Chainalysis

February 2022

The 2022 Crypto Crime Report

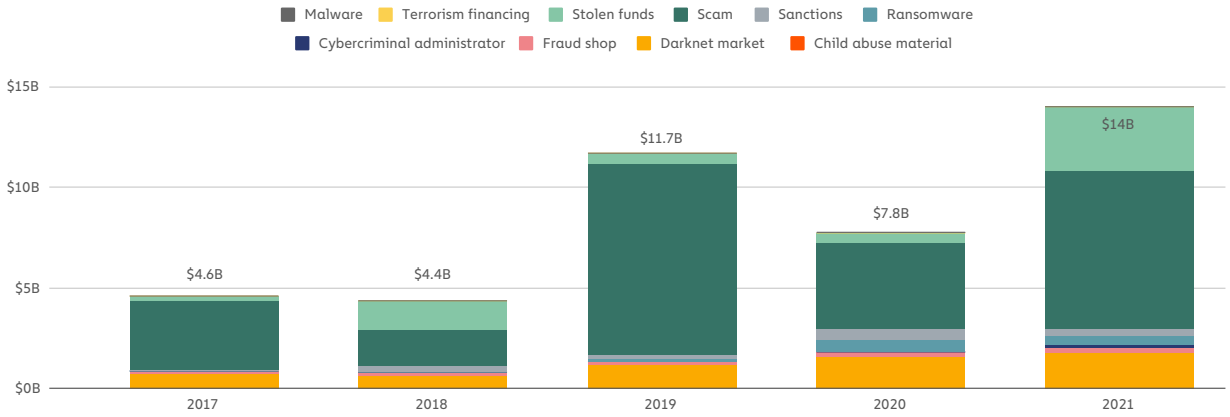
Original data and research into cryptocurrency-based crime

Introduction

Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-time Low in Share of All Cryptocurrency Activity

Cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020.

Total cryptocurrency value received by illicit addresses | 2017–2021

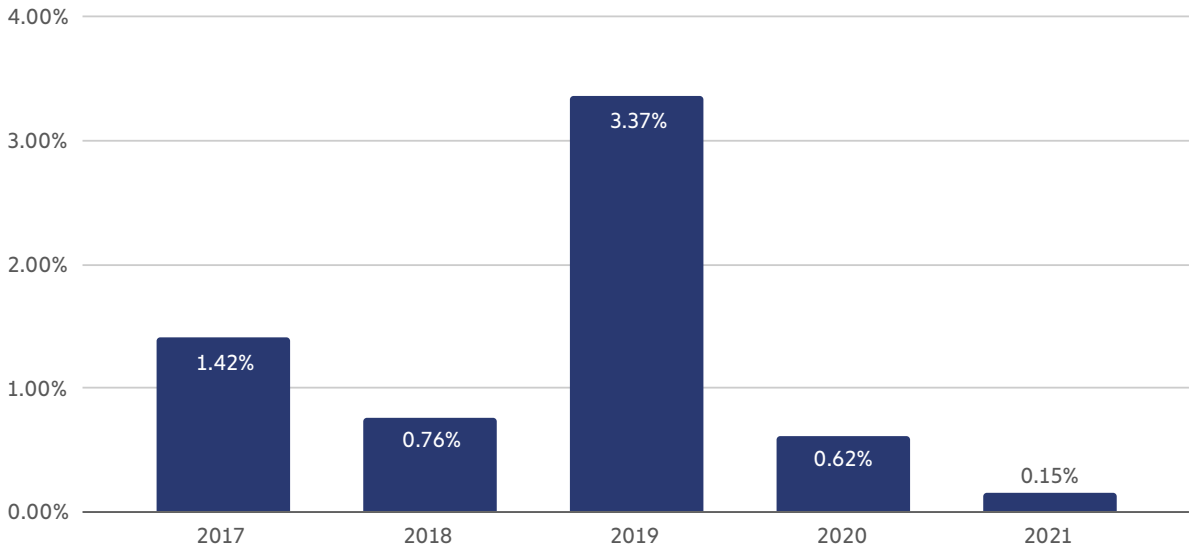


Note: "Cybercriminal administrator" refers to addresses that have been attributed to individuals connected to a cybercriminal organization, such as a darknet market.

But those numbers don't tell the full story. Cryptocurrency usage is growing faster than ever before. Across all cryptocurrencies tracked by Chainalysis, total transaction volume grew to $15.8 trillion in 2021, up 567% from 2020's totals. Given that roaring adoption, it's no surprise that more cybercriminals are using cryptocurrency. But the fact that the increase in illicit transaction volume was just 79% — nearly an order of magnitude lower than overall adoption — might be the biggest surprise of all.

In fact, with the growth of legitimate cryptocurrency usage far outpacing the growth of criminal usage, illicit activity's share of cryptocurrency transaction volume has never been lower.

Illicit share of all cryptocurrency transaction volume | 2017–2021



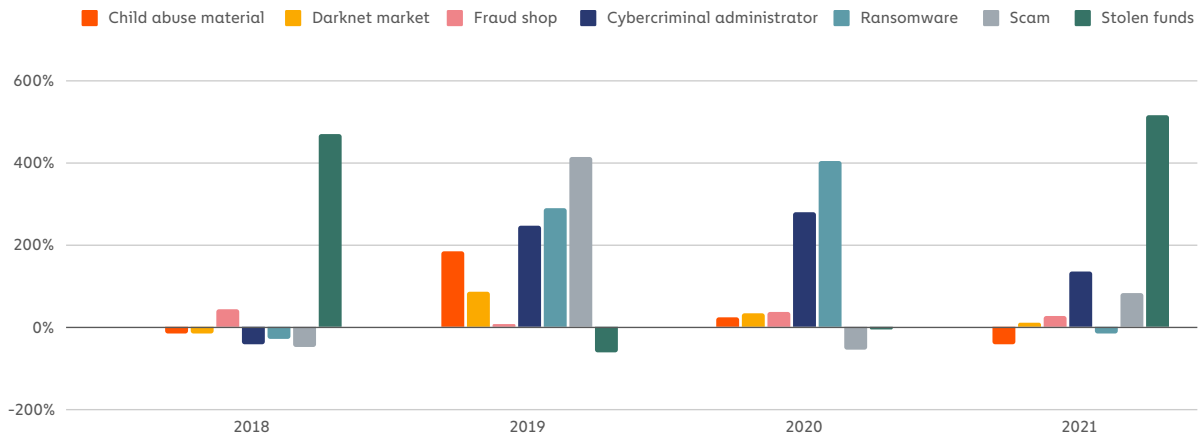
Transactions involving illicit addresses represented just 0.15% of cryptocurrency transaction volume in 2021 despite the raw value of illicit transaction volume reaching its highest level ever. As always, we have to caveat this figure and say that it is likely to rise as Chainalysis identifies more addresses associated with illicit activity and incorporates their transaction activity into our historical volumes. For instance, we found in our last Crypto Crime Report that 0.34% of 2020's cryptocurrency transaction volume was associated with illicit activity — we've now raised that figure to 0.62%. Still, the yearly trends suggest that with the exception of 2019 — an extreme outlier year for cryptocurrency-based crime largely due to the PlusToken Ponzi scheme — crime is becoming a smaller and smaller part of the cryptocurrency ecosystem. Law enforcement's ability to combat cryptocurrency-based crime is also evolving. We've seen several examples of this throughout 2021, from the CFTC filing charges against several investment scams, to the FBI's takedown of the prolific REvil ransomware strain, to OFAC's sanctioning of Suex and Chatex, two Russia-based cryptocurrency services heavily involved in money laundering.

However, we also have to balance the positives of the growth of legal cryptocurrency usage with the understanding that $14 billion worth of illicit activity represents a significant problem. Criminal abuse of cryptocurrency creates huge impediments for continued adoption, heightens the likelihood of restrictions being imposed by governments, and worst of all victimizes innocent people around the world. In this report, we'll explain exactly how and where cryptocurrency-based crime increased, dive into the latest trends amongst different types of cybercriminals, and tell you how cryptocurrency businesses and law enforcement agencies around the world are responding. But first, let's look at a few of the key trends in cryptocurrency-based crime.

DeFi's rise leads to new opportunities in crypto crime

What's changed in the last year? Let's start by looking at what types of cryptocurrency-based crime increased the most in 2021 by transaction volume.

Year over year percent change in value received by crime type | 2018–2021



Two categories stand out for their growth: stolen funds and, to a lesser degree, scams. DeFi is a big part of the story for both.

Let's start with scams. Scamming revenue rose 82% in 2021 to $7.8 billion worth of cryptocurrency stolen from victims. Over $2.8 billion of this total — which is nearly equal to the increase over 2020's total — came from rug pulls, a relatively new scam type in which developers build what appear to be legitimate cryptocurrency projects — meaning they do more than simply set up wallets to receive cryptocurrency for, say, fraudulent investing opportunities — before taking investors' money and disappearing. Please keep in mind as well that these figures for rug pull losses represent only the value of investors' funds that were stolen, and not losses from the DeFi tokens' subsequent loss of value following a rug pull.

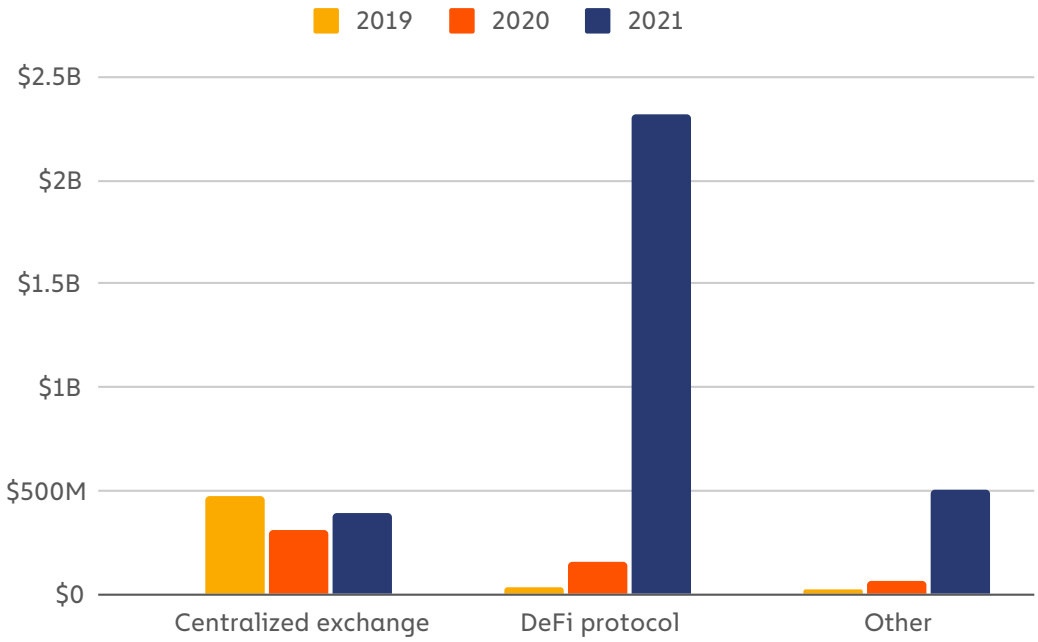
We should note that roughly 90% of the total value lost to rug pulls in 2021 can be attributed to one fraudulent centralized exchange, Thodex, whose CEO disappeared soon after the exchange halted users' ability to withdraw funds. However, every other rug pull tracked by Chainalysis in 2021 involved DeFi projects. In nearly all of these cases, developers have tricked investors into purchasing tokens associated with a DeFi project before draining the tools provided by those investors, sending the token's value to zero in the process.

We believe rug pulls are common in DeFi for two related reasons. One is the hype around the space. DeFi transaction volume has grown 912% in 2021, and the incredible returns on

decentralized tokens like Shiba Inu have many excited to speculate on DeFi tokens. At the same time, it's very easy for those with the right technical skills to create new DeFi tokens and get them listed on exchanges, even without a code audit. A code audit is a process by which a third-party firm or listing exchange analyzes the code of the smart contract behind a new token or other DeFi project, and publicly confirms that the contract's governance rules are iron clad and contain no mechanisms that would allow for the developers to make off with investors' funds. Many investors could likely have avoided losing funds to rug pulls if they'd stuck to DeFi projects that have undergone a code audit – or if DEXes required code audits before listing tokens.

Cryptocurrency theft grew even more, with roughly $3.2 billion worth of cryptocurrency stolen in 2021 — a 516% increase compared to 2020. Roughly $2.2 billion of those funds — 72% of the 2021 total — were stolen from DeFi protocols. The increase in DeFi-related thefts represents the acceleration of a trend we identified in last year's Crypto Crime report.

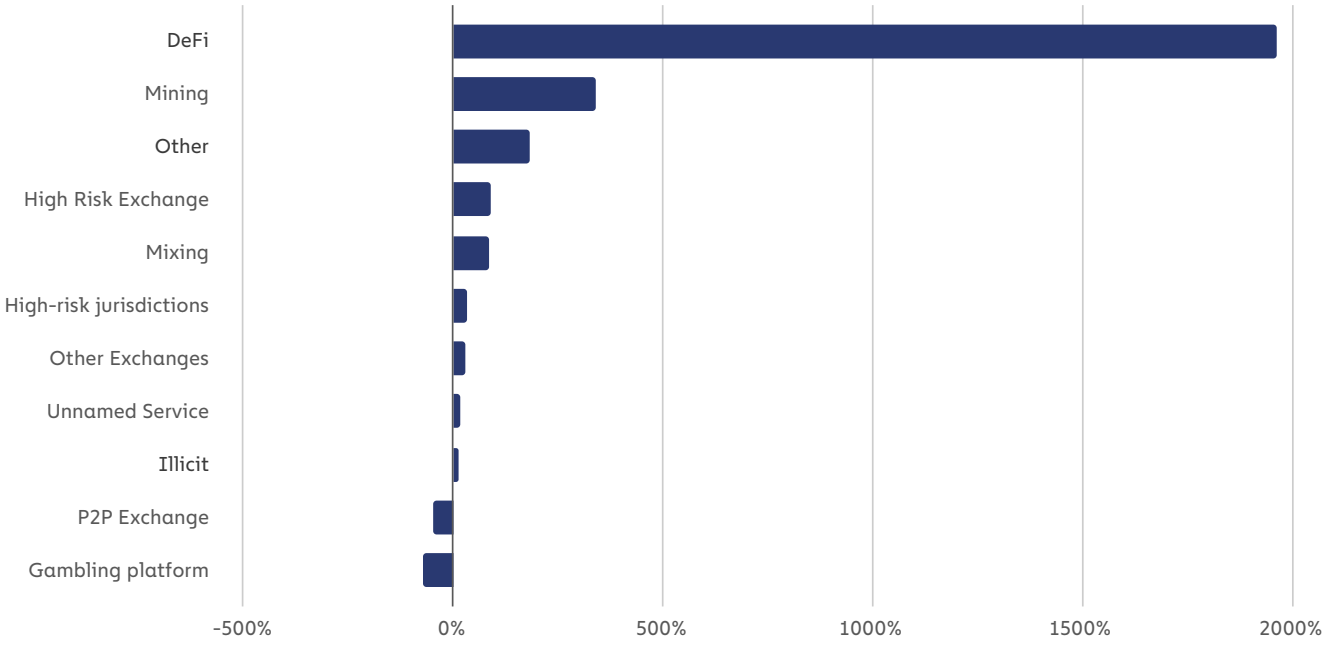
Annual total cryptocurrency stolen by victim type | JAN '19–DEC '21



In 2020, just under $162 million worth of cryptocurrency was stolen from DeFi platforms, which was 31% of the year's total amount stolen. That alone represented a 335% increase over the total stolen from DeFi platforms in 2019. In 2021, that figure rose another 1,330%. In other words, as DeFi has continued to grow, so too has its issue with stolen funds. As we'll explore in more detail later in the report, most instances of theft from DeFi protocols can be traced back to errors in the smart contract code governing those protocols, which hackers exploit to steal funds, similar to the errors that allow rug pulls to occur.

We've also seen significant growth in the usage of DeFi protocols for laundering illicit funds, a practice we saw scattered examples of in 2020 and that became more prevalent in 2021. Check out the graph below, which looks at the growth in illicit funds received by different types of services in 2021 compared to 2020.

Year over year percentage growth in value received by service from illicit addresses
2020–2021



DeFi protocols saw the most growth by far in usage for money laundering at 1,964%.

DeFi is one of the most exciting areas of the wider cryptocurrency ecosystem, presenting huge opportunities to entrepreneurs and cryptocurrency users alike. But DeFi is unlikely to realize its full potential if the same decentralization that makes it so dynamic also allows for widespread scamming and theft. One way to combat this is better communication — both the private and public sectors have an important role to play in helping investors learn how to avoid dubious projects. In the longer term, the industry may also need to take more drastic steps to prevent tokens associated with potentially fraudulent or unsafe projects from being listed on major exchanges.

Illicit cryptocurrency balances are growing. What can law enforcement do?

One promising development in the fight against cryptocurrency-related crime is the growing ability of law enforcement to seize illicitly obtained cryptocurrency. In November

2021, for instance, the IRS Criminal Investigations announced that it had seized over $3.5 billion worth of cryptocurrency in 2021 — all from non-tax investigations — representing 93% of all funds seized by the division during that time period. We've also seen several examples of successful seizures by other agencies, including $56 million seized by the Department of Justice in a cryptocurrency scam investigation, $2.3 million seized from the ransomware group behind the Colonial Pipeline attack, and an undisclosed amount seized by Israel's National Bureau for Counter Terror Financing in a case related to terrorism financing.

This raises an interesting question: How much cryptocurrency are criminals currently holding? It's impossible to know for sure, but we can estimate based on the current holdings of addresses Chainalysis has identified as associated with illicit activity. As of early 2022, illicit addresses hold at least $10 billion worth of cryptocurrency, with the vast majority of this held by wallets associated with cryptocurrency theft. Addresses associated with darknet markets and with scams also contribute significantly to this figure. As we'll explore later in this report, much of this value comes not from the initial amount derived from criminal activity, but from subsequent price increases of the crypto assets held.

We believe it's important for law enforcement agencies to understand these estimates as they build out their blockchain-based investigative capabilities, and especially as they develop their ability to seize illicit cryptocurrency.

Let's make cryptocurrency safer

DeFi-related crime and criminal cryptocurrency balances are just one area of focus for this report. We'll also look at the latest data and trends on other forms of cryptocurrency-based crime, including:

- The ongoing threat of ransomware
- Cryptocurrency-based money laundering
- Nation state actors' role in cryptocurrency-based crime
- Illicit activity in NFTs

  And much more!

As cryptocurrency continues to grow, it's imperative that the public and private sectors work together to ensure that users can transact safely, and that criminals can't abuse these new assets. We hope that this report can contribute to that goal, and equip law enforcement, regulators, and compliance professionals with the knowledge to more effectively prevent, mitigate, and investigate cryptocurrency-based crime.

Money Laundering

DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate

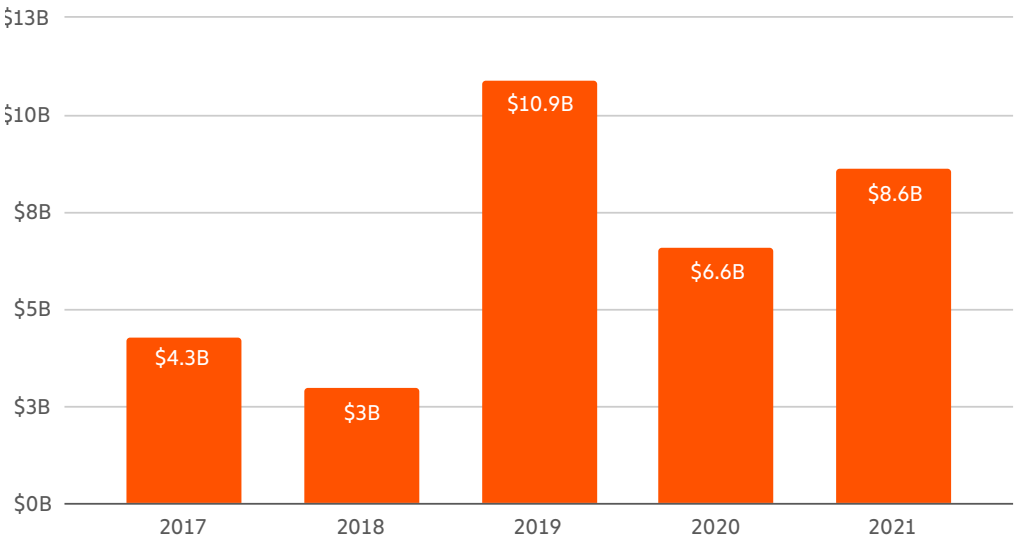
Cybercriminals dealing in cryptocurrency share one common goal: Move their ill-gotten funds to a service where they can be kept safe from the authorities and eventually converted to cash. That's why money laundering underpins all other forms of cryptocurrency-based crime. If there's no way to access the funds, there's no incentive to commit crimes involving cryptocurrency in the first place.

Money laundering activity in cryptocurrency is also heavily concentrated. While billions of dollars' worth of cryptocurrency moves from illicit addresses every year, most of it ends up at a surprisingly small group of services, many of which appear purpose-built for money laundering based on their transaction histories. Law enforcement can strike a huge blow against cryptocurrency-based crime and significantly hamper criminals' ability to access their digital assets by disrupting these services. We saw an example of this last year, when the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned two of the worst-offending money laundering services — Suex and Chatex — for accepting funds from ransomware operators, scammers, and other cybercriminals. But as we'll explore below, many other money laundering services remain active.

2021 cryptocurrency money laundering activity summarized

Overall, going by the amount of cryptocurrency sent from illicit addresses to addresses hosted by services, cybercriminals laundered $8.6 billion worth of cryptocurrency in 2021.

Total cryptocurrency value laundered by year | 2017–2021

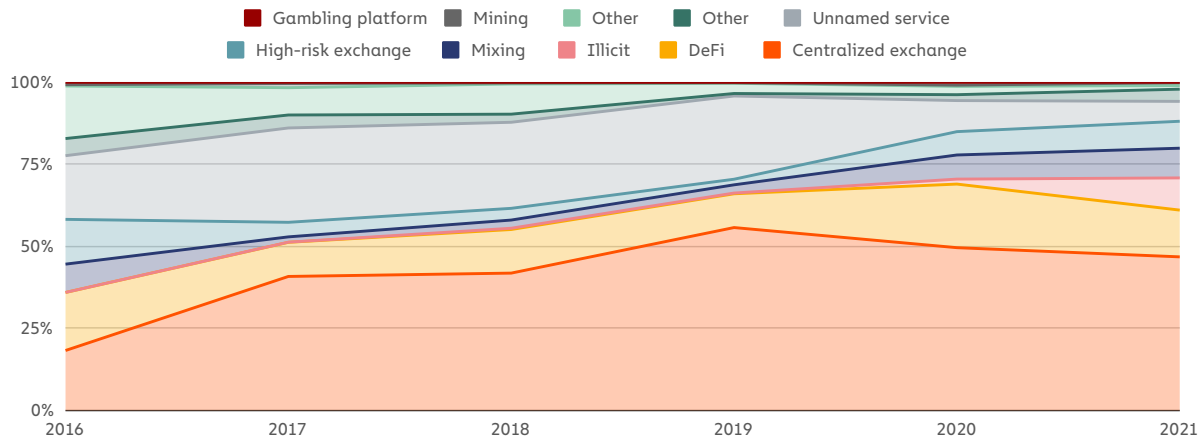


That represents a 30% increase in money laundering activity over 2020, though such an increase is unsurprising given the significant growth of both legitimate and illicit cryptocurrency activity in 2021. We also need to note that these numbers only account for funds derived from "cryptocurrency-native" crime, meaning cybercriminal activity such as darknet market sales or ransomware attacks in which profits are virtually always derived in cryptocurrency rather than fiat currency. It's more difficult to measure how much fiat currency derived from offline crime — traditional drug trafficking, for example — is converted into cryptocurrency to be laundered. However, we know anecdotally this is happening, and later in this section provide a case study showing an example of it.

Overall, cybercriminals have laundered over $33 billion worth of cryptocurrency since 2017, with most of the total over time moving to centralized exchanges. For comparison, the UN Office of Drugs and Crime estimates that between $800 billion and $2 trillion of fiat currency is laundered each year — as much as 5% of global GDP. For comparison, money laundering accounted for just 0.05% of all cryptocurrency transaction volume in 2021. We cite those numbers not to try and minimize cryptocurrency's crime-related issues, but rather to point out that money laundering is a plague on virtually all forms of economic value transfer, and to help law enforcement and compliance professionals be aware of just how much money laundering activity could theoretically move to cryptocurrency as adoption of the technology increases.

The biggest difference between fiat and cryptocurrency-based money laundering is that, due to the inherent transparency of blockchains, we can more easily trace how criminals move cryptocurrency between wallets and services in their efforts to convert their funds into cash. What kinds of cryptocurrency services do criminals rely on for this?

