is a sanctioned entity despite Conti itself not being one. Conti responded by announcing its closure in May, but soon after, much of the Conti team split up into smaller groups and continued their activity. Conti's closure drove many affiliates to conduct attacks for other strains whose ransoms victims were more likely to pay, as we showed above. We can see another example of this activity below.



Here, we see a Conti affiliate who began working with the Suncrypt, Monti, and Lockbit strains.

But it isn't just Conti affiliates who have rebranded. On-chain data shows that core administrators have also begun to work with and launch other strains, including the ransomware group's leader, who goes by the alias Stern. The Reactor graph below shows that Stern has transacted with addresses linked to strains like Quantum, Karakurt, Diavol, and Royal in 2022 following Conti's demise.



Notice that in many cases, the ransomware attackers re-used wallets for multiple attacks launched nominally under other strains. This on-chain activity confirms previous research from cybersecurity firm AdvIntel revealing plans by Conti's core leadership to shift operations to some of the strains seen above. It's a great example of how blockchain analysis in tandem with technical analysis of ransomware code and attack patterns can identify offshoots of ransomware strains that have been deemed too risky to pay.

With this data in mind, can Conti truly be said to have shut down if its leader, affiliates, and other members are still successfully carrying out ransomware attacks under new brand names? The data suggests that it may be more productive to think of the ransomware ecosystem not as a collection of distinct strains, but instead as a small group of hackers who rotate brand identities regularly. The fluidity with which affiliates move between ransomware brands makes the sector appear larger than it really is. "The number of core individuals involved in ransomware is incredibly small versus perception, maybe a couple hundred," said Bill Siegel, CEO and co-founder of ransomware incident response firm Coveware. "It's the same criminals, they're just repainting their get-away cars." Siegel indicated this activity has increased of late, and that affiliates are now much more likely to switch strains frequently rather than stick with one for an extended period of time. But, despite ransomware attackers' best efforts, the transparency of the blockchain allows investigators to spot these rebranding efforts virtually as soon as they happen.

The big story: Ransomware victims are paying less frequently

Based on the data available to us now, we estimate that 2022's total ransomware revenue fell to at least $456.8 million in 2022 from $765.6 million in 2021 — a huge drop of 40.3%. However, the evidence suggests that this is due to victims' increasing unwillingness to pay ransomware attackers rather than a decline in the actual number of attacks. We spoke with a number of ransomware experts to learn more.

The first question that jumps to mind: How can we actually know fewer victims are paying, given the lag we've noted previously in how long it takes to identify ransomware addresses, and the massive underreporting of attacks by victims? Michael Phillips, Chief Claims Officer of cyber insurance firm Resilience, indicated that businesses shouldn't rest easy just because ransomware revenue is down. "Data from claims across the cyber insurance industry show that ransomware remains an increasing cyber threat to businesses and enterprises. There have, however, been signs that meaningful disruptions against ransomware actor groups are driving lower than expected successful extortion attempts," he told us. Phillips cited among those disruptions the Russia-Ukraine war and the increased pressure on ransomware gangs from western law enforcement, including arrests and recovery of extorted cryptocurrency.

Recorded Future intelligence analyst and ransomware expert Allan Liska, also known as the Ransomware Sommelier, pointed to the data teams like his collect from data leak sites (DLS), where many ransomware attackers post data stolen from victims in an effort to pressure them into paying. "Most organizations scrape [DLS] data to collect a baseline victimology. By that measure, ransomware attacks decreased between 2021 and 2022 from 2865 to 2566 — a 10.4% drop," said Liska.

If we take DLS victim leaks as a proxy for the number of attacks, there's still a huge gap between a 10.4% drop in leaks and a 40.3% drop in overall ransomware revenue. Instead, our conversations with representatives of cyber insurance and incident response firms suggest much of the revenue drop is explained by victims paying less frequently. Bill Siegel of Coveware provided us with statistics on the probability of a ransomware victim to pay a ransom based on his firm's client matters over the last four years:

	2019	2022	2021	2022
Paid	76%	70%	50%	41%
Did Not Pay	24%	30%	50%	59%

The trend is highly encouraging — since 2019, victim payment rates have fallen from 76% to just 41%. But what exactly accounts for this shift? One big factor is that paying ransoms has become legally riskier, especially following an OFAC advisory in September 2021 on the potential for sanctions violations when paying ransoms. "With the threat of sanctions looming, there's the added threat of legal consequences for paying [ransomware attackers]," said Liska. Bill Siegel agreed, telling us that his firm refuses to pay ransoms if there's even a hint of connection to a sanctioned entity.

Another big factor is the outlook of cyber insurance firms, who are usually the ones reimbursing victims for ransomware payments. "Cyber insurance has really taken the lead in tightening not only who they will insure, but also what insurance payments can be used for, so they are much less likely to allow their clients to use an insurance payout to pay a ransom," said Liska. Phillips echoed this sentiment in his remarks to us. "Today, companies have to meet stringent cybersecurity and backup measures to be insured for ransomware coverage. These requirements have proven to actively help companies bounce back from attacks rather than pay ransom demands. An increased focus on underwriting against factors that contribute to ransomware has led to lower incident costs for companies and contributed to a decreasing trend in extortion payments."

Siegel agreed that cyber insurance firms' demand for better cybersecurity measures is a key driver of the trend toward less frequent ransom payments, and described some of the measures they push clients to implement. "A lot of the insurance carriers are tightening underwriting standards,

and will not renew a policy unless the insured has comprehensive backup systems, uses EDR, and has multi-authentication. This has driven a lot of companies to become more secure," said Siegel. Liska agreed that cybersecurity measures have improved greatly over the past few years. "Back in 2019 when big game hunting and RaaS really started taking off, a lot of security professionals really emphasized the importance of backups. Security professionals saying something and organizations implementing it can take a while. While having an effective backup solution doesn't stop ransomware attacks and doesn't help with data theft, it does give victims more options so they aren't forced to pay," he said.

Siegel described to us how companies with well segmented yet highly available data backups are much less likely to experience material business impact as the result of an attack, and said that they regularly advise clients not to pay unless the payment is economically justified due to the severity of the impact being experienced. Liska also emphasized that backups aren't a magic bullet, noting that the data recovery process can take months and leave ransomware victims vulnerable to follow-up attacks during this process, as we saw in the case of Australian logistics firm Toll Group, which suffered two attacks in three months in 2022.

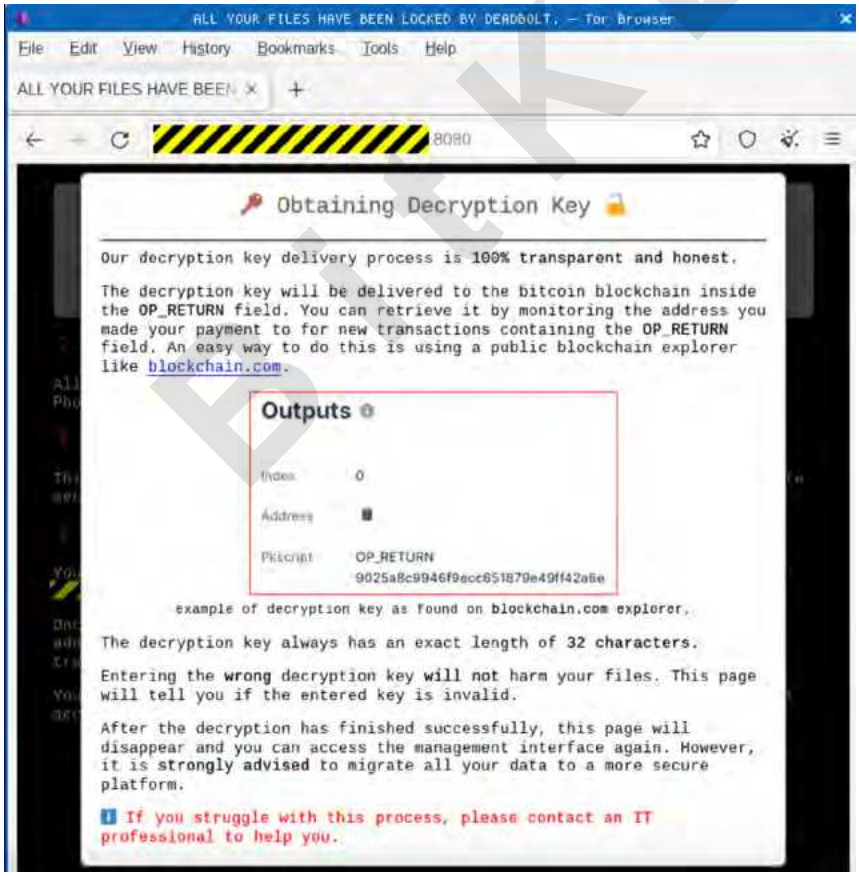
Of course, the best-case scenario is for organizations not to fall victim to ransomware attacks in the first place. To that end, Liska recommends organizations run recurring tabletop exercises, in which all relevant teams — cybersecurity, networking, IT, server administration, backup teams, PR, finance, etc. — meet with leadership to establish how the organization can keep itself secure, identify vulnerabilities, and understand who's responsible for all aspects of security. "Having a realistic picture of where your organization stands and what its weaknesses and strengths are will better prepare everyone in the event your organization is hit with a ransomware attack, and it also makes leadership aware of where it needs to invest to better secure the network, ahead of an attack," said Liska.

If more organizations can implement these best practices the way they have data backups and other security measures, we'll hopefully see ransomware revenue continue to fall in 2023 and beyond.

How the Dutch National Police Tricked Prolific Ransomware Strain Deadbolt Into Giving Up Victim Decryption Keys

Deadbolt is a ransomware strain that first became active in early 2021, and operates very differently from other notable strains of the last few years. While most ransomware gangs focus primarily on attacking large organizations who can afford heavy ransoms, Deadbolt does the opposite, instead taking more of a "spray and pray" approach, targeting small businesses and even individuals in high numbers, while demanding a relatively small ransom from each victim. The reason for this is that Deadbolt has built its operations on exploiting a security flaw in network-attached storage (NAS) devices produced by the provider QNAP, rather than infecting entire computer networks, which is the go-to tactic for the "big game hunting" favored by most ransomware attackers.

Deadbolt also communicates with victims differently from other ransomware strains. While many strains have set up websites to negotiate with victims and provide decryption keys to those who pay, Deadbolt simply instructs victims to pay a set amount to a specific Bitcoin address in a message that appears when the victim attempts to access the infected device.



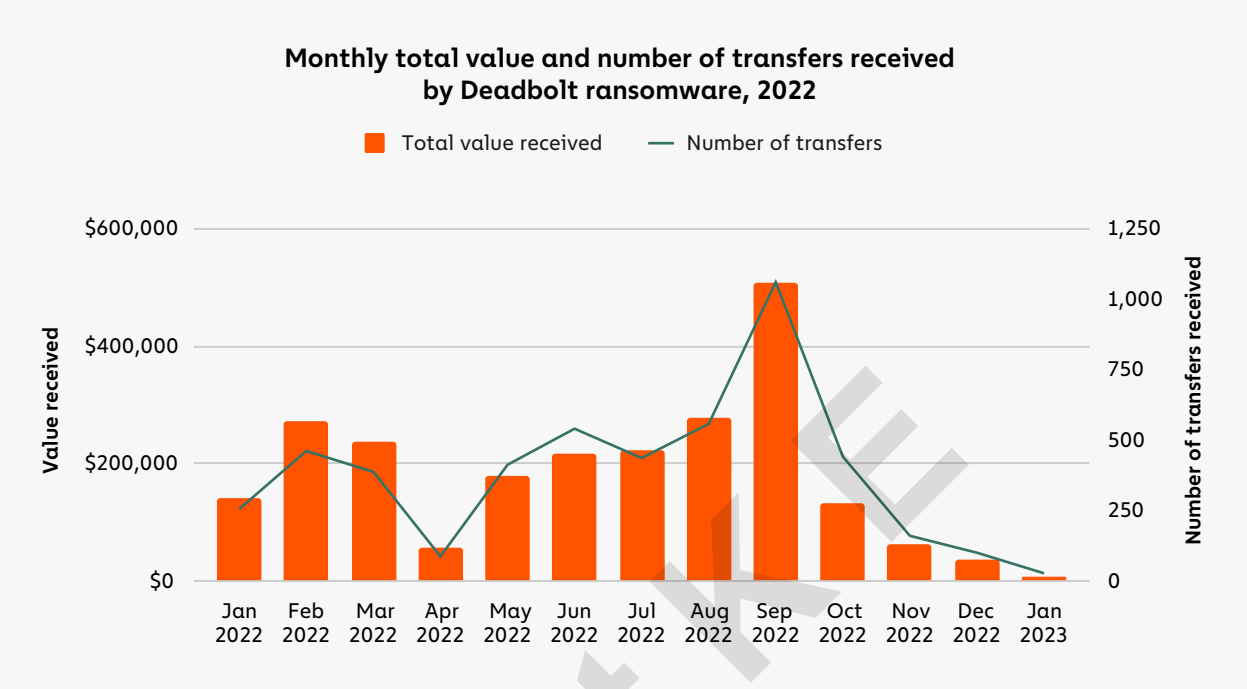
Source: Sophos blog

Once a victim pays, Deadbolt automatically sends them the decryption key via the blockchain, sending a low-value Bitcoin transaction to the ransom address with the decryption key written into the transaction's OP_RETURN field. In order to send the OP_RETURN, some amount of cryptocurrency must be transferred — blockchain analysis suggests that Deadbolt's developers pre-programmed transactions to send a negligible sum of .0000546 BTC (about $1 USD) to its own ransom payment wallet each time a victim pays, so that funds are available to then send transactions necessary to communicate the decryptor to each victim upon receipt of their ransom.

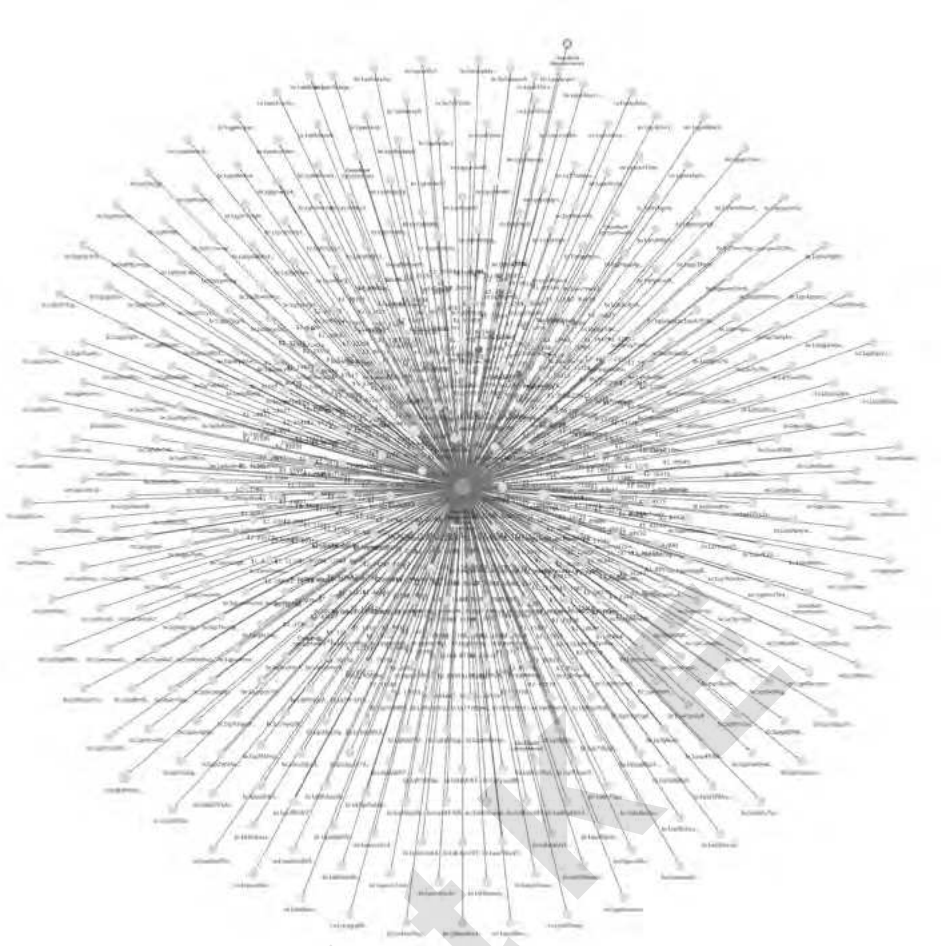
While that unique method for delivering decryption keys is slick, it's also exactly what the Dutch National Police were able to exploit to fool Deadbolt into handing decryption keys for hundreds of victims, enabling them to recover their data at no cost. We'll break down how they did that below, but first, let's look more closely at Deadbolt's activity over the last two years.

Deadbolt's ransomware activity summarized

Over the course of 2022, Deadbolt has taken in more than $2.3 million from an estimated 4,923 victims, with an average ransom payment size of $476, compared to over $70,000 for all ransomware strains.



Deadbolt's revenue last year makes it a relatively low earner amongst all ransomware strains last year, but in terms of sheer reach and number of victims, it was perhaps the most prolific of any strain in 2022. In fact, if we use all the unpaid Deadbolt addresses associated with victims who did not pay as a proxy for total number of infections, we can estimate Deadbolt's total victim count as roughly 5,500 individuals or businesses.



That reach really comes through the Chainalysis Reactor graph above, which shows thousands of victims making payments to Deadbolt.

How Dutch National Police disrupted Deadbolt and took decryption keys without paying

Cyber investigators with the Dutch National Police (Cybercrimeteam Oost-Nederland and Cybercrimeteam Oost-Brabant) had been investigating Deadbolt for months when they came to a crucial realization while analyzing transactions between Deadbolt and its victims, following a tip of the Dutch incident response company Responders.NU. "Looking through the transactions in Chainalysis, we saw that in some cases, Deadbolt was providing the decryption key before the victim's payment was actually confirmed on the blockchain," said one Dutch National Police investigator who worked on the case. Cryptocurrency transactions aren't actually finalized until a new block is confirmed to the blockchain — for Bitcoin, this process takes roughly ten minutes per block. However, during that

time, unconfirmed transactions are visible in Bitcoin's mempool. "This meant that a victim could send the payment to Deadbolt, wait for Deadbolt to send the decryption key, and then use replace-by-fee (RBF) to change the pending transaction, and have the ransomware payment go back to the victim," said the investigator.

With this information, the Dutch National Police hatched a plan to send and retract payments for as many Deadbolt victims as possible in order to get them their decryption keys. They knew they'd only have one shot, as Deadbolt would surely notice the flaw in their automated decryption key distribution system and fix it once the plan was attempted.

The first step was to find as many Deadbolt victims as possible who had yet to pay their ransom. "We searched police reports from all over the Netherlands for Deadbolt victims and extracted the Bitcoin addresses Deadbolt provided. In cases where there wasn't an address, we reached out to victims." The Dutch National Police also worked with Europol to find victims in other countries as well — 13 in total. Next, the team had to test that they could in fact send and retract a large number of payments to help as many victims as possible. "We wrote a script to automatically send a transaction to Deadbolt, wait for another transaction with the decryption key in return, and use RBF on our payment transaction. Since we couldn't test it on Deadbolt, we had to run it on testnets to make sure it worked," the investigator told us.

Once everything was ready to go, the team deployed their script and started the process of sending and retracting payments for Deadbolt victims. The Deadbolt team quickly realized what was happening and halted their automated OP_RETURN transactions. But in that time, the Dutch National Police retrieved decryption keys for nearly 90% of the victims who reported Deadbolt payment addresses via Europol, depriving Deadbolt of hundreds of thousands of dollars. While Deadbolt remains active, it's been forced to adopt a more manual process for providing decryption keys via Bitcoin transaction OP_RETURNs, which raises Deadbolt's overhead.

Overall, the Dutch National Police operation against Deadbolt is a valuable reminder that blockchain analysis has applications beyond tracing the flow of funds. In this case, police were able to discover a crucial vulnerability in Deadbolt's modus operandi by closely reviewing its transaction patterns and digging into the metadata of the transactions. The operation also underscores why it's so important for ransomware victims to report attacks to the authorities. No one who had their data hijacked by Deadbolt likely knew that an operation like this would be possible, but in cutting edge fields like cryptocurrency and cybersecurity, unique solutions can come from anywhere. The Dutch National Police could only reach out to victims who had reported to the police in their countries, and those who didn't may have missed an opportunity to recover their data at no cost.

Money Laundering

Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022

Money laundering is crucial to all financially motivated crime because it's what enables criminals to access the funds they generate from their activities. Otherwise, why commit the crimes in the first place? The same is true in cryptocurrency. The goal of money laundering in cryptocurrency is to move funds to addresses where its original criminal source can't be detected, and eventually to a service that allows cryptocurrency to be exchanged for cash — usually this means exchanges. If that weren't possible, there would be very little incentive to commit crimes involving cryptocurrency.

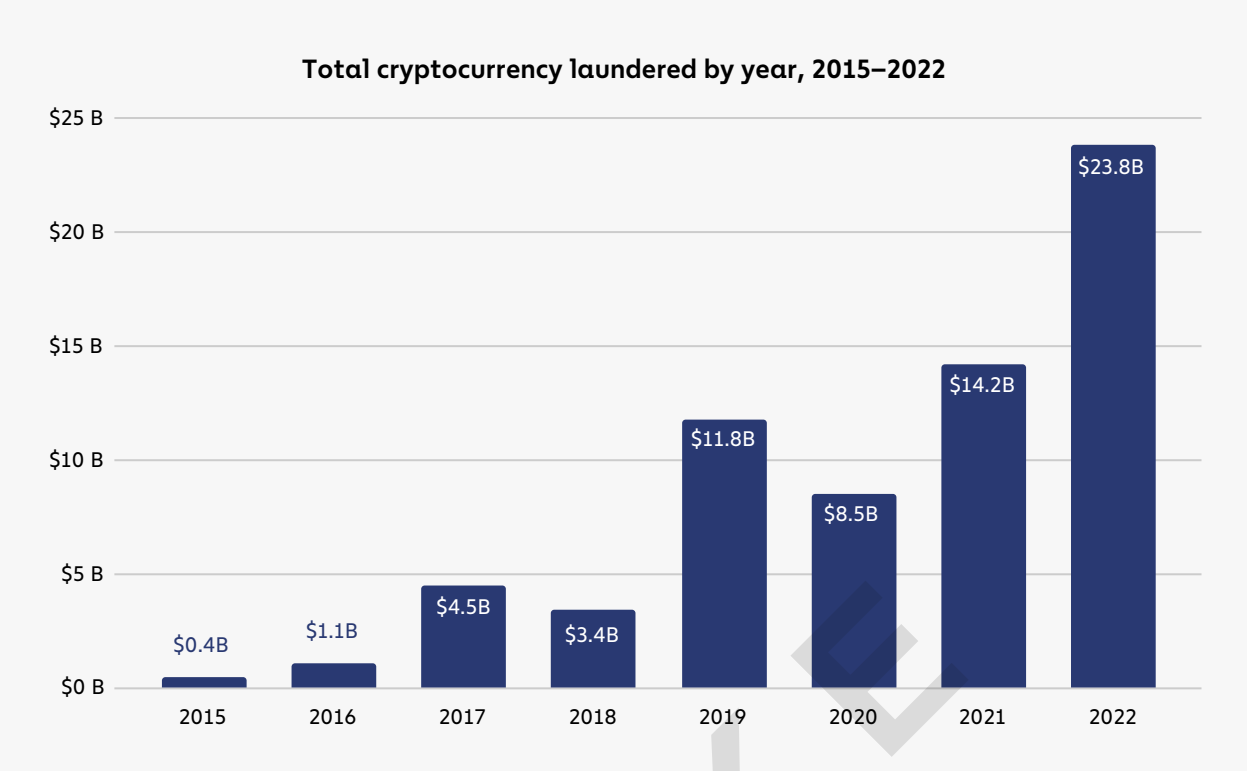
We've written in the past about how money laundering activity is highly concentrated to just a few services, and within those services, concentrated even further to a small number of deposit addresses. That remained true in 2022, though as we'll explore, with a few new wrinkles. In addition, we'll examine the rise of underground money laundering services that exist separately from the crypto businesses most are familiar with, and also analyze funds still held by crypto criminals on the blockchain.

2022 crypto money laundering activity summarized

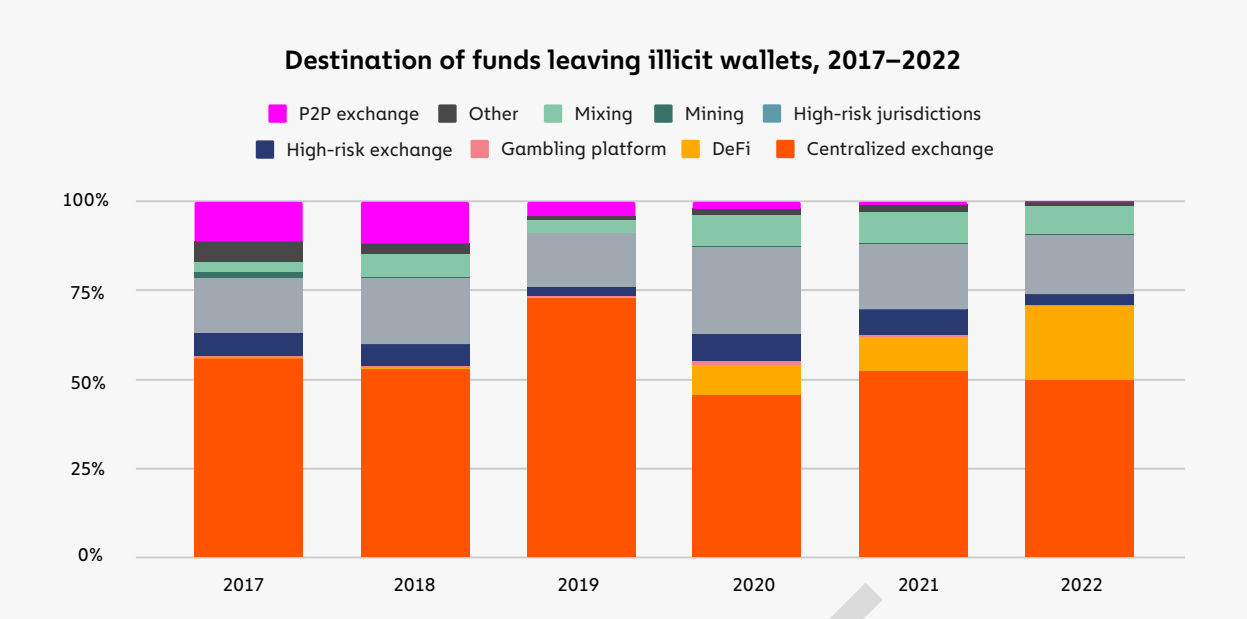
Money laundering in cryptocurrency typically involves two types of on-chain entities and services:

- **Intermediary services and wallets:** These can include personal wallets (also known as unhosted wallets), mixers, darknet markets, and other services both legitimate and illicit. Crypto criminals typically use these services to hold funds temporarily, obfuscate their movements of funds, or swap between assets. DeFi protocols are also used by illicit actors in order to convert funds but, as we will discuss, are not an efficient means of obfuscating the flow of funds.
- **Fiat off-ramps:** This refers to services that allow for cryptocurrency to be exchanged for fiat. This is the most important part of the money laundering process, as the funds can no longer be traced via blockchain analysis once they hit a service — only the service itself would have visibility into where they go next. Additionally, if the funds are converted into cash, they can only be followed further through traditional financial investigation methods. Most fiat off-ramps are centralized exchanges, but P2P exchanges and other services can also serve this function.