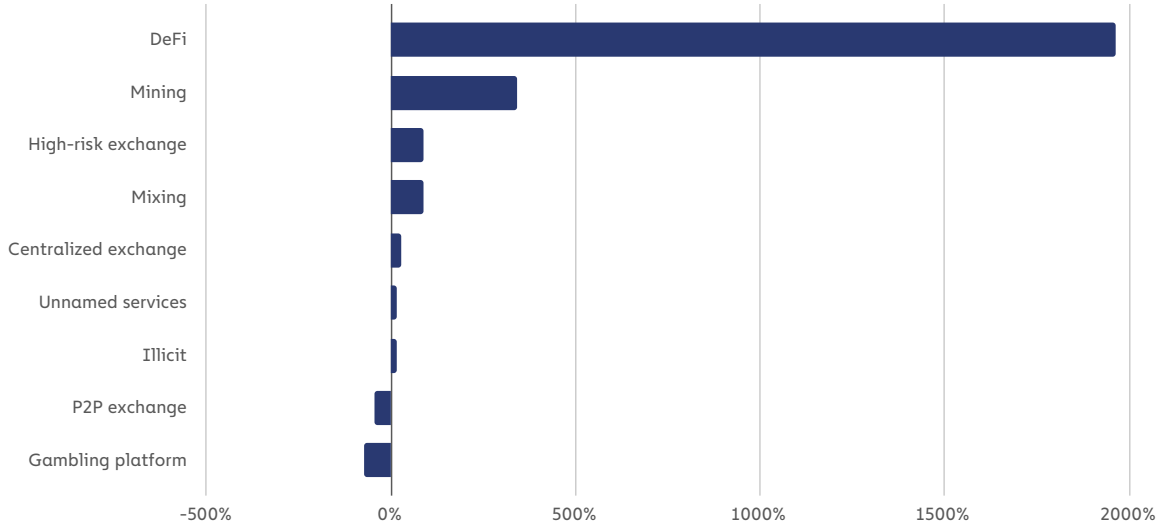
Destination of funds leaving illicit addresses | 2016–2021



For the first time since 2018, centralized exchanges didn't receive the majority of funds sent by illicit addresses last year, instead taking in just 47%. Where did cybercriminals

send funds instead? DeFi protocols make up much of the difference. DeFi protocols received 17% of all funds sent from illicit wallets in 2021, up from 2% the previous year.

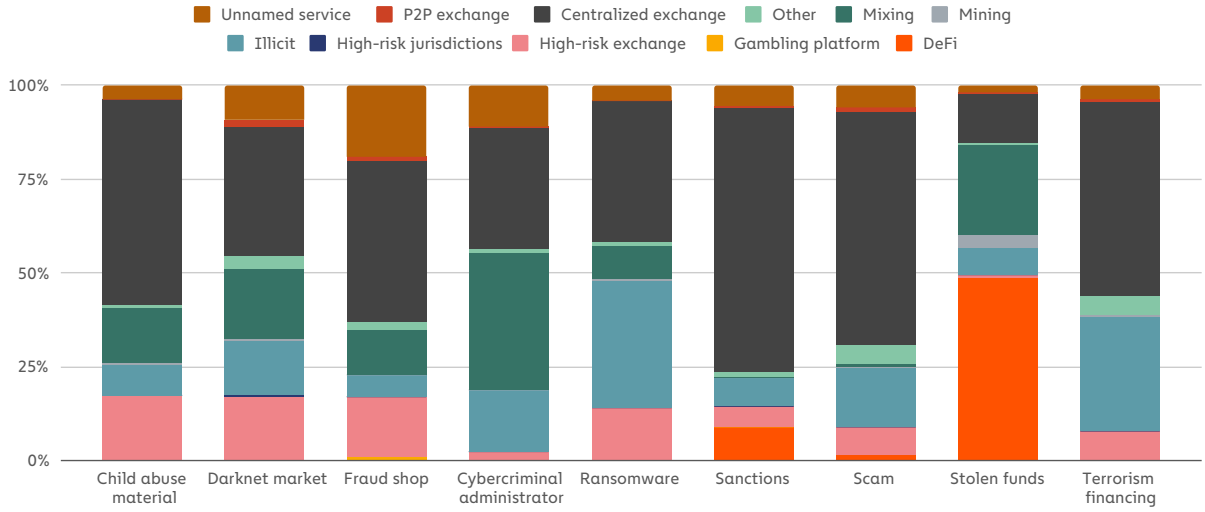
Year over year percentage growth in value received from illicit addresses by service category | 2020–2021



That translates to a 1,964% year-over-year increase in total value received by DeFi protocols from illicit addresses, reaching a total of $900 million in 2021. Mining pools, high-risk exchanges, and mixers also saw substantial increases in value received from illicit addresses as well.

We also see patterns in which types of services different types of cybercriminals use to launder cryptocurrency.

Destination of funds leaving illicit addresses by crime type | 2021



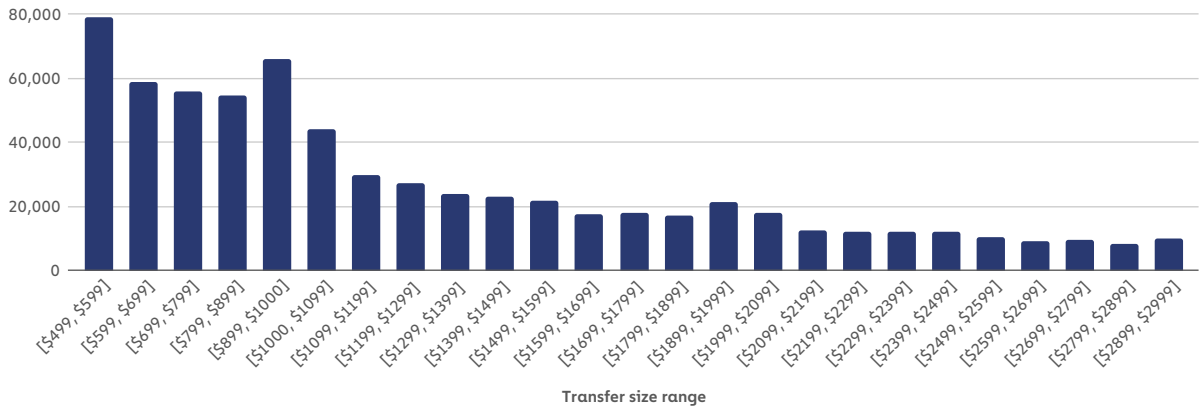
One thing that stands out is the difference in laundering strategies between the two highest-grossing forms of cryptocurrency-based crime in 2021: Theft and scamming.

Addresses associated with theft sent just under half of their stolen funds to DeFi platforms — over $750 million worth of cryptocurrency in total. North Korea-affiliated hackers in particular, who were responsible for $400 million worth of cryptocurrency hacks last year, used DeFi protocols for money laundering quite a bit. This may be related to the fact that more cryptocurrency was stolen from DeFi protocols than any other type of platform last year. We also see a substantial amount of mixer usage in the laundering of stolen funds.

Scammers, on the other hand, send the majority of their funds to addresses at centralized exchanges. This may reflect scammers' relative lack of sophistication. Hacking crypto-currency platforms to steal funds takes more technical expertise than carrying out most scams we observe, so it makes sense that those cybercriminals would employ a more advanced money laundering strategy.

We also need to reiterate that we can't track all money laundering activity by measuring the value sent from known criminal addresses. As stated above, some criminals use cryptocurrency to launder funds from crimes that happen offline, and there are many criminal addresses in use that have yet to be identified. However, we can account for some of these more obscured instances of money laundering by looking for transaction patterns suggesting that users were trying to avoid compliance screens. For instance, due to regulations like the Travel Rule, cryptocurrency businesses in many countries must conduct additional compliance checks, reporting, and information sharing related to transactions above $1,000 USD in value. As you might expect, illicit addresses send a disproportionate number of transfers to exchanges just below that $1,000 threshold.

Number of transfers from illicit addresses to exchanges by transfer size | 2021

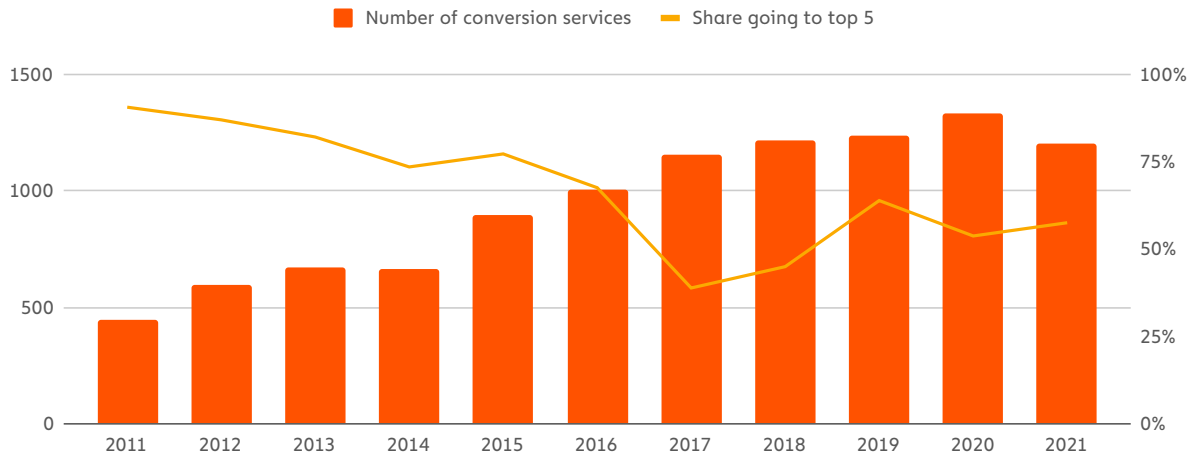


Exchanges using Chainalysis would be able to see that these funds are coming from illicit addresses regardless of transfer size. But more generally, compliance teams should consider treating users who consistently send or receive transactions of that size with extra scrutiny. Repeated instances of transactions just below the threshold may indicate users are doing what's known as structuring, meaning purposely breaking up large payments into smaller ones just below reporting thresholds in order to fool compliance teams.

Money laundering activity remains highly concentrated in 2021, but less so than in 2020

As we've discussed previously, money laundering activity is heavily concentrated to just a few services. We can see how that concentration has changed over time below.

Share of illicit cryptocurrency moving to top five services and total number of unique services receiving illicit cryptocurrency | 2011–2021

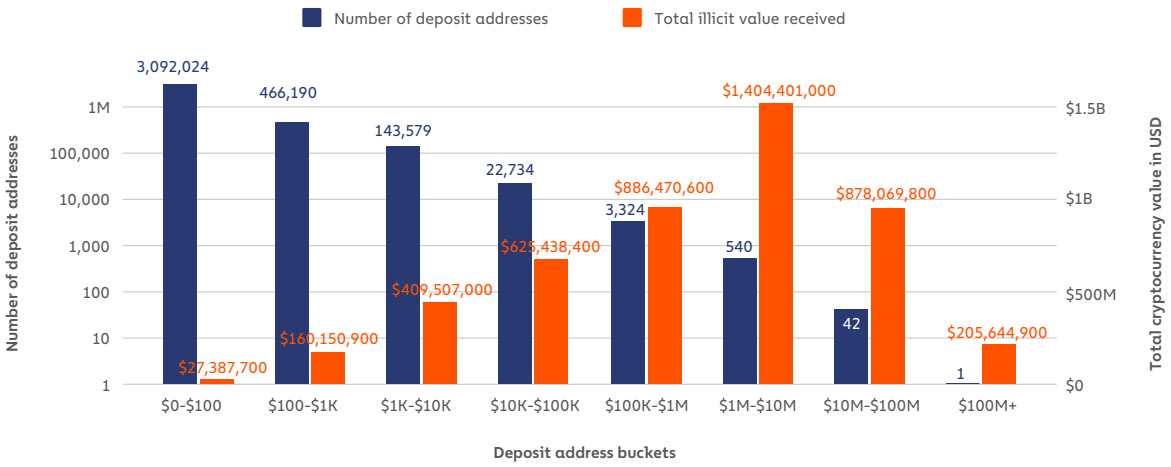


With fewer services used in 2021, money laundering concentration initially appears to have increased slightly. 58% of all funds sent from illicit addresses moved to five services last year, compared to 54% in 2020.

However, money laundering activity is better viewed at the deposit address level rather than the service level. The reason for that is that many of the money laundering services used by cybercriminals are nested services, meaning they operate using addresses hosted by larger services in order to tap into those larger services' liquidity and trading pairs. Over-the-counter (OTC) brokers, for example, often function as nested services with addresses hosted by large exchanges. In the graph below, we look at all service deposit addresses that received any illicit funds in 2021, broken down by the range of illicit funds received.

All illicit cryptocurrency received by service deposit addresses

Deposit addresses bucketed by total illicit cryptocurrency received | 2021



How to read this graph: This graph shows service deposit addresses bucketed by how much total illicit cryptocurrency value each address received individually in 2021. Each blue bar represents the number of deposit addresses in the bucket, while each orange 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 3,092,024 deposit addresses received between $0 and $100 worth of illicit cryptocurrency, and together all of those deposit addresses received a total of $27.4 million worth of illicit cryptocurrency.

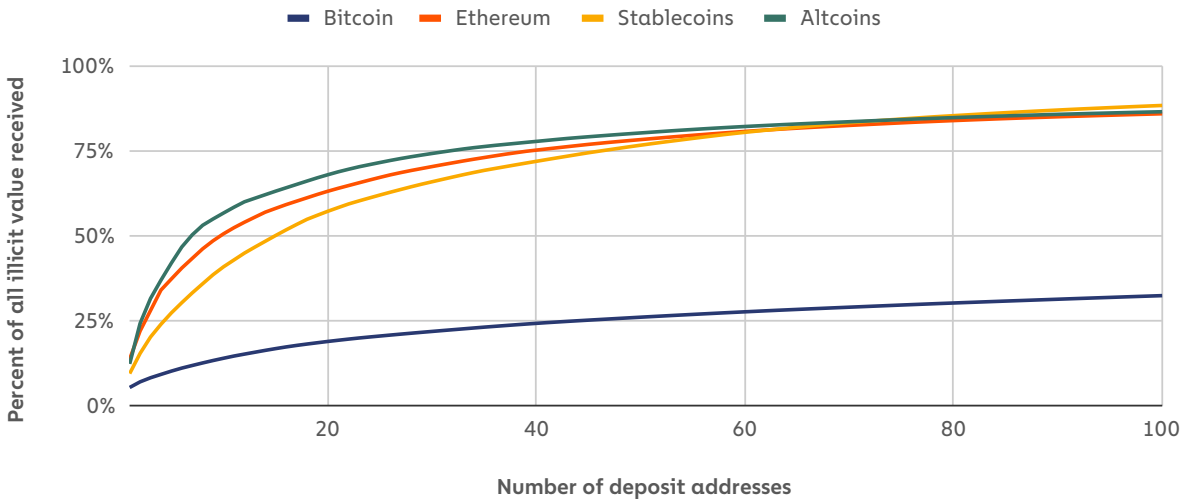
A group of just 583 deposit addresses received 54% of all funds sent from illicit addresses in 2021. Each of those 583 addresses received at least $1 million from illicit addresses, and in total they received just under $2.5 billion worth of cryptocurrency. An even smaller group of 45 addresses received 24% of all funds sent from illicit addresses for a total of just under $1.1 billion. One deposit address received just over $200 million, all from wallets associated with the Finiko Ponzi scheme.

While money laundering activity remains quite concentrated, it's less so than in 2020. That year, 55% of all cryptocurrency sent from illicit addresses went to just 270 service deposit addresses. Law enforcement action could be one possible reason money laundering activity became less concentrated. As we mentioned above, last year OFAC sanctioned Suex, a Russia-based OTC broker, that had received tens of millions' of dollars' worth of cryptocurrency from addresses associated with ransomware, scams, and other forms of criminal activity. Soon after, OFAC also sanctioned Chatex, a P2P exchange founded by the same person as Suex with a similar client profile. While we couldn't share their names at the time, addresses associated with both services appeared in the 270 we identified as the biggest laundering addresses in last year's report.

It's possible that some money laundering services ceased operations after seeing those and other actions taken against illicit platforms, forcing cybercriminals to disperse their money laundering activity to other operators. It's also possible that money laundering services have continued to operate but spread their activity across more deposit addresses, which would contribute to the lessening concentration we see above.

We also see differing levels of concentration in money laundering depending on the asset.

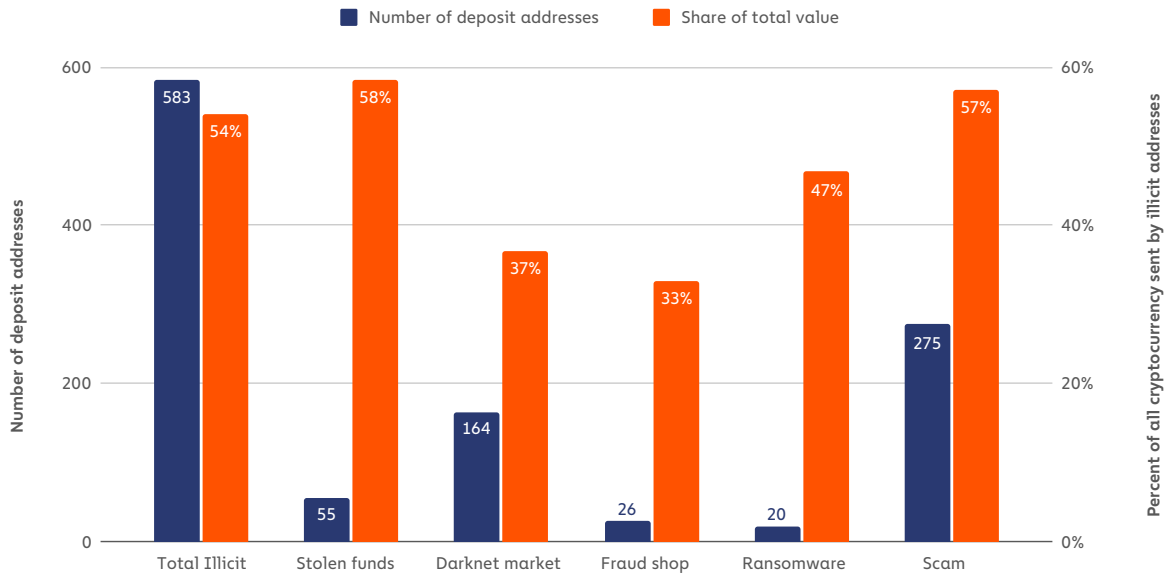
Money laundering concentration: Share of total illicit value received by top deposit addresses by asset | 2021



Bitcoin's money laundering activity is the least concentrated by far. The 20 biggest money laundering deposit addresses receive just 19% of all Bitcoin sent from illicit addresses, compared to 57% for stablecoins, 63% for Ethereum, and 68% for altcoins.

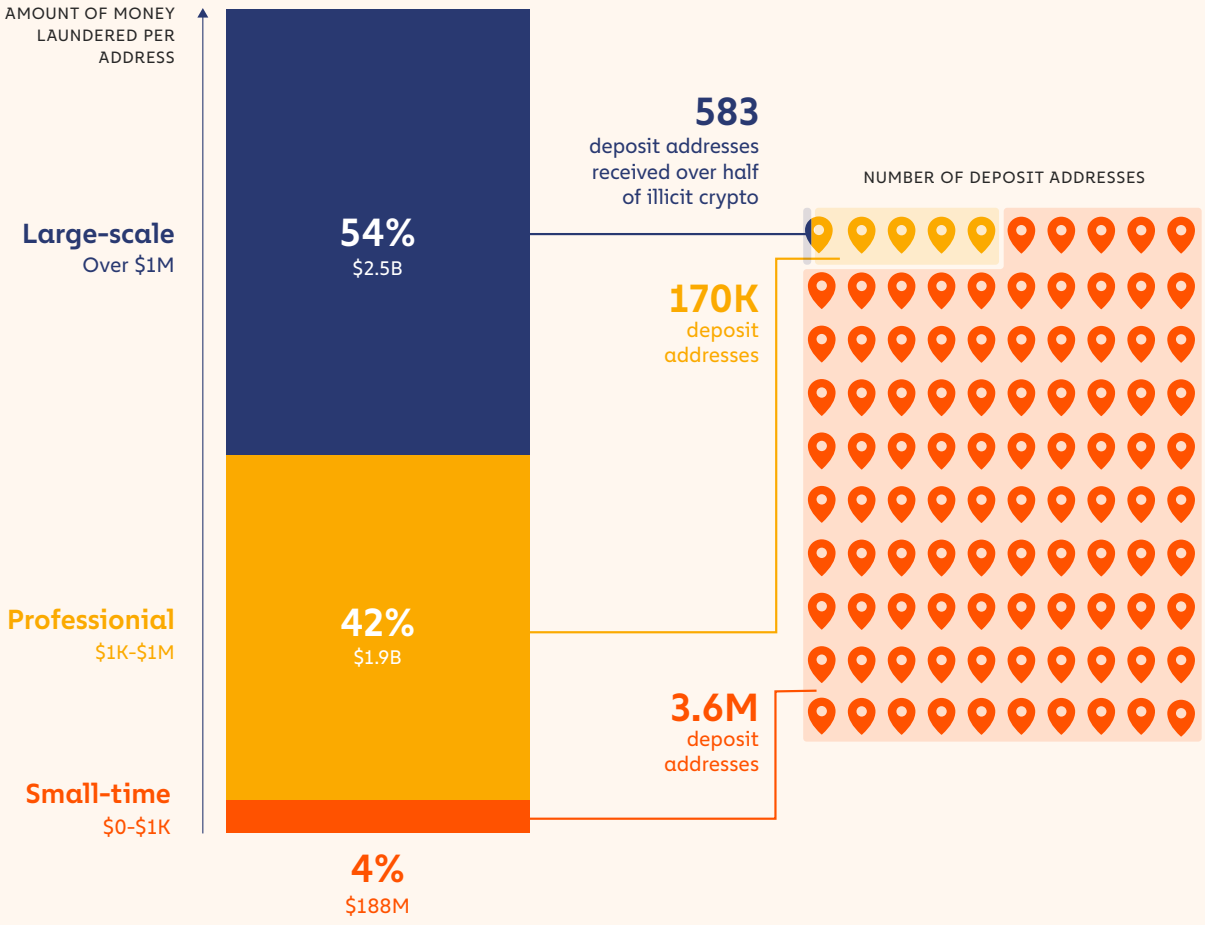
We also see differences in the level of money laundering concentration for different types of cybercriminals. The chart below breaks down by crime category all addresses that received over $1 million in illicit cryptocurrency in 2021, and the share of all funds sent from those criminal categories that the deposit addresses account for.

Number of deposit addresses receiving over $1M in illicit cryptocurrency by crime category and share of all value sent by crime category | 2021



What stands out most is how much less concentrated money laundering activity is for scammers and darknet market vendors and administrators compared to other crime categories. This may reflect the fact that the criminal activity for those categories is itself less concentrated. Many more cybercriminals at varying levels of sophistication are participating in darknet market sales and scamming, so it makes sense we'd see those cybercriminals' funds dispersed across more deposit addresses for money laundering — each player may follow their own strategy. For more sophisticated forms of cybercrime like ransomware, administrators at the biggest ransomware strains account for a greater share of all activity, so we'd expect to see their money laundering be more concentrated as well.

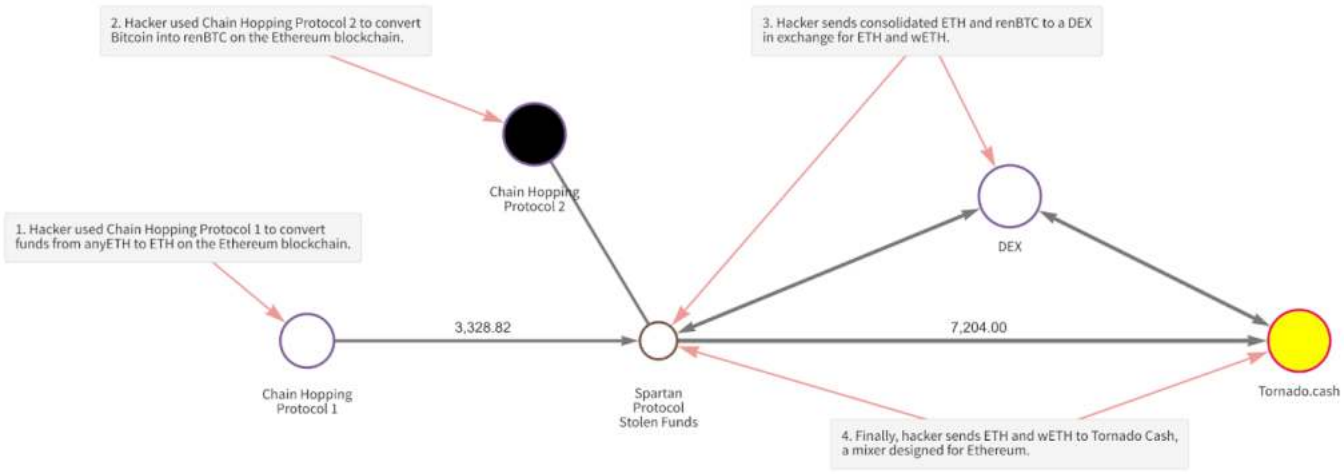
In 2021, money laundering activity in crypto was heavily concentrated.



Case study: Spartan Protocol hacker uses DeFi protocols and chain hopping to launder stolen funds

As we discussed above, usage of DeFi protocols for money laundering skyrocketed in 2021. The Spartan Protocol hack provides a good example of what this activity looks like.

In May 2021, one or more hackers exploited a code vulnerability to steal over $30 million worth of cryptocurrency from the protocol — mostly its native SPARTA token. The hacker then converted much of those funds into anyETH and anyBTC, which are Ethereum and Bitcoin composites respectively built on separate blockchains than the originals. Some of that anyBTC was then swapped for Bitcoin, thereby moving to the Bitcoin blockchain, which brings us to the transactions seen on the Chainalysis Reactor graph below.



Using two DeFi protocols that specialize in cross-chain transactions, the hacker chain hopped to the Ethereum blockchain, converting funds into Ethereum and renBTC. The hacker then sent those funds to a DEX, swapping them for new Ethereum and wrapped Ethereum. Finally, the hacker sent those funds to Tornado Cash, a mixer for the Ethereum blockchain.

While most of these transactions took place in the days immediately following the hack in early May, several took place months later, with the hacker continuing to launder funds well into October. This would be less likely to happen with centralized services, which unlike DeFi protocols typically ask customers for KYC information upon signup and have more ability as custodial platforms to freeze funds from suspicious sources. The Spartan Protocol hack is a great example not just of why DeFi holds appeal as a money laundering

mechanism, but also of how complex investigations can become when cybercriminals use DeFi — especially chain hopping protocols.

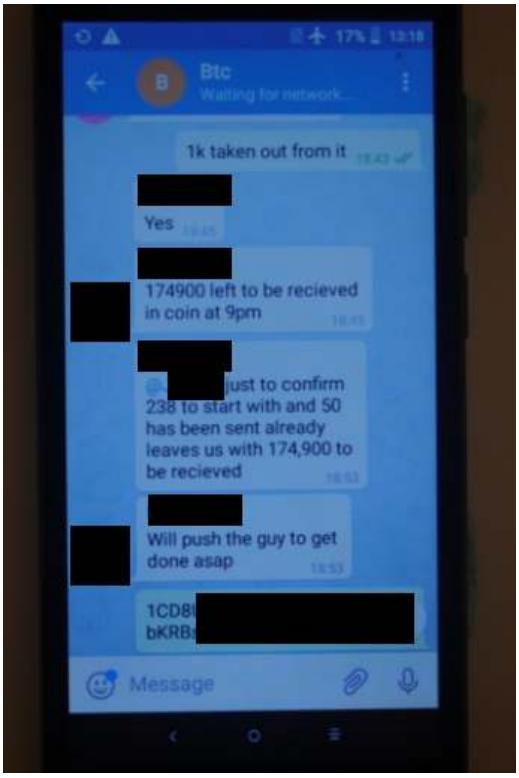
Law enforcement must become proficient in analyzing DeFi transactions in order to crack cases like that of the Spartan Protocol hack, but the teams behind DeFi protocols must also work to prevent their products from being abused by cybercriminals. One way they can do that is by screening the wallets interacting with their smart contracts for prior transactions with known illicit addresses. With the Chainalysis API, DeFi teams can automate the screening process and ensure that their protocols aren't being used to facilitate money laundering. If you work in DeFi, contact us here to learn more about automated wallet screening.

Case study: UK-based drug traffickers work with broker to launder drug money with Bitcoin

As we discussed previously, it's difficult to measure cryptocurrency's role in money laundering of funds derived from traditional, offline crimes. That's because in those cases, the cryptocurrency isn't moving from addresses that we've previously identified as associated with crime, but rather is initially deposited as fiat currency with no evidence of its criminal origins visible on the blockchain. The only way someone could know the origins of those funds would be if they were already investigating the criminals in question, and we know anecdotally that at least some criminals are doing this. Investigators can still use Chainalysis Reactor to investigate these cases, and we'll show you an example of how they do it in the following case study involving the successful investigation of a UK-based drug trafficking group.

The scheme was simple: The group supplied drugs across northern England and distributed them to street-level dealers, who would then sell them for cash which was later delivered back to the crime group. A courier would then collect the cash and deliver it to a broker who would arrange for the funds to be converted into bitcoin. The broker would then send the bitcoin to an address specified by the crime group, taking a small 4% fee. The Bitcoin network is essentially used as a value transfer system, and further analysis showed that the funds were ultimately sent to an OTC service nested at a popular cryptocurrency exchange.

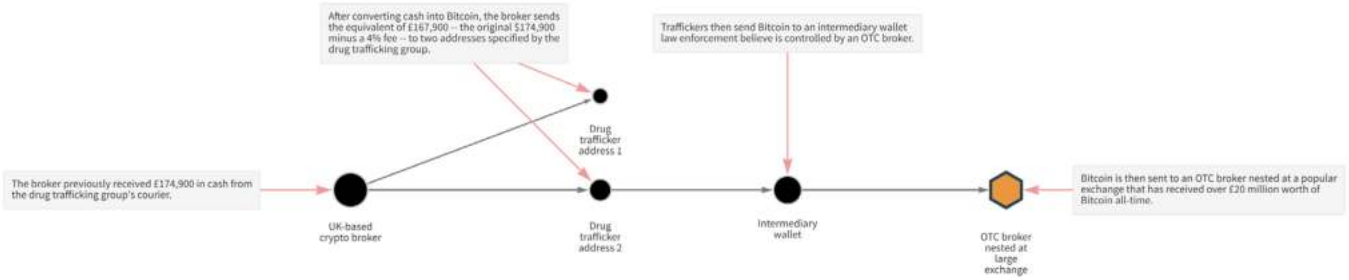
Greater Manchester Police's Serious and Organised Crime Group discovered Bitcoin's role in the money laundering operation after pulling over one of the couriers, whom they'd previously observed collecting cash from a safe house, finding £170,000 in cash concealed in his vehicle. Police arrested the suspect for money laundering and seized two mobile phones. A subsequent digital forensic examination of these devices showed



various WhatsApp and Telegram messages detailing the plan, complete with Bitcoin addresses and screenshots of transaction hashes.

With this information, the officers were able to utilize blockchain analysis to see the flow of funds. Using Chainalysis Reactor, we can see the activity discussed in the message screenshot.

An equivalent of £174,900 minus a 4% brokers fee was sent in bitcoin to the address specified by the traffickers. This represents a relatively low fee in comparison to more traditional money laundering typologies, suggesting that Bitcoin-based laundering could become increasingly attractive to traditional criminals. The funds are then sent to an intermediary wallet before being deposited to an OTC service nested at a popular cryptocurrency exchange. Analysis of other transactions yielded evidence that the courier working for the drug trafficking group laundered at least £1 million across several Bitcoin transactions using these methods.



The case shows how important it is for all criminal investigators — not just those tasked with cybercrime cases — to understand cryptocurrency and blockchain analysis. It also serves as an example of how blockchain analysis can supplement more established investigative techniques law enforcement is already well-versed in. In this case, officers used digital forensic analysis to discover a cryptocurrency nexus, and from there were able to analyze transactions on the blockchain to gain an understanding of the drug traffickers' money laundering scheme, leading to successful prosecutions.

Criminal Balances

Criminal Whales Hold over $25 Billion in Cryptocurrency From Multitude of Illicit Sources

One positive development in the last year has been law enforcement's growing ability to seize cryptocurrency from criminals. We saw several examples of this in 2021, including:

- The U.S. Department of Justice (DOJ) seizing $2.3 million worth of cryptocurrency from the DarkSide ransomware operators responsible for the attack on Colonial Pipeline, as we cover in-depth in our ransomware section.
- IRS-CI's cumulative seizures of over $3.5 billion worth of cryptocurrency over the course of 2021.
- London's Metropolitan Police Service (MPS) made the UK's largest ever seizure of cryptocurrency, taking £180 million worth from a suspected money launderer.

More recently in February 2022, the DOJ seized $3.6 billion worth of Bitcoin connected to the 2016 hack of Bitfinex, in what is currently the largest ever recovery of stolen assets in either cryptocurrency or fiat.

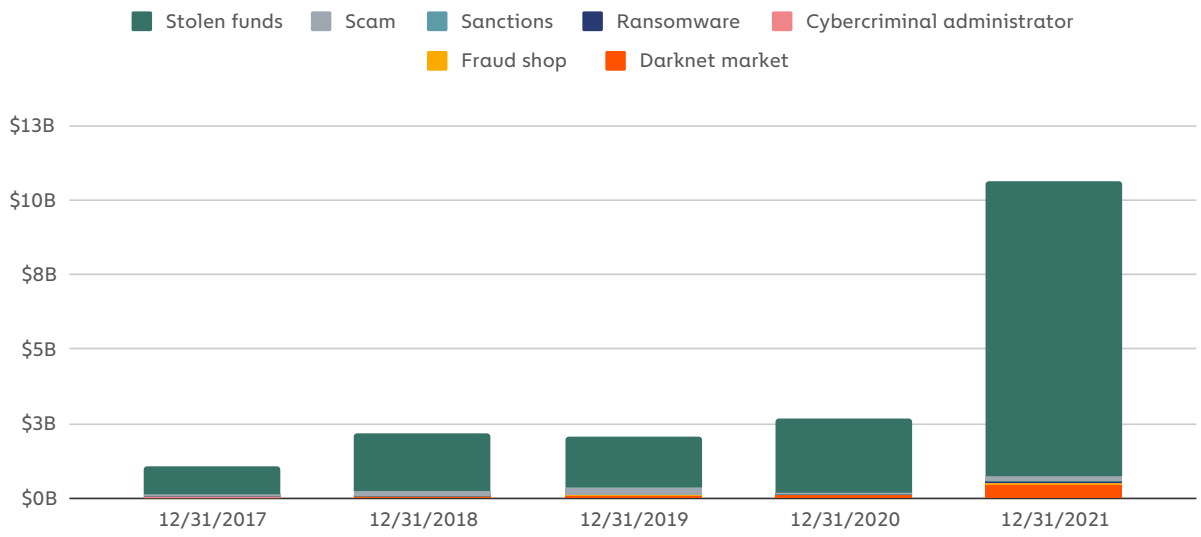
These stories are important not only because they allow financial restitution for victims of cryptocurrency-based crime, but also because they disprove the narrative that crypto-currency is an untraceable, unseizable asset perfect for crime. If cybercriminals know law enforcement is capable of seizing their cryptocurrency, it may lower their incentive to use it in the future.

These cases also raise an important question: How much cryptocurrency is currently held by known criminal entities on the blockchain, and could therefore theoretically be seized by law enforcement? The answer is a function not just of cryptocurrency-based crime revenue in 2021, but of the all-time criminal revenue still held by visible addresses. Below, we'll break down both the sum amount of cryptocurrency holdings that can be traced back to illicit sources, as well as the total balances of criminal whales, meaning criminals holding $1 million or more in cryptocurrency.

Stolen funds dominate total criminal balances

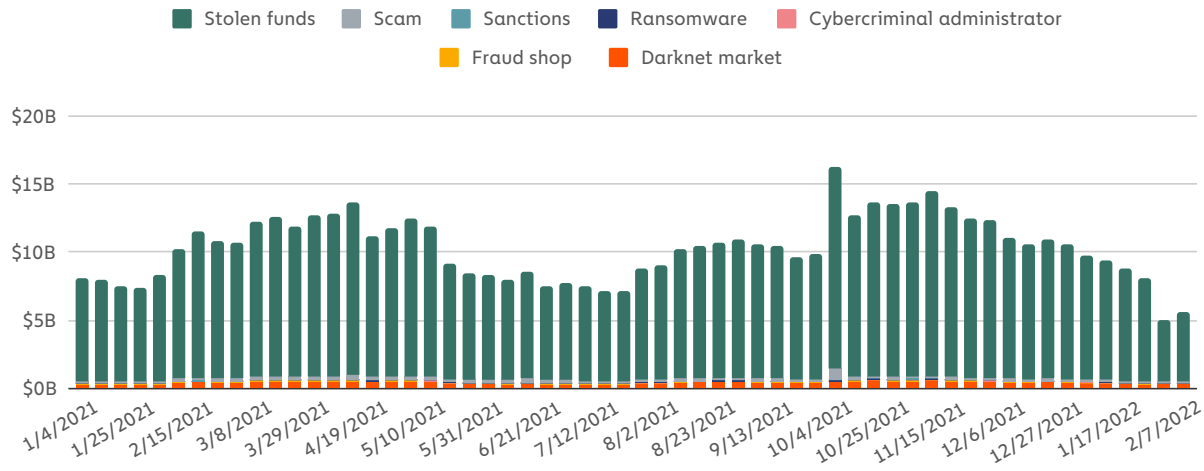
Let's start by looking at the year-end criminal balances over the last five years, broken down by the types of illicit activity the funds were derived from. In this analysis, criminal balances refer to any funds currently held by addresses Chainalysis has attributed to illicit actors. These addresses can belong to criminal services, like darknet markets, but in some cases can also be hosted by private wallets, such as in cases involving stolen funds.

Year end criminal balances | 2017–2021



Two things stand out most: The first is the huge increase in criminal balances in 2021 — at year's end, criminals held $11 billion worth of funds with known illicit sources, compared to just $3 billion at the end of 2020. The second is how much stolen funds dominate. As of the end of 2021, stolen funds account for 93% of all criminal balances at $9.8 billion. Darknet market funds are next at $448 million, followed by scams at $192 million, fraud shops at $66 million, and ransomware at $30 million.

Total weekly criminal balances by crime type | 2021



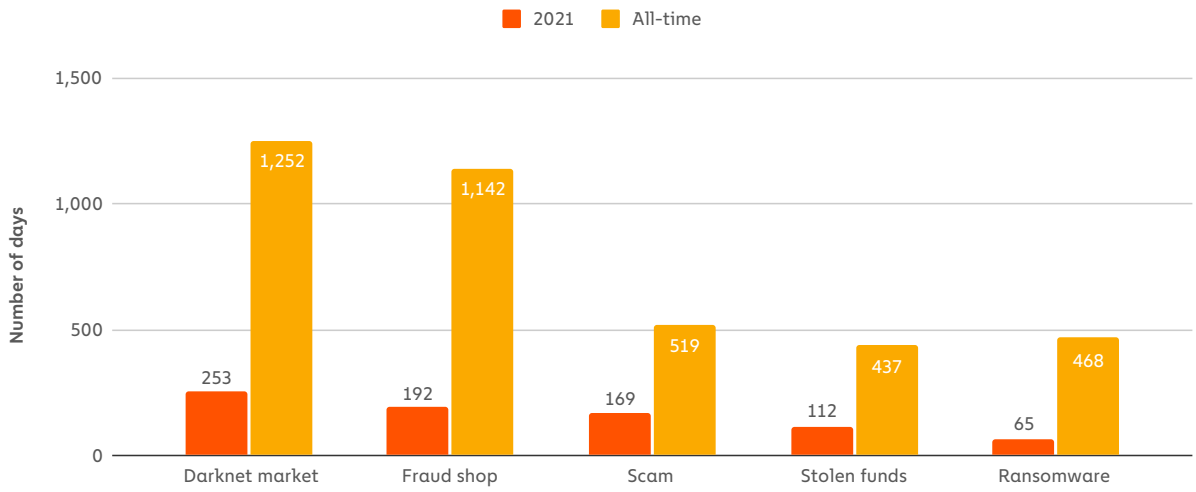
Note: "Cybercriminal administrator" refers to addresses that have been attributed to individuals connected to a cybercriminal organization, such as a darknet market.

Criminal balances also fluctuated throughout the year, from a low of $6.6 billion in July to a high of $14.8 billion in October. The fluctuations are a reminder of the importance

of speed in cryptocurrency investigations, as criminal funds that have been successfully traced on the blockchain can be liquidated quickly. Of course, criminal balances can also fall for good reasons as well. The large drop in criminal balances we see above in February 2022 is due to the DOJ's $3.6 billion seizure of Bitcoin stolen in the 2016 Bitfinex hack. Following that seizure, criminal balances currently stand at roughly $5 billion as of February 9, 2022.

Let's look at which types of cybercriminals tend to hold their funds the longest.

Average cryptocurrency holding time for criminal addresses | 2021 VS ALL-TIME



Looking at all-time trends, darknet market vendors and administrators tend to hold their funds the longest before liquidating, while wallets with stolen funds tend to hold for the shortest amount of time. That last bit may be surprising — how could stolen funds be held for such little time but account for the vast majority of criminal balances? It turns out that most of those holdings belong to extremely large wallets that hold longer than is typical for others in the stolen funds category. But what really stands out is how much holding times have decreased across the board, as the 2021 average holding times are at least 75% shorter than the all-time figures in all categories. Ransomware operators in particular exemplify this trend, as they now hold funds on average for just 65 days before liquidating. This may be a response to the mounting law enforcement pressure ransomware attackers face.

Criminal whales show more variation

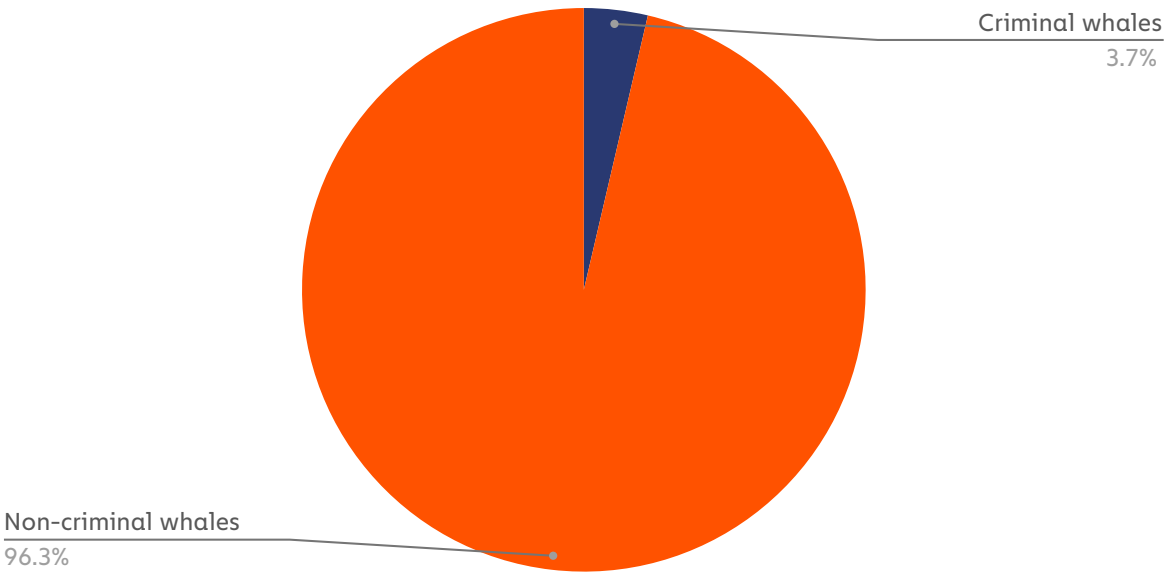
A question that naturally follows from our investigation into criminal balances: Which criminals hold the most cryptocurrency? We decided to investigate by analyzing the

balances of criminal whales. However, please note that we calculate criminal whale balances a bit differently than we do the overall criminal balances we discussed above. We define a criminal whale as any private wallet holding $1 million or more worth of cryptocurrency that has received more than 10% of its funds from illicit addresses.

Please recognize that because criminal whale balances are calculated based on private wallet holdings, while overall criminal balances are calculated based on the holdings of addresses tagged as illicit (meaning they can include funds held at services in addition to private wallets), the criminal whale balances discussed here won't align with the overall criminal balances calculated above.

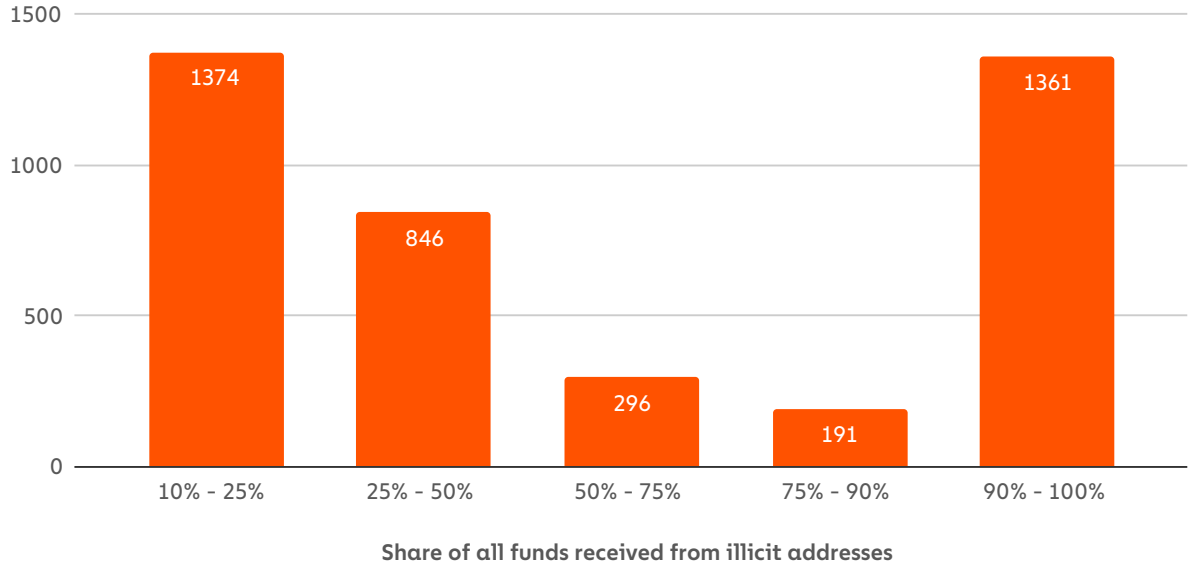
Overall, Chainalysis has identified 4,068 criminal whales holding over $25 billion worth of cryptocurrency. Criminal whales represent 3.7% of all cryptocurrency whales — that is, private wallets holding over $1 million worth of cryptocurrency.

Share of all cryptocurrency whales that received 10% or more of funds from illicit addresses



An interesting pattern emerges when we break down all criminal whales by the share of their total funds that have illicit origins: Most criminal whales received either a relatively small or extremely large share of their total balance from illicit addresses.

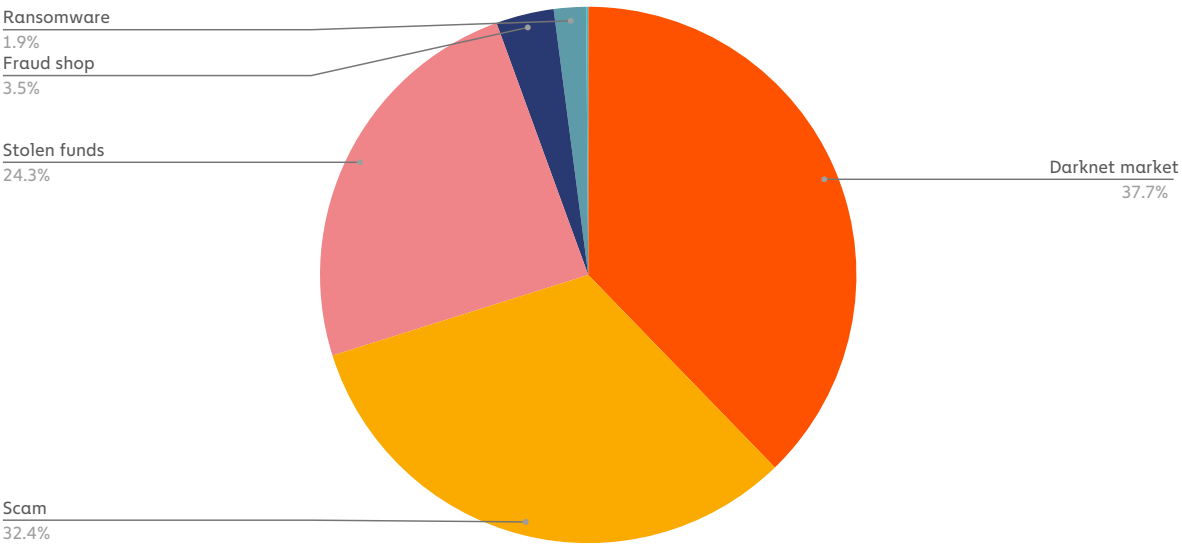
Criminal whales by share of all funds received from illicit addresses



Above, we bucket all criminal whales by the share of their total cryptocurrency received that came from illicit addresses. The lowest-share bucket is the biggest — 1,374 criminal whales received between 10% and 25% of their total balance from illicit addresses. However, the largest-share bucket is close behind, with 1,361 criminal whales that received between 90% and 100% of their total balance from illicit addresses. In total, 1,333 criminal whales received between 25% and 90% of all funds from illicit addresses.

Illicit funds received by criminal whales also come from more varied sources than the funds making up overall criminal balances.

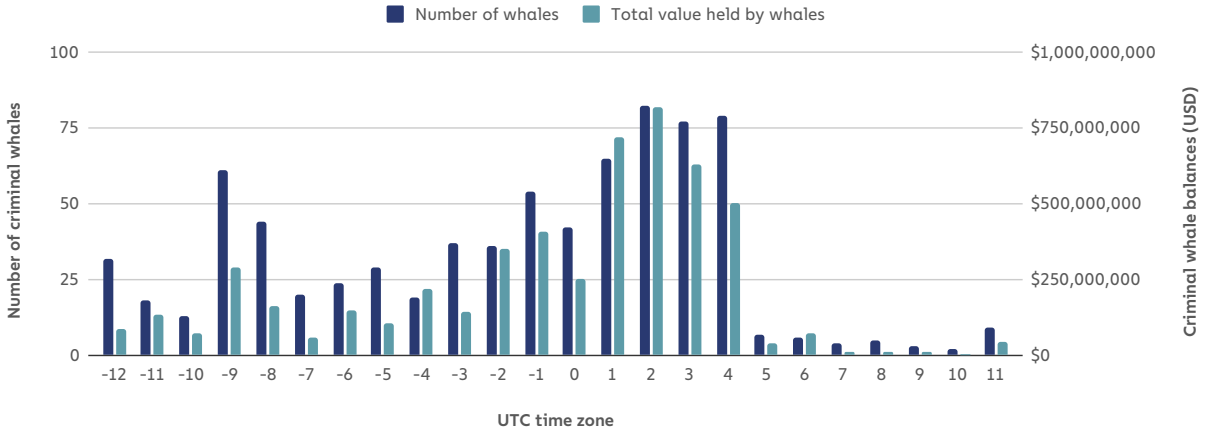
Source of illicit funds received by criminal whales



Whereas stolen funds dominate overall criminal balances, darknet markets are the biggest source of illicit funds sent to criminal whales, followed by scams second and stolen funds third.