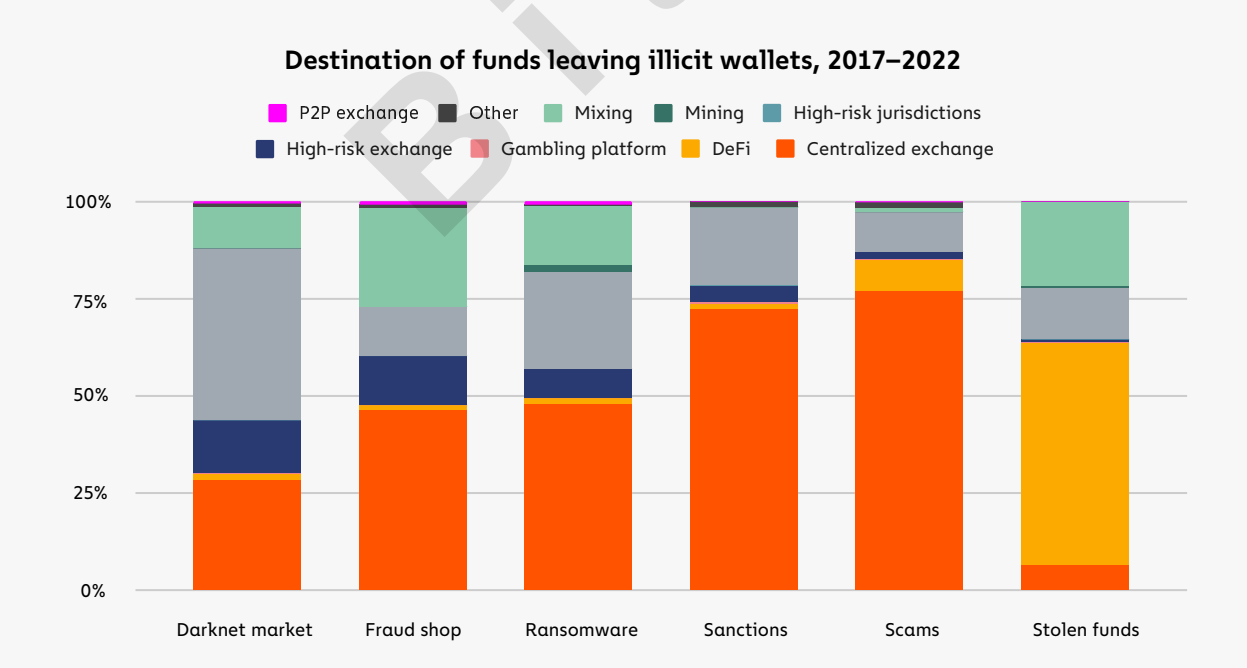
With that in mind, let's look at some of the money laundering trends we saw in 2022.



Overall, illicit addresses sent nearly $23.8 billion worth of cryptocurrency in 2022, a 68.0% increase over 2021. As is usually the case, mainstream centralized exchanges were the biggest recipient of illicit cryptocurrency, taking in just under half of all funds sent from illicit addresses. That's notable not just because those exchanges generally have compliance measures in place to report this activity and take action against the users in question, but also because those exchanges are fiat off-ramps, where the illicit cryptocurrency can be converted into cash.



More illicit funds were sent to DeFi protocols than ever before, a continuation of a trend that began in 2020. Cybercriminals send funds to DeFi protocols not because DeFi is useful for obscuring the flow of funds. In fact, quite the opposite is true, as unlike with centralized services, all activity is recorded on-chain. Keep in mind too that DeFi protocols don't allow for the conversion of cryptocurrency into fiat, so most of those funds likely moved next to other services, including fiat off-ramps. And as we see below, almost all usage of DeFi protocols for money laundering is carried out by one criminal group: hackers stealing cryptocurrency.



Hackers holding stolen cryptocurrency are the only criminal category sending the majority of funds to DeFi protocols, at a whopping 57.0%. 2022 was an enormous year for hacking, hence why these cybercriminals were almost single-handedly able to drive the overall increase in the usage of DeFi protocols for money laundering. The fact that DeFi protocols themselves were the biggest target of hacks in 2022 also influences these numbers. In DeFi hacks, attackers often end up with tokens that aren't listed on other exchanges, so they need to use decentralized exchanges (DEXes) to swap them for more liquid crypto assets. DEXes have historically been used to convert funds to Ether, which can then be sent to Ethereum-based mixers. DEXes have also been used to convert to assets that will be more likely to hold their value, or in the case of stablecoins, to swap to an asset that cannot be frozen by the stablecoin issuer. However, as noted previously, DEXes don't enable the conversion of funds from cryptocurrency to fiat currency — this must still be done through a centralized exchange or other fiat off-ramp.

Aside from hackers, crypto criminals send the majority of their funds directly to centralized exchanges, but there are some notable exceptions. For instance, darknet market vendors and administrators send most of their funds to other illicit services — primarily other darknet markets, some of whom may offer money laundering services similar to those of the now-shuttered Hydra Market. Darknet market addresses also sent a large share of funds to high-risk exchanges, such as Bitzlato, a Russia-based exchange shut down in an international law enforcement action recently for its money laundering activity. Ransomware attackers are another interesting case. Addresses associated with them send a disproportionately large share of funds to mixers, and also make heavy use of illicit services. Fraud shop vendors and administrators are also notable for their outsized mixer usage.

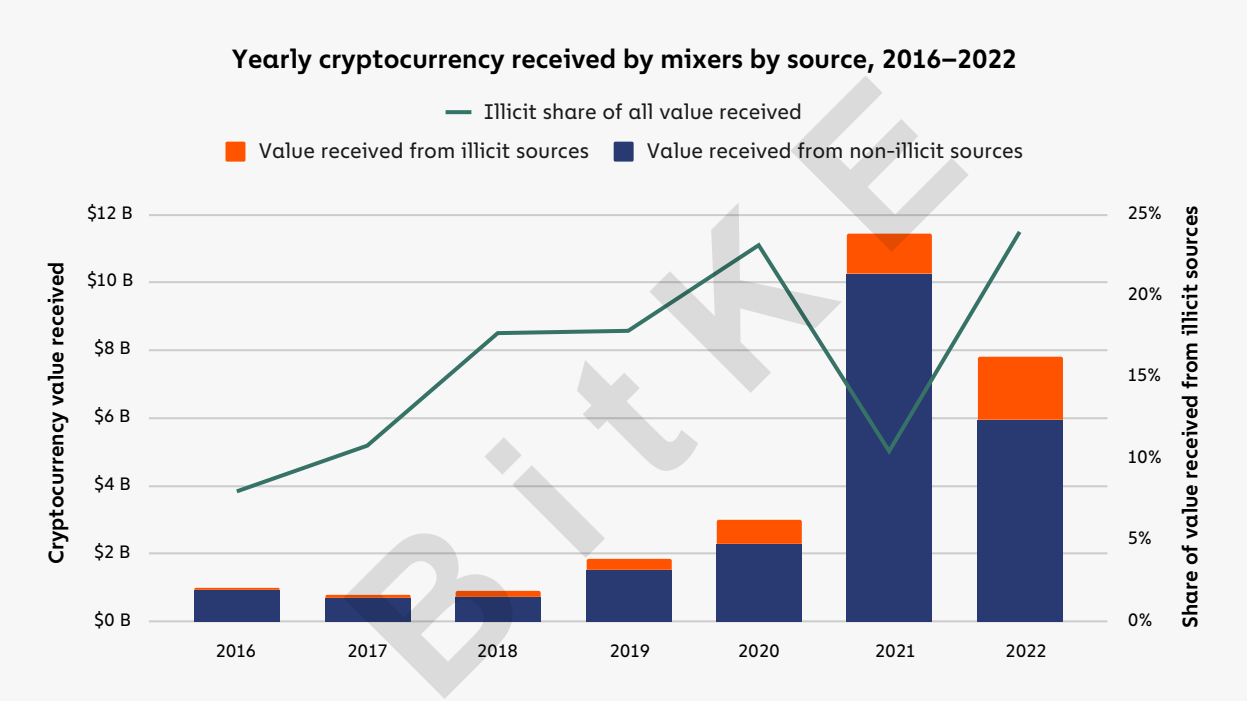
In total, we see that over half of all funds sent from illicit addresses travel directly to centralized exchanges, both mainstream and high-risk, where they can be exchanged for fiat unless compliance teams take action. However, over 40% of illicit funds move first to intermediary services — primarily mixers and illicit services or DeFi protocols — with most of those funds coming from ransomware, darknet market, and hacker addresses.

Overall mixer usage falls in 2022, but illicit usage hits all-time high

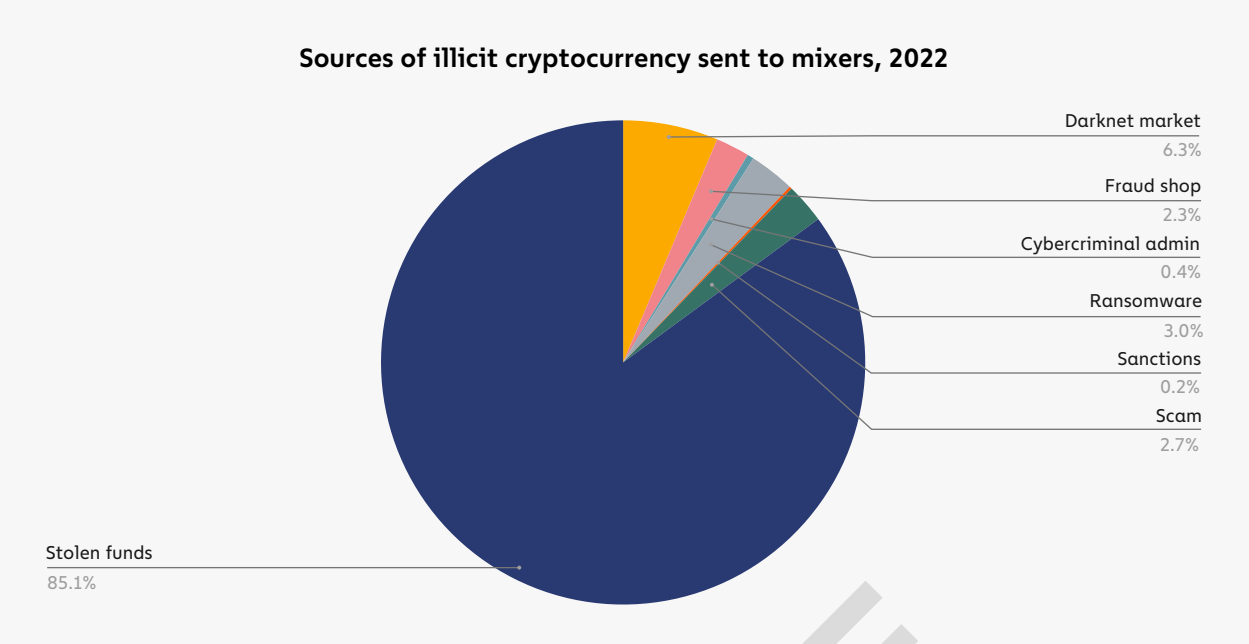
Mixers are a popular obfuscation service used by crypto criminals, taking in 8.0% of all funds sent from illicit addresses in 2022. Mixers function by taking in cryptocurrency from multiple users, mixing it all together, and sending each user an amount equivalent to what they put in. The result is that each user's cryptocurrency can now only be traced back to the mixer, rather than to its original source, unless special blockchain analysis techniques are employed. You can learn more about how different types of mixers work here.

There are many legitimate use cases for mixers, most of which are related to financial privacy. For example, if someone knows your cryptocurrency address, they can see virtually your entire transaction history on the blockchain, so it's reasonable for users to try and prevent this with mixers. Of course, the financial privacy provided by mixers is also valuable to criminals, hence their popularity as a destination for illicit funds. In May 2022, OFAC sanctioned a mixer for the first time ever when it designated Blender.io for its role in laundering cryptocurrency stolen by North Korean hacking syndicate Lazarus Group. OFAC didn't waste any time designating its second mixer, Tornado Cash, in August for the same reasons.

The sanctioning of prominent mixers may have contributed to two trends we observed in 2022: The total amount of cryptocurrency sent to mixers fell significantly, and the funds that did travel to mixers were more likely to come from illicit sources.



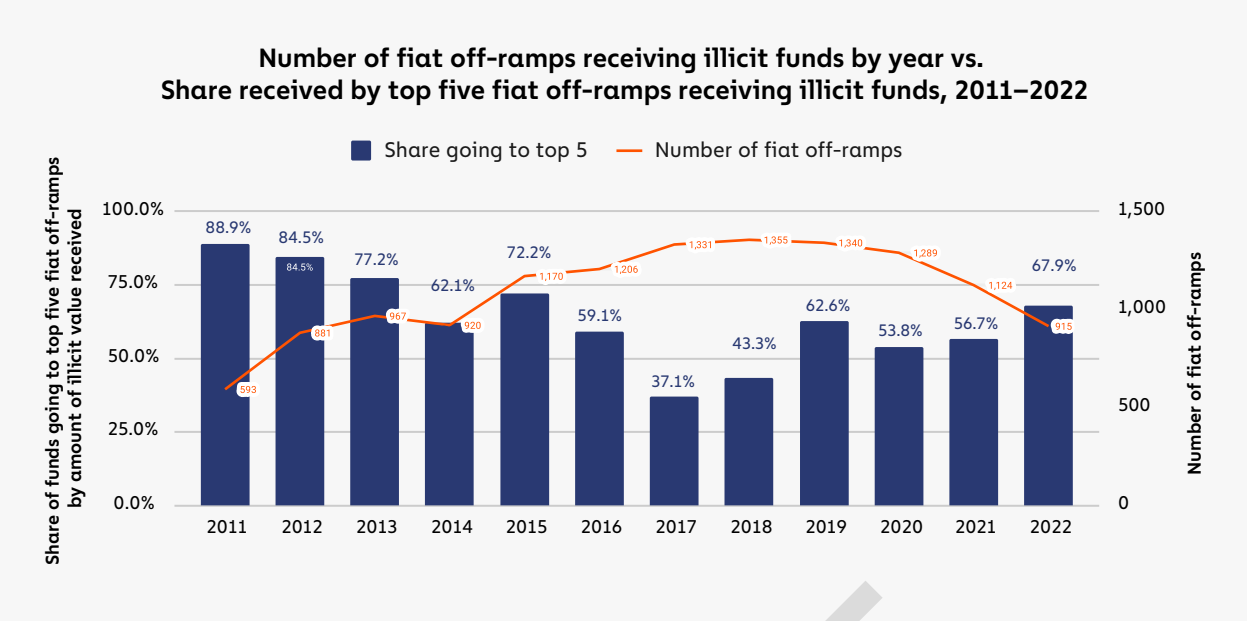
Mixers processed a total of $7.8 billion in 2022, 24% of which came from illicit addresses, whereas in 2021, they processed $11.5 billion, only 10% of which came from illicit addresses. The data suggests that legitimate users have decreased their use of mixers, possibly due to law enforcement actions against prominent ones, while criminals have continued to use them. It's also worth noting that the vast majority of illicit value processed by mixers is made up of stolen funds, a large share of which were stolen by North Korea-linked hackers, who are unlikely to be dissuaded by the threat of U.S. sanctions given they reside in a non-cooperative jurisdiction.



Other sanctioned entities and darknet markets also accounted for significant shares of value received by mixers in 2022.

Money laundering concentration at fiat off-ramps

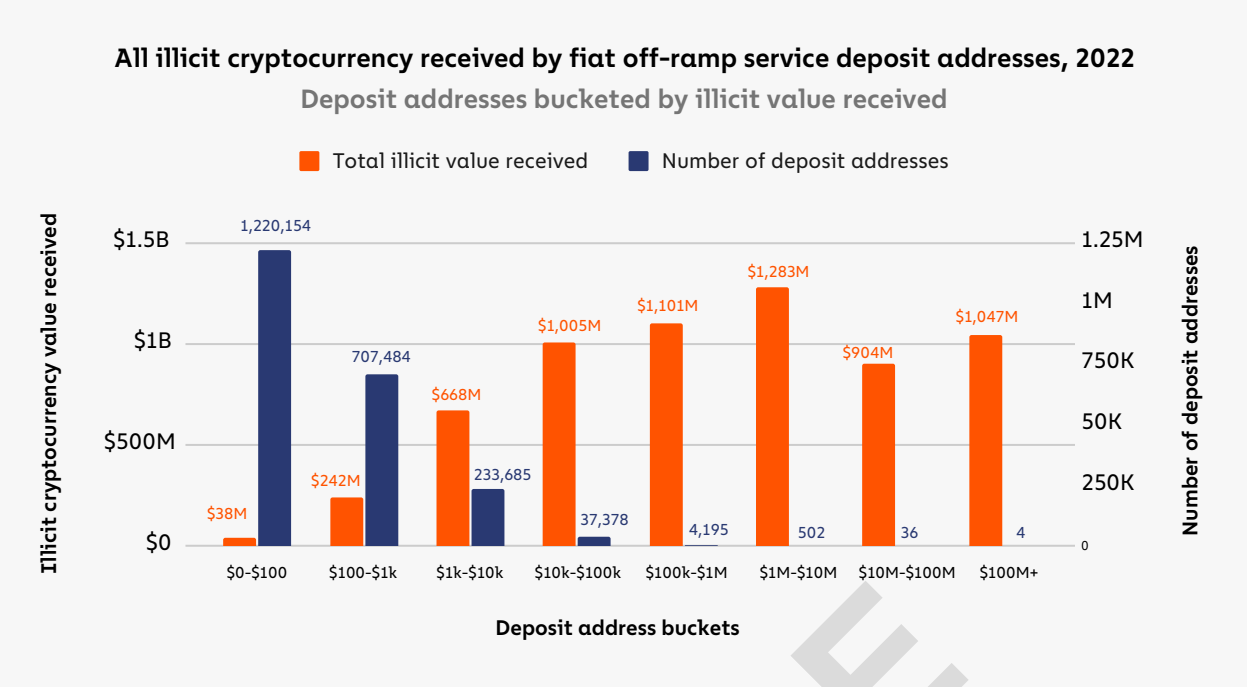
As we discussed above, fiat off-ramp services like exchanges are crucial for money laundering, as those are the services where criminals can turn crypto into cash, which is likely their ultimate goal. Fiat off-ramps are also among the most heavily regulated cryptocurrency services, and their compliance teams have an important role to play in flagging incoming illicit funds and preventing them from being exchanged for cash. But while there are thousands of cryptocurrency services offering fiat off-ramping, a select few receive most of the illicit funds we observe on-chain.



915 unique fiat off-ramping services received illicit cryptocurrency in 2022, down from 1,124 in 2021. Some of that dropoff is likely due to exchanges going out of business during the bear market. Of the illicit funds received by exchanges, 67.9% went to just five services, all of which are centralized exchanges. This represents an increased concentration compared to 2021, when the top five services received only 56.7% of illicit funds.

But what about the individual exchange users facilitating this activity? We can assume that many of the criminals sending funds to fiat off-ramps are using an account at the service that they themselves control. But in some cases, criminals work with specialized money laundering service providers, who control the accounts and help criminals convert their cryptocurrency into cash once it arrives at the exchange. Those businesses fall into the category of nested services, meaning services that are built on top of larger exchanges, using those exchanges' deposit addresses to access their liquidity and trading pairs. Most nested services are legitimate businesses — many prominent over-the-counter (OTC) brokers, for instance, operate as nested services. However, on-chain data suggests that a small group of nested services facilitate the majority of money laundering, either due to negligence or purposeful catering to crypto criminals.

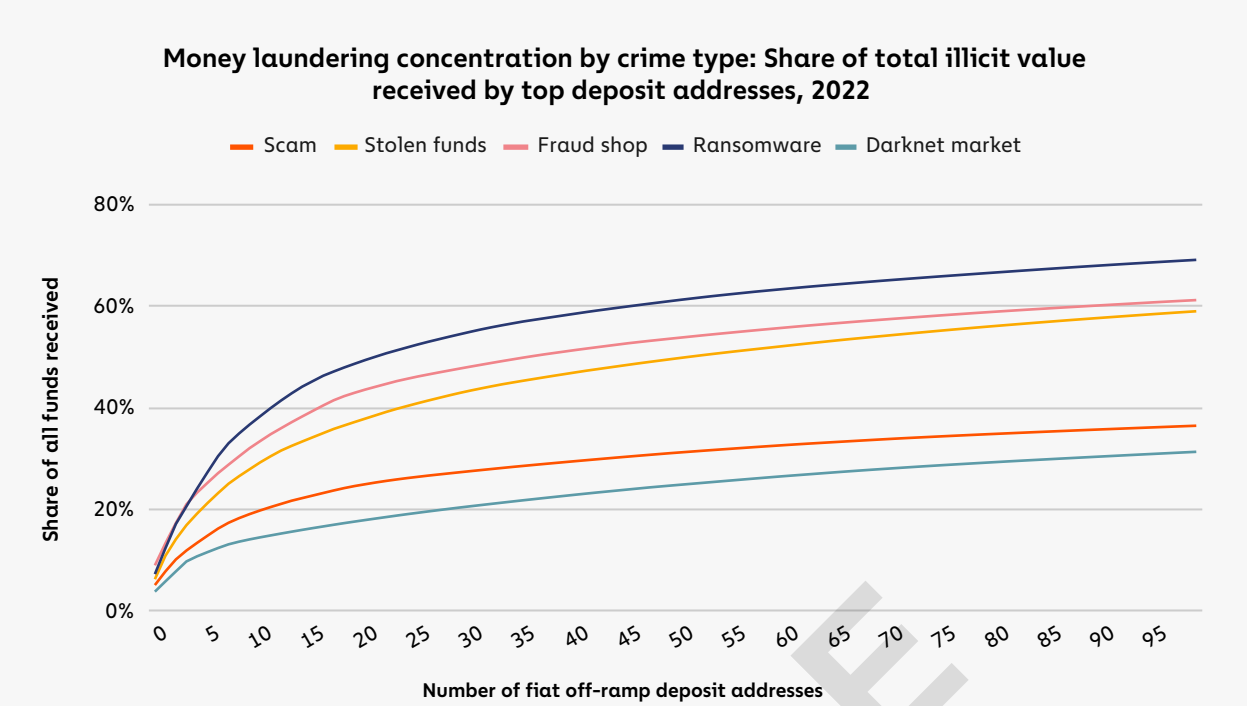
For that reason, it's useful to analyze the specific service deposit addresses that account for the majority of money laundering activity, as we can generally attribute the activity of a given deposit address to a user at the service whose account is linked to that deposit address. In the graph below, we look at all off-ramp service deposit addresses that received any illicit funds in 2022, bucketed by the range in value of illicit funds received.



How to read this graph: This graph shows service deposit addresses bucketed by how much total illicit cryptocurrency each address received individually in 2022. Each blue bar represents the number of deposit addresses in the bucket, while each grey bar represents the total illicit cryptocurrency value received by all deposit addresses in the bucket. Using the first bucket as an example, we see that 1,220,154 deposit addresses received between $0 and $100 worth of illicit cryptocurrency, and together all of those deposit addresses received a total of $38 million worth of illicit cryptocurrency.

The graph shows that most cryptocurrency money laundering is facilitated by a very small group of people. Four deposit addresses cracked $100 million in illicit cryptocurrency received in 2022, and combined received just over $1.0 billion, while the 1.2 million deposit addresses receiving under $100 in illicit funds account for $38 million in total. Further, 51% of the $6.3 billion in illicit funds received by fiat off-ramp services in 2022 went to a group of just 542 deposit addresses. Those numbers represent a lower level of money laundering concentration at the deposit address level than we saw in 2021, even though 2022 saw a slight uptick in concentration at the service level. One possible reason for this is that continued law enforcement crackdowns against crypto money launderers, such as the shutdown of the exchange Bitzlato, have spooked the biggest money laundering service providers, or encouraged them to spread their operations across more deposit addresses.

We also see high variance in the degree of money laundering concentration by crime type.



Just 21 deposit addresses account for 50% of all funds sent from ransomware to fiat off-ramps, while the top 21 deposit addresses for funds received from darknet markets account for just 18%.

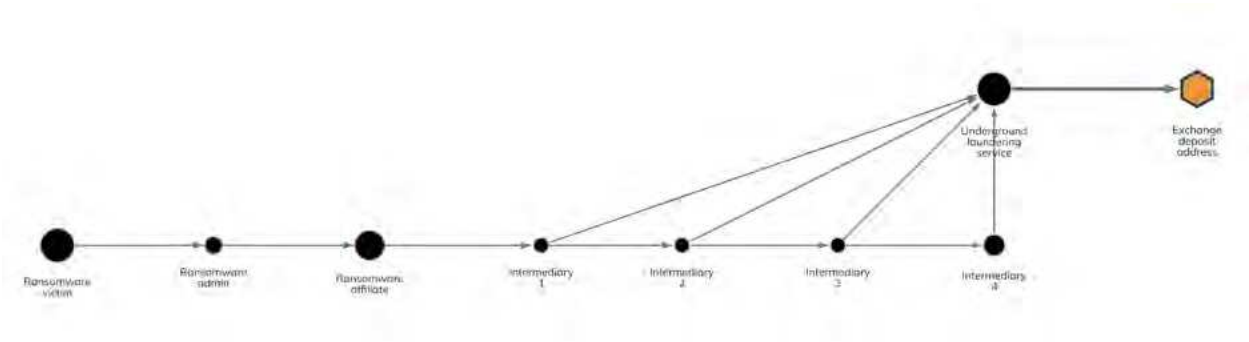
Despite the drop in overall concentration, 51% of illicit funds moving to just 542 deposit addresses at 83 exchanges still represents a high level of money laundering concentration. If law enforcement and compliance teams were able to disrupt the individuals and groups behind those addresses, it would be much more difficult for criminals to launder cryptocurrency at scale, and go a long way toward making the ecosystem safer.