Finally, we can also use time zone analysis to try and approximate the location of criminal whales. On the graph below, we've assigned UTC time zones to the 768 criminal whales whose wallets have enough activity for us to make a strong estimate.

Estimated UTC time zone of criminal whales



UTC time zones 2, 3, and 4 are estimated to contain the most criminal whales, while time zones 1 and -9 also have a large number. UTC time zones 2, 3, and 4 include much of Russia, including major population centers like Moscow and Saint Petersburg, which is especially interesting in the context of Russia's outsized role in cryptocurrency-based crime, as we explore elsewhere in this report. However, time zones of course only allow us to estimate longitudinal location, so it's possible some of these criminal whales are based in other countries within time zones 2, 3, and 4, such as South Africa, Saudi Arabia, or Iran.

The ability to efficiently track criminal whales and quantify their holdings from one public data set is a major difference between cryptocurrency-based crime and fiat-based crime. In fiat, the highest net worth criminals have murky networks of foreign banks and shell corporations to obfuscate their holdings. But in cryptocurrency, transactions are saved on the blockchain for all to see. Investigation of criminal whales represents a significant opportunity for government agencies around the world to continue their string of successful seizures, and bring to justice the biggest beneficiaries of cryptocurrency-based crime.

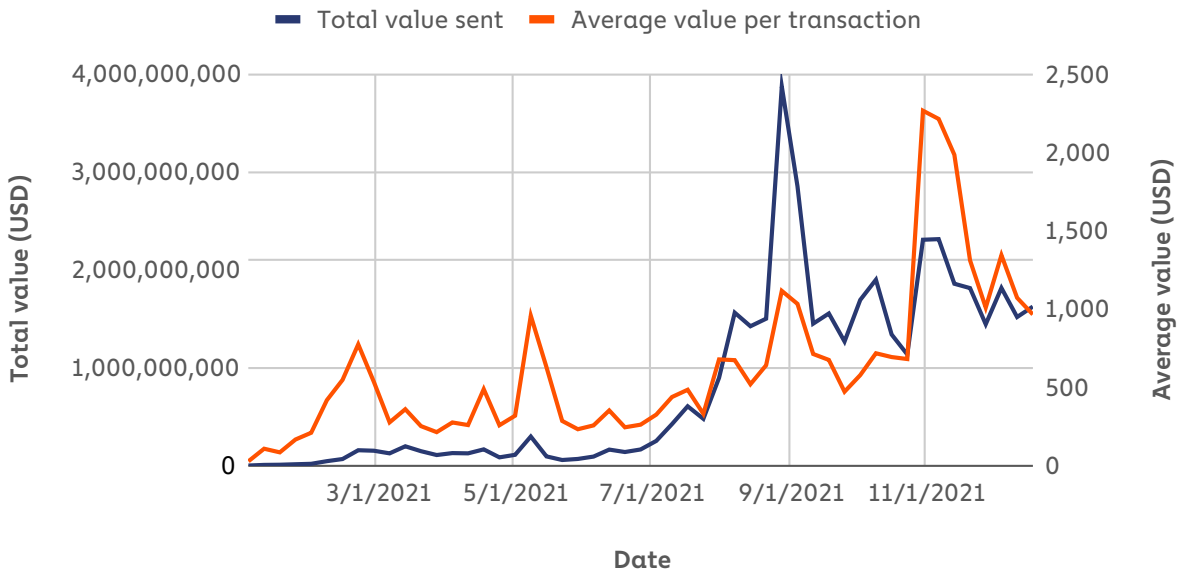
NFTs and Crime

Chainalysis Detects Significant Wash Trading and Some Money Laundering In this Emerging Asset Class

Non-fungible tokens (NFTs) were one of the biggest stories in cryptocurrency in 2021. NFTs are blockchain-based digital items whose units are designed to be unique, unlike traditional cryptocurrencies whose units are meant to be interchangeable. NFTs can store data on blockchains — with most NFT projects built on blockchains like Ethereum and Solana — and that data can be associated with images, videos, audio, physical objects, memberships, and countless other developing use cases. NFTs typically give the holder ownership over the data or media the token is associated with, and are commonly bought and sold on specialized marketplaces.

NFT popularity skyrocketed in 2021. Chainalysis tracked a minimum $44.2 billion worth of cryptocurrency sent to ERC-721 and ERC-1155 contracts — the two types of Ethereum smart contracts associated with NFT marketplaces and collections — up from just $106 million in 2020.

Weekly total cryptocurrency value and average value per transaction sent to NFT platforms | 2021



However, as is the case with any new technology, NFTs offer potential for abuse. It's important that as our industry considers all the ways this new asset class can change how we link the blockchain to the physical world, we also build products that make NFT

investment as safe and secure as possible. Below, we look at two forms of illicit activity we've observed in NFTs:

- Wash trading to artificially increase the value of NFTs
- Money laundering through the purchase of NFTs

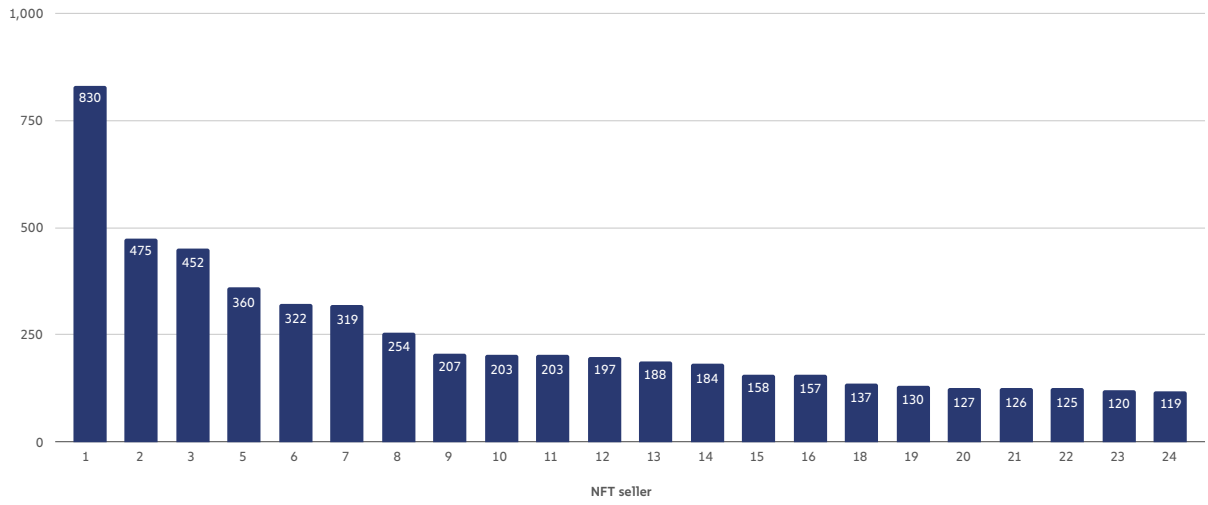
Let's dive in.

Some NFT sellers are making a killing with wash trading

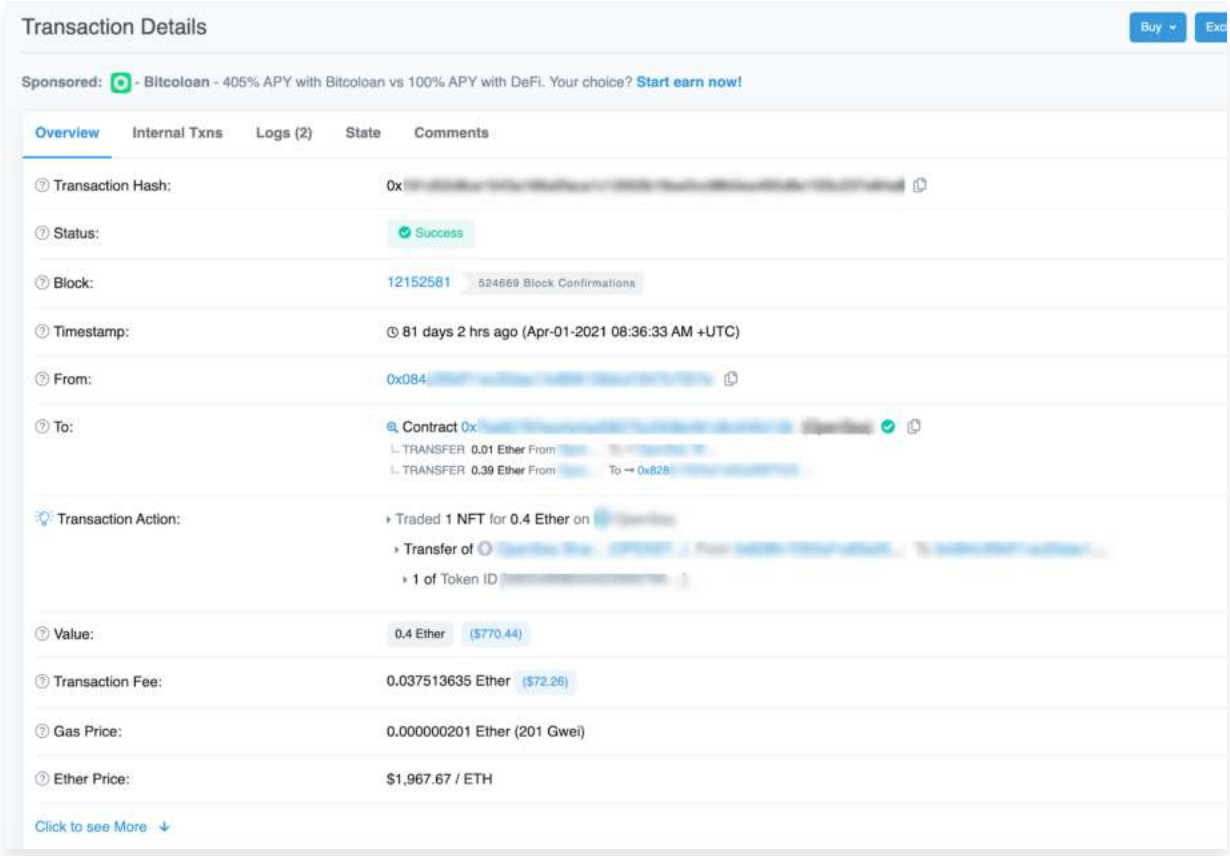
Wash trading, meaning executing a transaction in which the seller is on both sides of the trade in order to paint a misleading picture of an asset's value and liquidity, is another area of concern for NFTs. Wash trading has historically been a concern with cryptocurrency exchanges attempting to make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

With blockchain analysis, however, we can track NFT wash trading by analyzing sales of NFTs to addresses that were self-financed, meaning they were funded either by the selling address or by the address that initially funded the selling address. Analysis of NFT sales to self-financed addresses shows that some NFT sellers have conducted hundreds of wash trades.

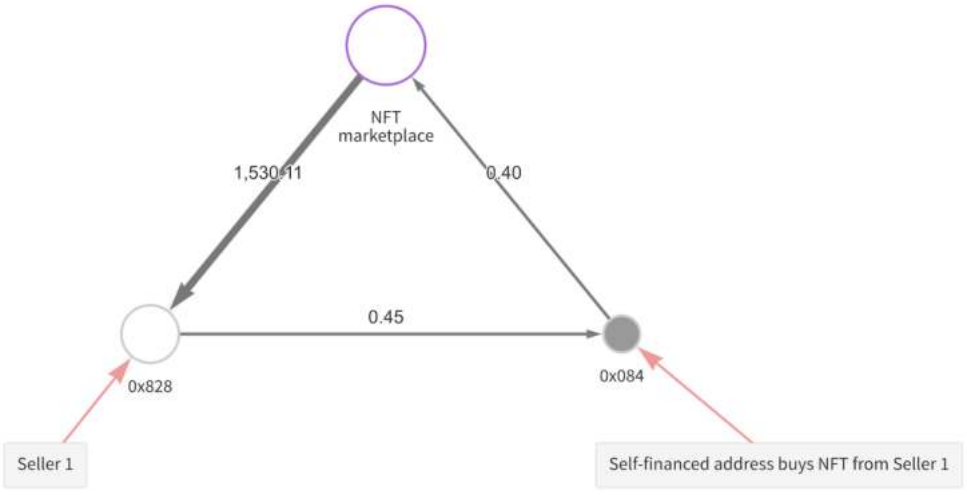
NFT sellers by number of sales to self-financed addresses | 2021



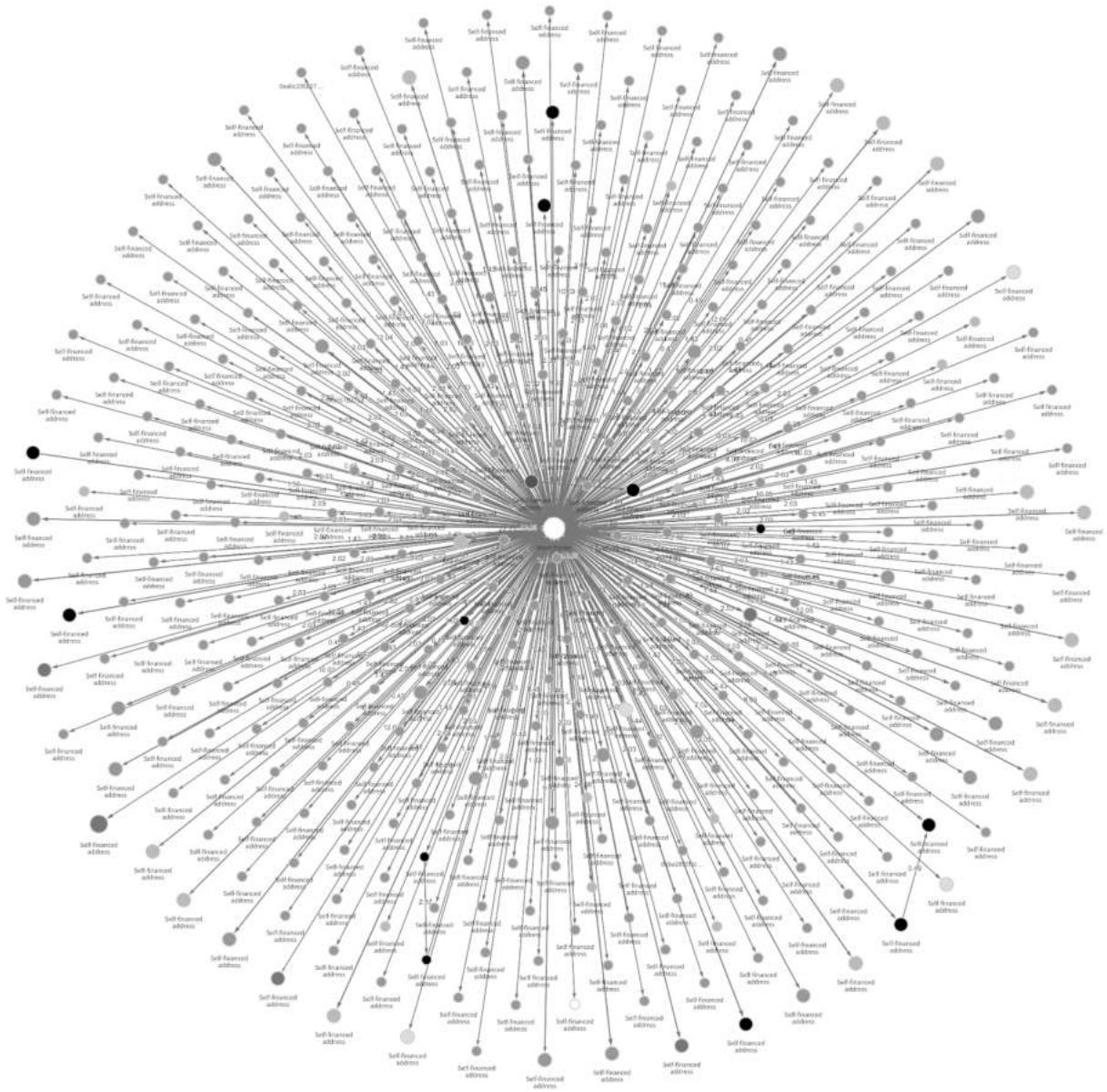
Let's look more closely at Seller 1, the most prolific NFT wash trader on the chart above, who has made 830 sales to addresses they've self-financed. The Etherscan screenshot below shows a transaction in which that seller, using the address beginning 0x828, sold an NFT to the address beginning 0x084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



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



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



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

Seller 1 address	Amount spent on gas fees in wash trading transactions	Revenue from sales of wash traded NFTs to victims	Profits
0x828...	- $35,642	$27,258	- $8,383

However, the story changes if we look at a bigger piece of the NFT ecosystem. Using blockchain analysis, we identified 262 users who have sold an NFT to a self-financed address more than 25 times. While we can't be 100% sure that all instances of NFT sales to self-financed wallets are intended for wash trading, the 25-transaction threshold gives us a higher degree of confidence that these users are habitual wash traders. Just as we did above for one wash trader, we calculated these 262 wash traders' overall profits by subtracting the amount they've spent on gas fees from the amount they've made selling NFTs to unsuspecting buyers. One caveat for this analysis is that it only captures trades made in Ethereum and Wrapped Ethereum, so there's likely wash trading activity we're not considering here.

Nonetheless, an interesting story emerges: Most NFT wash traders have been unprofitable, but the successful NFT wash traders have profited so much that, as a whole, this group of 262 has profited immensely overall.

Wash trader group	Number of addresses	Profits from wash trading
Profitable wash traders	110	$8,875,315
Unprofitable wash traders	152	- $416,984
All	262	$8,458,331

The 110 profitable wash traders have collectively made nearly $8.9 million in profit from this activity, dwarfing the $416,984 in losses made by the 152 unprofitable wash traders. Even worse, that $8.9 million is most likely derived from sales to unsuspecting buyers who believe the NFT they're purchasing has been growing in value, sold from one distinct collector to another.

NFT wash trading exists in a murky legal area. While wash trading is prohibited in conventional securities and futures, wash trading involving NFTs has yet to be the subject of an enforcement action. However, that could change as regulators shift focus and apply existing anti-fraud authorities to new NFT markets. More generally, wash trading in NFTs can create an unfair marketplace for those who purchase artificially inflated tokens, and

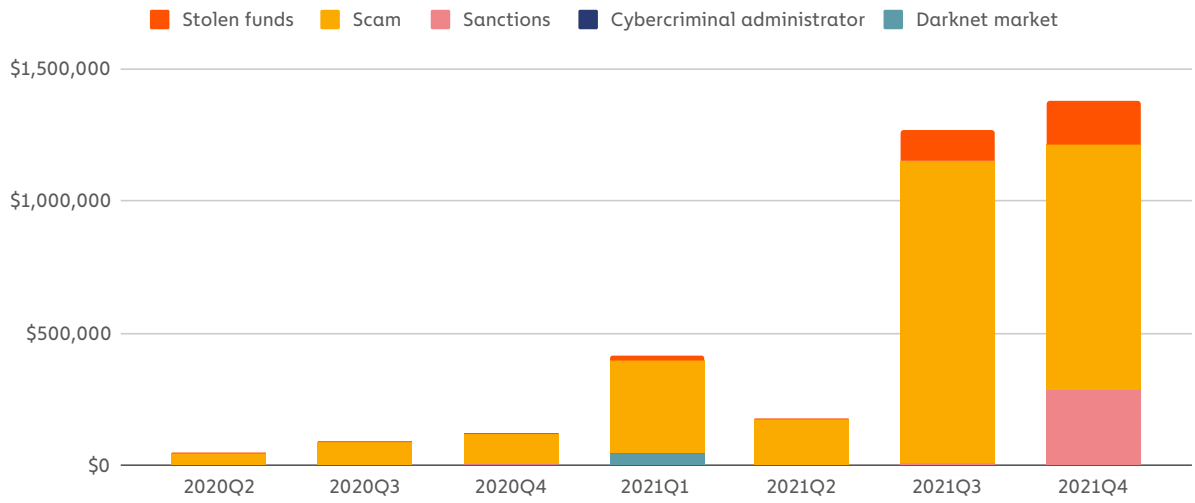
its existence can undermine trust in the NFT ecosystem, inhibiting future growth. We encourage NFT marketplaces to discourage this activity as much as possible. Blockchain data and analysis makes it easy to spot users who sell NFTs to addresses they've self-financed, so marketplaces may want to consider bans or other penalties for the worst offenders.

Money laundering activity small but visible in NFTs

Money laundering has long been an issue in the fine art world, and it's not hard to see why. As one 2019 article from the National Law Review points out, art pieces like paintings are easy to move, have relatively subjective prices, and may offer certain tax advantages. Criminals can therefore purchase art with illegally gained funds, sell them later, and poof — they have seemingly clean money with no connection to the original criminal activity. This background, along with the pseudonymity of cryptocurrency, has many wondering if NFTs are vulnerable to similar abuses. But while money laundering in physical art is difficult to quantify, we can make more reliable estimates of NFT-based money laundering thanks to the inherent transparency of the blockchain.

So, are cybercriminals using illicit funds to purchase NFTs? Let's take a look.

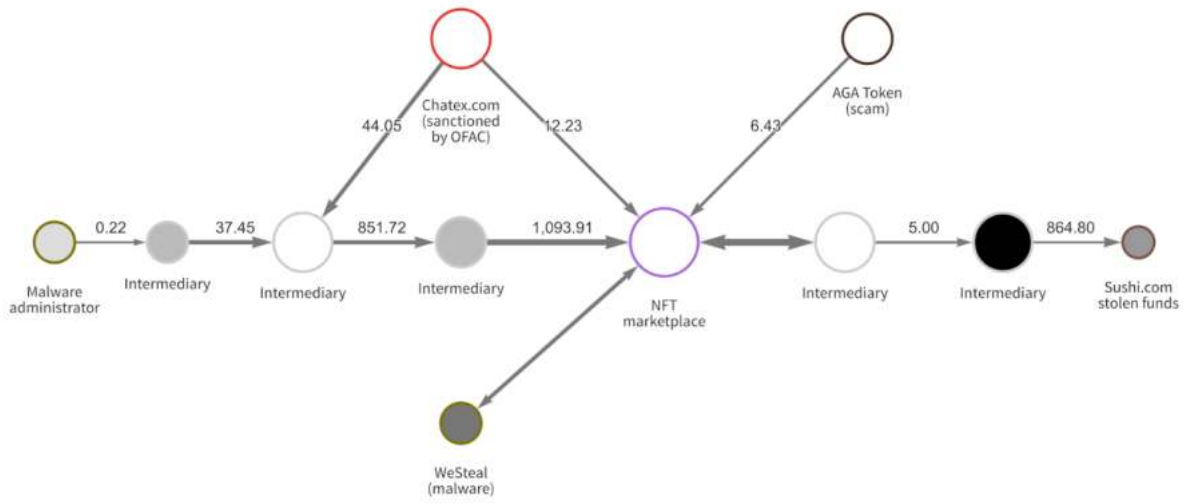
Illicit value received by NFT platforms | 2020Q2–2021Q4



Value sent to NFT marketplaces by illicit addresses jumped significantly in the third quarter of 2021, crossing $1 million worth of cryptocurrency. The figure grew again in the fourth quarter, topping out at just under $1.4 million. In both quarters, the vast majority of this activity came from scam-associated addresses sending funds to NFT marketplaces to make purchases. Both quarters also saw significant amounts of stolen funds sent to

marketplaces as well. Perhaps most concerningly, in the fourth quarter, we saw roughly $284,000 worth of cryptocurrency sent to NFT marketplaces from addresses with sanctions risk. All of that was due to transfers from the P2P exchange Chatex, which the U.S. Treasury's Office of Foreign Asset Control (OFAC) added to its Specially Designated Nationals (SDN) list last year.

We can see examples of different types of criminals buying NFTs in the Reactor graph below.



Here, we can see addresses associated with several different types of cybercriminals sending funds to a popular NFT marketplace, including malware operators, scammers, and Chatex.

All of this activity represents a drop in the bucket compared to the $8.6 billion worth of cryptocurrency-based money laundering we tracked in all of 2021. Nevertheless, money laundering, and in particular transfers from sanctioned cryptocurrency businesses, represents a large risk to building trust in NFTs, and should be monitored more closely by marketplaces, regulators, and law enforcement.

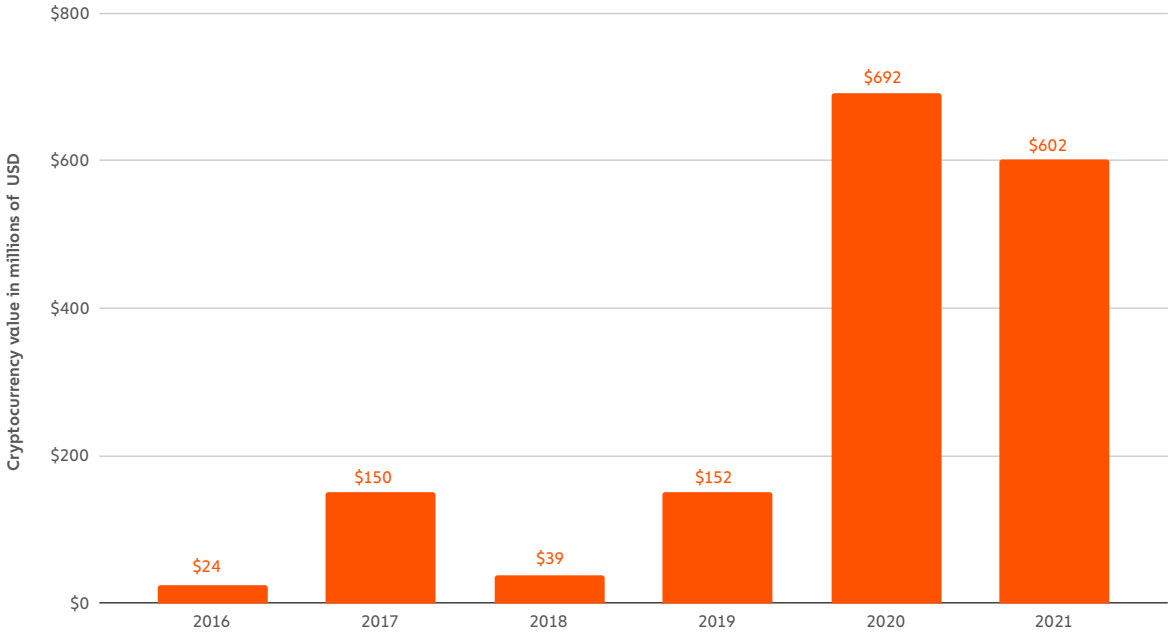
Ransomware

As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict

In our last Crypto Crime Report, we deemed 2020 the "Year of Ransomware" due to the huge growth in cryptocurrency extorted in ransomware attacks. When we first released that report last year, we announced that we had tracked roughly $350 million worth of payments from victims to ransomware operators. However, we explained at the time that this figure was likely an underestimate we would raise in the future due to both underreporting by ransomware victims and our continuing identification of ransomware addresses that have received previous victim payments.