Underground money laundering services are a growing concern

Another money laundering trend we've observed is the growth of underground services that aren't as publicly accessible or well-known as standard mixers, as they are typically accessible only through private messaging apps or the Tor browser, and usually only advertised on darknet forums.

We've written above and in past Crypto Crime Reports about OTC brokers nested on exchanges that launder large quantities of illicit funds, many of which seem to explicitly cater to cybercriminals. While this activity still exists, we're also seeing the rise of underground money laundering services with brand names and custom infrastructure, which vary in terms of complexity. Some function simply as networks of private wallets, while others are more akin to an instant exchanger or mixer. But generally, what links them is that they typically move cryptocurrency to exchanges on behalf of

cybercriminals, exchange them for either fiat currency or clean crypto, then send that back to the cybercriminals. Like the nested OTC services, many of these underground services also use those exchanges for liquidity. We can see one example on the Chainalysis Reactor graph below, though names of relevant illicit organizations have been redacted due to ongoing investigations.

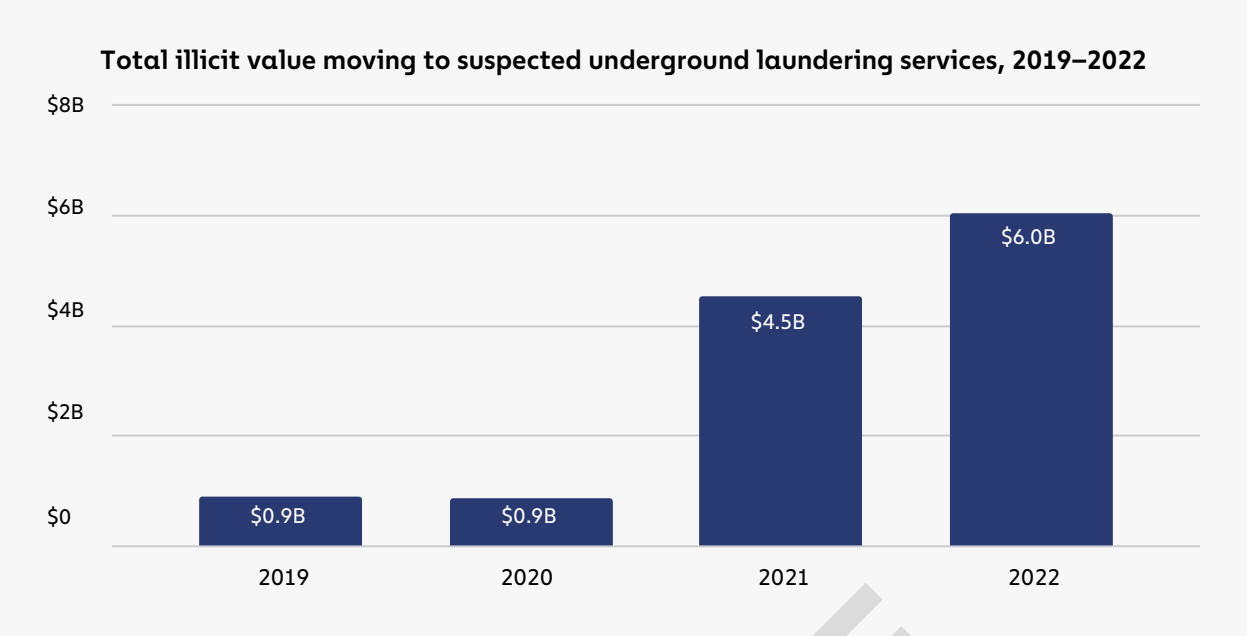


In this case, the underground laundering service, which functions similarly to a mixer, helped an affiliate for a prominent ransomware strain move funds to a deposit address at a large, centralized exchange. The deposit address is believed to be controlled by the laundering service itself.

Underground money laundering service activity like that shown above isn't as easy to spot as most activity on public blockchains — identifying these services' addresses requires extensive investigative work, and untangling their transactions requires advanced blockchain analysis techniques such as demixing. That means it's difficult to analyze these services' activity at scale. However, we can estimate their activity by analyzing the activity of all wallets and networks of wallets that meet the following criteria:

- Receive large amounts of cryptocurrency from illicit services
- Send large amounts of cryptocurrency to exchanges and other fiat off-ramps

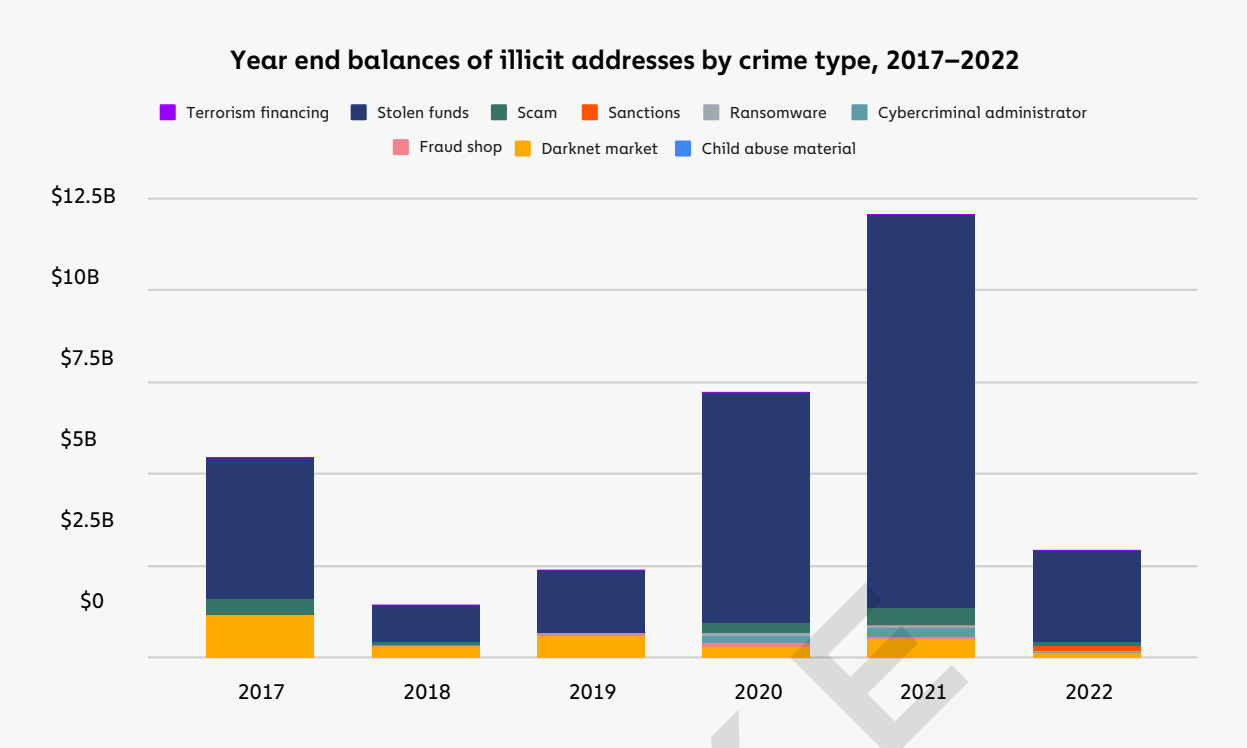
The graph below shows the yearly cryptocurrency value received by wallets that fit those criteria.



Total cryptocurrency moving to wallets fitting those criteria has grown over the last few years, and hit $6 billion in 2022. Again, these are estimates — we can't guarantee that all of the wallets included in this analysis are necessarily underground laundering services, but their on-chain activity suggests that they could be. It's also possible that usage of underground money laundering services will pick up as high-risk exchanges, which have facilitated this activity in the past, face increased pressure from law enforcement, as we saw with Garantex and Bitzlato.

Criminal balances dropped in 2022

As we mentioned previously, criminals will often leave funds in a personal wallet, or in a wallet associated with a criminal service for extended periods of time. In some cases, this may be because their crimes have generated enough attention that they don't feel it's possible to move the funds without investigators or industry observers calling it out — we see this often with funds stolen in hacks. In other cases, this may reflect an intention to hold cryptocurrency in the expectation its price will rise, or to continue using it for other criminal endeavors. Thanks to the transparency of the blockchain, we can track these criminal balances granularly to know how much confirmed illicit entities are holding at any given time. Below, we'll take a look at how criminal balances changed in 2022.



Two things stand out: The first is that criminal balances have plummeted in value in 2022, from $12.0 billion at the end of 2021 to just $2.9 billion. Price declines in the ongoing bear market and large, successful seizures by law enforcement in 2022 are the most likely causes of this.

Second, we can see that stolen funds dominate on-chain criminal balances. This is likely due to the fact that the amount of cryptocurrency stolen in hacks has skyrocketed over the last two years, and that these hacks often become huge points of discussion on crypto Twitter and in other industry forums, with many tracking the funds publicly and sharing the addresses holding stolen funds. This can make it difficult for hackers to move stolen funds to a fiat off-ramp, which could be one reason they choose to leave the funds sitting in personal wallets.

Criminal balances are valuable to track as they represent a lower-bound estimate of cryptocurrency that could potentially be seized by law enforcement — the true number for criminal balances is likely much higher, as it includes funds associated with addresses we've yet to attribute to criminal entities and funds derived from offline criminal activity and converted to cryptocurrency after the fact.

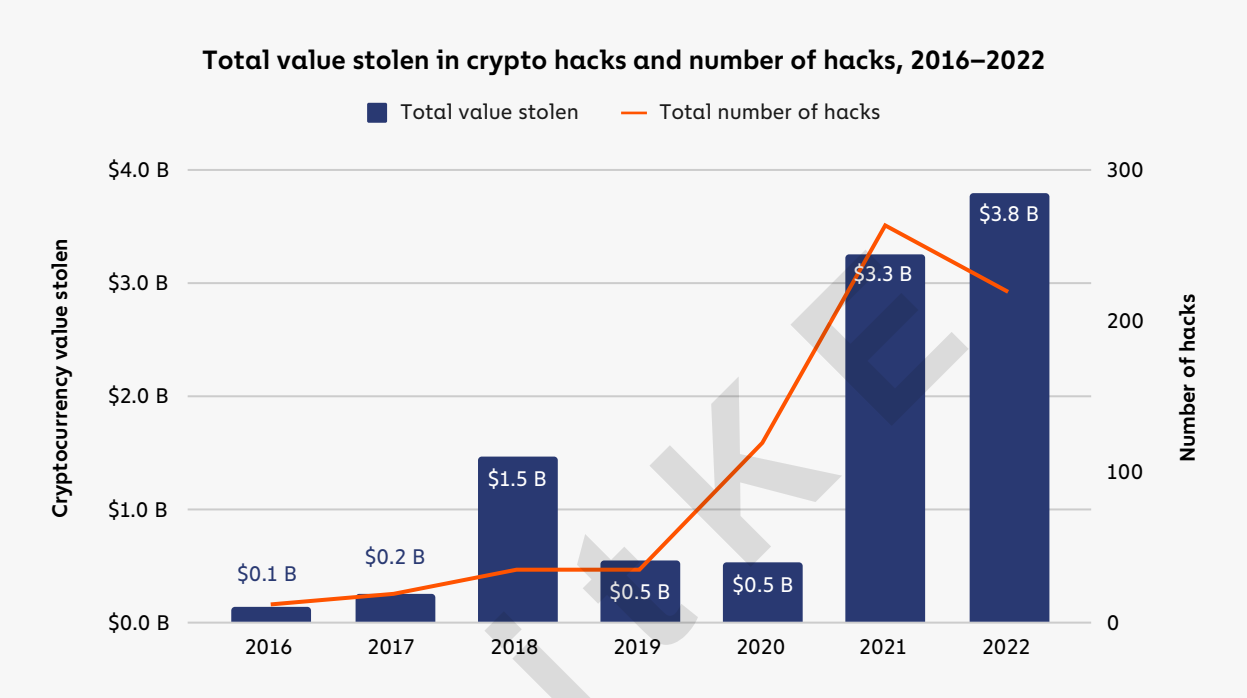
Investigative agencies have continued to ramp up their ability to seize cryptocurrency in 2022, with the IRS Criminal Investigation Unit announcing they seized $7 billion worth of digital assets last year, more than double the amount seized in 2021. 2022 saw several other notable stories of crypto-currency seized from criminals, including:

- A record $3.6 billion seized from two individuals accused of laundering funds stolen in the 2016 hack of Bitfinex
- The November 2021 seizure of $3.36 billion in Bitcoin stolen from darknet market Silk Road, which was later announced publicly in November 2022
- The seizure of $30 million worth of cryptocurrency stolen from Axie Infinity's Ronin Bridge, marking the first successful seizure of cryptocurrency stolen by North Korean hacking syndicate Lazarus Group

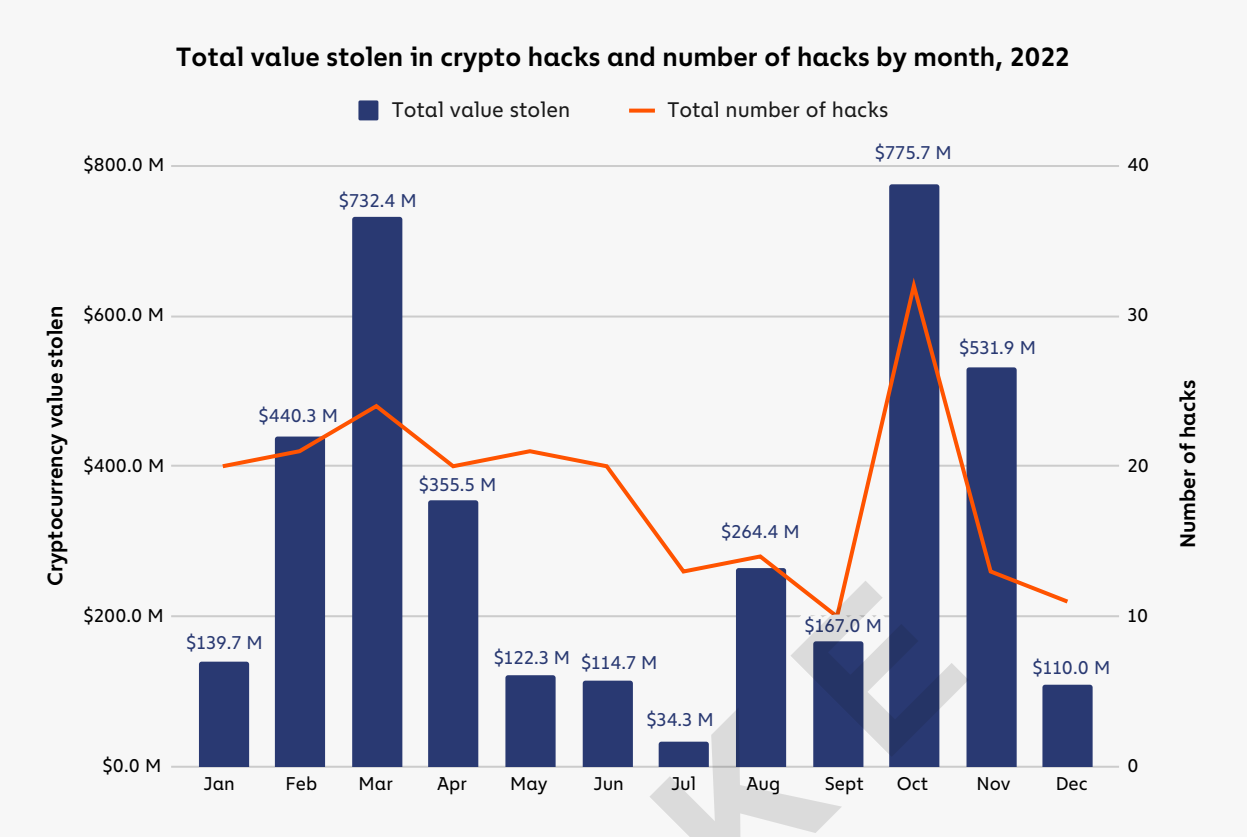
Our data on criminal balances suggests there are still more opportunities for successful seizures, and more generally, illustrates a crucial difference between financial investigations in cryptocurrency versus fiat: In cryptocurrency, criminal holdings can't be stashed away in opaque networks of banks and shell corporations — almost everything is out in the open.

Stolen Funds

2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers



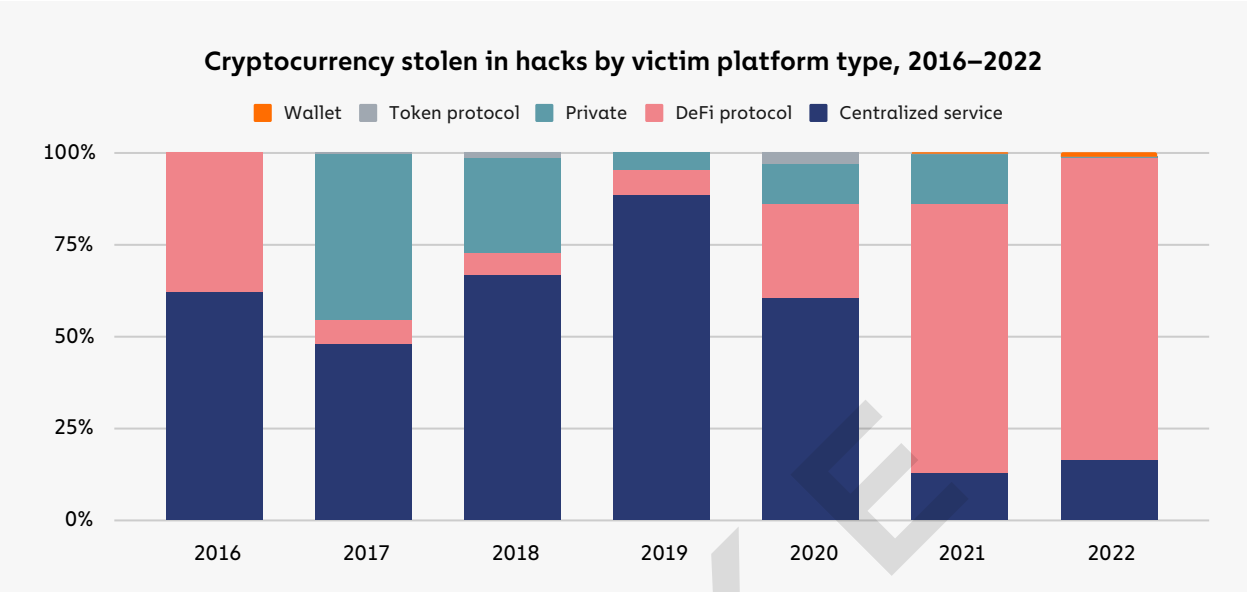
2022 was the biggest year ever for crypto hacking, with $3.8 billion stolen from cryptocurrency businesses. Hacking activity ebbed and flowed throughout the year, with huge spikes in March and October, the latter of which became the biggest single month ever for cryptocurrency hacking, as $775.7 million was stolen in 32 separate attacks.



Below, we'll dive into what kinds of platforms were most affected by hacks, and take a look at the role of North Korea-linked hackers, who drove much of 2022's hacking activity and shattered their own yearly record for most cryptocurrency stolen.

DeFi protocols by far the biggest victims of hacks

In last year's Crypto Crime Report, we wrote about how DeFi protocols in 2021 became the primary target of crypto hackers. That trend intensified in 2022.



DeFi protocols as victims accounted for 82.1% of all cryptocurrency stolen by hackers — a total of $3.1 billion — up from 73.3% in 2021. And of that $3.1 billion, 64% came from cross-chain bridge protocols specifically. Cross-chain bridges are protocols that let users port their cryptocurrency from one blockchain to another, usually by locking the user's assets into a smart contract on the original chain, and then minting equivalent assets on the second chain. Bridges are an attractive target for hackers because the smart contracts in effect become huge, centralized repositories of funds backing the assets that have been bridged to the new chain — a more desirable honeypot could scarcely be imagined. If a bridge gets big enough, any error in its underlying smart contract code or other potential weak spot is almost sure to eventually be found and exploited by bad actors.

How do we make DeFi safer?

DeFi is one of the fastest-growing, most compelling areas of the cryptocurrency ecosystem, largely due to its transparency. All transactions happen on-chain, and the smart contract code governing DeFi protocols is publicly viewable by default, so users can know exactly what will happen to their funds when they use them. That's especially attractive now in 2023, as many of the market blowups of the past year were due to a lack of transparency into the actions and risk profiles of centralized cryptocurrency businesses. But that same transparency is also what makes DeFi so vulnerable — hackers can scan DeFi code for vulnerabilities and strike at the perfect time to maximize their theft

DeFi code auditing conducted by third-party providers is one possible remedy to this. Blockchain security firm Halborn is one such provider, and is notable for its clean track record — no DeFi protocol to pass a Halborn audit has subsequently been hacked. We spoke with Halborn COO David Schwed, whose background includes stints in risk and security at large banks like BNY Mellon, about how DeFi protocols can better protect themselves. He emphasized that many of the issues in DeFi come down to a lack of investment in security. "A big protocol should have 10 to 15 people on the security team, each with a specific area of expertise," he told us. He indicated that the core issue is that DeFi developers prioritize growth over all else, and direct funds that could fund security measures to rewards in order to attract users. "The DeFi community generally isn't demanding better security — they want to go to protocols with high yields. But those incentives lead to trouble down the road."

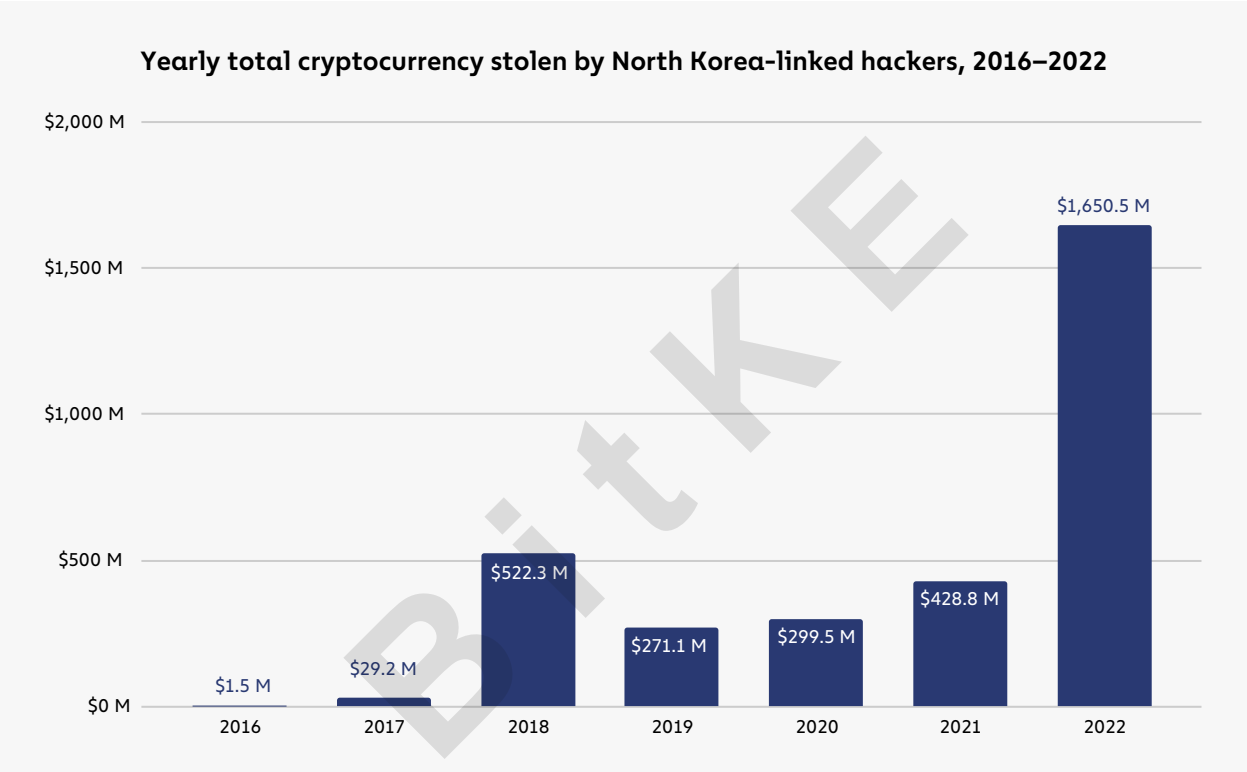
Schwed told us that DeFi developers should look to traditional financial institutions for examples of how to make their platforms more secure. "You don't need to move as slow as a bank, but you can borrow from what banks do." Some measures he recommends include:

- **Test protocols with simulated attacks.** DeFi developers can simulate different hacking scenarios on testnets in order to test how their protocol stands up to the most common attack vectors.
- **Take advantage of crypto's transparency.** One huge advantage of a blockchain like Ethereum is that transactions are visible in the mempool before they're confirmed on the blockchain. Schwed recommended that DeFi developers monitor the mempool closely for suspicious activity on their smart contracts to detect possible attacks as early as possible.
- **Circuit breakers.** DeFi protocols should build out automated processes to pause their protocols and halt transactions if suspicious activity is detected. "It's better to briefly inconvenience users than to have the entire protocol get drained," said Schwed.