Sure enough, we updated our ransomware numbers a few times throughout 2021, reflecting new payments we hadn't identified previously. As of January 2022, we've now identified just over $692 million in 2020 ransomware payments — nearly double the amount we initially identified at the time of writing last year's report.

Total cryptocurrency value received by ransomware addresses | 2016–2021



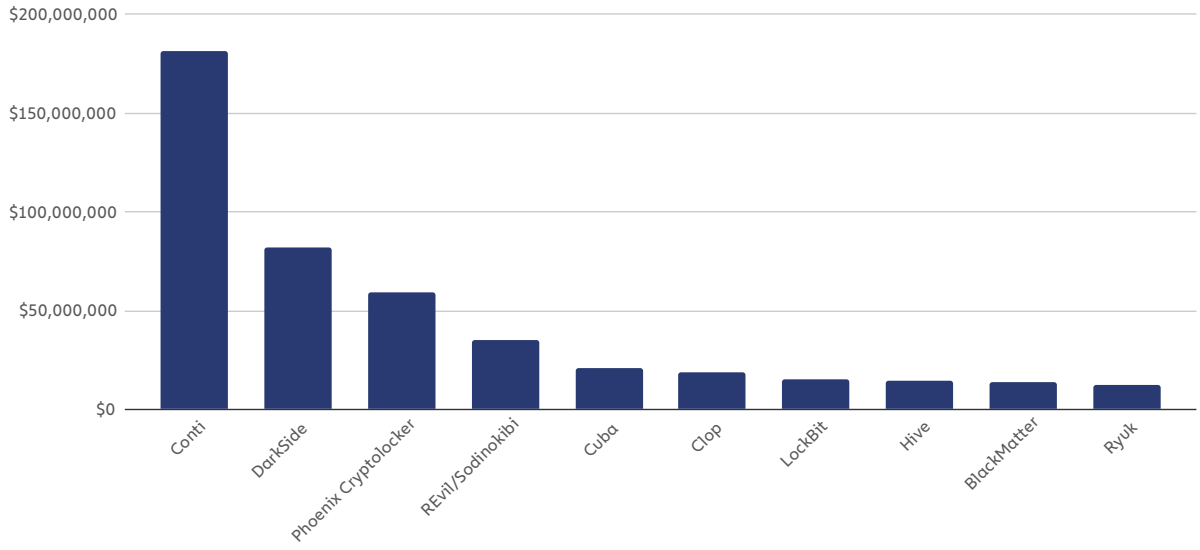
You'll also see above that as of now, we've identified just over $602 million worth of ransomware payments in 2021. However, just like last year, we know that this too is an underestimate, and that the true total for 2021 is likely to be much higher. In fact, despite these numbers, anecdotal evidence, plus the fact that ransomware revenue in the first half of 2021 exceeded that of the first half of 2020, suggests to us that 2021 will eventually be revealed to have been an even bigger year for ransomware. Below, we'll look

more at which ransomware strains were most prolific in 2021, how ransomware operators laundered their funds, and examples of how law enforcement and security agencies are fighting back against ransomware.

2021 ransomware activity summarized

Conti was the biggest ransomware strain by revenue in 2021, extorting at least $180 million from victims.

Top 10 ransomware strains by revenue | 2021



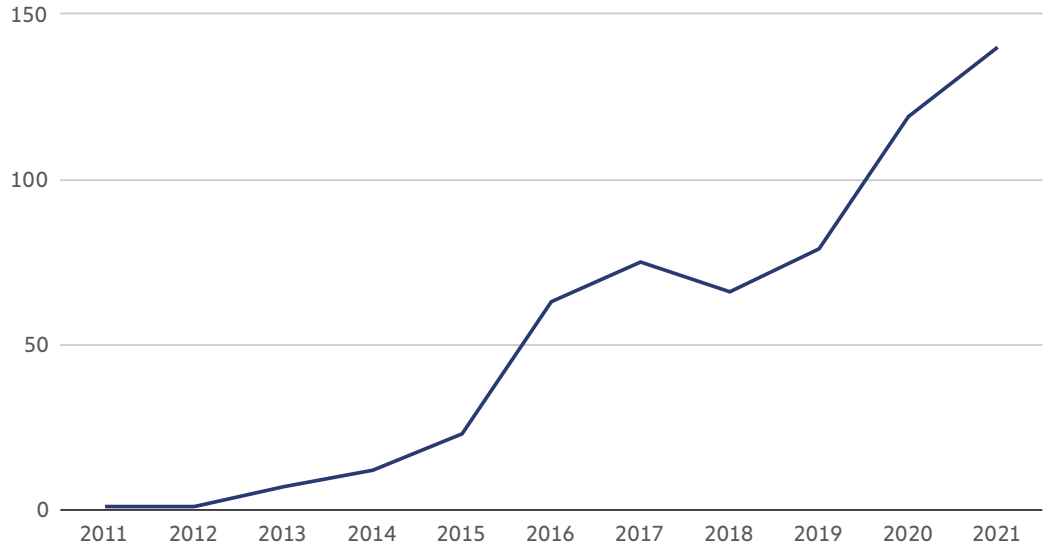
Believed to be based in Russia, Conti operates using the ransomware-as-a-service (RaaS) model, meaning Conti's operators allow affiliates to launch attacks using its ransomware program in exchange for a fee.

DarkSide is also notable, both for ranking second in 2021 in funds extorted from victims that we've been able to identify, and also for its role in the attack on oil pipeline Colonial Pipeline, one of the year's most notable ransomware attacks. The attack caused fuel shortages in some areas, which were exacerbated by subsequent panic buying as word of the attack's impact spread. The Colonial story serves as an important reminder of one reason ransomware attacks are so dangerous: They frequently target critical infrastructure we need to keep the country running — not just energy providers, but food providers, schools, hospitals and financial services companies as well.

However, the Colonial Pipeline attack also turned into a success story, as the U.S. Department of Justice was able to track and seize $2.3 million of the ransom that Colonial paid to DarkSide. We'll look more at how agents were able to do this later in the

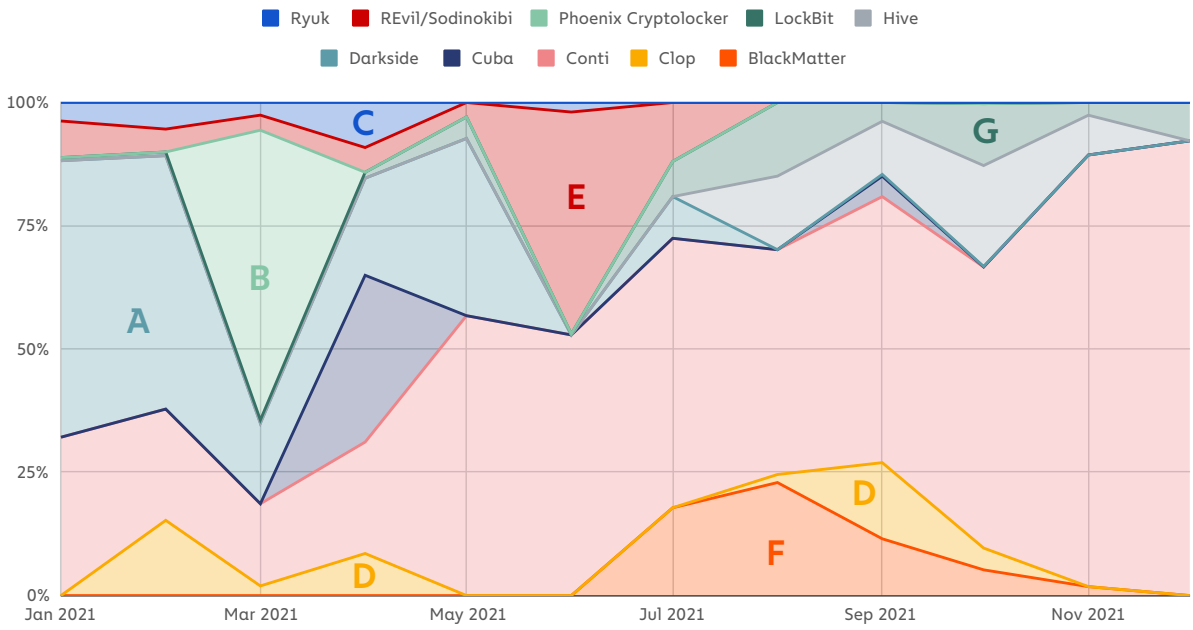
section, but suffice it to say that law enforcement's growing ability to seize payments after they're made represents a huge step forward in the fight against ransomware. It also serves as one more reason why more victims should report attacks — even if you pay, law enforcement may be able to help you get those funds back. Overall, 2021 also saw more active individual ransomware strains than any other year.

Active ransomware strains by year | 2011–2021



At least 140 ransomware strains received payments from victims at any point in 2021, compared to 119 in 2020, and 79 in 2019. Those numbers are emblematic of the intense growth of ransomware we've seen over the last two years. Most ransomware strains come and go in waves, staying active for a short amount of time before becoming dormant. We show this on the graph below, which shows how the top ten ransomware strains ebbed and flowed in activity throughout the year.

Top 10 most active strains in 2021 by monthly revenue | JAN–NOV 2021



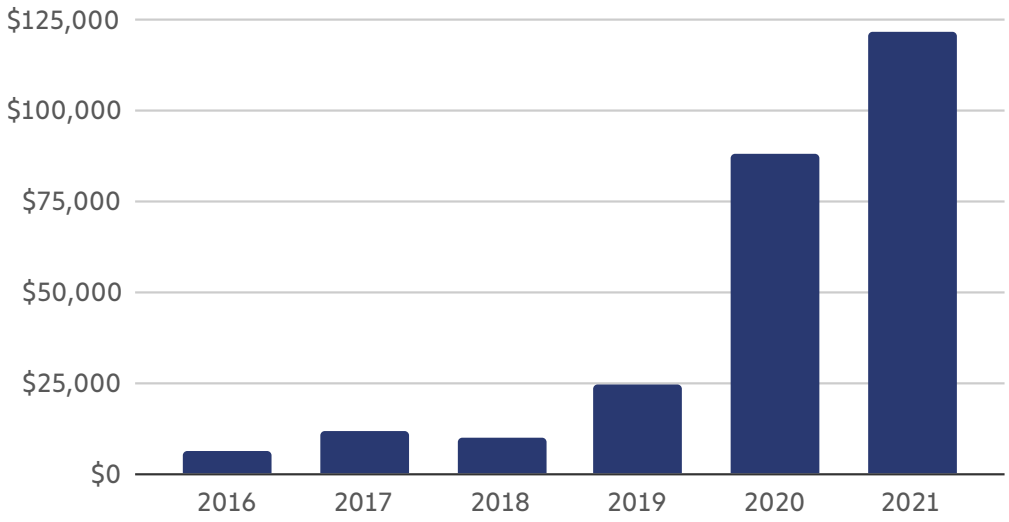
- **A** DarkSide momentum falters after May Colonial Pipeline attack
- **B** Evil Corp-spinoff Phoenix Cryptolocker disappears after a record-breaking haul
- **C** Ryuk wanes in second half of year, perhaps shifting operations to Diavol
- **D** Clop remerges in the fall after several arrests throughout the year likely reduce activity
- **E** REvil sparked retirement rumors after Kaseya attack in July. It ultimately self-closed in Q4 under LE pressure
- **F** BlackMatter picks up where DarkSide left off, but a decryptor released by Emsisoft likely depressed revenue
- **G** LockBit went dark while it rebranded to LockBit 2.0 in June and remains a persistent threat into 2022

Conti was the one strain that remained consistently active for all of 2021, and in fact saw its share of all ransomware revenue grow throughout the year. Overall though, Conti's staying power is increasingly outside the norm.

As we'll explore more later on, the growing number of active strains and generally short lifespan of most strains is also a result of rebranding efforts. More and more in 2021, we've seen the operators of strains publicly "shut down" before re-launching under a new name, presenting themselves as a separate cybercriminal group. Often, the rebranded strain's financial footprint on the blockchain aligns with that of the original, which can tip investigators off as to who's really behind the new strain.

Ransomware payment sizes also continued to grow in 2021, a trend we've observed every year since 2018.

Average ransomware payment size | 2016–2021

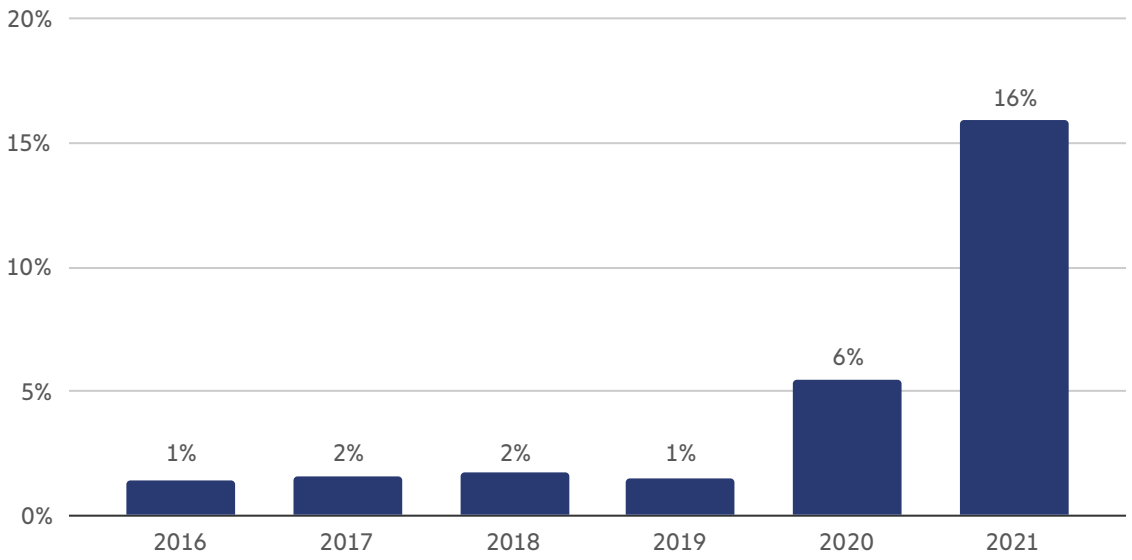


The average ransomware payment size was over $118,000 in 2021, up from $88,000 in 2020 and $25,000 in 2019. Large payments such as the record $40 million received by Phoenix Cryptolocker spurred this all-time high in average payment size. One reason for the increase in ransom sizes is ransomware attackers' focus on carrying out highly-targeted attacks against large organizations. This "big game hunting" strategy is enabled in part by ransomware attackers' usage of tools provided by third-party providers to make their attacks more effective. These tools range from illicit hacking aids to legitimate products, and include:

- Rented infrastructure such as bulletproof web hosting, domain registration services, botnets, proxy services, and email services to carry out attacks.
- Hacking tools like network access to already-infiltrated networks, exploit kits that scan victims' networks for vulnerabilities, and malware programs that help attackers distribute ransomware more effectively.
- Stolen data such as passwords, individuals' personally identifiable information, and compromised remote desktop protocol (RDP) credentials, which help attackers break into victims' computer networks.

Usage of these services by ransomware operators spiked to its highest ever levels in 2021.

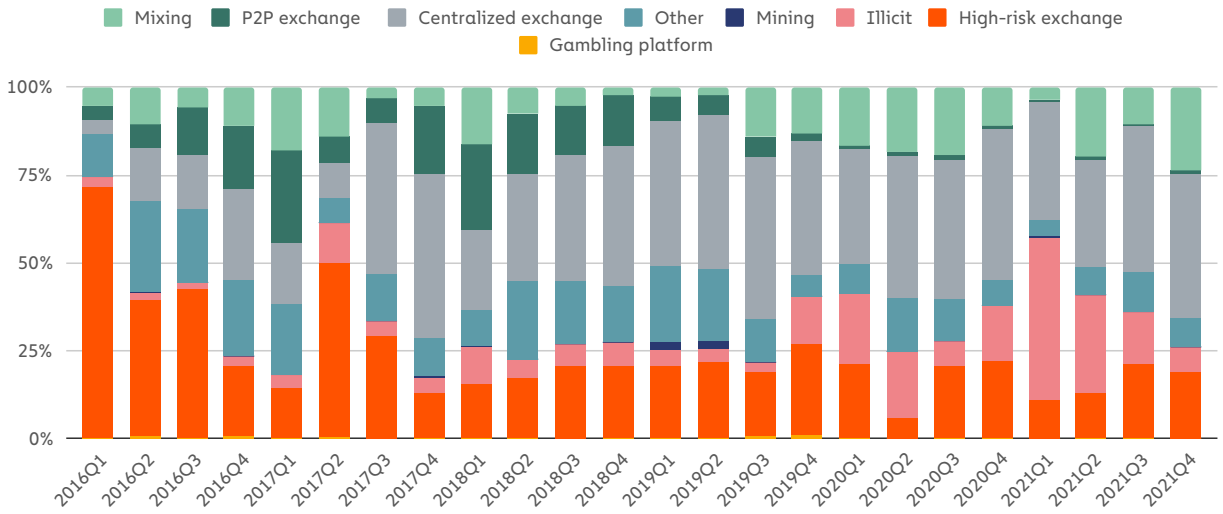
Share of ransomware funds going to third-party sellers | 2016–2021



16% of all funds sent by ransomware operators were spent on tools and services used to enable more effective attacks, compared to 6% in 2020. While it's possible some of that activity constitutes money laundering rather than the purchase of illicit services, we believe that increasing use of those services is one reason ransomware attackers became more effective in 2021, as evidenced by rising average victim payment sizes.

Another important trend to monitor in ransomware is money laundering. The graph below shows where attackers move the cryptocurrency they extort from victims.

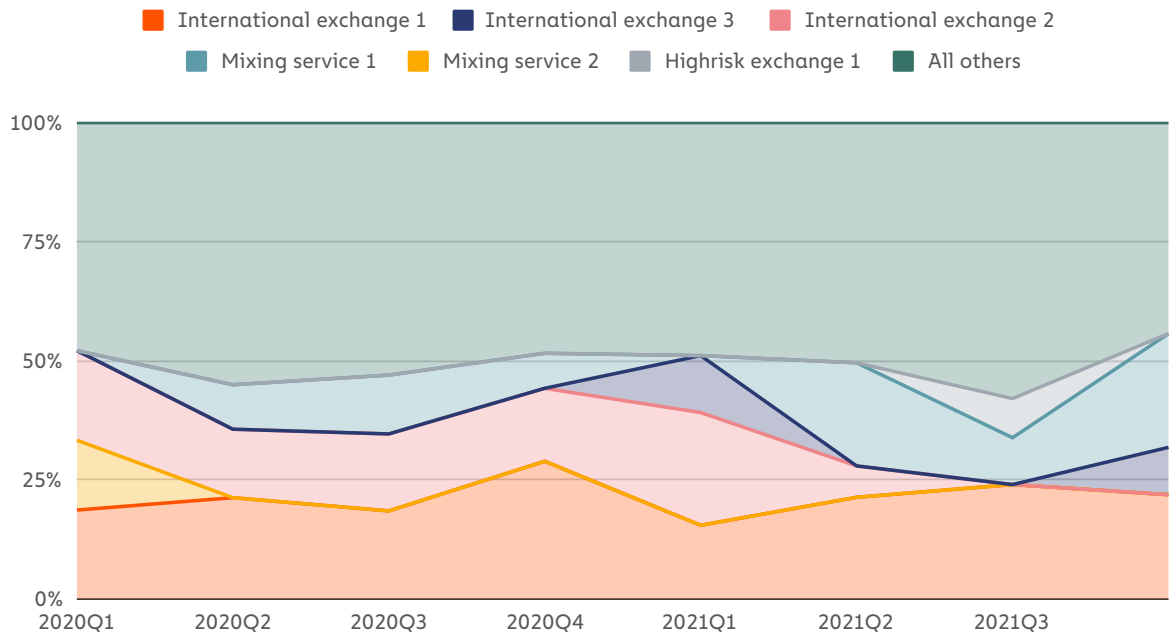
Destination of funds leaving ransomware addresses | 2016–2021



Over the last few years, most ransomware strains have laundered their stolen funds by sending them to centralized exchanges. Some are in the high-risk category, meaning that they tend to have relaxed compliance procedures, but mostly to mainstream exchanges with more established compliance programs. We also see substantial funds sent to both mixers and addresses associated with other forms of illicit activity.

The money laundering trends get even more interesting if we drill down to the individual services receiving funds from ransomware.

Services receiving funds from ransomware addresses | 2020–2021



Amazingly, 56% of funds sent from ransomware addresses since 2020 have wound up at one of six cryptocurrency businesses:

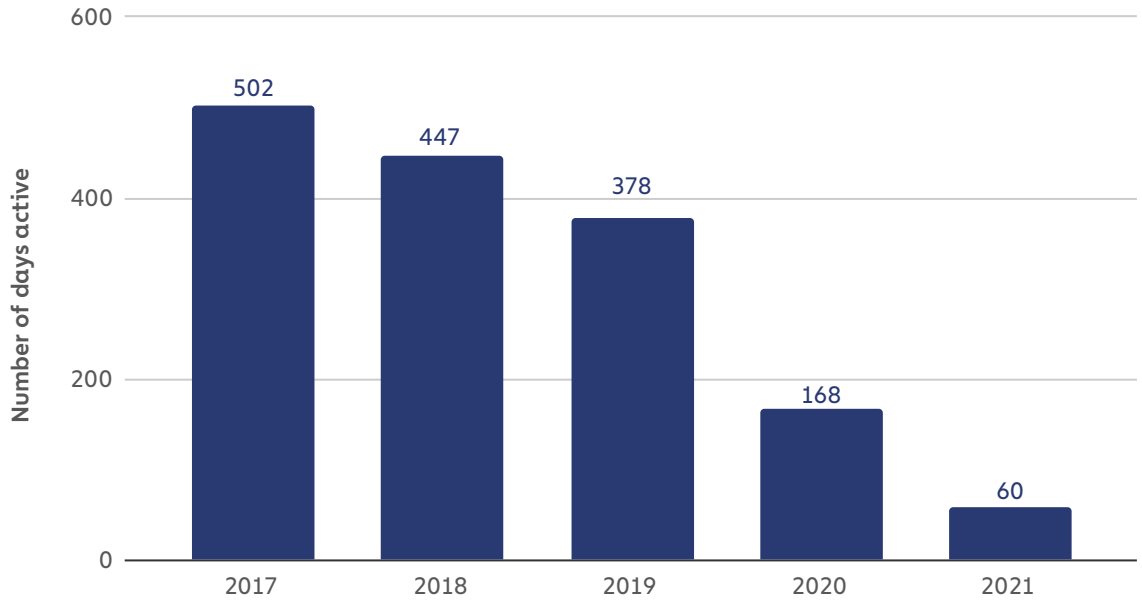
- Three large, international exchanges
- One high-risk exchange based in Russia
- Two mixing services

Similar to the rebranding activity we described above, these money laundering trends show how small the ransomware ecosystem really is. That's good news, as it means the strategy for fighting ransomware is likely simpler than it appears at first glance. By cracking down on the small number of services that facilitate this money laundering activity, law enforcement can significantly reduce attackers' options for cashing out, reducing the financial incentive to carry out ransomware attacks and hampering ransomware organizations' ability to operate.

2021's rebranding craze shows the ransomware ecosystem is smaller than we think

As we discussed above, most ransomware strains aren't active for very long. While this has always been the case to some degree, the trend has become even more pronounced in 2021.