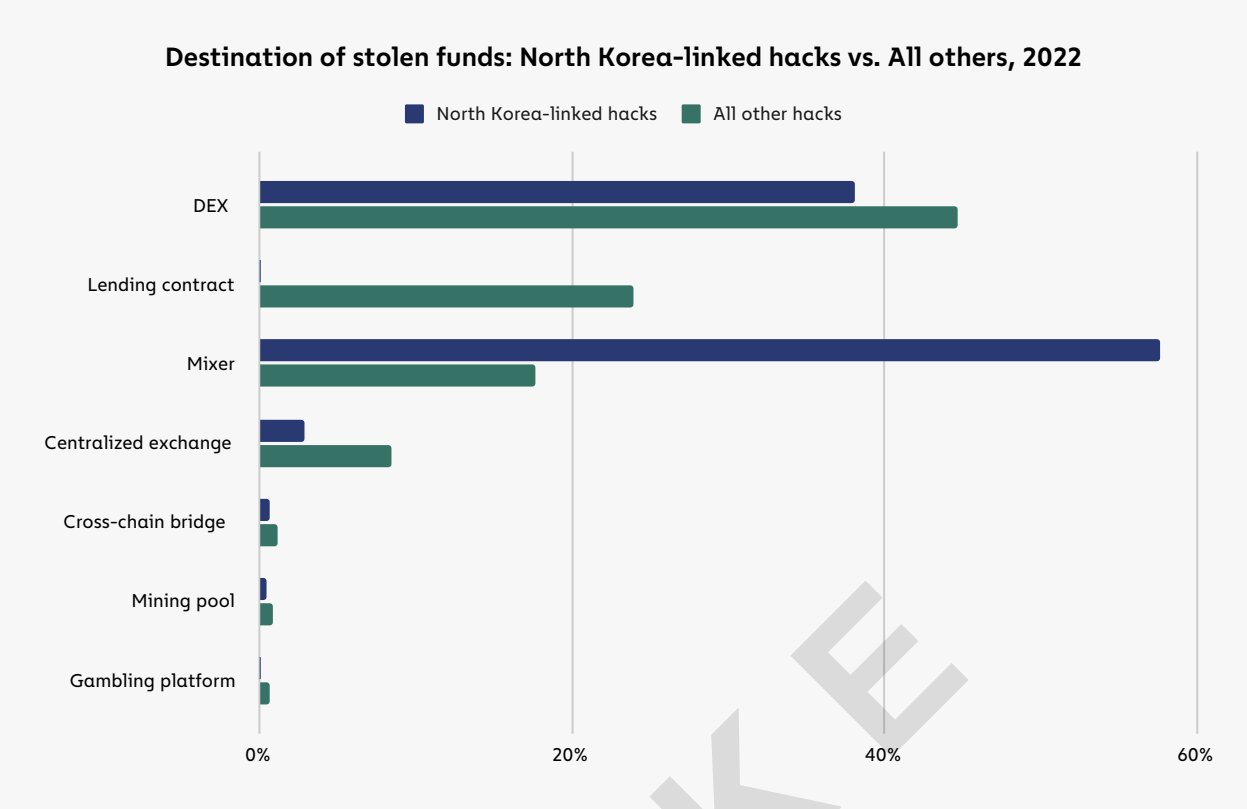
Schwed also told us that regulators have a role to play here, and can help make DeFi safer by setting minimum security standards that protocol developers must follow. The data on DeFi hacks makes one thing clear: Whether achieved through regulation or voluntary adoption, DeFi protocols will greatly benefit from adopting better security in order for the ecosystem to grow, thrive, and eventually penetrate the mainstream.

North Korea-linked hackers break theft records yet again: $1.7 billion stolen

North Korea-linked hackers such as those in cybercriminal syndicate Lazarus Group have been by far the most prolific cryptocurrency hackers over the last few years. In 2022, they shattered their own records for theft, stealing an estimated $1.7 billion worth of cryptocurrency across several hacks we've attributed to them. For context, North Korea's total exports in 2020 totalled $142 million worth of goods, so it isn't a stretch to say that cryptocurrency hacking is a sizable chunk of the nation's economy. Most experts agree the North Korean government is using these stolen to fund its nuclear weapons programs.



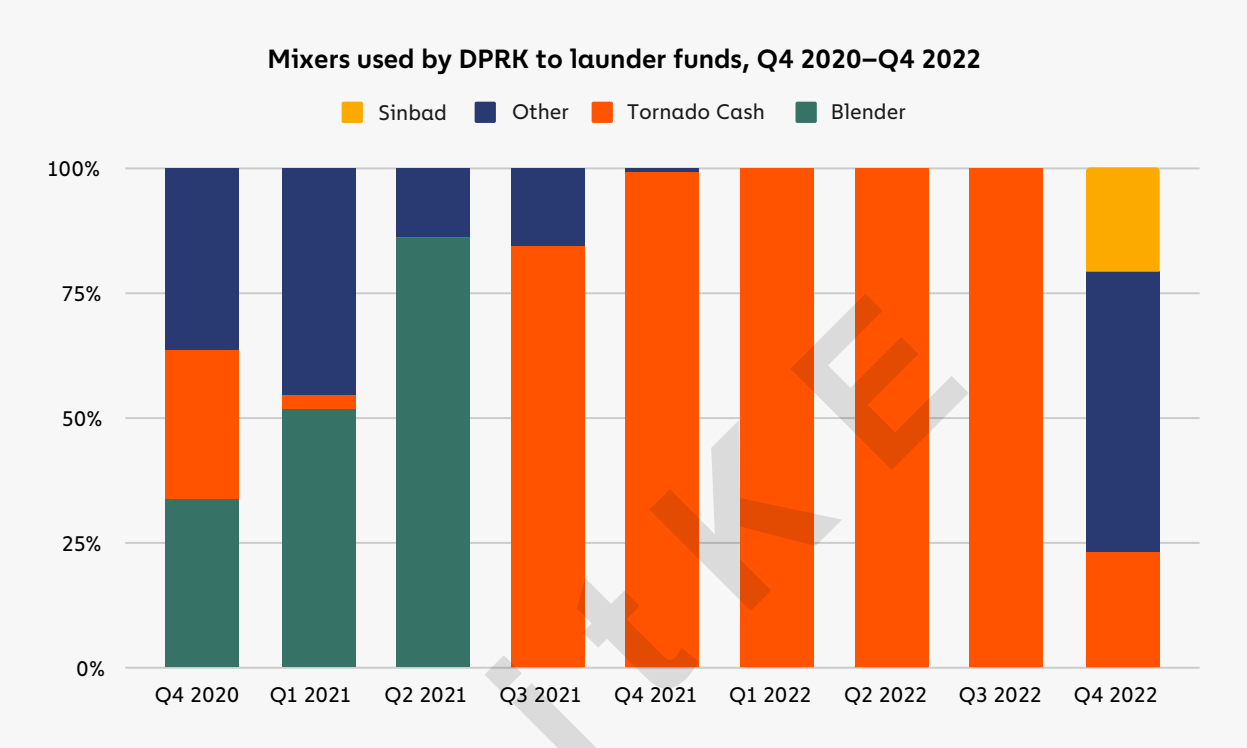
$1.1 billion of that total was stolen in hacks of DeFi protocols, making North Korea one of the driving forces behind the DeFi hacking trend that intensified in 2022. North Korea-linked hackers tend to send much of what they steal to other DeFi protocols, not because these protocols are effective for money laundering — they're actually quite bad for money laundering given their increased transparency compared to centralized services — but rather because DeFi hacks often result in cyber-criminals acquiring large quantities of illiquid tokens that aren't listed at centralized exchanges. The hackers therefore must turn to other DeFi protocols, usually DEXes, to swap for more liquid assets.



Besides DeFi protocols, North Korea-linked hackers also tend to send large sums to mixers, which have typically been the cornerstone of their money laundering process. In fact, funds from hacks carried out by North Korea-linked hackers move to mixers at a much higher rate than funds stolen by other individuals or groups. But which mixers do they use? We'll dig in below.

Meet the new mixer North Korean hackers have turned to following Tornado Cash's OFAC designation

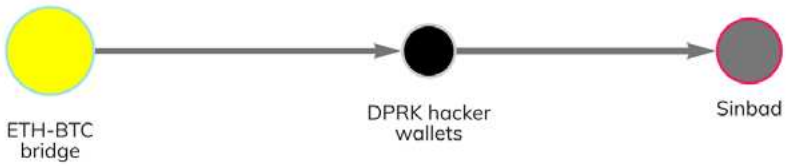
For much of 2021 and 2022, North Korea-linked hackers almost exclusively used Tornado Cash to launder cryptocurrency stolen in hacks. It's not hard to see why — Tornado Cash was for a time the biggest mixer operating, and its unique technical attributes made the funds it mixes relatively difficult to trace.



However, the hackers adapted when Tornado Cash was sanctioned in August 2022. While North Korea-linked hackers have still sent some funds to Tornado Cash since then, we can see above that they diversified their mixer usage in Q4 2022, soon after the mixer's designation. This may be due to the fact that, while still operational, Tornado Cash's overall transaction volume has fallen since its designations, and mixers generally become less effective when fewer people are using them. Since then, the hackers have turned to another mixer, Sinbad, which we'll look at in more detail below.

Sinbad

Sinbad is a relatively new custodial Bitcoin mixer that began advertising its services on the BitcoinTalk forum in October 2022. Chainalysis investigators first observed wallets belonging to North Korea-linked hackers sending funds to the service in December 2022, which we can see on the Reactor graph below.



As we've seen in many North Korea-directed hacks, the hackers bridge the stolen funds from the Ethereum blockchain — including a portion of the funds stolen in the Axie Infinity hack — to Bitcoin, then send that Bitcoin to Sinbad. During December 2022 and January 2023, North Korea-linked hackers have sent a total of 1,429.6 Bitcoin worth approximately $24.2 million to the mixer.

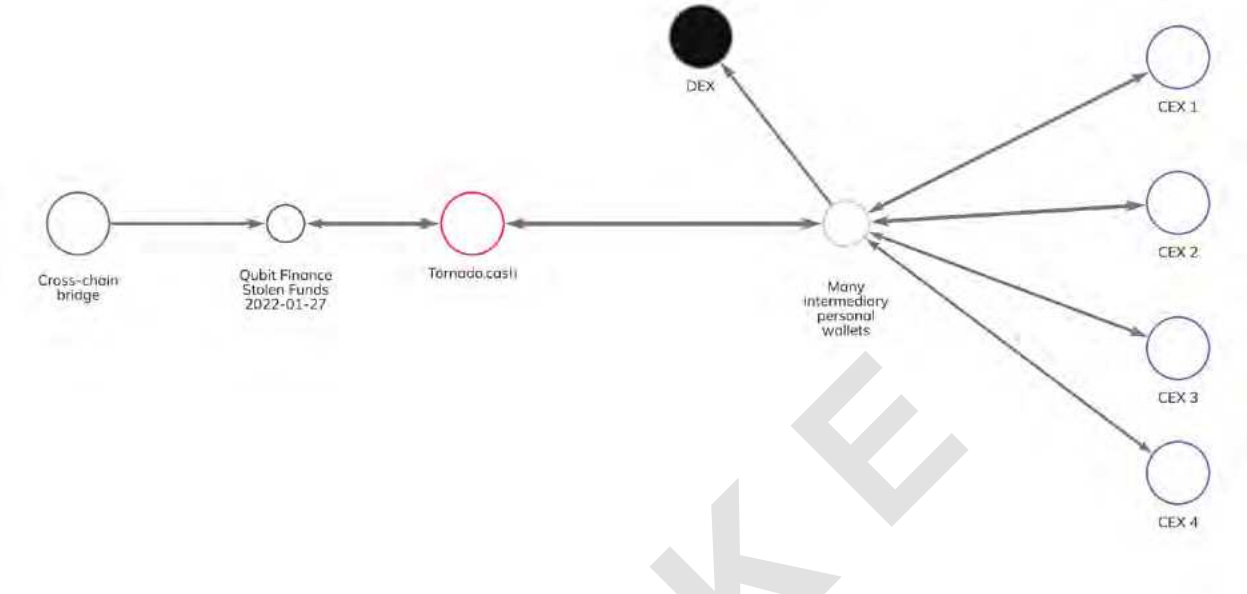
North Korea-linked hackers in action: How the Qubit hack unfolded

Qubit was a South Korea-based DeFi lending protocol built on the BNB chain. Qubit also ran an associated protocol, the QBridge, that allows users to use assets on other chains as collateral to borrow against on Qubit, without actually moving those other assets onto BNB Chain. Users send assets they want to collateralize to a QBridge smart contract on those assets' chains, and QBridge mints an equivalent asset on the BNB Chain.

Unfortunately, as has happened with many cross-chain bridges, hackers found an exploitable error in the code governing QBridge, and were able to drain the protocol of all of its holdings — roughly $80 million in assets, making it South Korea's largest crypto theft of 2022. We can now share publicly for the first time that we have attributed this attack to North Korea-linked hackers, as was the case with so many other large DeFi hacks in 2022. Let's take a look at how the Qubit hack unfolded.

The exploit the Qubit hackers discovered allowed them to mint unlimited qXETH — an asset meant to represent Ether bridged from the Ethereum blockchain — from the QBridge, without actually depositing any Ether. The hackers used the unbacked qXETH as collateral to "borrow" all of the assets held by the protocol — mostly BNB coin but also several BEP-20 tokens — worth roughly $80 million at the time of the theft. The hackers then bridged those funds to the Ethereum blockchain.

Once they bridged the funds from BNB Chain to Ethereum, the North Korean hackers used what was at the time their go-to money laundering strategy: They sent the funds to the mixer Tornado Cash. We can see an example of some of that activity following the Qubit hack below.



The hackers received their newly mixed Ether from Tornado Cash, and from there sent a portion to a decentralized exchange to be swapped for different ERC-20 tokens, while the rest was moved to deposit addresses at various centralized exchanges. The Qubit hack exemplifies many of the key elements of the North Korean hacking strategy we saw in 2022: Exploit a DeFi protocol, bridge the funds to a blockchain where funds can't be frozen, mix them, and move them to a centralized exchange. In this case, South Korea's Transnational Crime Information Center (TCIC) of the National Intelligence Service (NIS) was able to trace the funds in partnership with Chainalysis following the theft.

While North Korea-linked hackers are undoubtedly sophisticated and represent a significant threat to the cryptocurrency ecosystem, law enforcement and national security agencies' ability to fight back is growing. Last year, for example, we saw the first ever seizure of funds stolen by North Korea-linked hackers, when agents recovered $30 million worth of cryptocurrency stolen in the Axie Infinity Ronin Bridge hack. We expect more such stories in the coming years, largely due to the transparency of the blockchain. When every transaction is recorded in a public ledger, it means that law enforcement always has a trail to follow, even years after the fact, which is invaluable as investigative techniques improve over time. Their growing capabilities, combined with the efforts of agencies like OFAC to cut off hackers' preferred money laundering services from the rest of the crypto ecosystem, means that these hacks will get harder and less fruitful with each passing year.

Oracle Manipulation Attacks

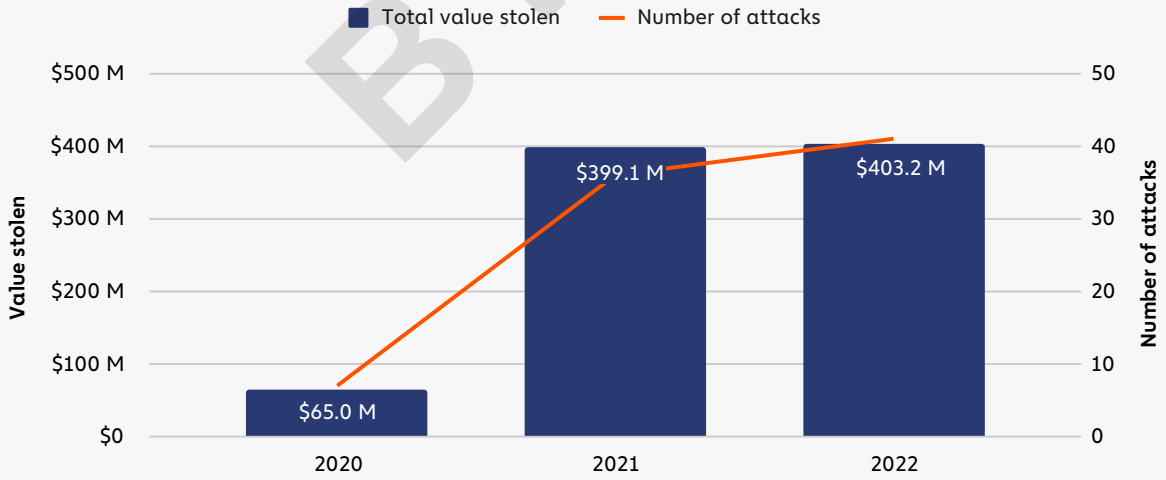
Oracle Manipulation Attacks a Rising, Unique Concern for DeFi

As we covered in our section on stolen funds, 2022 was the biggest year in crypto hacking history, with more than $3.8 billion stolen. However, not all of those attacks were what one may think of as hacks in the traditional sense. In some cases, bad actors were able to drain DeFi protocols of funds without actually taking advantage of an error in the protocol's code. These attackers were able to do this by manipulating the price oracles DeFi protocols use to ensure the assets available on their platforms are priced in accordance with the wider cryptocurrency market. As such, we'll refer to these unique instances as **oracle manipulation attacks**.

Bad actors typically carry out oracle manipulation attacks by using large amounts of cryptocurrency to quickly increase the trading volume of low-liquidity tokens on the targeted DeFi protocol, which can lead to fast, significant price increases not reflective of the wider market. Those initial funds are often sourced through a flash loan if the attacker doesn't have the funds on hand. Once an asset's price has been driven up, the attacker can then exchange their artificially inflated holdings for other tokens with greater liquidity and a more consistent value, or use them as (worthless) collateral to borrow assets, never to be repaid.

Overall, we estimate that in 2022, DeFi protocols lost $386.2 million in 41 separate oracle manipulation attacks.

Oracle manipulation attacks: Total value stolen and number of attacks by year, 2020 - 2022



Some attackers have tried to argue that oracle manipulation attacks aren't criminal in the same way a more straightforward hack is. In fact, Avraham Eisenberg, the individual behind one of the biggest oracle manipulation attacks of the year, claimed that his actions were perfectly legal and represented nothing more than a "profitable trading strategy." However, the SEC and CFTC both filed charges of market manipulation against him, with the DOJ also bringing an indictment. While the trial hasn't happened yet, the complaint suggests that authorities won't allow these attackers to evade responsibility, even if the targeted protocol *technically* behaved as designed. Below, we'll look at Eisenberg's infamous million attack on Mango Markets as an example of how oracle manipulation attacks can work.

Breaking down the Mango Markets exploit

One of the biggest oracle manipulation attacks of last year was the October 2022 attack of Mango Markets, a DEX on the Solana blockchain, which saw $117 million in assets drained from the protocol. The Mango Markets exploit was particularly interesting in that the perpetrator, Avraham Eisenberg, identified himself publicly afterwards and argued that his actions didn't constitute a crime. Here's how the exploit occurred from an on-chain perspective:

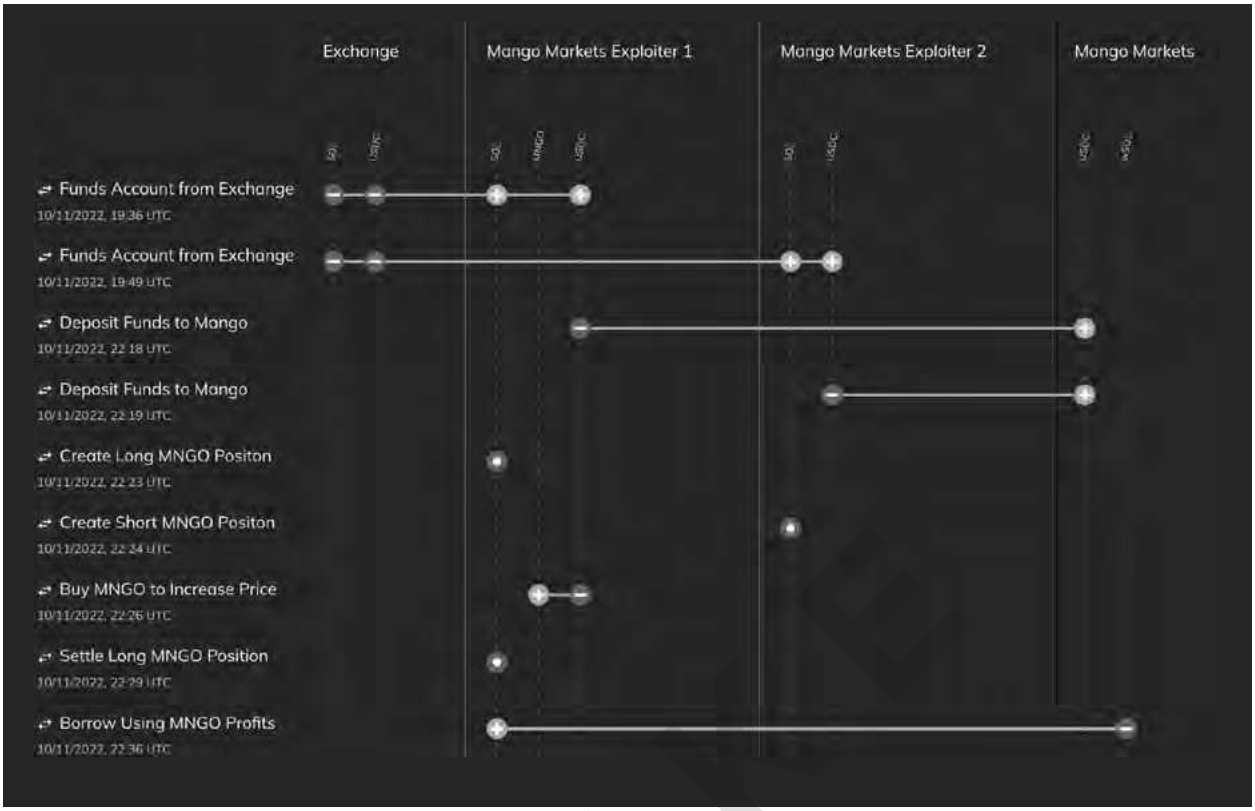
1. Eisenberg started with $10 million USDC (it's possible he also used funds not attributable to him on-chain to manipulate asset prices on other exchanges), split across two separate accounts at Mango Markets.

2. Eisenberg used one account to short 488 million MNGO (MNGO, or Mango, is the governance token for Mango Markets) — effectively selling 488 million MNGO on leverage — while the other account took the opposite side of that trade, using leverage to buy the same amount.

3. Eisenberg's leveraged purchase of MNGO, combined with further buying of MNGO on other DEXes, pushed the price of MNGO up very quickly on spot exchanges. This was possible because MNGO was a low-liquidity asset without much trading volume. The account used to purchase MNGO immediately profited roughly $400 million in paper gains because all of Eisenberg's buying activity significantly boosted the asset's price.

4. With such a high portfolio value, Eisenberg was able to borrow against his artificially inflated MNGO holdings and remove virtually all of the assets held by Mango Markets. This activity caused MNGO's price to drop immediately, so his long positions were liquidated due to loss of collateral value, but it was too late — Eisenberg had already "borrowed" all of Mango Market's assets with any real value.

We can see this activity on the Chainalysis Storyline below:



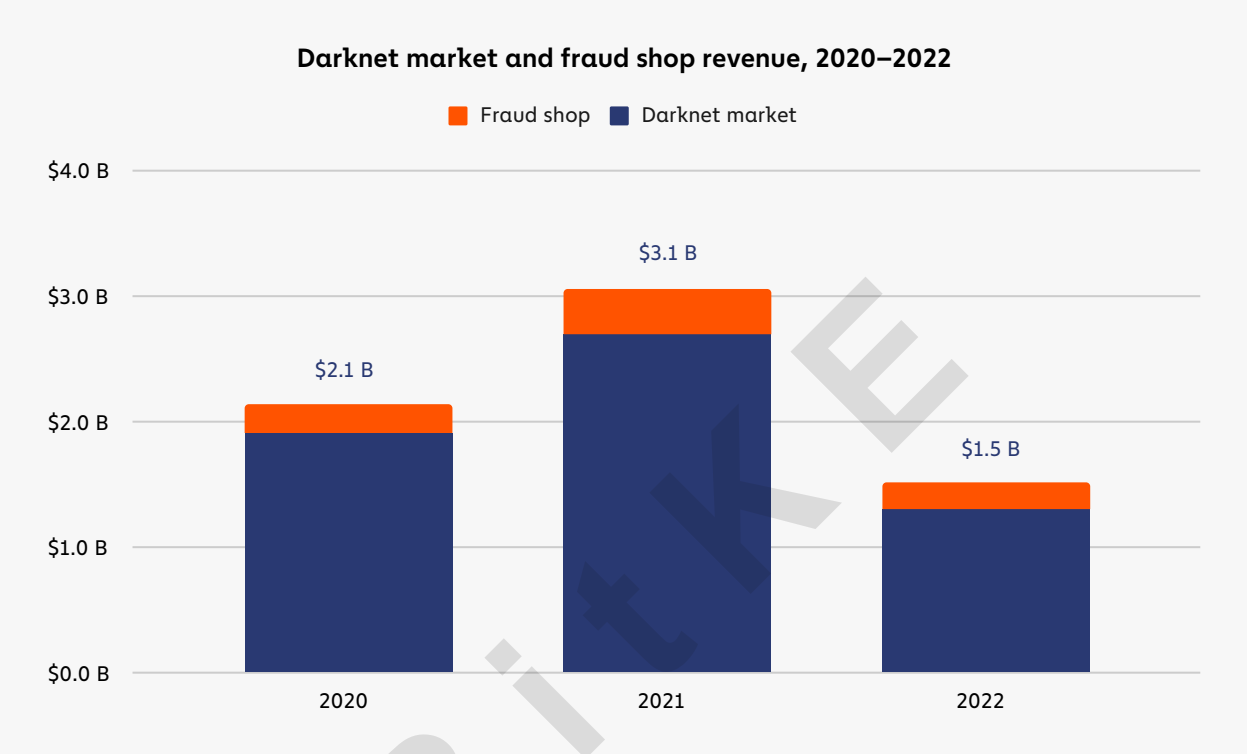
Adding insult to injury, Eisenberg used the MNGO he still held after the exploit to propose and vote on a governance proposal that would allow him to return $10 million worth of cryptocurrency stolen in the attack, and keep the rest as a "bug bounty." The proposal eventually passed. While most hackers avoid publicity, Eisenberg was open about his role in the Mango Markets exploit, and seemed convinced that because the code had at all times technically run as designed, he had done nothing wrong. He even appeared on Laura Shin's popular *Unchained Podcast* to explain this perspective.

However, as the SEC lays out in its complaint, Eisenberg's actions allegedly qualify as market manipulation due to the false increase in MNGO trading volume — 2,000% higher on the day of the exploit compared to the average over the previous ten days — that he orchestrated. Since charges were filed, Mango Markets has also sued Eisenberg for the difference between what he stole and what he returned as a result of his governance proposal, arguing that Eisenberg was not engaged in "lawful bargaining" when he negotiated his bug bounty with the Mango Markets DAO.

Darknet Markets

How Darknet Markets Fought for Users In the Wake of Hydra's Collapse

2022 saw a decline in revenue from the previous year for darknet markets and fraud shops. Total darknet market revenue for 2022 ended at $1.5 billion, down from $3.1 billion in 2021.



Four of the top five highest-earning darknet markets in 2022 were conventional, drug-focused darknet markets, while just one, Brian Dumps, was a fraud shop.

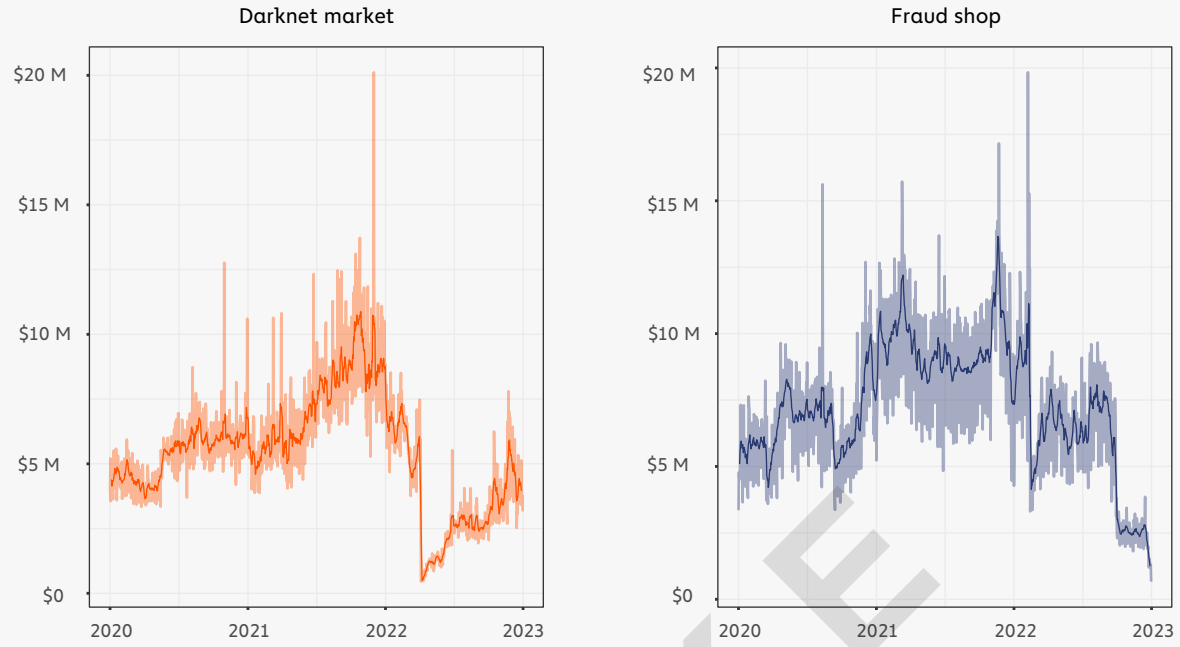
Hydra Market led the way once again as the highest-earning darknet market in 2022, even though it was sanctioned by OFAC and shut down in a joint U.S.-German operation in April — no other market beat the revenue lead it built up in those four months. Salih Altuntas, a German Federal Police agent who worked on the case said, "Hydra had a monopoly, and that gave it the time and resources to build out unique services other markets couldn't."

For instance, Hydra prided itself on customer service, with perks and thoughtfulness one would expect more from a legitimate business than an online drug market. "Hydra had a service where users could send drugs in to be tested for purity," said Altuntas. "They had a Telegram bot users could contact for first aid information in the event someone overdosed. They helped vendors connect with legal services in the event they were raided by police."

As we'll explore later, the three next-highest earning markets of the year — Mega Darknet Market, Blacksprut Market, and OMG!OMG! Market — all gained their initial market share in the wake of Hydra's collapse, with on-chain data suggesting these markets made concerted efforts to attract former Hydra users and vendors.

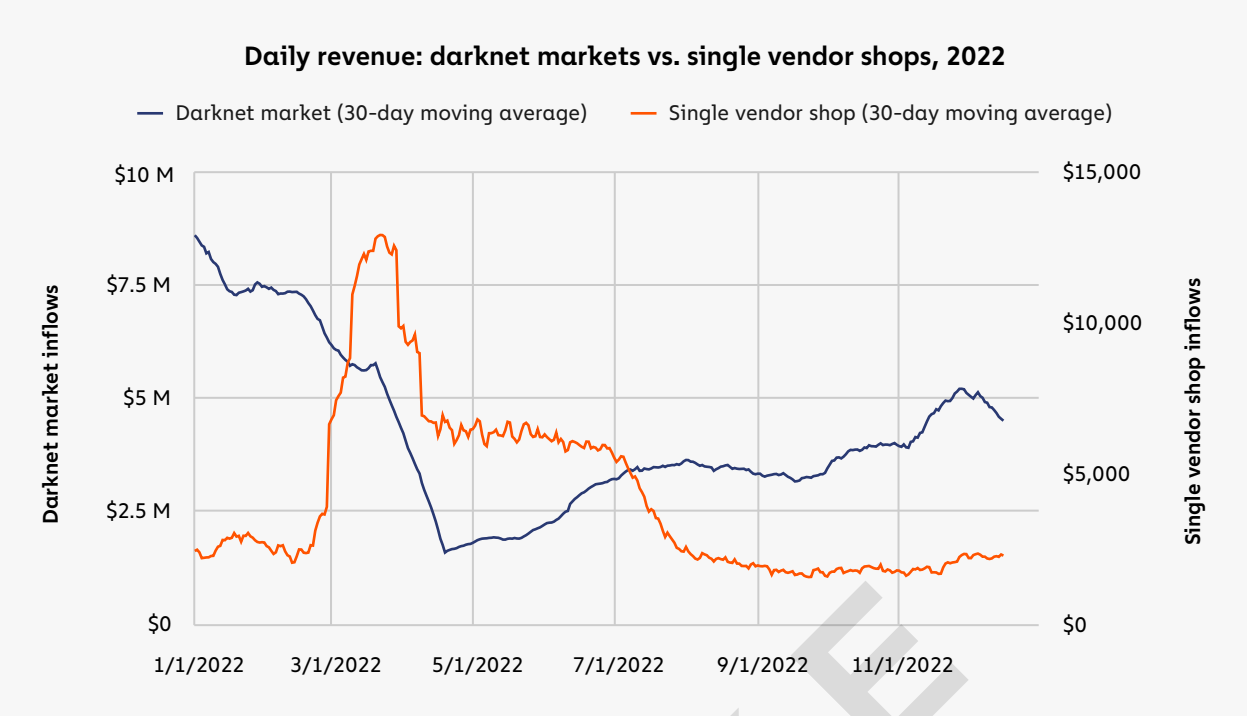
Hydra's closure prompted a sector-wide decline in darknet market revenues, with average daily revenue for all markets falling from $4.2 million just prior to its closure and to $447,000 immediately after. While drug markets' collective revenue hasn't recovered fully, it climbed slowly back toward previous levels in the second half of 2022. Fraud shops, however, have continued to decline.

Daily revenue for darknet markets vs. fraud shops, 2020–2022



Fraud shops are a unique segment of darknet markets that sell compromised data such as stolen credit card information and other forms of personally identifying information (PII) that can be used for fraudulent activity. This decline was triggered in part by the closure of prominent fraud shops like Bypass Shop, which was shut down in March. Brian Dumps, the biggest overall fraud shop for the year, also appears to have suffered a disruption as its revenue fell almost to zero in October, though it's unclear exactly why.

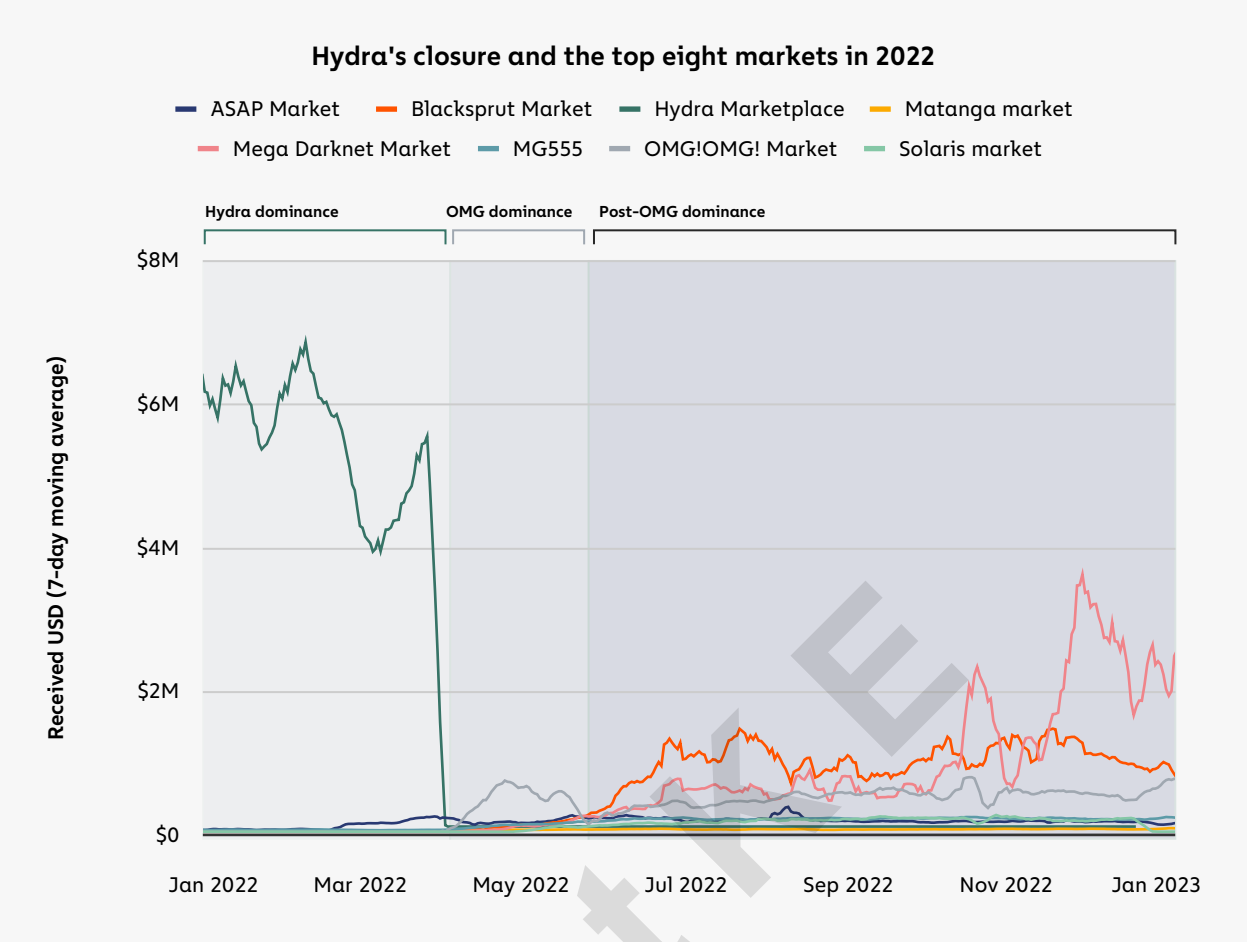
While darknet markets have largely recovered after Hydra's closure and fraud shops have not, single vendor shops showed a different pattern. Single vendor shops are standalone shops set up by individual drug vendors who have typically gathered a large customer base on a larger, traditional darknet market. Setting up a single vendor shop allows those vendors to save on fees that would ordinarily go to the administrators of a traditional darknet market.



Throughout 2022, we observed a negative relationship between funds sent to regular darknet markets and those sent to single vendor shops. For instance, we see single vendor shop revenue spike beginning around March, around the same time traditional darknet market revenue began to fall. Similarly, single vendor shop revenue fell concurrently with the recovery of traditional darknet markets from around June through end of year.

The battle for market dominance, post-Hydra shutdown

Before law enforcement shut down Hydra, it was the largest darknet market in the world. Prior to its demise, Hydra Marketplace captured 93.3% of all economic value received by darknet markets in 2022 — some $357.4 million. The Russia-based darknet market enabled drug sales and offered cybercriminals unique money laundering services. “Hydra had an internal mixer called Bitcoin Bank Mixer, which vendors could use to withdraw Bitcoin from Hydra that appeared clean on-chain,” said Altuntas.



Through most of April and May, OMG captured well over 50% of total market share, reaching a peak of 65.2% on April 23, and operated virtually unchallenged by competition, indicating its potential as a Hydra successor. In June, OMG suffered a distributed denial of service (DDoS) attack, which likely caused vendors and customers to migrate to Mega Darknet Market and Blacksprut Market around that time. Similarly, Blacksprut was hacked in late November, which coincides with its decline from its peak revenue share of 68.5% a few weeks prior. Given the illicit nature of darknet markets, it's unsurprising that vendors and users would seek to leave a market that has suffered a data breach.

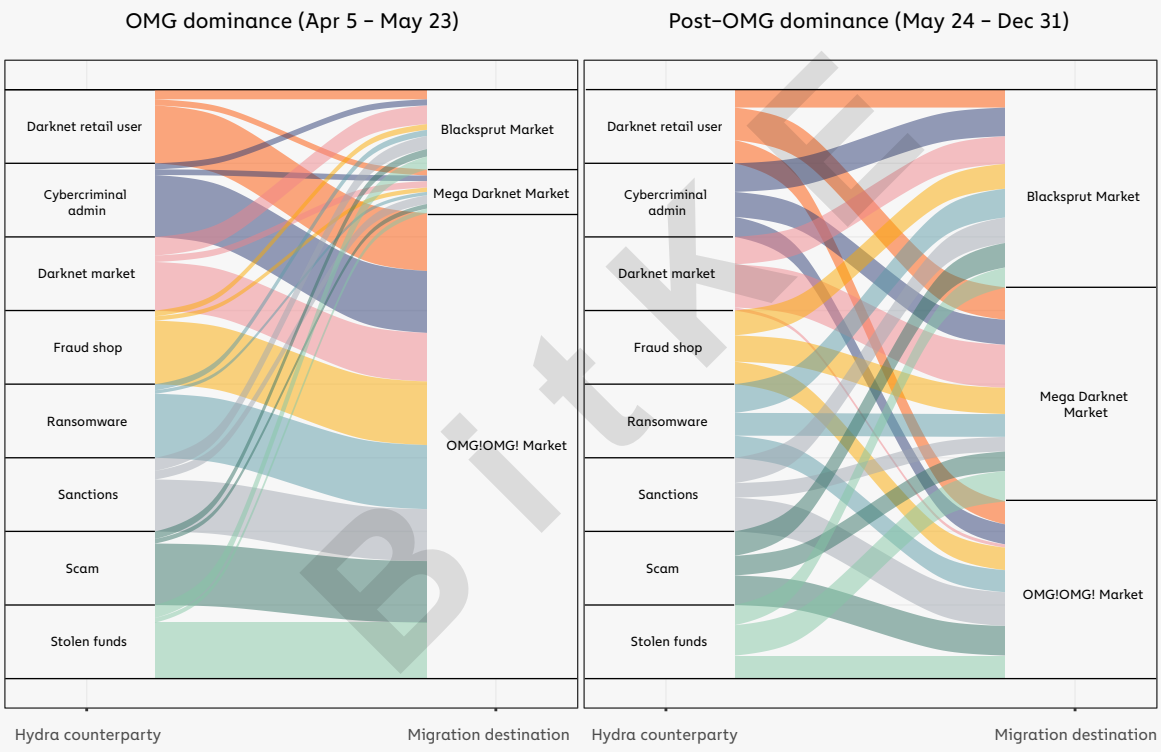
How drug buyers and illicit users migrated from Hydra to other darknet markets

If we dig deeper into how Hydra's three primary successor markets jockeyed for position following Hydra's shutdown, we find that capturing the specific customers who previously relied on Hydra — both retail market customers and illicit users of Hydra's money laundering services — was crucial to the battle. We can investigate this by using on-chain data to look at where former Hydra users migrated after the market was closed. For this analysis, we'll split the remainder of 2022 after the April 5 Hydra shutdown into two time periods:

- **OMG dominance**: The 50 day-period immediately after Hydra's shutdown when OMG captured close to 100% of darknet market share.
- **Post-OMG dominance**: The rest of 2022, when OMG became one of three sizable markets alongside Blacksprut and Mega.

The two charts below show which markets Hydra's previous counterparties used the most in both of those two time periods. The color of the lines show the former Hydra users' category of activity and the thickness of the lines show the proportion of their activity flowing to new markets after Hydra was shut down.

Hydra counterparty migration post-closure

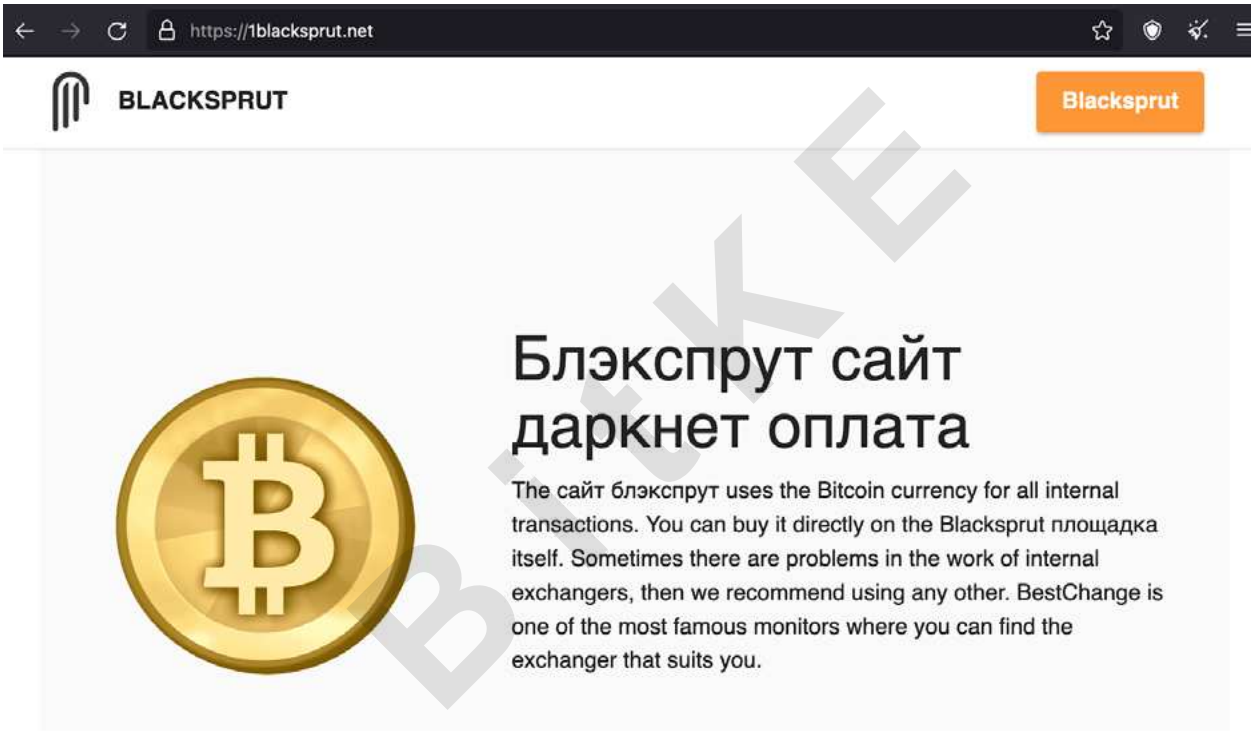


Like the vast majority of all darknet market users, former Hydra counterparties across all categories — both retail drug buyers and criminal users — transacted almost exclusively with OMG during the OMG dominance period. In the post-OMG dominance period, OMG retained a number of those former Hydra counterparties, but lost a significant share of their activity to the other two markets across all categories.

There are two primary takeaways from this: first, signs point to these three markets having launched money laundering services similar to what Hydra offered, which would explain why so many of

Hydra's criminal users migrated to those markets. The second takeaway is just how dominant OMG was amongst Hydra's counterparties immediately following Hydra's closure. This is especially interesting given the connections between OMG and Hydra that we'll explore later.

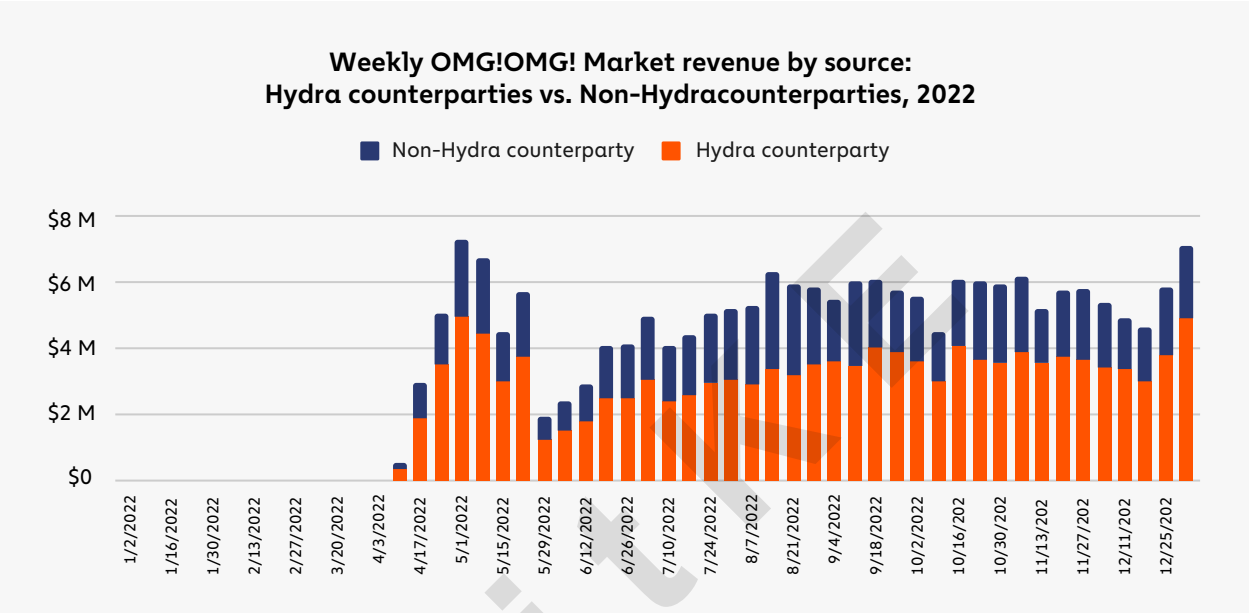
There is direct evidence that two of the three markets in question offer money laundering services. In early January 2023, Blacksprut vendor RedBull Exchange made a post titled "Transfer from platform" that said users could withdraw Bitcoin with a 4% fixed commission fee and that funds would instantly transfer to their private wallets without going through any "checks or cleanings." The image below shows a Blacksprut overview site indicating that the service offers internal exchanges for moving funds off market, and also recommending the Russia-based BestChange exchange aggregator service should those fail.



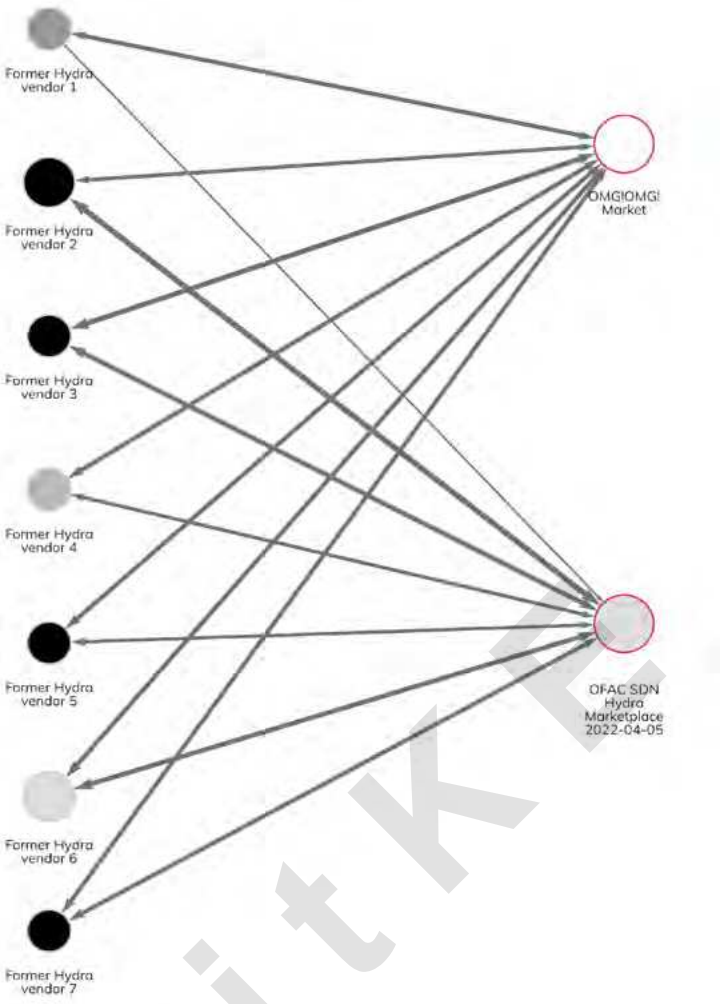
Similar posts on Mega Darknet Market confirm it offers these services, too. We don't yet have confirmation of OMG offering money laundering services, but again, the on-chain data suggests it likely does.

OMG, Blacksprut, and Mega Darknet markets show potential vendor and admin overlap with Hydra

Advertised as "the most advanced darknet market ever," OMG primarily provides illicit drugs, but also offers products like hacking utilities, banking information, and more. The market has a peculiar history. It first became active in early July 2020, with deposit volumes so low it appeared to be less of a darknet market and more a personal operation. However, nearly as soon as Hydra shut down, OMG began seeing high inflows for the first time, more than half of which came from Hydra counterparties.