Average lifespan of a ransomware strain | 2017–2021



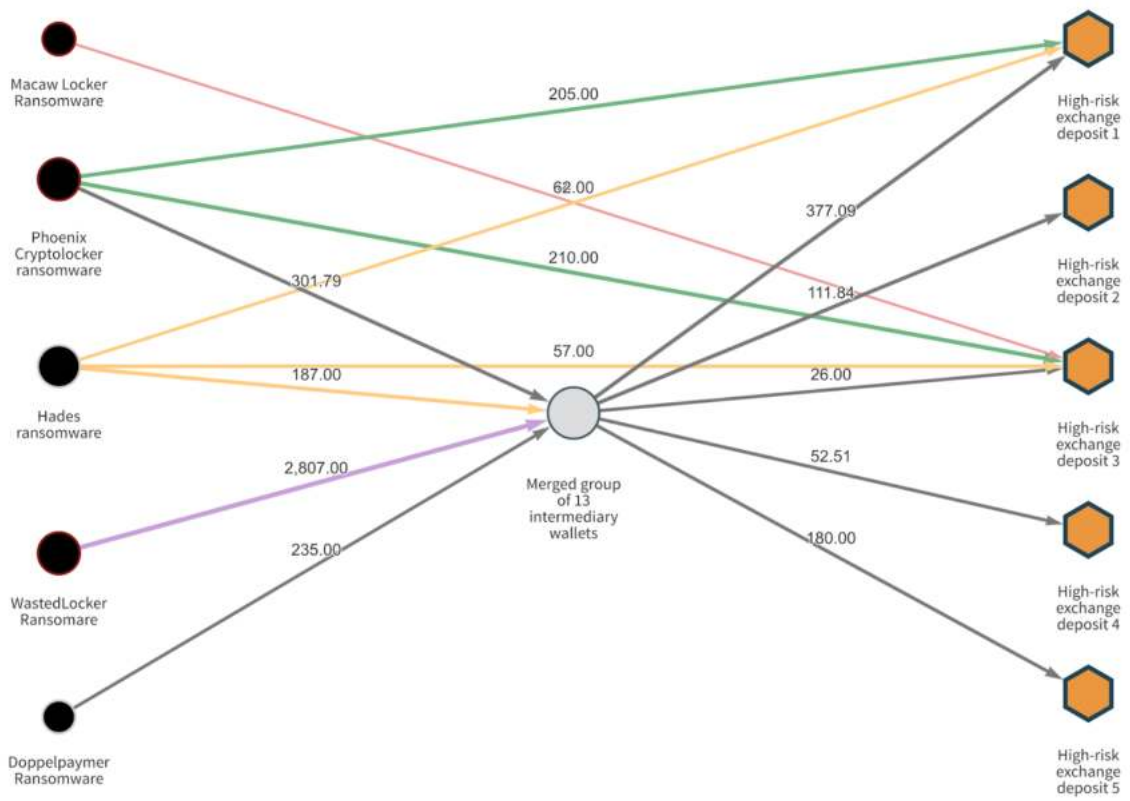
Two years ago, the average ransomware strain remained active for exactly one year. In 2021, the average strain is active for no more than two months. Why is the average ransomware lifespan dropping so quickly?

One big reason is rebranding. More than ever in 2021, cybersecurity researchers have noted instances of ransomware attackers publicly claiming to cease operations, only to relaunch later under a new name — the giveaway is usually similarities in the ransomware's code, as well as intelligence gathered from cybercriminal forums and blockchain analysis. So, while at least 140 ransomware strains were active in 2021, many of those strains were in fact run by the same cybercriminal groups.

These strains attempt to create the illusion that they belong to different cybercriminal organizations by setting up separate victim payment sites and other infrastructure, but share similarities in their code. Evil Corp, a Russia-based cybercriminal gang behind several ransomware attacks in recent years, has launched several rebranded strains throughout its history, including:

- **Doppelpaymer**
- **Bitpaymer**
- **WastedLocker**
- **Hades**
- **Phoenix Cryptolocker.** This strain is notable for "shutting down" after one attack that extorted $40 million — the largest known ransom ever paid.
- **Grief.** Grief exhibits code similarities to Doppelpaymer ransomware, including the telltale use of Dridex malware. As of 2021, Grief is notable for demanding ransomware payments in Monero.
- **Macaw.** Interestingly, Macaw uses a completely different negotiation method than previous Evil Corp strains. In this way, Macaw could be described less as a "rebrand" of an old strain and more as a unique strain launched by an existing ransomware organization.
- **PayloadBIN.** Many cybersecurity analysts have reported that Evil Corp's launch of the PayloadBIN strain is intended to look like a rebrand of an old strain used by another ransomware group, making PayloadBIN a double rebrand of sorts.

We can also see evidence of some of these strains' common ownership in their cryptocurrency transaction histories. Check out the Chainalysis Reactor graph below.

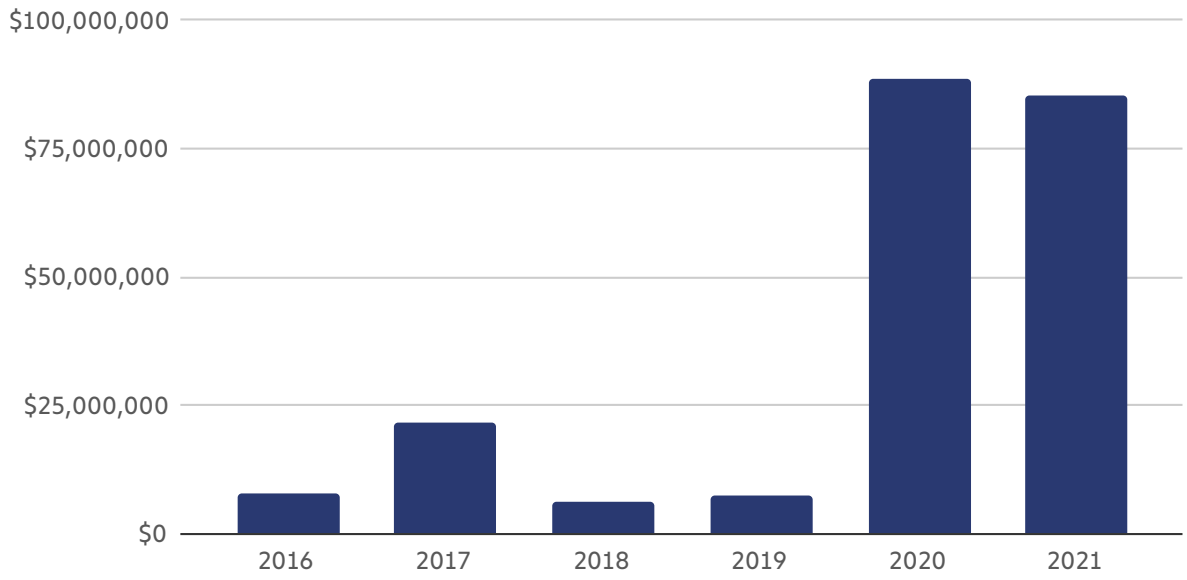


This graph shows the money laundering process for five of the Evil Corp ransomware strains we mentioned above. While all of them appear to be run by separate organizations, most send funds derived from attacks to the same group of intermediary wallets, and from there move funds to many of the same deposit addresses at high-risk exchanges.

But why does Evil Corp rebrand its ransomware strains so often? Most analysts believe it's an effort to evade sanctions. Evil Corp, whose leaders are suspected to have ties to the Russian government, has been sanctioned by the United States since December 2019. In October 2020, the U.S. Treasury's Office of Foreign Asset Control (OFAC) reiterated guidance that ransomware victims who pay ransoms to sanctioned groups could face penalties. This put Evil Corp in a bad position, as it meant that many victims and their representatives would likely be reluctant to pay them following due diligence on the sanctions risk. By rebranding, Evil Corp likely believes it can fool victims into paying before researchers can discover the potential sanctions risk.

Unfortunately, rebranding appears to have worked for Evil Corp in many cases, as victims paid at least $85 million in ransoms to strains associated with the organization.

Ransomware payment value to strains associated with Evil Corp | 2016–2021



Of course, Evil Corp isn't the only organization rebranding its ransomware strains. In July 2021, the group behind the DarkSide ransomware strain began launching attacks with a very similar strain called BlackMatter. This came following DarkSide's attack on Colonial Pipeline and the FBI's subsequent seizing of most of that ransom, and it's our belief that the rebrand came in response to pressure from law enforcement. One piece of evidence supporting this is BlackMatter's stated unwillingness to attack oil and gas companies — that would make sense for a rebranded DarkSide, as the group's attack on Colonial ended poorly for them.

The uptick in ransomware rebranding is an important reminder that the ransomware ecosystem is smaller than it appears at first glance. While new strains pop up all the time, many of them are ultimately run or deployed by the same groups and individuals, all of whom are likely feeling the pressure from law enforcement's increasing efforts to prevent attacks, seize extorted funds, and arrest the individuals responsible. Rebranding is one way of evading those efforts, and suggests that investigators and cybersecurity professionals may be best served by studying ransomware attackers at the organizational level, and focusing less on the unique strains.

Ransomware as a geopolitical weapon

Most ransomware attacks appear to be financially motivated. However, others appear to be motivated by geopolitical goals, and seem more geared toward deception, espionage, reputational damage and disruption of the enemy government's operations.

In cases where a ransomware strain contains no mechanism to collect payment or allow victims to recover their files, we can be more certain that money isn't the attackers' primary motivation. And that's exactly what we saw in a recent ransomware attack on Ukrainian government agencies by hackers believed to be associated with the Russian government.

As the Computer Emergency Response Team of Ukraine (CERT-UA) describes here, the attack occurred on the night of January 13, 2022, and disrupted several government agencies' ability to operate. The attack came against a backdrop of increasing tensions between the two countries, with Russian troop build-ups along the Ukrainian border causing concern that an invasion could be imminent. We saw a similar situation unfold in 2017, when tensions between the two nations were also running high. At that time, the Russia-based NotPetya ransomware strain, which contained no viable payment mechanism, targeted several Ukrainian organizations and was also widely judged to be a geopolitically motivated disruption attempt by the Russian military rather than a money-making effort.

Microsoft Security published its own analysis of the recent attack, noting that the ransomware strain in question — dubbed DEV-0586 or more commonly known as WhisperGate— has no way of returning victims' access to their files. Microsoft Security's blog also includes the message the ransomware group displayed to its Ukrainian victims.

```
Your hard drive has been corrupted.
In case you want to recover all hard drives
of your organization,
You should pay us $10k via bitcoin wallet
1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via
tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23054C057ECED5496F65
with your organization name.
We will contact you to give further instructions.
```

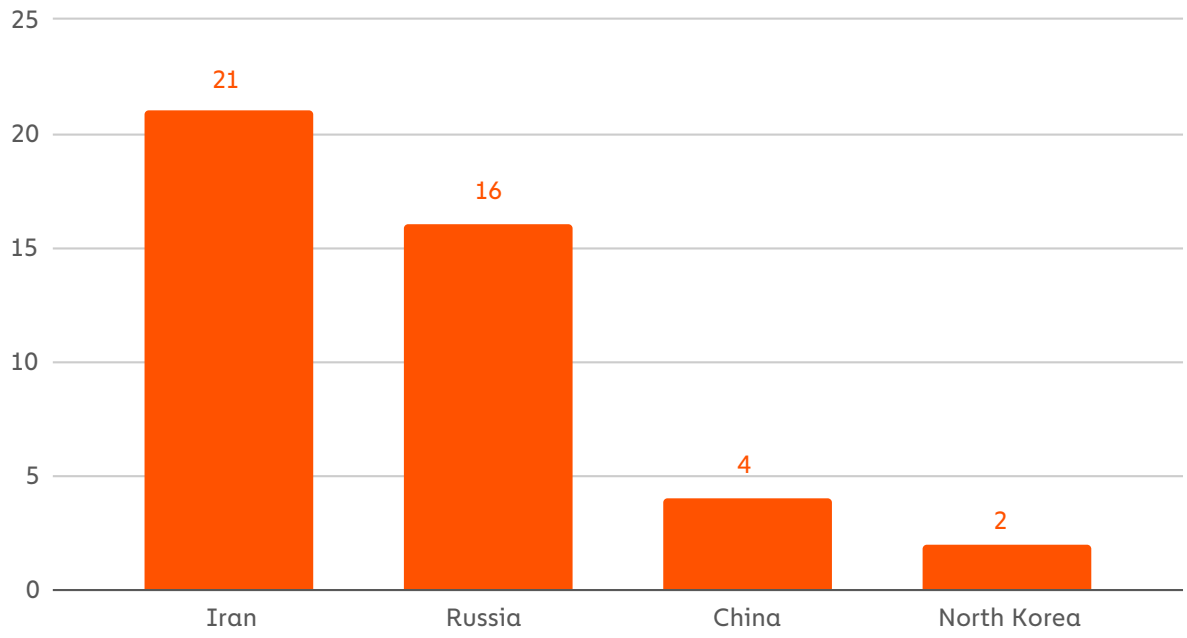
Credit: Microsoft Security Blog

DEV-0586's address doesn't have an extensive transaction history for us to draw from. But further analysis of the ransomware's technical characteristics indicates even more geopolitical gamesmanship. On January 26, CERT-UA released a report showing that DEV-0586 contains code repurposed from WhiteBlackCrypt, a ransomware strain active in 2021 that, like DEV-0586, is designed to wipe victims' systems rather than extort them for money. But there's a twist: WhiteBlackCrypt targeted Russian organizations rather than Ukrainian ones. Cybersecurity analysts believe DEV-0586's reuse of code previously

used by WhiteBlackCrypt, as well as the presence of other similarities linking the two strains, is a gambit by Russian hackers to make DEV-0586 appear to be of Ukrainian rather than Russian origin — in other words, a false flag attack. The gambit shows how far state actors using ransomware to attack foes will go to conceal their attacks' origins and maintain plausible deniability. We'll continue to monitor DEV-0586's address for more activity and provide updates when possible.

Russia-affiliated attackers aren't the only ones using ransomware for geopolitical ends. Cybersecurity analysts at Crowdstrike and Microsoft have concluded that many attacks by ransomware strains affiliated with Iran, mostly targeting organizations in the U.S., the E.U., and Israel, are geared more toward causing disruption or serving as a ruse to conceal espionage activity. Generally speaking, Chainalysis has seen significant growth over the last year in the number of ransomware strains attributed to Iranian cybercriminals in the past year — in fact, Iran accounts for more individual identified strains than any other country.

Number of ransomware strains with suspected links to specific countries



To be clear, many of those Iranian ransomware strains are used for conventional, financially motivated attacks by cybercriminals operating in the country. Iran has a highly educated population but limited occupational opportunities, which likely contributes to the allure of ransomware. However, other strains behave more like tools of espionage, extorting negligible amounts of cryptocurrency from victims. Other analysts have previously identified instances of strains affiliated with China, such as ColdLock, carrying out similar geopolitical attacks on Taiwanese organizations.

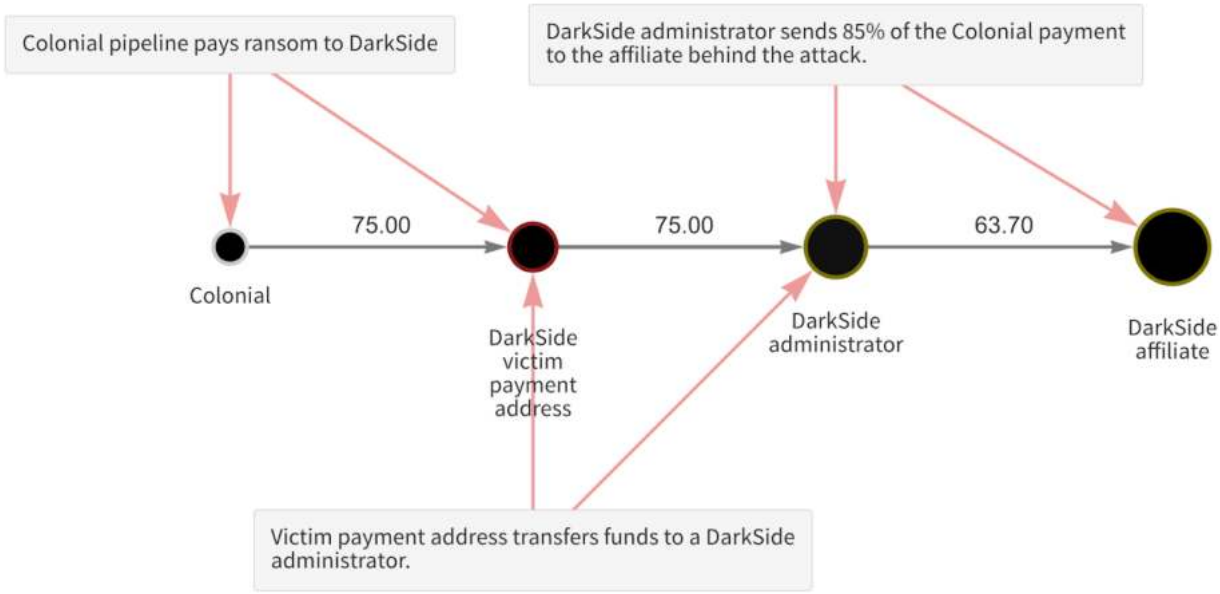
Ransomware is a useful cover for strategic denial and deception against enemy states because attacks can be carried out cheaply, and it gives the attacking nation some measure of plausible deniability, as they can always claim the attack was carried out by mere cybercriminals or another nation state. But even ransomware attacks carried out for non-financial reasons leave a trail on the blockchain. For that reason, it's crucial that agencies focused on national security understand how to trace funds using blockchain analysis, as this is the key to identifying the individuals involved in the attacks themselves, the tools they use, and how they launder any funds obtained from victims.

Chainalysis in action: How FBI investigators tracked and seized funds from DarkSide following the Colonial Pipeline ransomware attack

On May 7, 2021, Colonial Pipeline, an oil pipeline company that supplies energy to the southeastern United States, fell victim to a ransomware attack, forcing it to temporarily cease operations. Within hours of the attack, Colonial paid a ransom of 75 Bitcoin — worth roughly $4.4 million at the time — to DarkSide, the Russia-based cybercriminal group responsible for the attack. Six days later, Colonial was able to resume operations, but during that time, the shutdown combined with panic buying as the news spread resulted in fuel shortages in several areas.

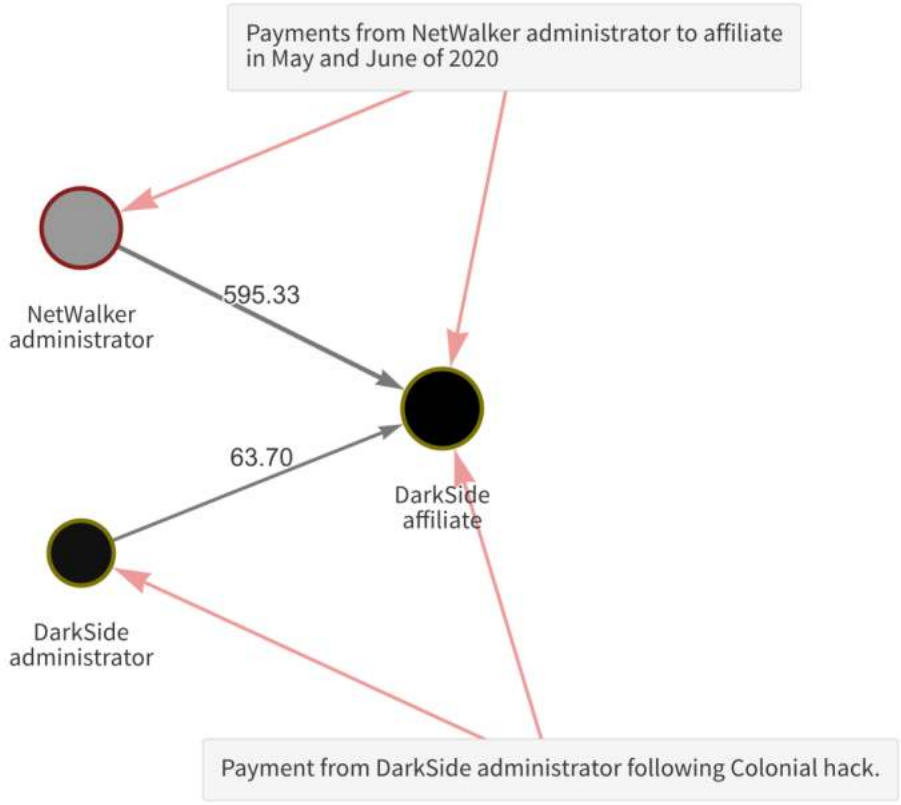
One month later, there was good news: The Department of Justice announced that it had managed to seize $2.3 million worth of Bitcoin from Colonial's ransom payment following an FBI investigation. Chainalysis is proud to say that our tools aided the FBI, and that we can now share details of how investigators tracked the funds following the attack.

Let's start by looking at the ransom payment itself and the initial movement of funds using Chainalysis Reactor.



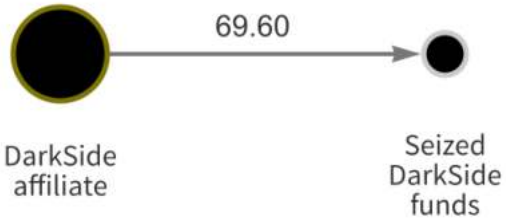
First, on the left, we see the initial payment of 75 Bitcoin from Colonial to the address provided by the attackers. Soon after, that address transferred the funds to an address controlled by DarkSide's administrators, who then sent 63.7 Bitcoin — 85% of Colonial's payment — to the affiliate who controlled the attack. That point is key — DarkSide operates on the Ransomware as a Service (RaaS) model, meaning the affiliates who carry out the attack effectively "rent" usage of DarkSide's technology from the core group of administrators who created and manage the ransomware strain itself. Administrators take a small cut of the payment from each successful attack in return, as we see above.

Interestingly, the affiliate in question had previously received payments from addresses associated with NetWalker, another ransomware strain operating on the RaaS model that was disrupted by law enforcement in January 2021.



The affiliate received a total of 595.3 Bitcoin from the NetWalker administrator in a series of four payments in late May and early June of 2020, suggesting that they may have also carried out attacks for that strain as well. This wouldn't be surprising, as we've noted other instances of affiliate overlap between ransomware strains in the past.

After tracking the funds to the affiliate's address, FBI investigators were able to seize the funds on May 28, 2021.



The seizure represents a huge step forward in the fight against ransomware, and especially ransomware strains that attack our critical infrastructure. We continue to monitor the movement of funds using our tools so that we can provide helpful insight to authorities as they investigate further and, hopefully, seize the remainder of the funds.

What's next for ransomware?

Ransomware isn't just dangerous. It's also one of the most dynamic, constantly changing forms of cryptocurrency-based crime. Between constant rebrands, shifting money laundering strategies, and the influence of geopolitics, it's hard to know what's coming next. One trend to look out for though is Monero ransoms. Analysts have noted that more and more attackers are demanding victims pay in Monero, likely due to the heightened anonymity it offers. While the vast majority of attackers continue to demand Bitcoin, law enforcement and cybersecurity professionals should keep an eye out for ransom notes requesting Monero or assets associated with other protocols with privacy-enhancing features, as this will change the investigative tactics they must employ.

There's only one thing that's certain in ransomware: Law enforcement will continue to investigate the cybercriminals responsible, and Chainalysis software and services will be there to help them every step of the way. Events like the seizure of funds from DarkSide show that we're making progress, and we look forward to keeping up the fight in 2022.

Malware

Meet the Malware Families Helping Hackers Steal and Mine Millions in Cryptocurrency

When it comes to cryptocurrency theft, industry observers tend to focus on attacks against large organizations — namely hacks of cryptocurrency exchanges or ransomware attacks against critical infrastructure. But over the last few years, we've observed hackers using malware to steal smaller amounts of cryptocurrency from individual users.

Using malware to steal or extort cryptocurrency is nothing new. In fact, nearly all ransomware strains are initially delivered to victims' devices through malware, and many large-scale exchange hacks also involve malware. But these attacks take careful planning and skill to pull off, as they're typically targeted against deep-pocketed, professional organizations and, if successful, require hackers to launder large sums of cryptocurrency. With other types of malware, less sophisticated hackers can take a cheaper "spray-and-pray" approach, spamming millions of potential victims and stealing smaller amounts from each individual tricked into downloading the malware. Many of these malware strains are available for purchase on the darknet, making it even easier for less sophisticated hackers to deploy them against victims.

We're equipping our partners in law enforcement, compliance, and cybersecurity to combat this problem by adding a new tag for malware operator addresses in all Chainalysis products. Below, we'll examine trends in hackers' usage of cryptocurrency-focused malware over the last decade and share two case studies to help you understand this under-discussed area of crypto crime.