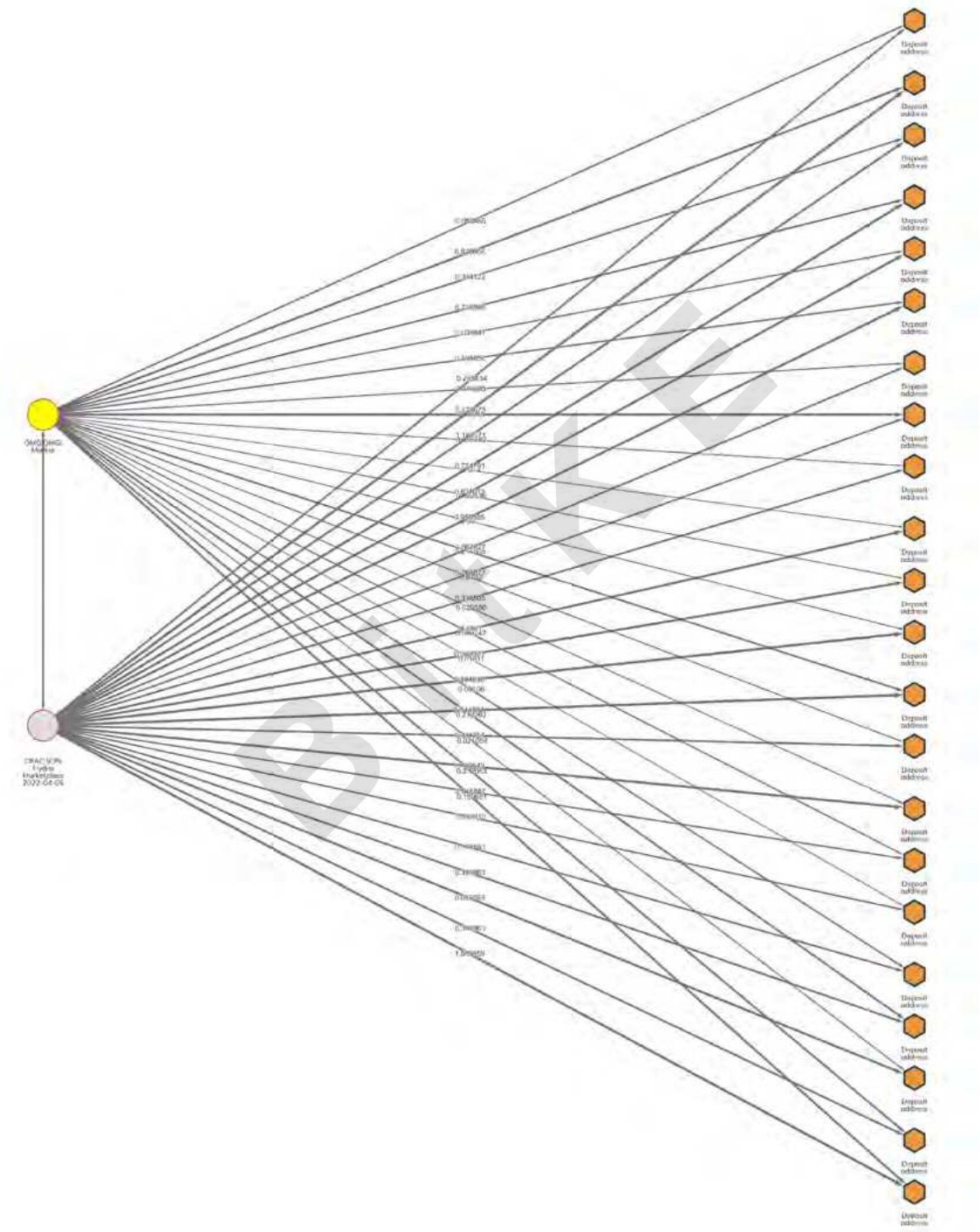


Blockchain analysis also reveals that several Hydra vendors migrated to OMG following Hydra's shutdown. The Chainalysis Reactor graph below shows several personal wallets associated with known Hydra vendors subsequently transacting with OMG.

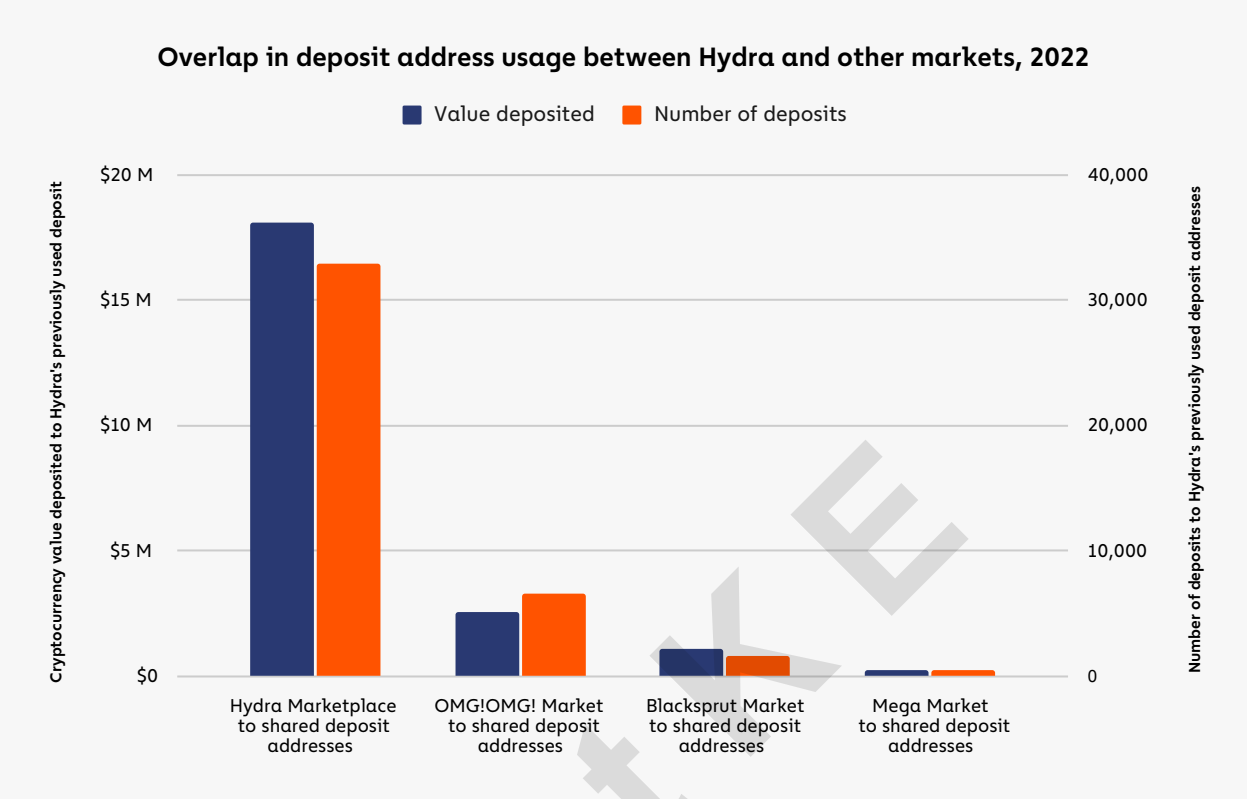


The migration of vendors, plus the timing and source of OMG's initial revenue suggests that Hydra administrators may have been involved with the development of OMG. Additionally, the two markets show certain operational similarities. For instance, Hydra was unique from its competitors in that it offered location-based courier services. Upon account creation, the user would select their location and arrange "dead-drop"-style exchanges from vendor to buyer. Upon sale, the vendor would send the buyer geographic coordinates and a picture of where their well-hidden purchase could be found. OMG offers this same service, too.

Further blockchain analysis reveals an even more interesting connection: OMG's central wallets send high volumes of cryptocurrency to the same group of deposit addresses at a high-risk exchange with a heavy presence in Russia. The overlap in deposit address usage suggests that those deposit addresses may be controlled by the same individuals, which would suggest further vendor overlap or possibly even administrator overlap.



Both Blacksprut and Mega have also sent funds to deposit addresses on this exchange used previously by Hydra, but none as much as OMG. We can see this on the chart below, which shows the total amount sent by each market to shared deposit addresses.



We don't have definitive evidence confirming that any of OMG's creators or administrators were formally associated with Hydra. However, the deposit address overlap and instantaneous mass migration of Hydra users to OMG following Hydra's shutdown suggests that it's certainly possible.

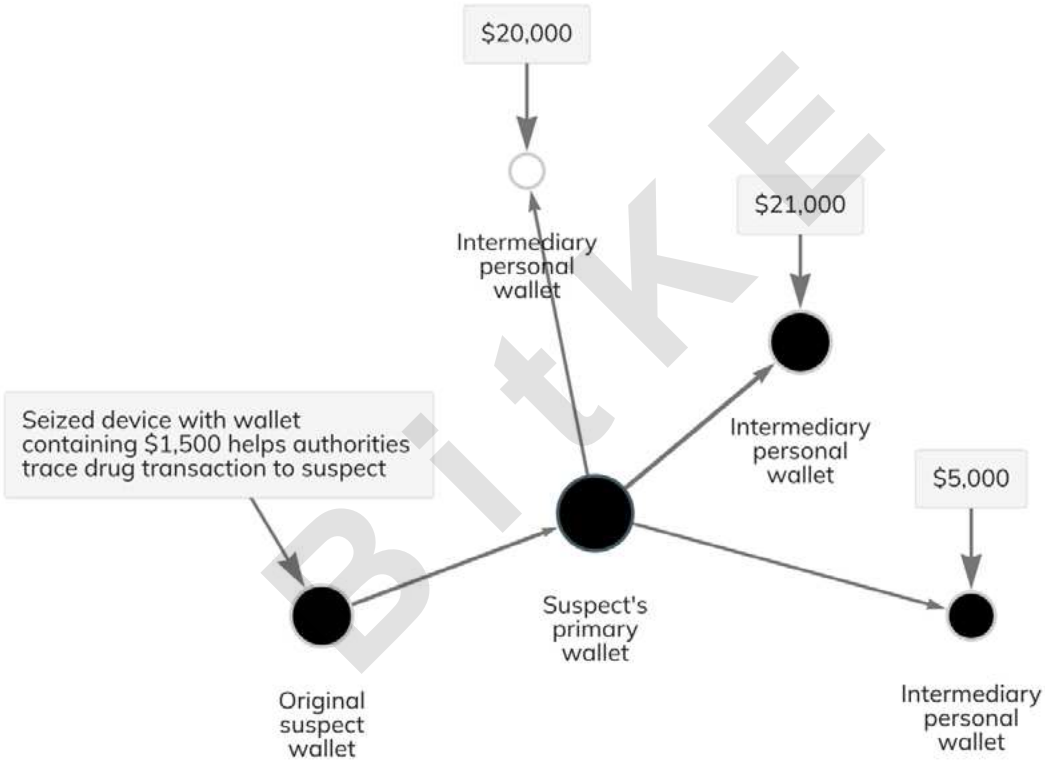
How London's Metropolitan Police used blockchain analysis to investigate drug traffickers

With the right tools for tracing cryptocurrency transactions, law enforcement can not only investigate the activity of vendors selling illicit drugs on darknet markets, but also follow their transactions to discover larger criminal enterprises.

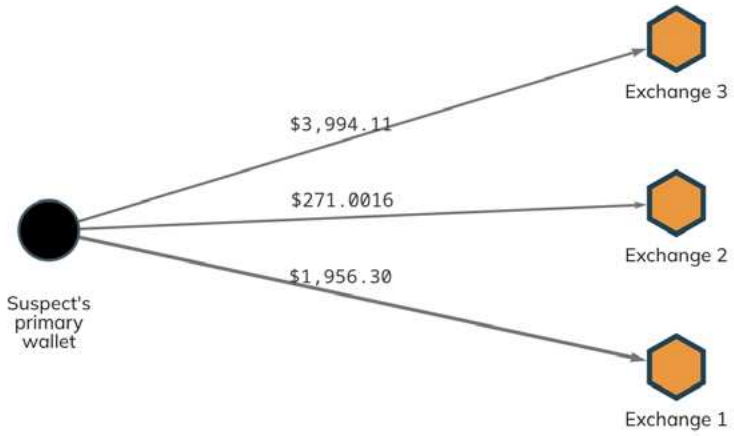
A recent Metropolitan Police (MET) investigation — Operation Cyanic — provides a great example. This investigation into the international supply of Class A, B and C drugs examined a vendor profile on a dark web marketplace. The MET identified that the profile, run by a family network, had completed thousands of cryptocurrency transactions. As such, investigators tracked and traced crypto funds to identify assets held, calculate the benefit derived from drug supply, and support the traditional financial side of the operation's investigation.

Performing digital forensics after the suspect's arrest, investigators examined a number of mobile devices, during which they identified a transaction tied to a transfer of £1,500 worth of crypto-currency. This was used as a starting point to map the suspect's criminal activity. Tracing a recent transaction from that wallet, police found that the suspect had sent funds to another high-activity wallet also thought to be under his control. That wallet had a much higher balance, and an extensive transaction history with many other wallets. This new information helped identify other elements of a larger organized gang, providing further actionable intelligence opportunities.

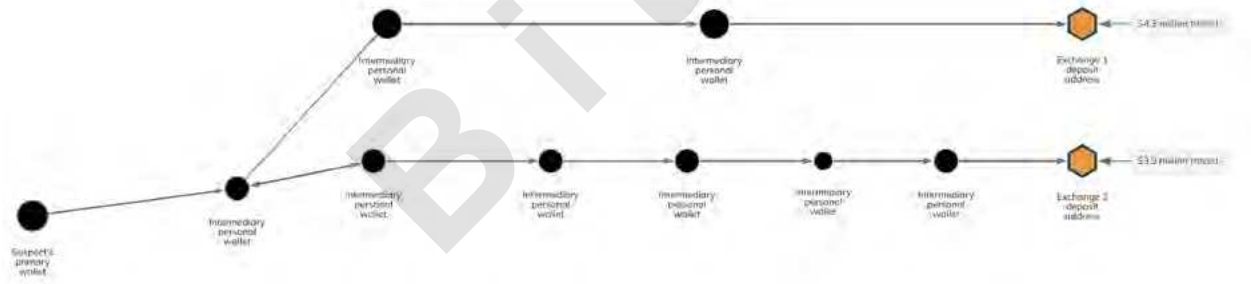
The graphs below illustrate how the MET traced funds from the initial wallet to other destinations, which indicate that the suspect was part of a large-scale drug trafficking ring using cryptocurrency as a primary means of payment and money laundering.



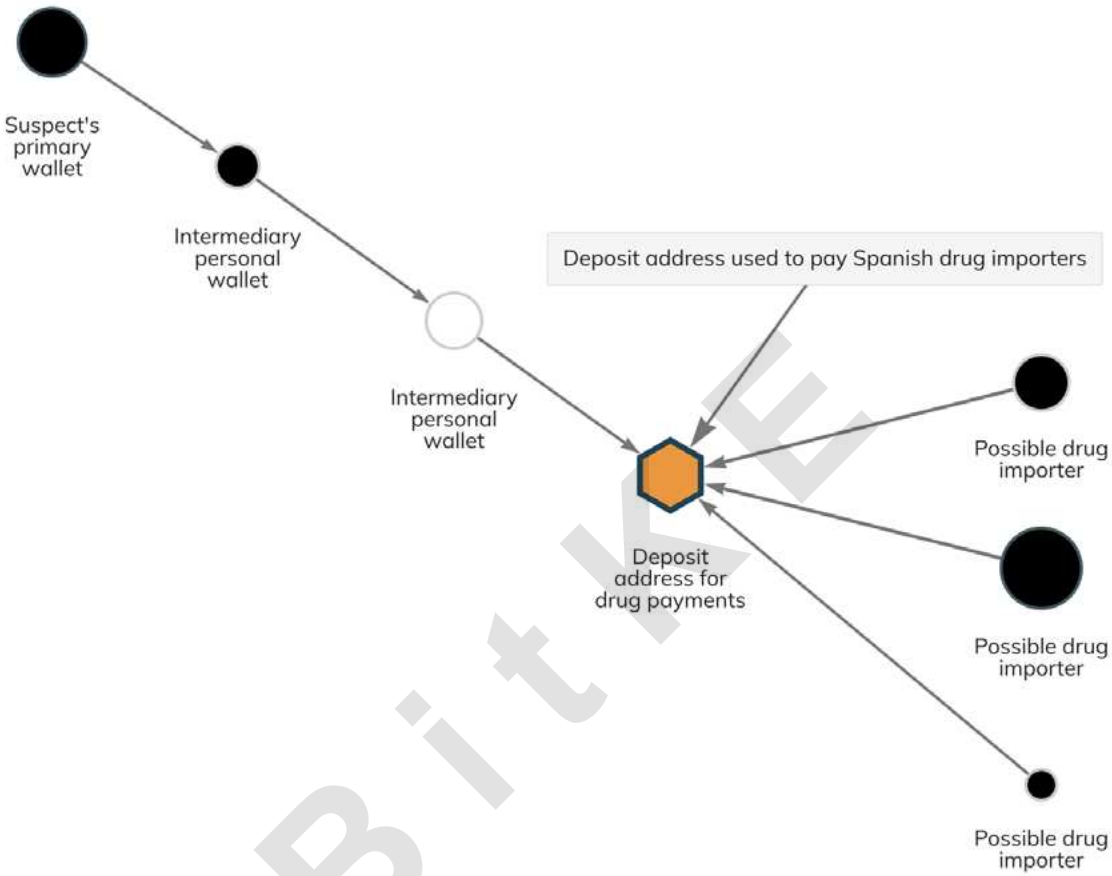
As we see below, the suspect sent funds to several exchanges from the larger wallet one transaction away from the original, presumably to convert his cryptocurrency into cash.



Similarly, the suspect's largest wallet had sent funds via intermediary personal wallets to two highly active exchange deposit addresses, both of which held millions of dollars' worth of cryptocurrency. Those deposit addresses may also belong to the original suspect, or could have belonged to other criminal associates. While that information wasn't immediately apparent, police could leverage it to subpoena the exchanges in question for more information on who controlled those deposit addresses.



Another highly active exchange deposit address to which the suspect sent funds had a balance of over $6 million. Supporting intelligence indicated that this address had received considerable funds from individuals based in Spain, suggesting that drugs were being exported from that region to the UK. This information provided opportunities for further investigation.



In addition to these findings, the MET was able to locate the organized crime group's current assets and calculate its realizable benefit figure — found to be over £600,000 — which resulted in confiscation orders for each defendant after they had been convicted of conspiracy to supply Class A, B and C drugs.

Scams

Crypto Scam Revenue Dropped 46% in 2022, While Blockchain Analysis Finds Links Between What Appear to be Distinct Scams

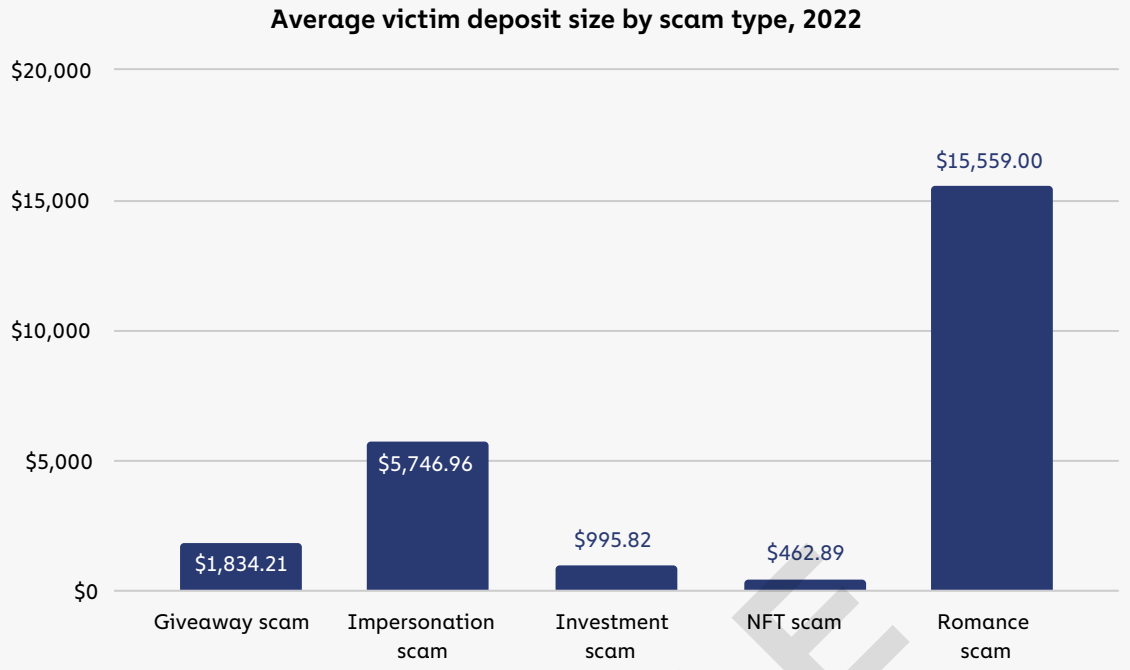
While scams remain the largest form of cryptocurrency-based crime (that is, if we ignore transactions associated with OFAC-sanctioned entities, which can be criminal or not depending on jurisdiction), crypto scam revenue fell significantly in 2022, from $10.9 billion the year prior to just $5.9 billion.

As we'll explore below, we attribute most of this decline to market conditions, as scam performance tends to worsen when cryptocurrency prices are in decline. However, some crypto scam types are growing despite the ongoing bear market. We must also add that our numbers are a lower-bound estimate. As with all forms of crypto crime, our estimates of the true amount lost to fraudsters will grow as we identify more addresses associated with scams. Underreporting exacerbates this problem, particularly in the case of so-called "pig butchering" scams, which we know to be a growing issue. In addition to scamming trends, we'll look at how some investigators on the cutting edge are using blockchain analysis to combat pig butchering scams, and also share data that points to the interconnected nature of the crypto scam ecosystem.

2022 crypto scam activity summarized

While scam revenue dropped overall, we still saw a number of highly successful scams, the top being Hyperverse, which pulled in nearly $1.3 billion in revenue.

All ten of 2022's top scams were investment scams, which as a category dominated overall scam revenue last year. However, that doesn't mean we can ignore other types of scams. Despite having lower overall revenue as a category, romance scams appear to have been the most destructive on a revenue-per-victim basis.



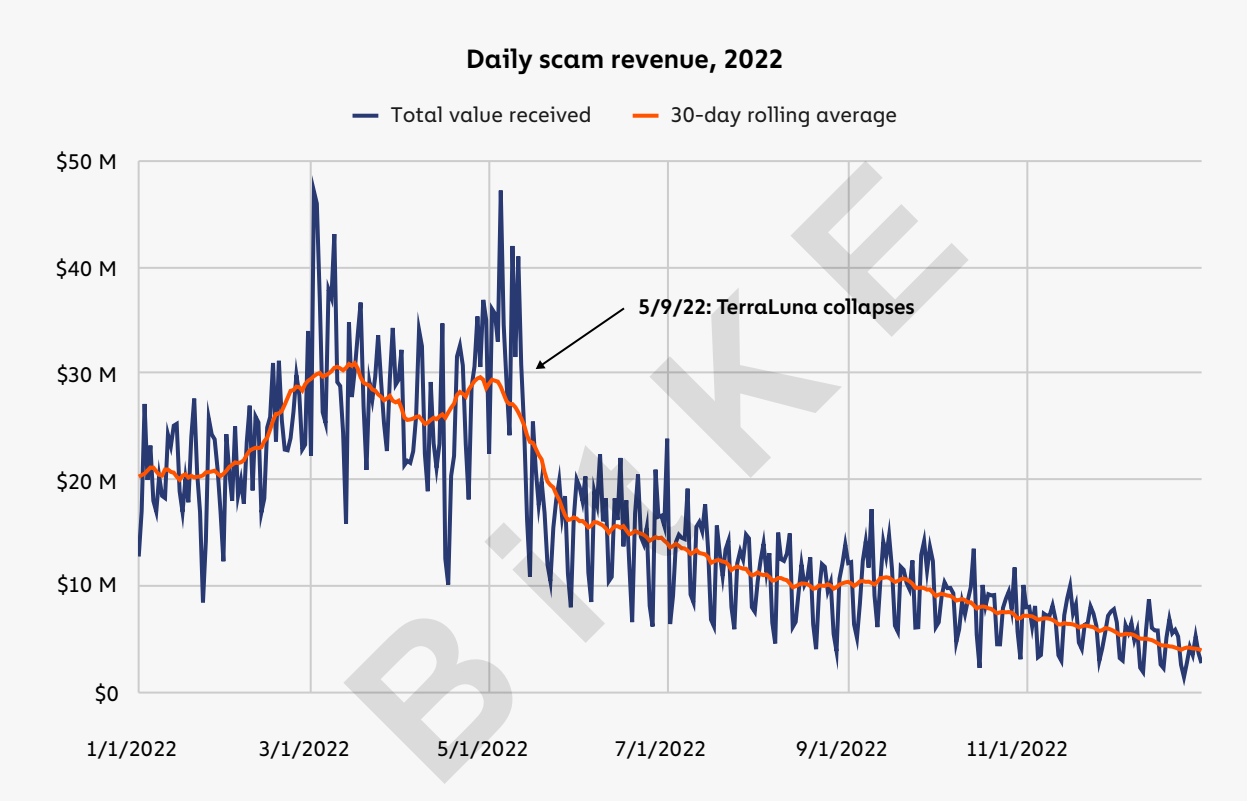
A guide to the scam categories we track:

- **Giveaway scams** are scams in which fraudsters solicit victims to send them cryptocurrency, promising to send them more in return. Giveaway scammers often impersonate celebrities to lend credence to the promise.
- **Impersonation scams** are scams in which fraudsters pretend to be someone in a position of authority or expertise — for instance, an IRS or Social Security representative — and tell victims they must send in cryptocurrency to correct some kind of problem or avoid getting in trouble.
- **Investment scams** are scams in which fraudsters promote a fake investment company promising outsized returns.
- **NFT scams** are scams in which fraudsters trick victims into buying fake NFTs designed to resemble more notable collections.
- **Romance scams** are scams in which the fraudster pretends to build a romantic relationship with the victim in order to convince or guilt them into sending them money. Romance scams can also include "pig butchering scams," which blend elements of romance scams and investment scams.

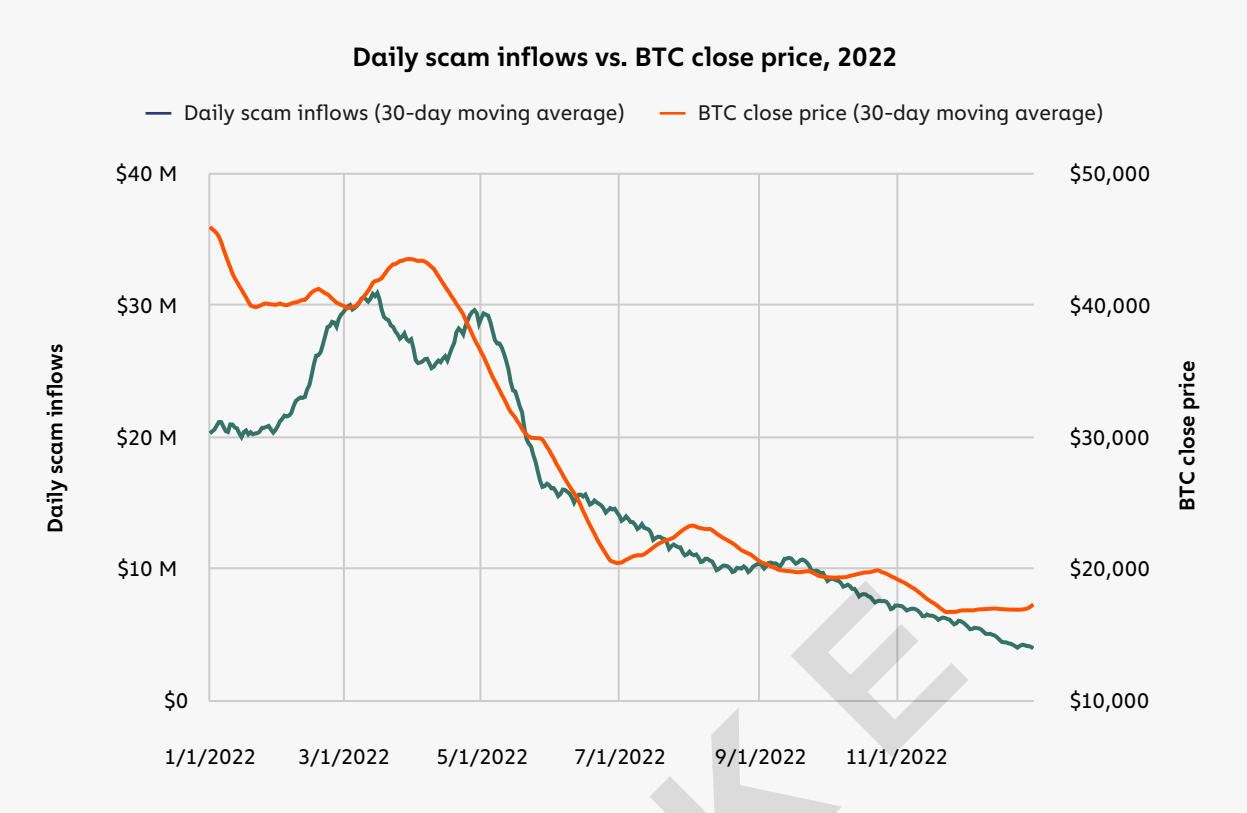
Romance scams took an average victim deposit of almost $16,000, nearly triple the next-closest category. It's also important to remember that underreporting by victims is likely more prevalent in romance scams due to their uniquely personal nature, so their total revenue and overall reach is probably higher than one would think based strictly on on-chain data.

Crypto scams and market dynamics

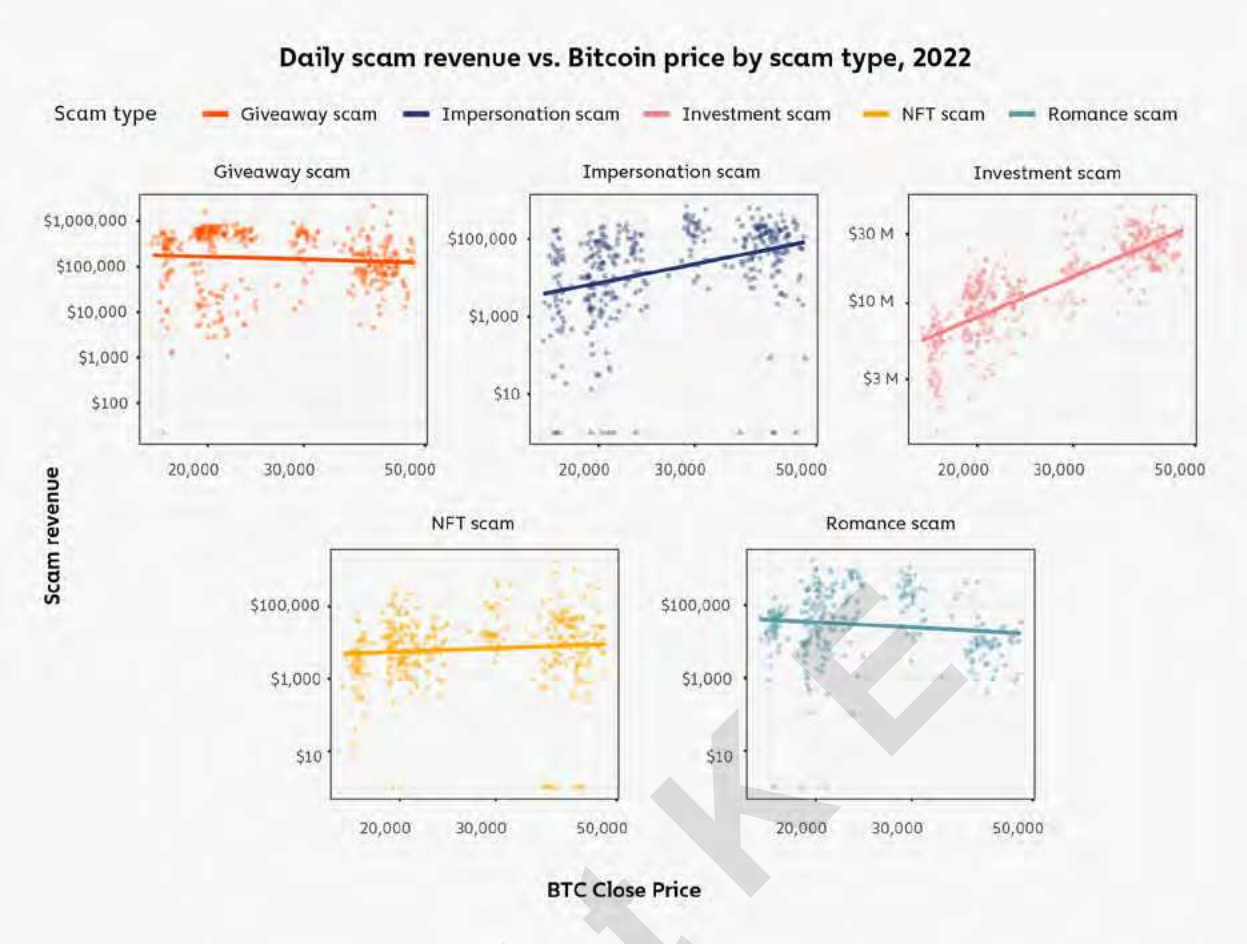
Cryptocurrency scam revenue began the year trending upwards, but plummeted in early May — the same time the bear market set in following the collapse of TerraLuna — and then declined steadily throughout the rest of the year.



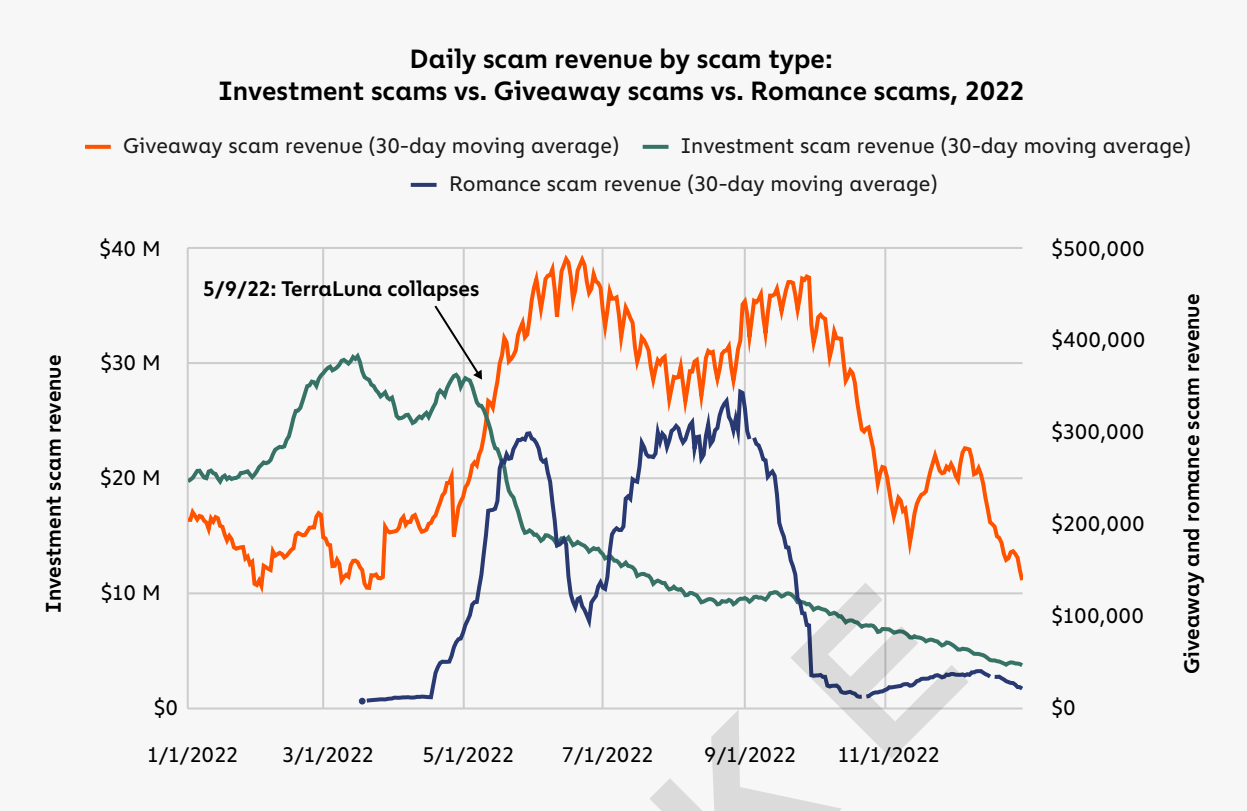
This fits with trends we've previously observed on how wider trends in crypto markets affect scamming. Generally speaking, scams take in less revenue from victims at times when crypto asset prices are declining. We can see this clearly on the graph below, which tracks scam revenue against the price of Bitcoin throughout 2022.



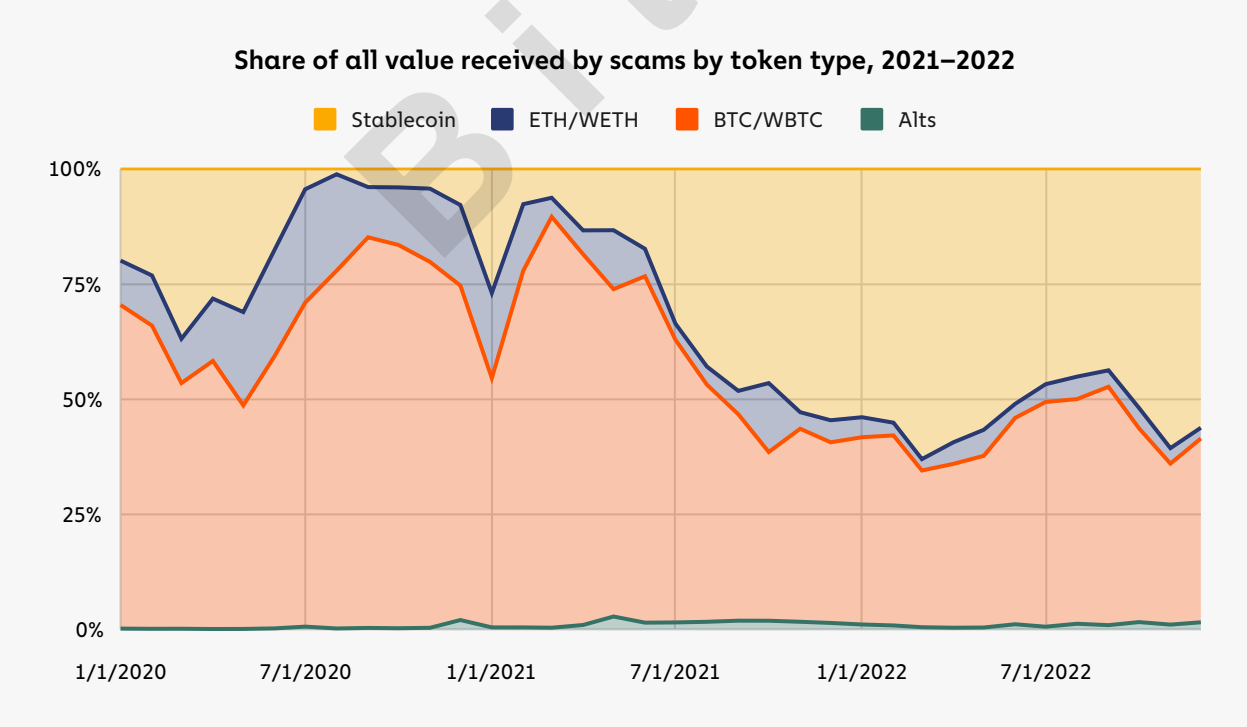
Scam revenue throughout the year tracks almost perfectly with Bitcoin's price, consistently maintaining a three-week lag between price moves and changes in revenue. However, not every distinct type of scam follows this pattern — some types of scams see revenue changes increase as crypto asset prices decrease.



For instance, unlike other kinds of scams, romance and giveaway scams don't show a positive correlation with Bitcoin's price (we use Bitcoin here because it's the biggest cryptocurrency by market cap and its price movements are generally correlated with those of other crypto assets). Investment scams, which also happen to get by far the most revenue of any other scam type, are one of the most correlated with Bitcoin's price. The reason for the difference likely lies in how the scams are pitched to victims. Investment scams typically promise users outsized investment returns, often based on an algorithmic, "can't lose" trading strategy. That pitch is probably more likely to succeed when the asset prices are growing, and the news is filled with stories of crypto investors striking it rich. Romance scams, on the other hand, are more about building a personal relationship with the victim, and the scammer convincing them that they care about the victim and need their help. That kind of emotional pitch is probably equally effective regardless of trends in the wider market, because the victim's primary goal isn't to get rich quick, but rather to help someone they believe to be a potential romantic partner. In fact, scammers may even pivot to romance scams versus investment scams in times of declining asset prices for those very reasons, which would intensify this trend further. Because of this, romance scams and other scam types whose performance doesn't track with Bitcoin price followed different revenue patterns throughout the year compared to investment scams.



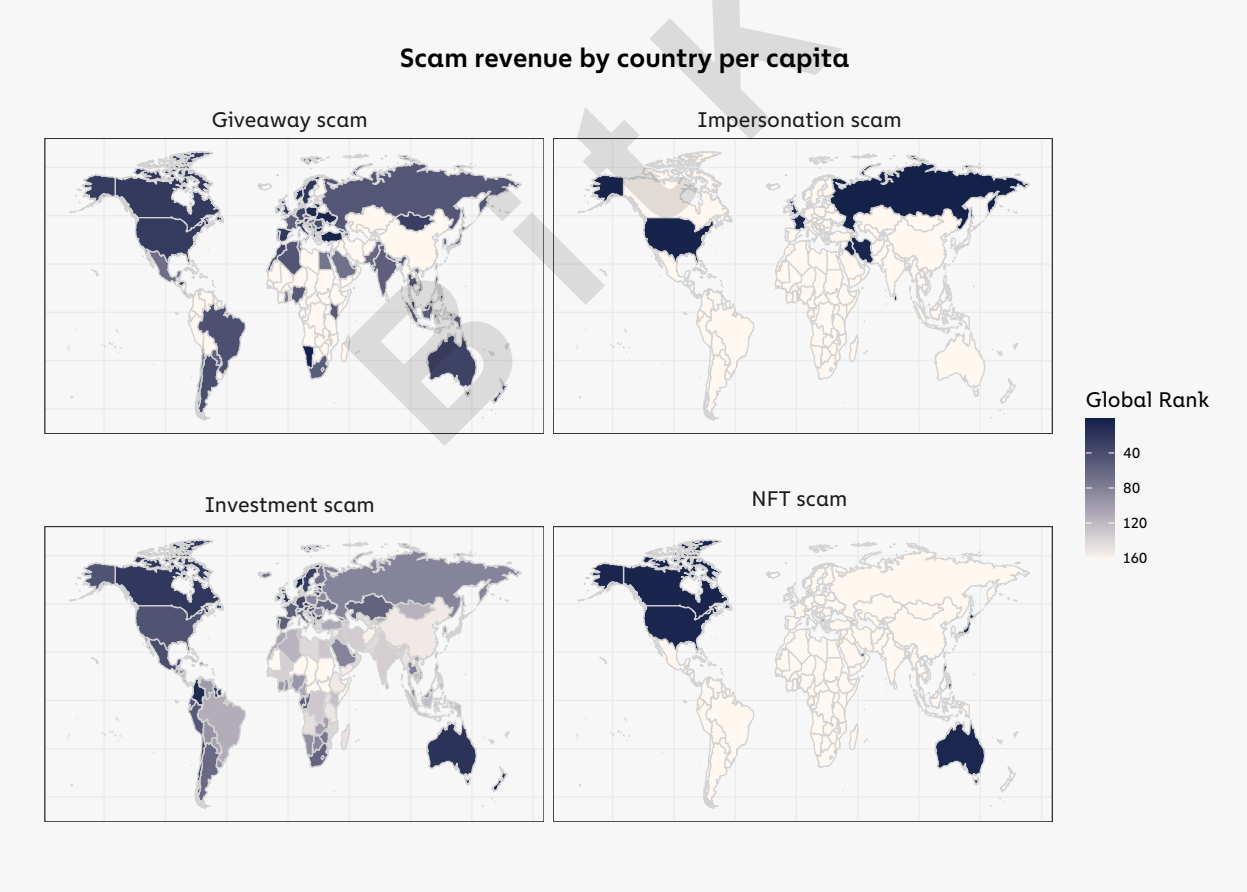
Market conditions may have also influenced another trend we've seen develop over the past two years: the rise in usage of stablecoins by scammers.



Prior to 2022, most scams took payments primarily in Bitcoin. But this started to change in 2021, with scammers taking more and more of their revenue from victims in stablecoins, during a period of time when the price of crypto assets like Bitcoin was trending upward. Similarly, we see a spike in scammers' use of Bitcoin in mid-2022, when asset prices were trending down. This seems counterintuitive — wouldn't scammers prefer to accept victim payments in Bitcoin when Bitcoin is trending up? Scammers' solicitation of stablecoins over Bitcoin during bull markets may represent a hedge against a possible market crash. Scammers may also have better luck soliciting stablecoins in a bull market given that they have no price upside, while potential victims may be more inclined to hold their Bitcoin in the expectation it will go up in value.

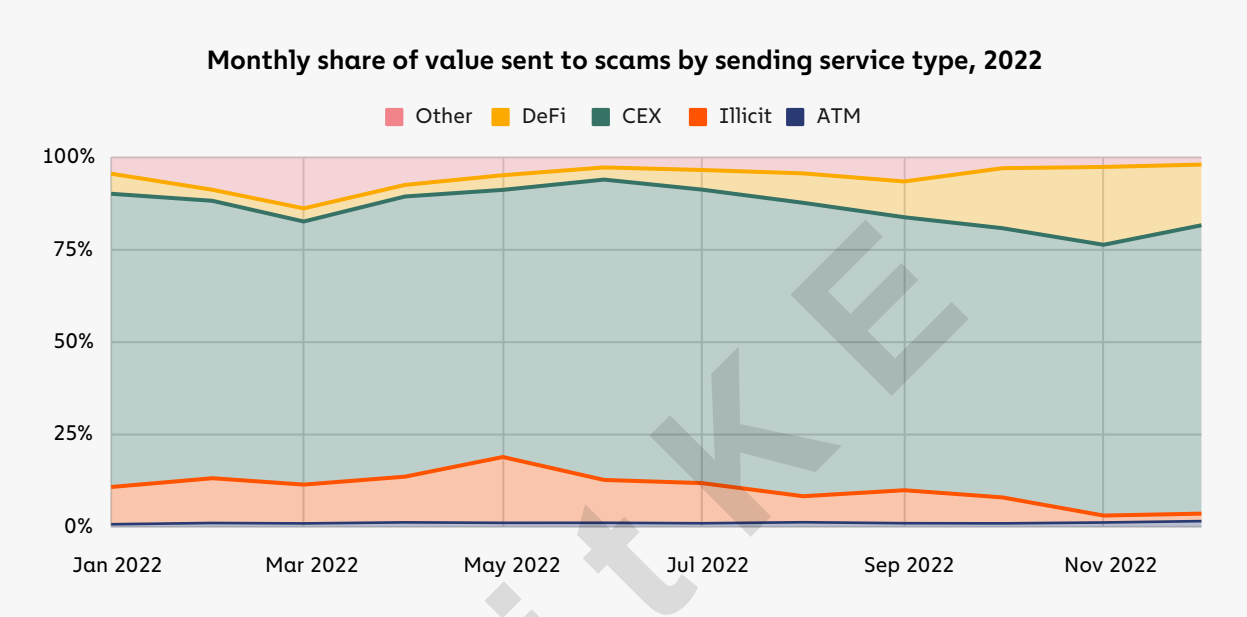
Who's falling victim to scams?

Different types of scams show different levels of effectiveness depending on the geographic area of the victim. Much of this is likely due to the location of the scammers themselves, as this will impact their ability to pitch victims based on their shared language and cultural context. But the geographic trends in scamming in many cases also match the geographic trends we've seen in the wider cryptocurrency ecosystem. We can see this on the chart below, which quantifies the amount different types of scams have taken from victims in different countries on a per capita basis.



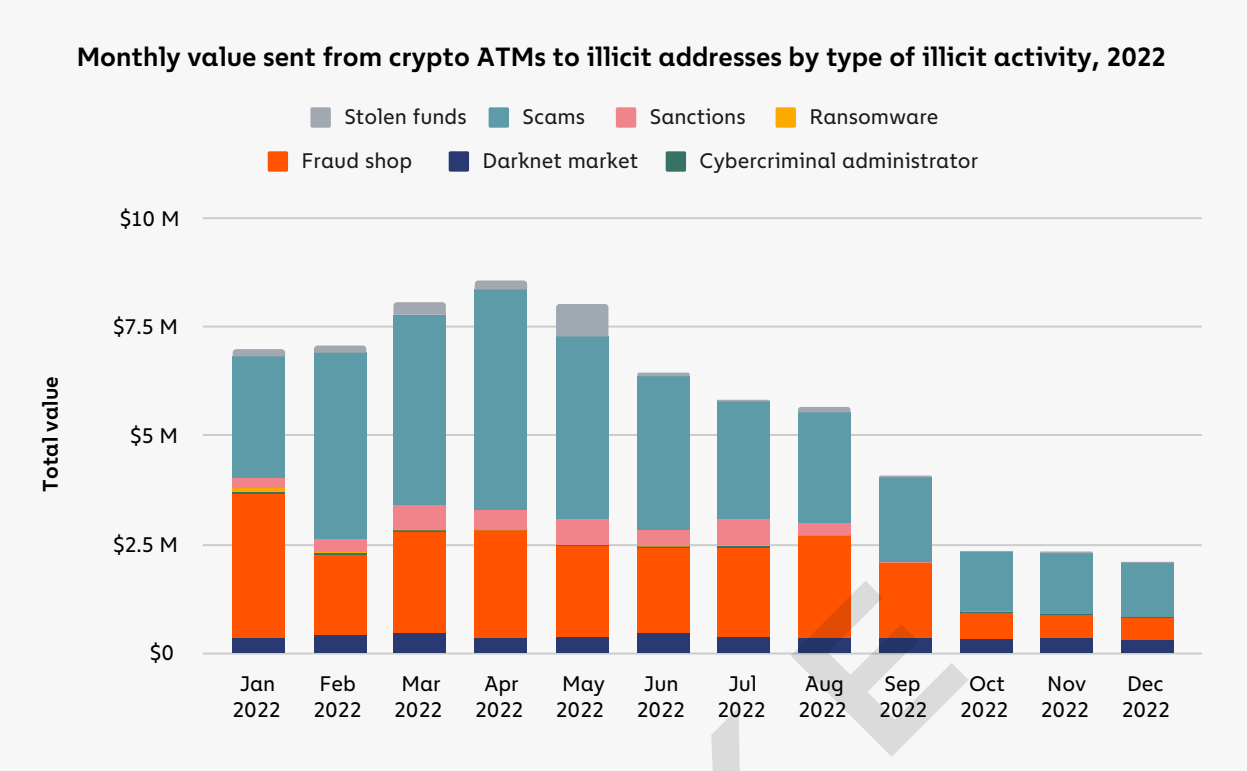
Most scam types disproportionately receive revenue from the U.S., but this is especially true for NFT-related scams. We've written previously about the fact that NFTs are especially popular in North America, particularly when it comes to onboarding new cryptocurrency users — who are probably more likely to fall for scams given they're less experienced in the space — so this doesn't come as a huge surprise. Investment scams, which are the largest type of scam by revenue, draw on a wider array of countries, with Australia and parts of South America being the hardest hit.

What services are these users relying on to send to scams?



The vast majority of victim payments to scams come from centralized exchanges. We also see scams receiving significant amounts from other illicit addresses, many of which are themselves other scams and could indicate that many distinct scams are actually controlled by the same individuals or groups, which is a topic we'll explore further below. DeFi protocols also send a significant amount to scams.

Our data also indicates that roughly 1.0% of victim payments to scams come from crypto ATMs. ATMs are an interesting category to dig into, as they aren't generally used to send funds to many other illicit address types — in fact, just 2.2% of funds sent from ATMs in 2022 went to illicit addresses, for a total of $67.5 million. However, a disproportionate share of that total goes to addresses associated with scams. Industry observers and law enforcement have noted this trend before, and blockchain analysis allows us to quantify it.



In 2022, crypto ATMs were used to send at least $35.3 million to scammers, which represents more than half of all funds sent to illicit addresses using ATMs. While the dollar figures represent lower-bound estimates, the disproportionate share of funds leaving ATMs for scam addresses may be a result of crypto scammers' targeting of those who are new to cryptocurrency and not technologically adept. For that audience, an ATM similar to the ones they use for fiat may offer what appears to be the easiest way to initiate a cryptocurrency transaction, as users can simply insert cash, type in a cryptocurrency address, and complete their transfer. The data indicates that crypto ATM businesses could better serve their customers and significantly reduce their exposure to illicit activity by educating customers on scams, or even taking steps to warn customers before they transfer funds to an address known to be associated with a scam.

Concentration in crypto scamming: Blockchain analysis indicates large scam networks may account for lots of fraudulent activity

We've often talked about how many forms of cryptocurrency-based crime appear to be driven primarily by small groups of prolific criminals despite what appear at first glance to be a large number of distinct on-chain entities participating in a given type of crime. For instance, in our ransomware section, we discuss how despite there being many ransomware strains active in any given year, a small group of ransomware affiliates are responsible for many of the attacks carried out by different strains, which we can see by analyzing those affiliates' wallets and observing that they receive cryptocurrency from many different strains.

Does the same thing hold true for crypto scams? We attempt to answer that question below by looking for evidence of on-chain interconnectedness between several different scam entities active in 2022. We'll also show how analysis of off-chain data — specifically, the copy on the public-facing websites associated with many crypto investment scams — can enable investigators to find more scams once they've identified one.