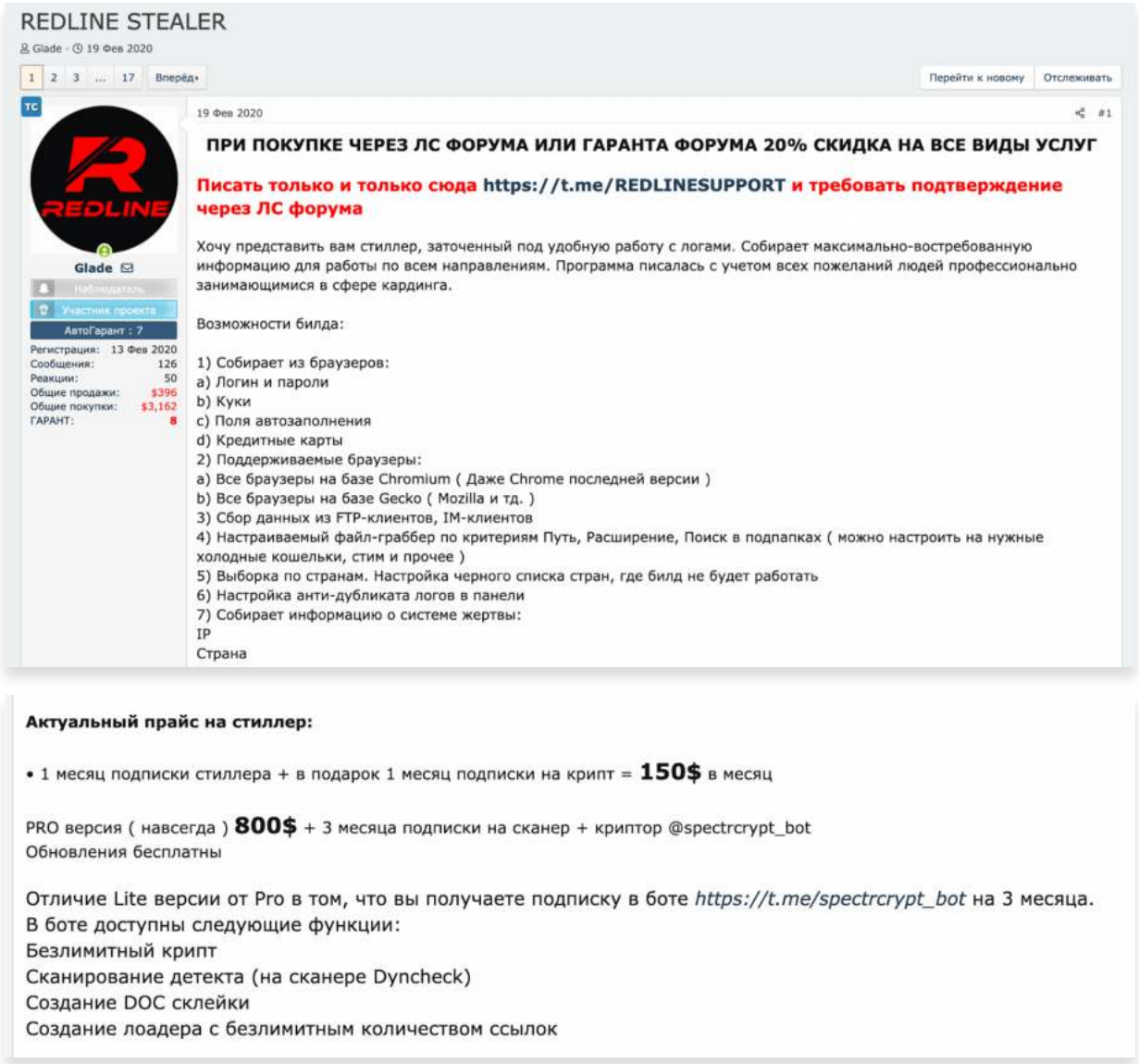
Malware and cryptocurrency summarized

Malware refers to malicious software that carries out harmful activity on a victim's device, usually without their knowledge. Malware-powered crime can be as simple as stealing information or money from victims, but can also be much more complex and grand in scale. For instance, malware operators who have infected enough devices can use those devices as a botnet, having them work in concert to carry out distributed denial-of-service (DDOS) attacks, commit ad fraud, or send spam emails to spread the malware further.

The malware families we discuss here are all used to steal cryptocurrency from victims, though some of them are used for other activities as well. The grid below breaks down the most common types of cryptocurrency-focused malware families.

Type	Description	Example
Info stealers	Collect saved credentials, files, autocomplete history, and cryptocurrency wallets from compromised computers.	Redline
Clippers	Can insert new text into the victim's clipboard, replacing text the user has copied. Hackers can use clippers to replace cryptocurrency addresses copied into the clipboard with their own, allowing them to reroute planned transactions to their own wallets.	HackBoss
Cryptojackers	Makes unauthorized use of victim device's computing power to mine cryptocurrency.	Glupteba
Trojans	Virus that looks like a legitimate program but infiltrates victim's computer to disrupt operations, steal, or cause other types of harm.	Mekotio banking trojan

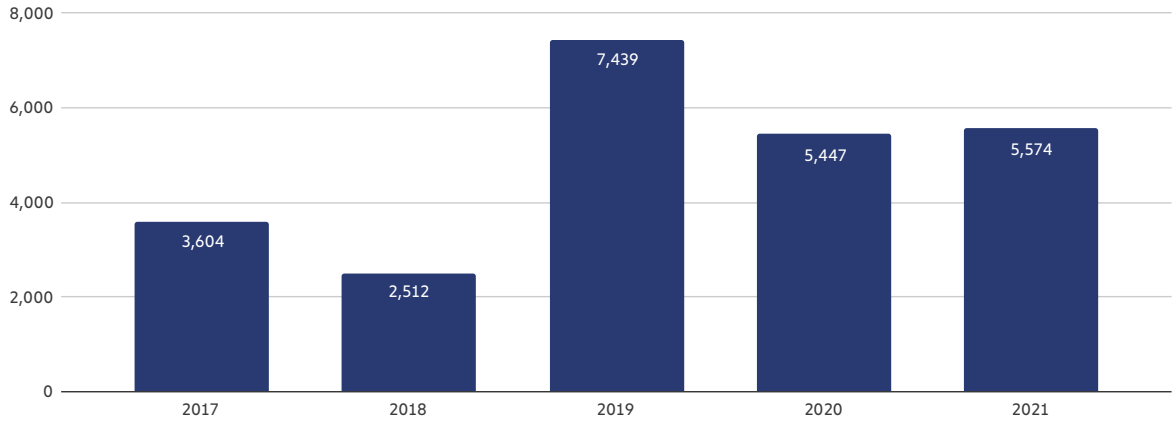
Many of the malware families described above are available to purchase for relatively little money on cybercriminal forums. For instance, the screenshots below show an advertisement for Redline, an info stealer malware, posted on a Russian cybercrime forum.



The seller offers cybercriminals one month of Redline access for $150 and lifetime access for $800. Buyers also get access to Spectrum Crypt Service, a Telegram-based tool that allows cybercriminals to encrypt Redline so that it's more difficult for victims' antivirus software to detect it once it's been downloaded. The proliferation of cheap access to malware families like Redline means that even relatively low-skilled cybercriminals can use them to steal cryptocurrency. Law enforcement and compliance teams must keep this in mind, and understand that the malware attacks they investigate aren't necessarily carried out by the administrators of the malware family itself, but instead are often carried out by smaller groups renting access to the malware family, similar to ransomware affiliates.

The graph below shows the number of victim transfers to cryptocurrency addresses associated with a sample of malware families in the info stealer and clipper categories investigated by Chainalysis.

Transfers to known info stealer and clipper malware addresses | 2017–2021

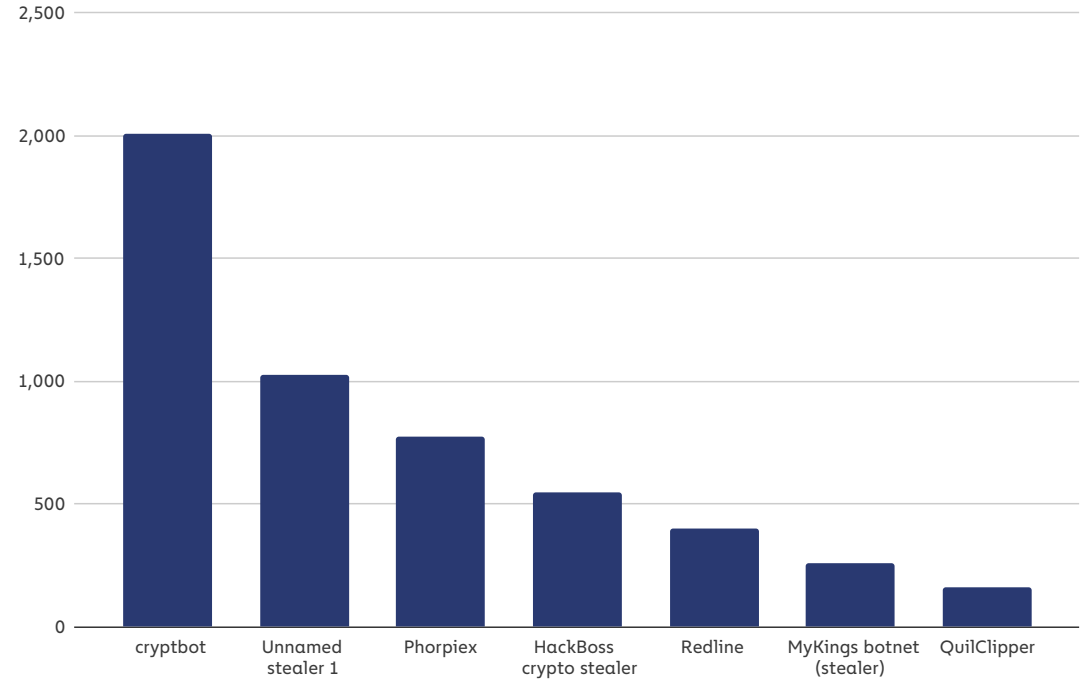


Note: This graph does not reflect activity by cryptojackers or ransomware.

Overall, the malware families in this sample have received 5,574 transfers from victims in 2021, up from 5,447 in 2020.

Which malware families were most active?

Sample of malware strains by number of cryptocurrency transfers from victims | 2021



Note: This graph does not reflect activity by cryptojackers or ransomware.

Cryptbot, an infostealer that takes victims' cryptocurrency wallet and account credentials, was the most prolific malware family in the group, raking in almost half a million dollars in pilfered Bitcoin. Another prolific family is QuilClipper, a clipboard stealer or "clipper," ranked eighth on the graph above. Clippers can be used to insert new text

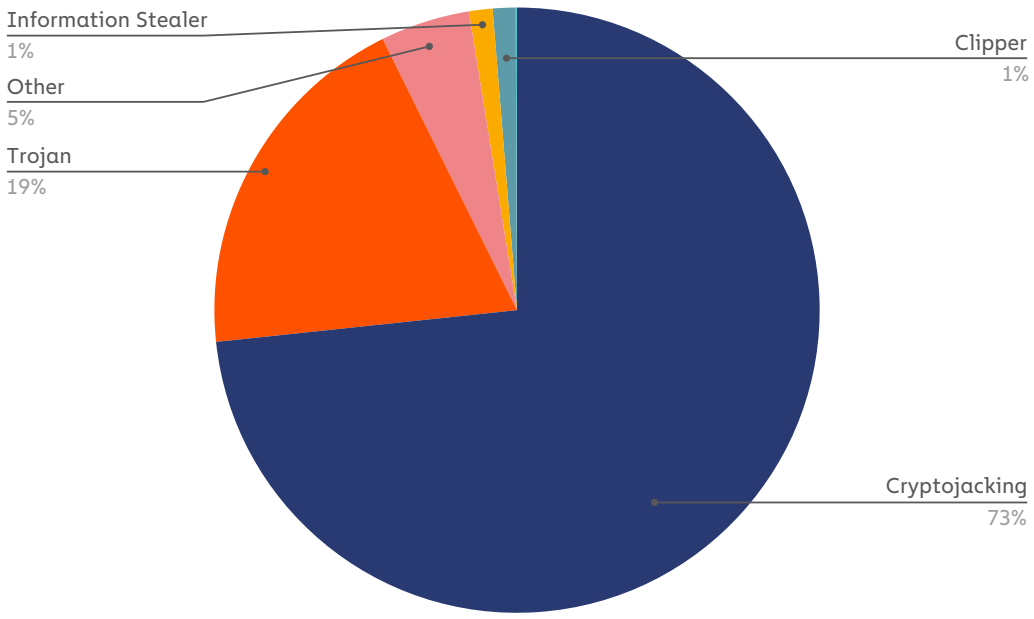
into the "clipboard" that holds text a user has copied, usually with the intent to paste elsewhere. Clippers typically use this functionality to detect when a user has copied a cryptocurrency address to which they intend to send funds — the clipper malware effectively hijacks the transaction by then substituting an address controlled by the hacker for the one copied by the user, thereby tricking the user into sending cryptocurrency to the hacker.

However, none of those numbers reflect totals from what we believe to be the most prolific type of cryptocurrency-focused malware: Cryptojackers.

Cryptojacker activity is murky but substantial

Cryptojackers obtain funds for malware operators by utilizing the victim's computing power to mine cryptocurrency — usually Monero, but we've seen Zcash and Ethereum mined as well. Since funds are moving directly from the mempool to mining addresses unknown to us, rather than from the victim's wallet to a new wallet, it's more difficult to passively collect data on cryptojacking activity the way we can other forms of cryptocurrency-based crime. However, we know it's a big problem. In 2020, Cisco's cloud security division reported that cryptojacking malware affected 69% of its clients, which would translate to an incredible amount of stolen computer power, and therefore a significant amount of illicitly-mined cryptocurrency. A 2018 report from Palo Alto Networks estimated that 5% of all Monero in circulation was mined by cryptojackers, which would represent over $100 million in revenue, making cryptojackers the most prolific form of cryptocurrency-focused malware.

Total value received by malware type

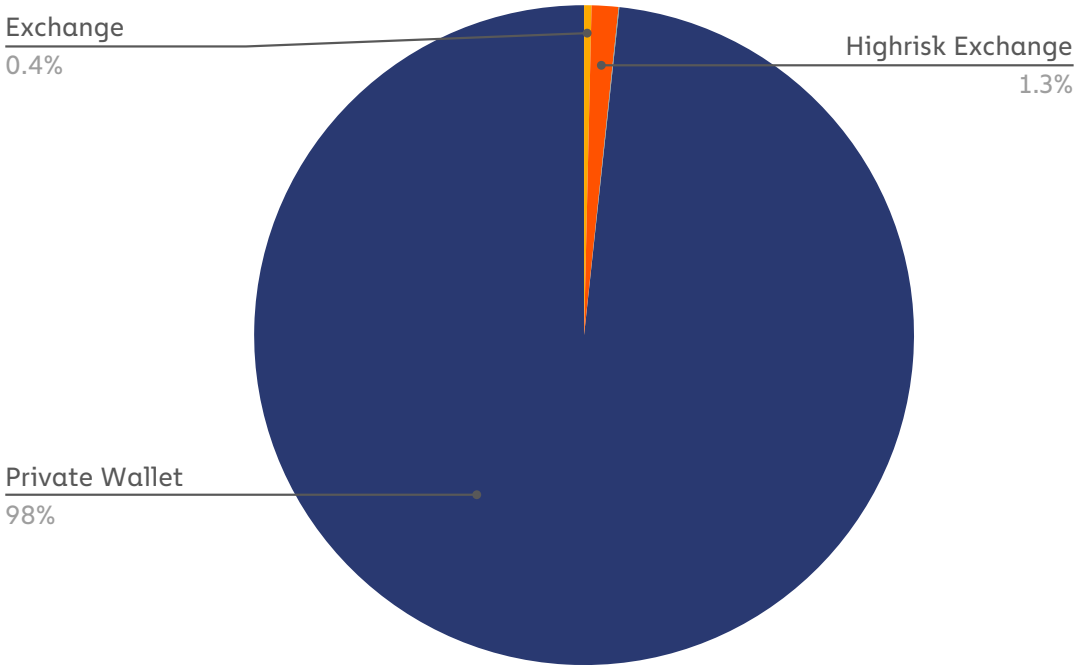


These numbers are likely only scratching the surface for cryptojacking. As we identify more malware families involved in this activity, we expect to learn that total revenue for the category is even bigger than it currently appears.

Malware and money laundering

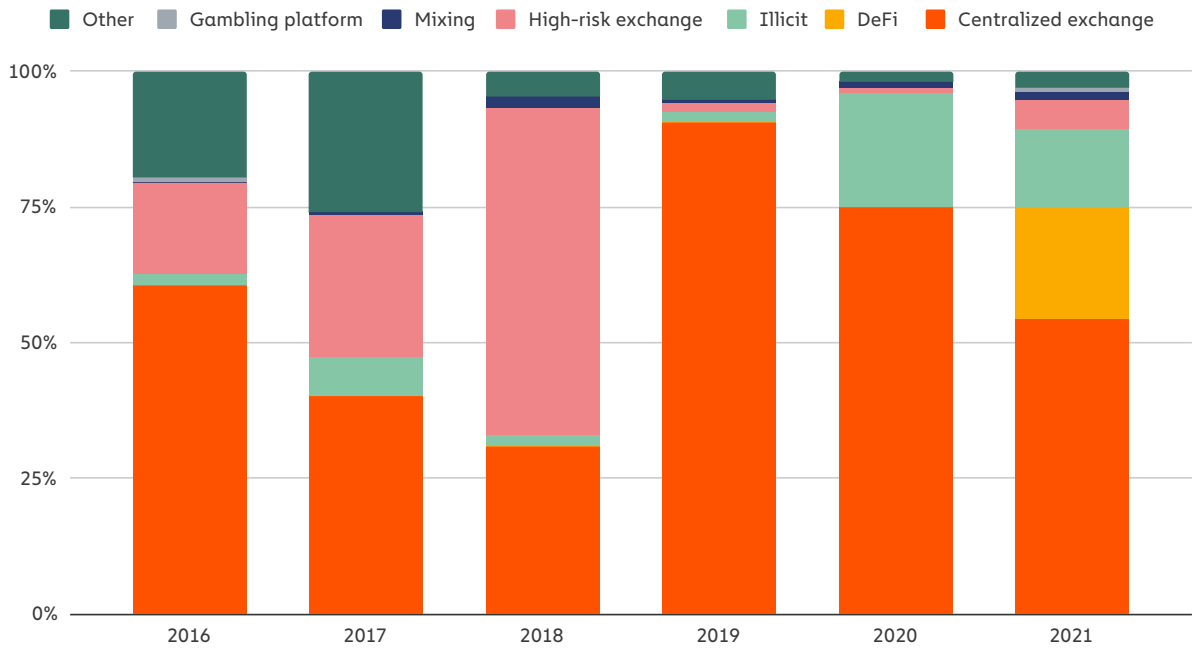
The vast majority of malware operators receive initial victim payments at private wallet addresses, though a few use addresses hosted by larger services. Of that smaller group, the majority use addresses hosted by exchanges — mostly high-risk exchanges that have low or no KYC (Know Your Customer) requirements.

Malware operator addresses by hosting platform



After receiving cryptocurrency from victims, malware operators then send the majority of funds on to addresses at centralized exchanges.

Destination of funds leaving malware family addresses | 2016–2021



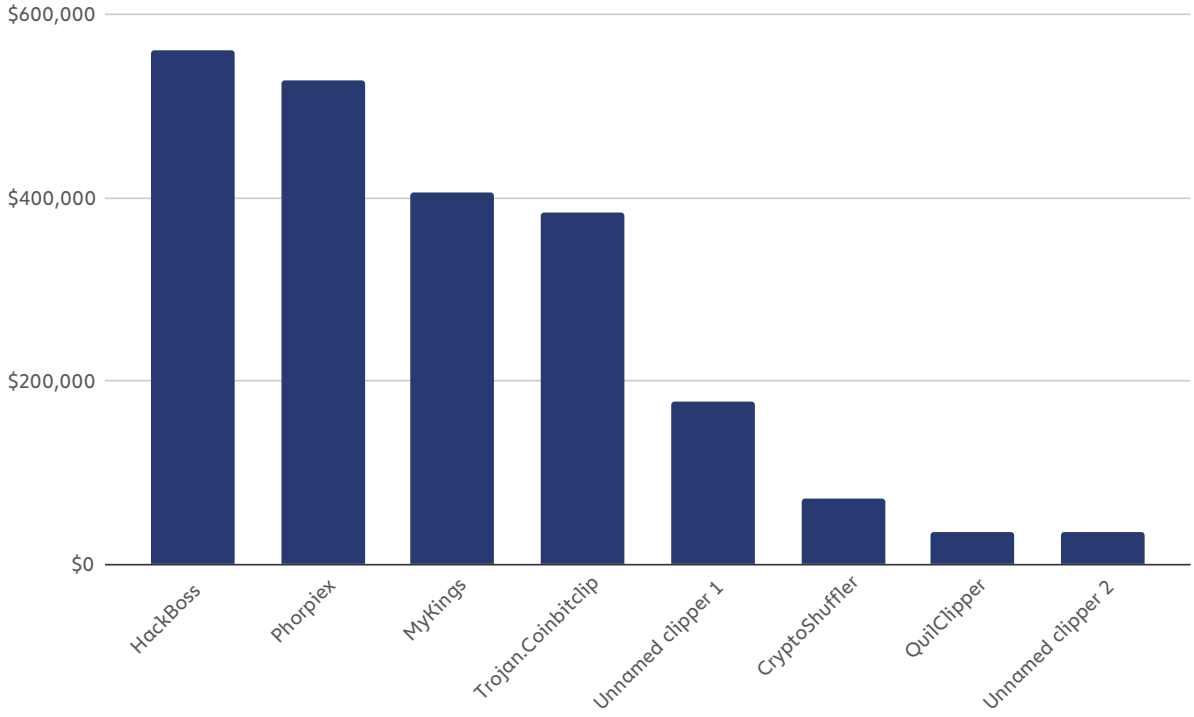
However, that majority is slim and getting slimmer. Exchanges only received 54% of funds sent from malware addresses in 2021, down from 75% in 2020. DeFi protocols make up much of the difference at 20% in 2021, after having received a negligible share of malware funds in 2020. Illicit services seemingly unrelated to malware — mostly darknet markets — are also a significant money laundering avenue for malware operators, having received roughly 15% of all funds sent from malware addresses in 2021.

Malware-based cryptocurrency theft is difficult to investigate in part due to the large number of less sophisticated cybercriminals who can rent access to these malware families. But studying how cybercriminals launder stolen cryptocurrency may be investigators' best bet for finding those involved. Using blockchain analysis, investigators can follow the funds, find the deposit addresses cybercriminals use to cash out, and subpoena the services hosting those addresses to identify the attackers.

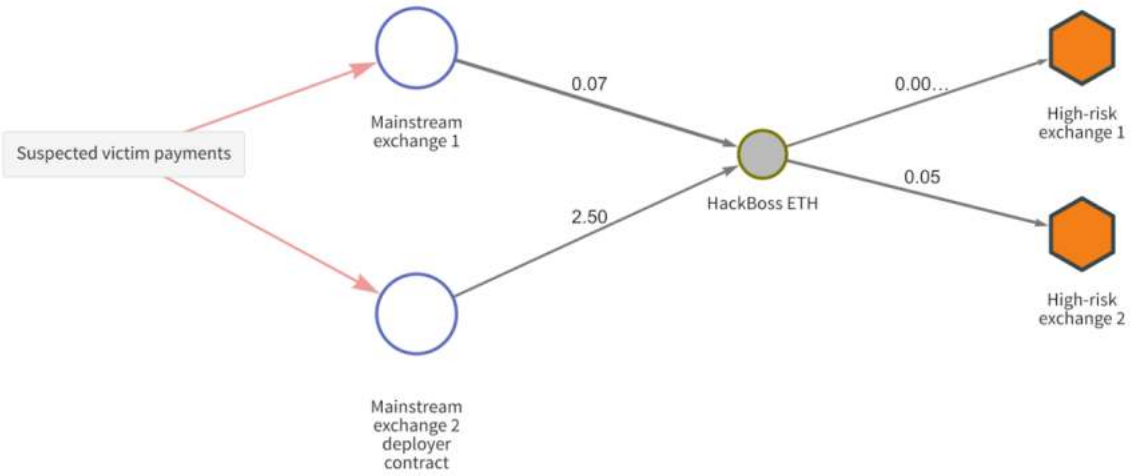
Investigating the HackBoss clipper

According to Chainalysis data, the HackBoss clipper stole over $80,000 worth of cryptocurrency throughout 2021. Since 2012, HackBoss has been the most prolific clipper malware overall, having taken over $560,000 from victims in assets like Bitcoin, Ethereum, Ripple, and more.

Clipper malware families by all-time revenue



Interestingly, HackBoss is targeted at fellow hackers rather than what we think of as ordinary victims. According to reporting from Avast.io's Decoded, HackBoss is distributed through a Telegram channel that purports to provide hacking tools such as social media site crackers. However, instead of those tools, the channel's users are actually downloading the HackBoss clipper, which steals cryptocurrency from them by inserting its own addresses into the clipboard when victims attempt to copy and paste another address to carry out a cryptocurrency transaction.



The Chainalysis Reactor graph above shows HackBoss receiving cryptocurrency from victims on the left. From there, the malware operators move funds to deposit addresses hosted by high-risk exchanges.

While HackBoss is uniquely targeted at hackers attempting to download tools to carry out their own cybercrimes, most other clippers are targeted at ordinary cryptocurrency users. It's extremely difficult to know if one has fallen victim to a clipper until a transaction has been hijacked given how long and complex cryptocurrency addresses are — most people don't read through the recipient's entire address between pasting it into their wallet and sending a transaction. However, that may be necessary for users trying to be as careful as possible. At the very least, cryptocurrency users need to be vigilant about what links they click and programs they download, as there are several active malware strains — not just clippers, but others too — attempting to steal their funds.

Case study: Glupteba botnet hijacks computers to mine Monero and harnesses the Bitcoin blockchain to evade shutdown

A complaint filed by Google in late 2021 named multiple Russian nationals and entities alleged to be responsible for operating the Glupteba botnet, which has compromised over 1 million machines. Glupteba's operators have used these machines for several criminal schemes, including utilizing their computing power to mine cryptocurrency — specifically, in this case, Monero — in a practice known as cryptojacking.

Perhaps most notable is Glupteba's use of the Bitcoin blockchain to withstand attempts to take it offline, encoding updated command-and-control servers (C2) into the Op_Returns of Bitcoin transactions. Google used Chainalysis software and Chainalysis Investigative Services to analyze the Bitcoin addresses and transactions responsible for sending updated C2 instructions. Below, we'll break down how the Glupteba botnet uses the Bitcoin blockchain to defend itself and what it means for cybersecurity and law enforcement.

A primer on the Glupteba botnet

The cybercriminals behind the Glupteba botnet have used it to carry out a variety of criminal schemes. In addition to cryptojacking, the botnet has been used to acquire and sell Google account information stolen from infected machines, commit digital advertising fraud, and sell stolen credit card data.

Google was able to identify the individuals named in the complaint by obtaining and examining an IP address used by one of Glupteba's C2 servers. All individuals were also

listed as owners or administrators of shell companies connected to Glupteba-related crimes, such as one used to sell fraudulent digital advertising impressions supplied by the botnet. Google was able to successfully take down the current C2 server, however as Glupteba has proven to be infallible against these actions through it's blockchain failsafe, we will soon see a new C2 assigned.