Our analysis starts with five crypto scams the CFTC identified and filed charges against in September 2022:

- Cryptostockoptionstrade Ltd
- Global Smart Option Broker Ltd
- Hypertradingoption Ltd
- Stockbrokertechniques Ltd.
- SprintTrade

The CFTC's press release doesn't explicitly state whether all five scams are believed to be controlled by the same individual or group, but it does note that they purport to be located at the same Los Angeles street address. That alone doesn't necessarily mean all of these scams are associated with the same individual or group — the idea of a scammer simply copying text from the website of another scam, such as the listed street address, doesn't seem to be out of the question. With that in mind, we decided to search the web for other websites of purported crypto investment companies whose websites contained identical copy to those of the scams in the CFTC press release — not just street addresses, but other pieces of web copy such as customer testimonials — and cross-reference them with our own data to see if textual analysis of scam websites could turn up other scams that may or may not be connected to the original five named by CFTC. Ultimately, we were able to find functioning websites and cryptocurrency addresses for three of the five scams named by CFTC, so those three were what we used as reference points to find more scams.

In total, this analysis uncovered another 200 confirmed scams whose websites contain pieces of copy identical to that of the three CFTC-identified scams for which we found active websites. In other words, website analysis led to a 66x increase in the number of scams uncovered. The grid below breaks down the newly identified scams by the specific website elements they had in common with the five scams in the CFTC press release.

Number of new scams identified	How we found them
88	Same street address as CFTC-identified scam
102	Identical customer testimonial as CFTC-identified scam

Right off the bat, we can see how scanning for websites with copy identical to that of known scam websites can be valuable, as we quickly unearthed an additional 200 scams. But again, that on its own doesn't prove that all 200 are run by the same individual or group, as it's entirely possible scammers are just stealing web copy from each other due to laziness, or even in an effort to throw investigators off and give the impression that their scam is the work of someone else. However, we can use blockchain analysis to find another commonality between scams in this set of 200 that could be a stronger indicator of interconnectedness or common control: Deposit address overlap.

As we discuss in our money laundering analysis, criminals dealing in cryptocurrency generally want to move their ill-gotten funds to a fiat off-ramp service where the crypto can be converted into cash — usually, this means a centralized exchange. If we see two scams moving their cryptocurrency to the same deposit address at an exchange, it means one of two things: Either one scammer controls the deposit address, meaning they are behind both scams, or the deposit address belongs to a nested service that's being used to launder funds — in that case, a single scammer may still be behind both scams and simply prefers to funnel funds from both to the same nested service, but it could also mean that two separate scammers simply happen to use the same service. So, while deposit address overlap isn't proof positive that two scams are controlled by the same individual or group, it certainly adds to the likelihood that they are.

Given that, our next step was to analyze the exchange deposit addresses to which all 203 scams had ever sent funds, and sort the scams into distinct, mutually exclusive **scam networks** based on deposit address overlap. For the purposes of this analysis, we consider two scams to be part of the same network if they sent any amount of cryptocurrency to the same deposit address. Two scams can also be part of the same scam network without depositing to the same deposit address if they are both connected to a third scam via another deposit address. In other words, if Scam A sends funds to Deposit Address 1 and Deposit Address 2, Scam B sends funds to Deposit Address 2 and Deposit Address 3, and Scam C sends funds to Deposit Address 3 and Deposit Address 4, then we would consider all three scams to be part of the same scam network. Scams that never deposited anything to an exchange were excluded from the analysis.

After applying this methodology to the 203 scams in our dataset — the original three identified by CFTC plus the 200 additional scams with website commonalities — we found that 73 of them had never deposited to an exchange. The remaining 130 fit into 43 distinct scam networks based on deposit address overlap, but ultimately, one network stood out above the rest.

Scam network	Number of distinct scams in network	Total revenue of all scams in network	Number of exchanges used by scams in network to cash out	Number of exchange deposit addresses used by network
1	86	$3,400,080	69	1667
2	1	$45,177	2	6
3	1	$42,868	3	7
4	1	$20,223	3	10
5	2	$17,133	3	5
6	1	$16,940	3	3
7	1	$16,882	1	3
8	1	$16,294	2	5
9	2	$15,384	3	6
10	1	$13,193	7	11
11	1	$11,401	1	1
12	1	$9,968	1	1
13	1	$8,489	7	16
14	1	$7,532	1	1
15	1	$6,817	5	8
16	1	$6,633	6	10
17	1	$6,375	2	3
18	1	$6,039	1	2
19	1	$5,848	2	4
20	1	$5,296	2	3
21	1	$3,650	1	1

Scam network	Number of distinct scams in network	Total revenue of all scams in network	Number of exchanges used by scams in network to cash out	Number of exchange deposit addresses used by network
22	1	$3,339	1	2
23	1	$3,210	5	43
24	1	$2,876	9	66
25	1	$2,823	1	3
26	1	$2,417	2	6
27	1	$2,105	1	1
28	1	$2,061	2	2
29	1	$2,015	1	2
30	1	$1,885	1	4
31	1	$1,773	1	1
32	1	$1,387	1	3
33	1	$1,080	1	2
34	1	$971	4	11
35	1	$831	1	3
36	1	$755	1	1
37	1	$295	1	2
38	1	$170	1	1
39	1	$150	2	2
40	1	$137	1	1
41	1	$123	1	1
42	1	$117	1	1
43	1	$110	1	2

Network 1 contains 86 active scams that have made a combined $3.4 million from victims, and utilize 1,667 total exchange deposit addresses. Interestingly, all of the scams identified in the CFTC press release that kicked off this analysis are part of Network 1 as well. Two of the remaining 42 networks are composed of two scams, while the rest only have one scam apiece. Overall, the 86 scams in Network 1 account for 91.6% of the total revenue of all 130 scams included.

We can't know from on-chain data alone whether the 86 scams in that network are each run by the same individual or group. The only way to know for sure would be for law enforcement to carry out an investigation, which would likely include sending subpoenas to the exchanges to which the scammers are depositing funds to see whose user accounts they're associated with. However, even if the scams in each network just coincidentally depend on the same nested services or money launderers to convert their crypto into cash, that would still be positive news for investigators, as it would mean that they could disrupt several scams at once by going after a small number of money laundering service providers.

Overall, our data suggests that the cryptocurrency scamming ecosystem is smaller than it appears at first glance. We look forward to applying our scam network methodology to a wider number of scams beyond the 203 included in this analysis, and will share insights from that expanded analysis where possible.

How investigators are fighting back against pig butchering scams

What are pig butchering scams?

One particularly sophisticated type of crypto scam, pig butchering, gained media attention in 2022. Analogized to fattening a pig before slaughter, pig butchering is a slow-burn scam focused on building trusting relationships. Most of these operations function in similar fashion. Scammers find targets with whom they develop relationships over time. They create fake social media accounts and dating site profiles showcasing lavish lifestyles and send random messages to connect with victims. Frequently used apps include WeChat, WhatsApp, and even LinkedIn.

While the scammers are relationship-building, they're also performing reconnaissance to see which victims have the most investment potential. Once targets are identified and trust is built, the scammer subtly mentions a crypto investment website with which they've had personal success.

Alastair McCready, Southeast Asia Editor at Vice World News says, "You're not getting an email saying 'there's a million dollars that needs releasing in a bank account in Switzerland.' This is just kind of subtle little messages, like on WhatsApp. And if you were the kind of person who was kind of looking for some sort of connection, you could see how you'd be easily lured in, sucked in by a seemingly innocuous conversation with a nice person."

Over weeks or months, scammers coach victims on how to use these fake sites, convincing them to invest everything they possibly can. These platforms falsify returns and make it appear as though victims have access to the funds. Initially, they can make withdrawals. Once scammers believe they've exhausted their victims' potential, they try convincing them to take out loans. When victims become wary, the scammer restricts access to funds and attempts to extort them for even more money.

Sadly, those on the receiving end of pig butchering are not the only victims. Most of these crimes originate in Southeast Asia and require human trafficking to run. Around 2016, a large construction project began in Sihanoukville, a coastal town in Cambodia. Chinese investors built hundreds of casinos to attract tourists from mainland China, where gambling is illegal. In 2019, Cambodia banned online gambling and then COVID-19 hit, devastating Sihanoukville's tourist economy. Many businesses turned to criminal activity to generate revenue; some recruited workers for customer service jobs under false pretenses. On arrival, new employees were ushered into hotel casino complexes — now walled, guarded compounds — and weren't allowed to leave. Casino-based scam centers like these are also found in Laos and Myanmar.

As for pig butchering scam victim profiles, those run the gamut from elderly to millennial and across genders, too. Asian Americans are often targeted because it's easier for scammers to communicate with them using a common language. Pig butchering also preys on people's kindness and vulnerability; one woman was targeted after she responded to a Facebook ad about adopting a dog.

How the REACT Task Force and Santa Clara County are helping victims

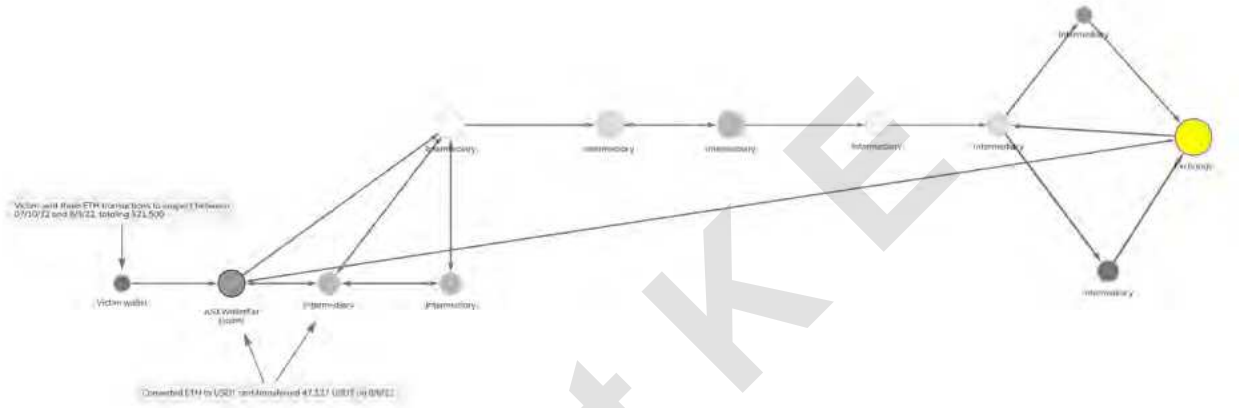
Agents from California's Regional Enforcement Allied Computer Team (REACT) investigated several pig butchering scams last year; to date it has investigated over 50 cases. Comprised of local, state, and federal agencies covering five counties in the Bay Area, the REACT task force, including Santa Clara County's Deputy District Attorney, Erin West, is demonstrating how law enforcement can successfully conduct crypto crime investigations and recover funds for victims.

Rather than shutting down easily-replaceable websites or trying to arrest overseas scammers in problematic jurisdictions, REACT's main goals are to quickly assess stolen funds by tracing the victim's initial transfer out of an exchange or wallet to a suspect, and attempt to effect a seizure. When tracing funds during investigations, the agency doesn't dwell on pass-through wallets; it targets those containing funds that it can directly attribute to victims as California law states that law enforcement can only seize funds that meet that criteria.

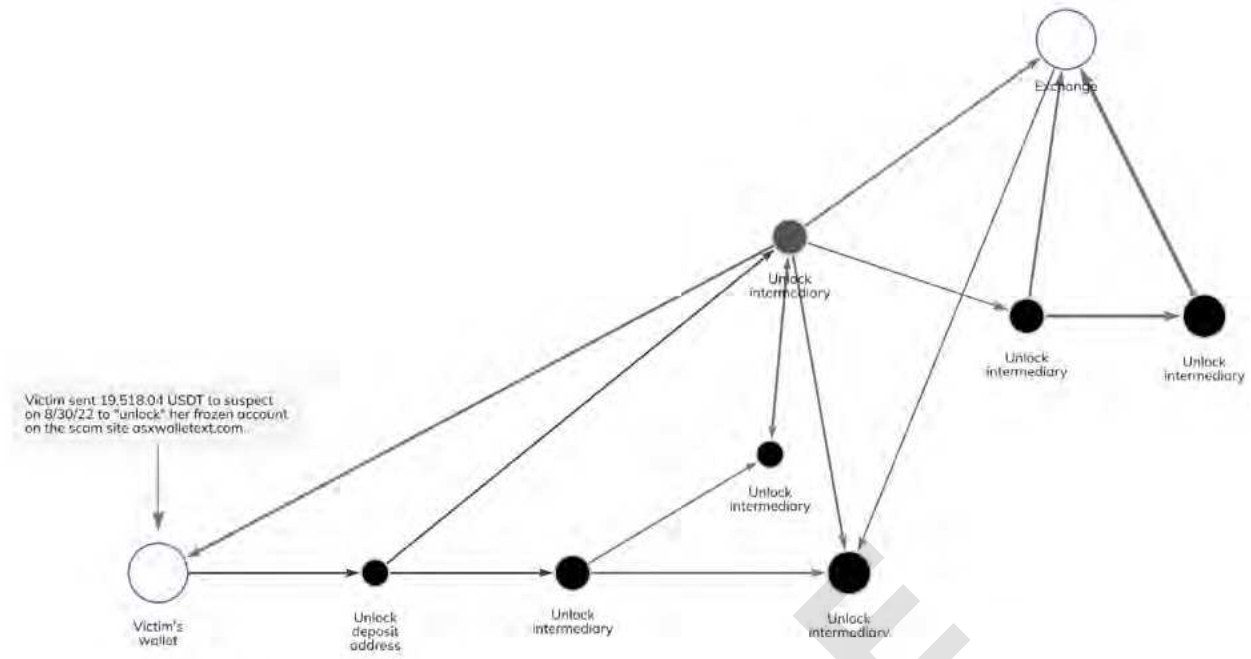
Since many citizens and even law enforcement agencies believe that crypto transactions aren't traceable, these investigations are full of unique challenges. REACT detective Chris Vigil says that when crypto scams affecting private individuals occur, investigators don't typically get involved until weeks or months later — victims often don't realize they have any recourse or don't know where to go for help. Meanwhile, most local law enforcement doesn't have the resources to investigate these

crimes. However, in cases where victims do reach out to more than one agency, deconflicting information poses a substantial challenge.

To successfully investigate crypto scams requires tools that help law enforcement trace funds in order to effect seizure. The graph below illustrates how REACT tracks cryptocurrency transactions for a typical pig butchering scam, and demonstrates how bad actors transfer funds through intermediary wallets in order to move them to an exchange. In this case, the victim transferred cryptocurrency to wallets associated with four different versions of the same scam over a period of months. By following transfers across intermediary wallets, the investigation tied different pig butchering sites together, too.



Between July 10 and August 3, 2022, the victim sent three ETH transactions to the fraudulent investment site ASXWalletExt.com, totaling almost $21,500. From there, the suspect converted the ETH to USDT and transferred funds to various intermediary wallets with exposure to three other investment scam sites. They later cashed out funds at an exchange. Next, the scammer extorted the victim further, saying they would "unlock" her frozen account on ASXWalletExt.com, compelling her to send roughly $19,500 USDT from her exchange account, as we see on the second graph below. By tracing subsequent transactions across intermediate addresses, REACT observed the suspect cashing out at a large exchange.



Once REACT agents are able to obtain judicial authorization for a seizure, the cryptocurrency is then transferred to a government-controlled account. When the funds are secured, the case is referred to West who works with the courts to release the funds to the rightful owner. To date, REACT and Santa Clara County have recovered funds in 15 of the pig butchering cases they have investigated. While the organization can only work cases with a victim or suspect in its jurisdiction, it often advises adjacent agencies and others across the country, too. REACT sees education and resources as the biggest roadblocks for law enforcement in investigating crypto crimes, but believes there are ways for more agencies to get involved. Having the statutory authority to effect seizures and obtaining buy-in from leadership — along with backing from prosecutors — are key to getting started. Then having the right policies in place to conduct investigations and using robust blockchain analysis tools to trace funds are essential for success.

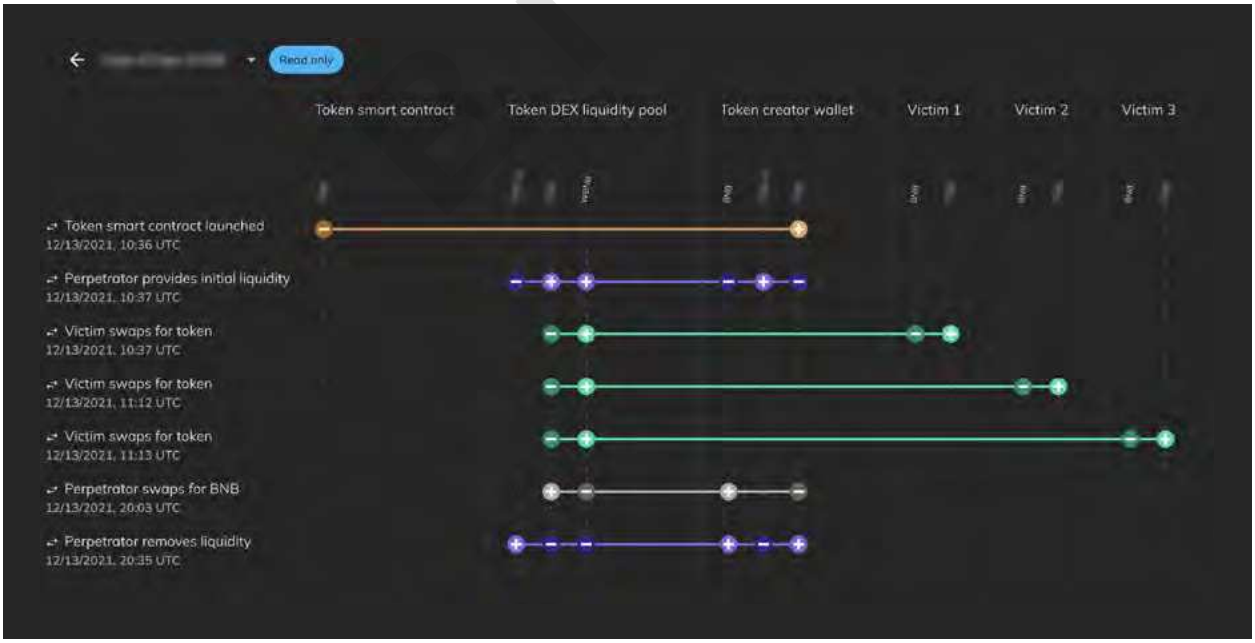
Pump and Dump Tokens

24% of New Tokens Launched in 2022 Bear On-Chain Characteristics of Pump and Dump Schemes

Pump and dump schemes in traditional finance are quite simple: Holders of a tradable asset, such as stock in a company, will heavily promote the asset to other investors, often using misleading statements, causing the price to rise rapidly as new investors buy. The holders will then sell their overvalued shares at a profit, causing the price to plummet, leaving the newer investors stuck with a low-value asset.

Unfortunately, pump and dump schemes have also become common in the crypto world. This is largely due to the relative ease with which bad actors can launch a new token and establish an artificially high price and market capitalization for it "on paper" by seeding the initial trade volume and controlling the circulating supply. Additionally, teams launching new projects and tokens can remain anonymous, which makes it possible for serial offenders to carry out multiple pump and dump schemes.

We can see an example of what a typical pump and dump scheme looks like on-chain below in Chainalysis Storyline, using an undisclosed token example. The token bears all the telltale signs of a pump and dump scheme, with the asset's price dropping 90% in the first week of trading following the token creator dumping their holdings.



The token provides a good model for how pump and dump tokens work. The creator launched this token's smart contract and funded a new liquidity pool for it on a popular DEX in December 2021, after promoting the launch to crypto enthusiasts on social media. Hundreds of victims bought the token on that DEX, allowing the price to rise quickly in a matter of hours. However, within the same day of launch, the creator sold off all of his tokens, leaving buyers holding the bag. Overall, the perpetrator made just under $20,000.

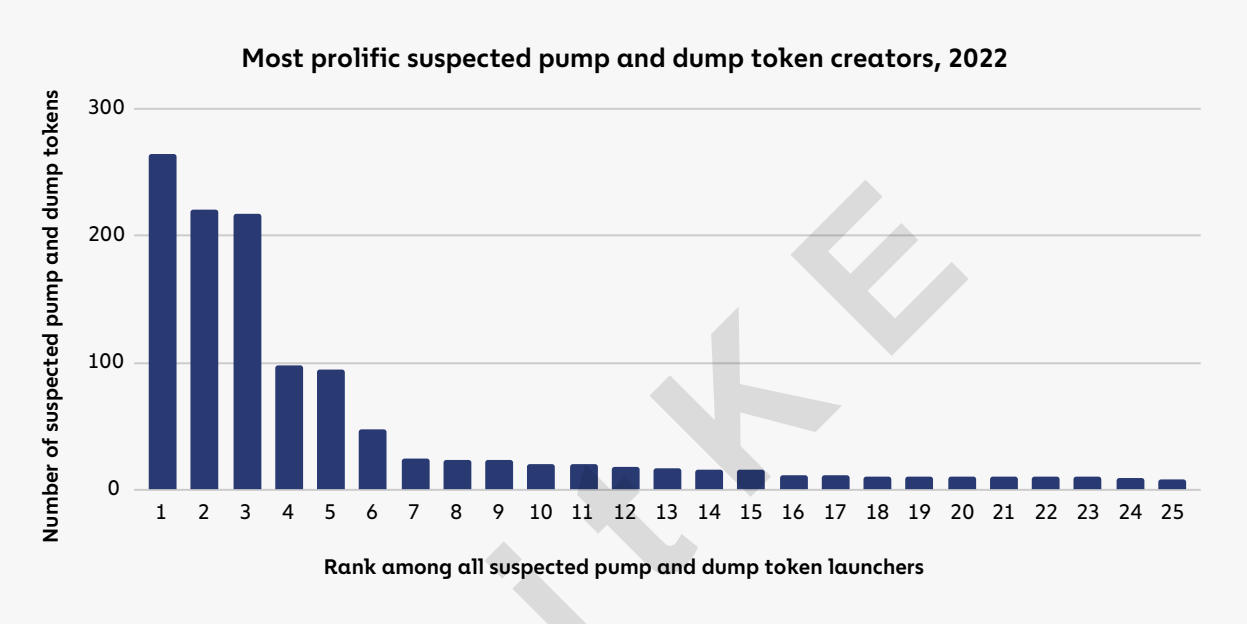
Below, we attempt to quantify the scale of pump and dump schemes in cryptocurrency by analyzing all tokens launched on the Ethereum and BNB blockchains in 2022. While more than 1.1 million tokens were launched last year, **the vast majority got virtually no traction**, as measured by the frequency of swapping happening on DEXes. Since we want to focus on projects that had an impact on the crypto ecosystem, we'll only count tokens that achieved a minimum of ten swaps and four consecutive days of trading in the week following their launch. With that criteria in place, the number of new tokens falls from 1.1 million to 40,521.

The next criteria we'll look for is a drastic price decline of 90% or more in the first week of trading, which could suggest the token's originators and earliest holders dumped the token extremely quickly, making it a relatively strict standard for assessing a token as a possible pump and dump. **Of the 40,521 tokens launched in 2022 that gained sufficient traction to be worth analyzing, 9,902, or 24%, saw a price decline in the first week indicative of possible pump and dump activity.**

	Number of tokens	Percent of all tokens launched
Total tokens launched	1,105,239	100.0%
Tokens with over 10 swaps and 4 consecutive trading days in first week after launch	40,521	3.7%
Tokens with a 90% price drop in first week after launch	9,902	0.9% (24% of tokens that got traction)

It's possible, of course, that in some cases, teams involved with token launches did their best to form a healthy offering, and the subsequent drop in price was simply due to market forces and challenges stemming from less established infrastructure for market creation in the digital asset space. While it's impossible to know the promotional strategy or intentions behind all 9,902 tokens, we did check the 25 with the biggest first-week price drop on Token Sniffer, a service that scores new tokens on a scale of zero to 100 based on their trustworthiness and docks points for any scam-like characteristics. According to Token Sniffer, those 25 tokens all scored zero, indicating that, according to Token Sniffer's evaluation criteria, they were almost certainly designed for a pump and dump. Token Sniffer also found that many of them contained malicious "honeypot" code that prevents new buyers from selling the token — one of the surest possible signs that the coin is part of a pump and dump scheme.

In total, buyers not believed to be associated with the tokens' creators spent a total of $4.6 billion worth of cryptocurrency acquiring some of the 9,902 suspected pump and dump tokens we identified — a relatively trivial amount compared to the trillions in crypto transaction volume in 2022, but still a substantial amount of damage for unsuspecting investors. We estimate that the creators of these tokens made a total of $30 million in profits from selling off their holdings before the tokens' value plummeted. In many cases, the same wallet provided initial liquidity for several tokens that fit our pump and dump criteria, or provided funding to the wallet that did, suggesting those wallets share common ownership. Using this methodology, we found that 445 individuals or groups accounted for 24% of the 9,902 suspected pump and dump tokens launched in 2022.



The most prolific suspected pump and dump token creator we identified launched 264 tokens that fit our criteria in 2022.

Pump and dump schemes are uniquely destructive in the cryptocurrency world due to the ease with which new tokens can be launched and the social media-driven nature of crypto investment news and discussion. Many believe that cryptocurrency is approaching an inflection point that could spark mass adoption, but that could be difficult if the general public perceives cryptocurrency as rife with pump and dump schemes designed to prey on newcomers. We look forward to working with our partners in both the public and private sectors to investigate this activity and build a safer ecosystem in the future.

Chainalysis

Thanks for reading the 2023 Crypto Crime Report

Chainalysis Authors

Kim Grauer
Director of Research

Eric Jardine
Cybercrimes Research Lead

Erin Leosz
Content Marketing Manager

Henry Updegrave
Senior Content Marketing Manager

Chainalysis

Building trust in blockchains

About 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 in over 70 countries. Our data powers investigation, compliance, and market intelligence software that has been used to solve some of the world's most high-profile criminal cases and grow consumer access to cryptocurrency safely. Backed by Accel, Addition, Benchmark, Coatue, GIC, Paradigm, Ribbit, and other leading firms in venture capital, Chainalysis builds trust in blockchains to promote more financial freedom with less risk. For more information, visit www.chainalysis.com.

FOR MORE INSIGHTS
blog.chainalysis.com

GET IN TOUCH
info@chainalysis.com

FOLLOW US ON TWITTER
@chainalysis

FOLLOW US ON LINKEDIN
linkedin.com/company/chainalysis