How Glupteba weaponizes the blockchain

In order to direct botnets, cybercriminals rely on command-and-control (C2) servers, which allow them to send commands to machines infected with malware. Botnets look for domain addresses controlled by their C2 servers in order to receive instructions, with directions on where to look for those domain addresses hard coded into the malware itself.

In order to combat botnets, law enforcement and cybersecurity professionals try to take those domains offline so that the botnets can no longer receive instructions from the C2 server. In response, botnet operators typically set up a number of backup domains in case the active domain is taken down. Most malware algorithmically generates new domain addresses for botnets to scan until they find one of those backups, allowing them to receive new instructions from the C2 server.

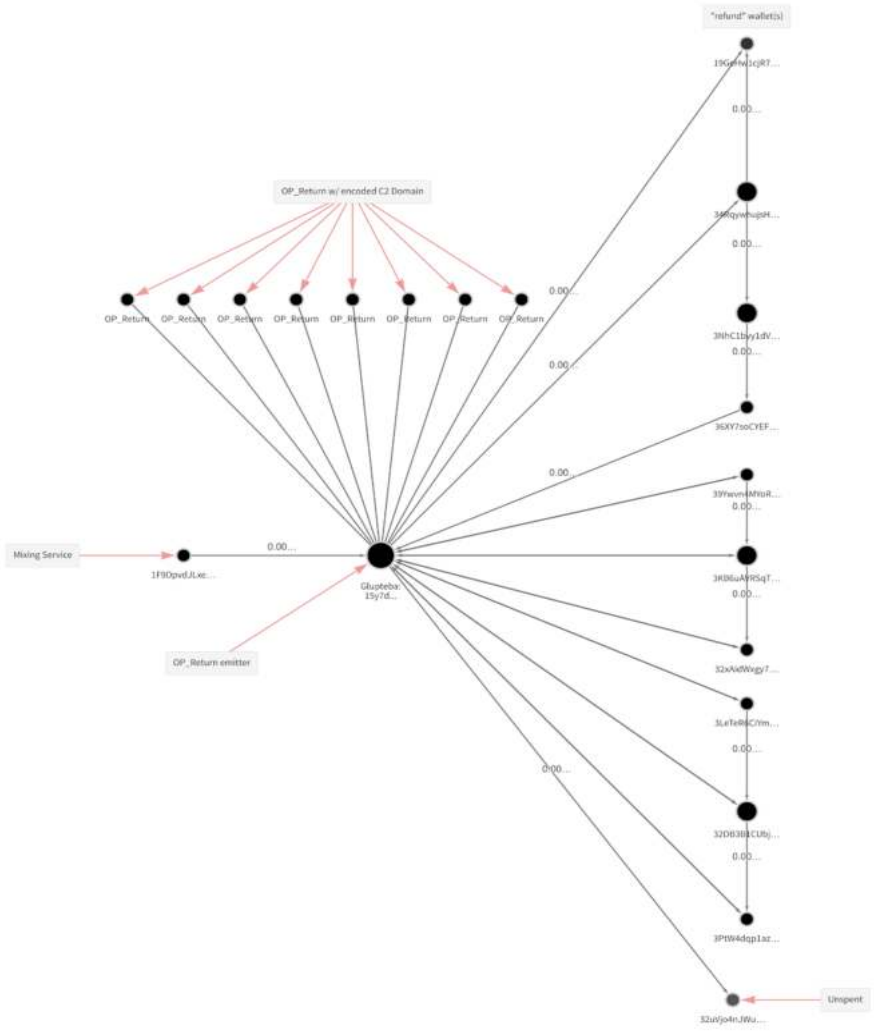
However, Glupteba does something new. When its C2 server is disrupted, Glupteba is programmed to search the Bitcoin blockchain for transactions carried out by three addresses controlled by its operators. Those addresses carry out transactions of little or no monetary value, with encrypted data written into the transaction's Op_Return field, which is used to mark transactions as invalid. Glupteba malware can then decode the data entered into the Op_Return field to obtain the domain address of a new C2 server.

In other words, whenever one of Glupteba's C2 servers is shut down, it can simply scan the blockchain to find the new C2 server domain address, hidden amongst hundreds of thousands of daily transactions. This tactic makes the Glupteba botnet extremely difficult to disrupt through conventional cybersecurity techniques focused on disabling C2 server domains. This is the first known case of a botnet using this approach.

Here's what we know about the three Bitcoin addresses we've identified as being used by Glupteba's operators to keep the botnet online:

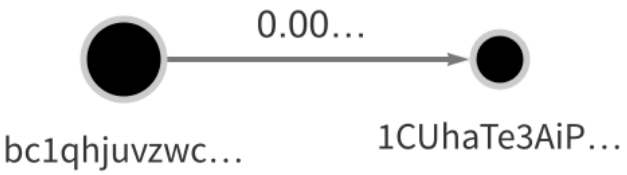
Address	Dates active	Number of transfers	Number of Op_Returns
15y7dskU5TqNHXRtu5wzBpXdY5mT4RZNC6	6/17/2019 - 5/13/2020	32	8
1CgPCp3E9399ZFodMnTSSvaf5TpGiym2N1	4/8/2020 - 10/19/2021	16	6
1CUhaTe3AiP9Tdr4B6wedoe9vNsymLiD97	10/13/21 - present	18	6

Combined, the three addresses have only transacted a few hundred dollars' worth of Bitcoin, but the messages encoded into the Op_Returns on some of those transactions have helped the Glupteba botnet remain operational. Let's look more closely at address 157d... in Chainalysis Reactor as an example.



We see that the Glupteba address received its initial funding from a mixing service, before initiating the invalid transactions with Op_Returns we see at the top of the graph. The funds associated with those invalid transactions then travel to the refund wallets on the right, and eventually back to the original Glupteba address. The other two addresses show similar transaction patterns. Google identified the three Glupteba addresses and brought them to Chainalysis, at which point our investigators were able to decode the data contained in the Op_Returns' message fields, allowing them to discover the new C2 server domain addresses being sent to the botnet.

Like address 15y7d..., address 1CgPC... was initially funded through outputs from mixing transactions. However, the third address, 1Cuha..., received initial funding from another private wallet address: bc1qhjuvzwcv0pp68kn2sqvx3d2k3pqfllv3c4vywd.



Interestingly, other transactions sent by bc1qh... have been associated with Federation Tower, a luxury office building in Moscow that also housed Suex, a now-sanctioned cryptocurrency OTC broker involved in money laundering for several forms of cyber-crime, including ransomware. Reporting from Bloomberg and The New York Times discusses other cryptocurrency businesses headquartered in Federation Tower, including EggChange, an exchange that's also been linked to cybercrime and whose founder, Denis Dubnikov, was arrested by U.S. authorities in November 2021. These links raise more questions about the interconnectedness of illicit, Russia-based cryptocurrency businesses associated with malware and ransomware attacks.

Glupteba shows why all cybersecurity teams need to understand cryptocurrency and blockchain analysis

Glupteba's blockchain-based method of avoiding the shutdown of its botnet represents a never-before-seen threat vector for cryptocurrencies. In the private sector, cryptocurrency businesses and financial institutions have thus far typically been the ones tackling cases involved in blockchain analysis, usually from an AML/CFT compliance perspective. But this case shows that cybersecurity teams at virtually any company that could be a target

for cybercriminals — especially those possessing large amounts of sensitive customer data — must be well-versed in cryptocurrency and blockchain analysis in order to stay ahead of cybercriminals. At Chainalysis, we're eager to work with those teams to help them understand how our tools can assist them in diagnosing and fighting these threats, so that cryptocurrencies can't be weaponized against them or their users.

The convergence of malware and cryptocurrency: Same cybercriminals, new methods

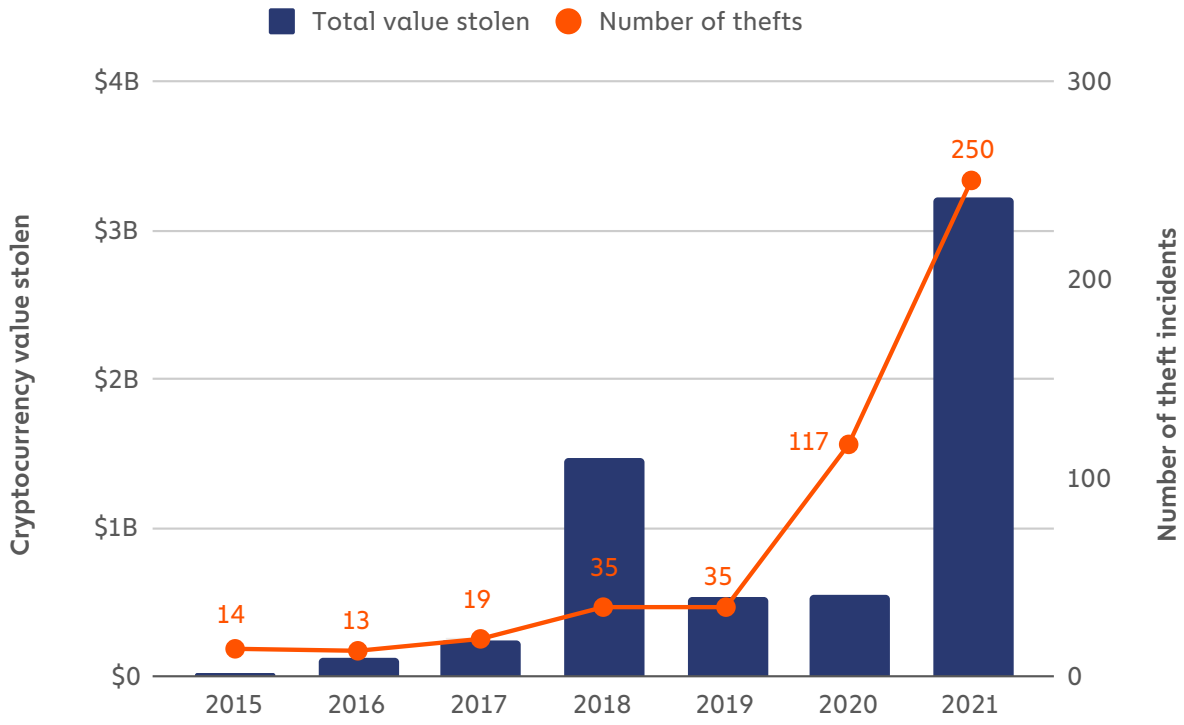
The cybersecurity industry has been dealing with malware for years, but the usage of these malicious programs to steal cryptocurrency means cybersecurity teams need new tools in their toolbox. Chainalysis gives cybersecurity teams new avenues of investigation for malware, allowing them to take advantage of blockchains' transparency and track the movement of funds that have been stolen until they reach an address whose owner can be identified. Likewise, cryptocurrency compliance teams already well-versed in blockchain analysis must educate themselves on malware in order to ensure these threat actors aren't taking advantage of their platforms to launder stolen cryptocurrency.

Stolen Funds

More Than $3 Billion Stolen in 2021 As DeFi Thefts Leap 1,330%

2021 was a big year for digital thieves. Throughout the year, $3.2 billion in cryptocurrency was stolen from individuals and services — almost 6x the amount stolen in 2020.

Total value stolen and total number of thefts | 2015–2021



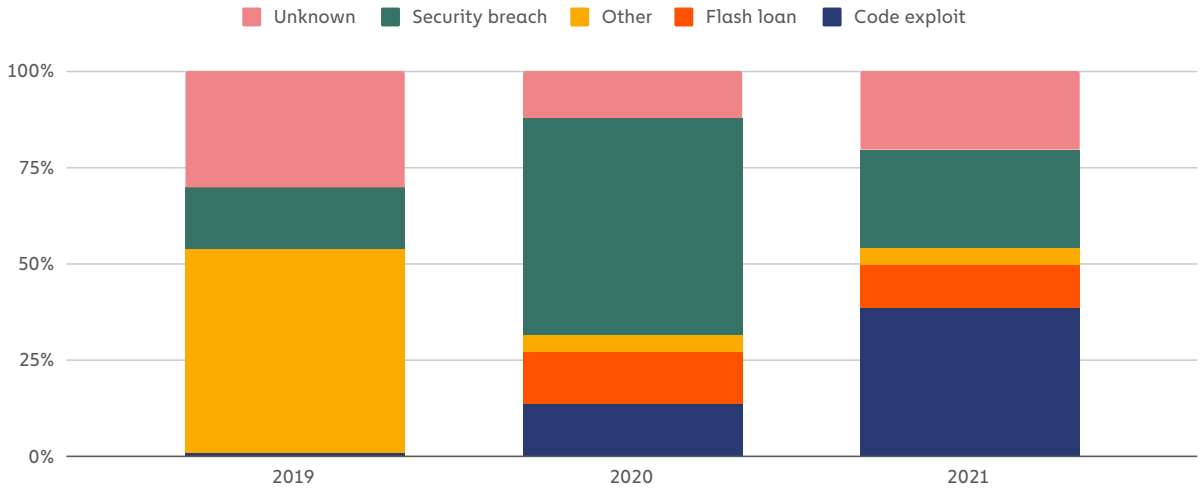
And that's just part of the story: Approximately $2.3 billion of those funds were stolen from DeFi platforms in particular, and the value stolen from these protocols catapulted 1,330%.

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

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

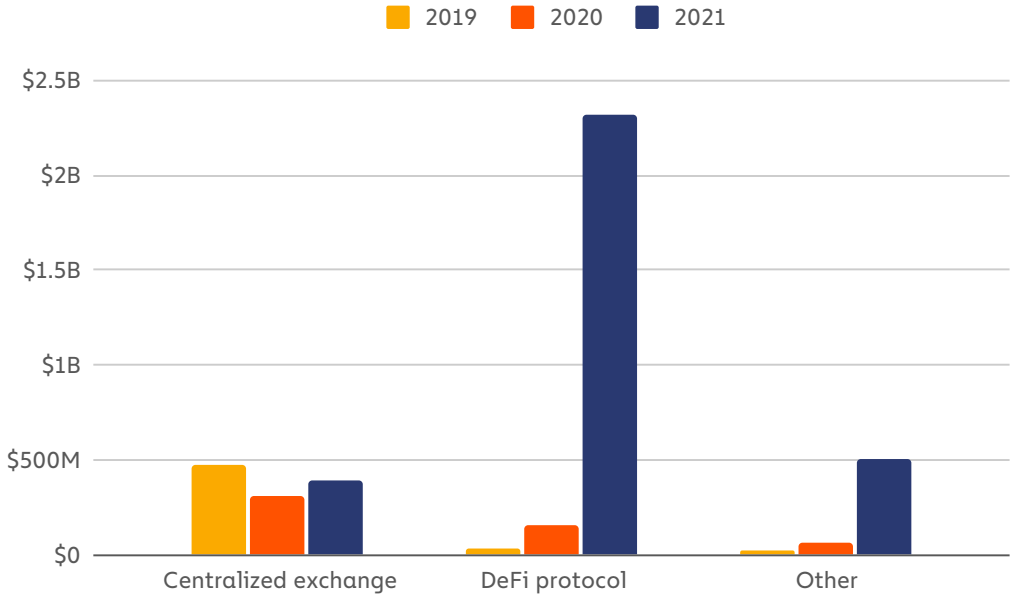
Historically, cryptocurrency thefts have largely been the result of security breaches in which hackers gain access to victims' private keys — the crypto-equivalent of pickpocketing. These keys could be acquired through phishing, keylogging, social engineering, or other techniques. From 2019 to 2021,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

Total value stolen by type of attack | 2019–2021



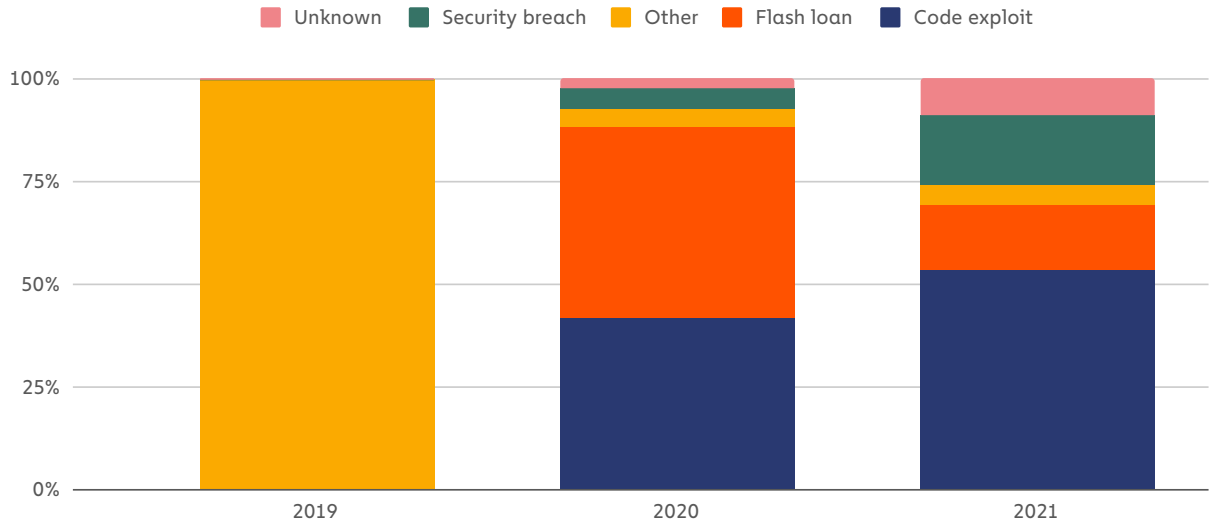
Note: The "unknown" label means information about hack type is not publicly available. The "other" label means the hack type is known but does not fit within our defined categories.

Annual total cryptocurrency value stolen by victim type | 2019–2021



But with the rise of DeFi and the extensive smart contract capabilities that power those platforms, deeper vulnerabilities have begun to emerge around the software underpinning these services. In 2021, code exploits and flash loan attacks—a type of exploit involving price manipulation—accounted for a near-majority of total value stolen across all services at 49.8%. And when examining only hacks on DeFi platforms, that figure increases to 69.3%.

Total value stolen from DeFi protocols by attack type | 2019–2021



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

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

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

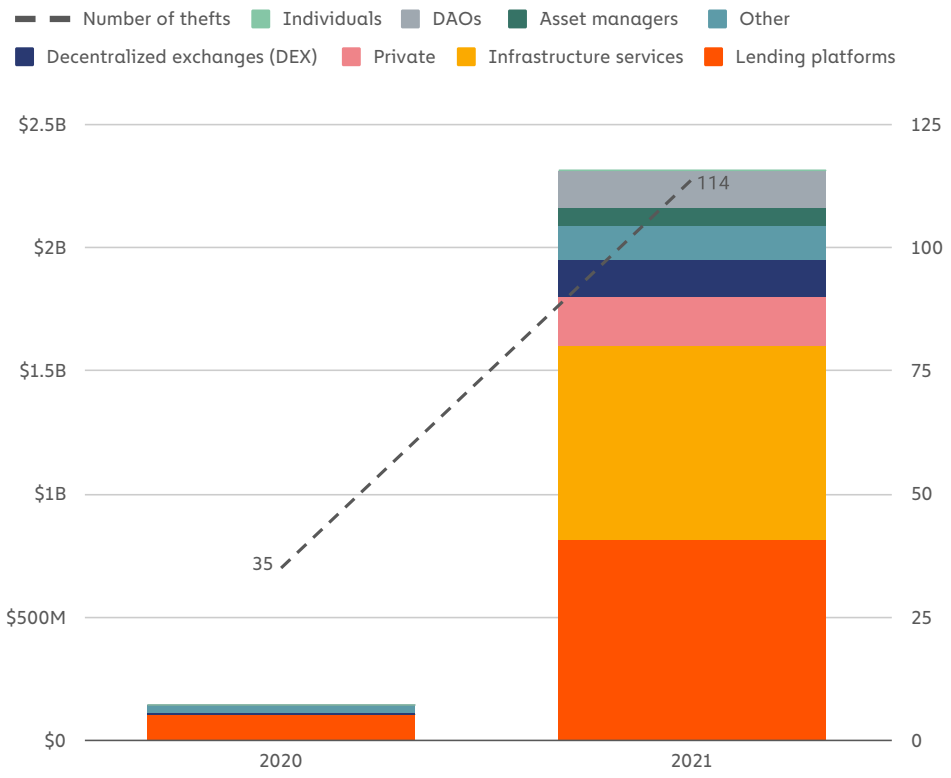
But code audits aren't infallible. Nearly 30% of code exploits occurred on platforms audited within the last year, as well as a surprising 73% of flash loan attacks. This highlights two potential shortfalls of code audits:

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

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

Lending platforms, Web3 infrastructure providers, DEXes and DAOs are especially vulnerable

DeFi-related theft losses vs. number of theft incidents | 2020–2021

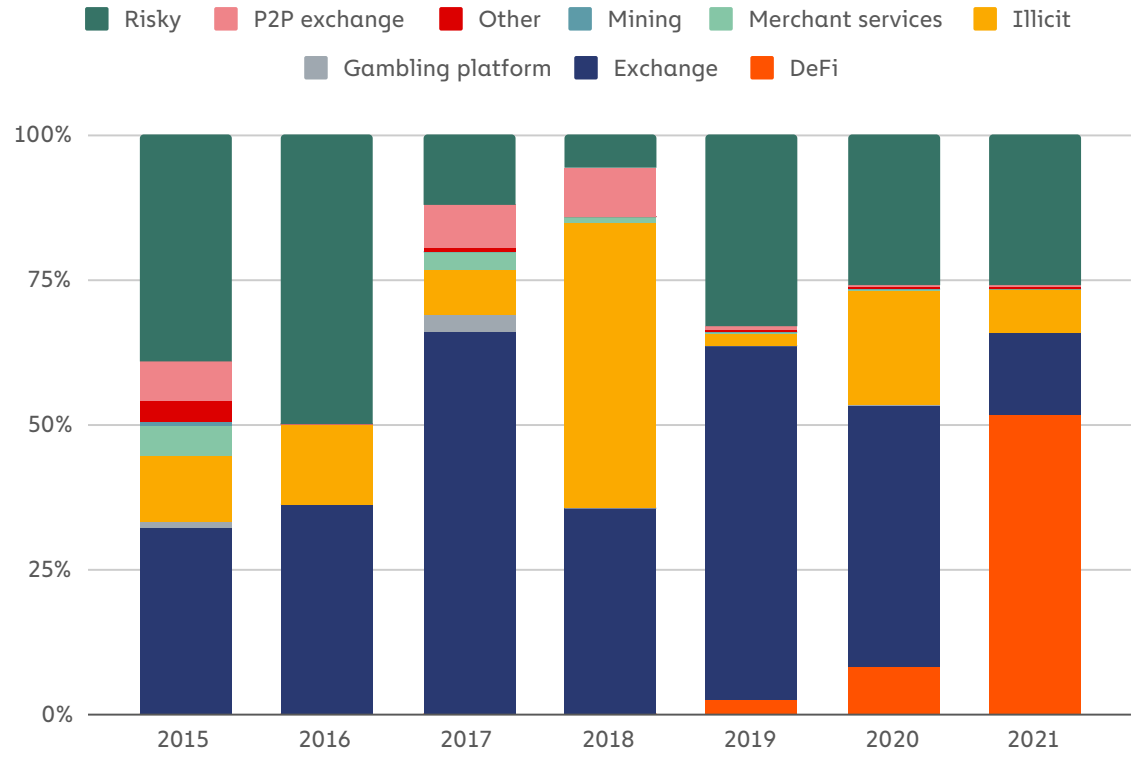


In 2020 and 2021, lending platforms such as yield farming protocols endured the largest losses, with $923 million in total stolen funds and 64 theft incidents. Infrastructure services like cross-chain protocols and oracles-as-a-service came in close second, with DEXes and DAOs reckoning with significant thefts as well.

Following the money: the final destinations of stolen cryptocurrencies

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

Destination of stolen funds | 2015–2021



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

The biggest cryptocurrency thefts of 2021

As is the case most years, the ten largest hacks of 2021 accounted for a majority of the funds stolen at $1.81 billion. Seven of these ten attacks targeted DeFi platforms in particular. The table below breaks down the details of each theft.

The 10 Largest Cryptocurrency Thefts of 2021

Victim	Amount stolen (USD)	Service Type	Hack Type	Description
Poly Network	$613 million	DeFi platform	Code exploit	An attacker exploited cross-chain relay contracts to extract Poly Network funds from three different chains: Ethereum, BSC, and Polygon. The attacker ultimately returned the stolen funds. Read our complete case study.
BitMart	$200 million	Exchange	Security Breach	Attackers stole a private key that compromised two of BitMart's hot wallets.
BadgerDAO	$150 million	DeFi platform	Security Breach	Attackers used a compromised cloudflare API key to periodically inject malicious scripts into the Badger application. The scripts intercepted transactions and prompted users to allow a foreign address to operate on the ERC-20 tokens in their wallet. Once approved, the attacker siphoned funds from the user's wallets.
Undisclosed	$145 million	Private	Other — Embezzlement	Employee allegedly diverted funds to a personal account when the company attempted to transfer funds between financial accounts.

Continued on the next page

Venus	$145 million	DeFi platform	Code Exploit	Attackers manipulated the price of XVS, Venus Protocol's governance token, in order to borrow quantities of BTC and ETH in excess of XVS's actual value. When the governance token's price declined and the collateral of the users who defaulted on their loans was liquidated, Venus was left with a debt of $145 million.
BXH	$139 million	DeFi platform	Other — Leaked Private Keys	An unidentified member of BXH's technical team allegedly leaked an administrator's private key.
Cream Finance	$130 million	DeFi platform	Flash Loan	First, attackers initiated a series of flash loans to mint ~$1.5M of crYUSD. Then, the attacker took advantage of Cream's PriceOracleProxy function to artificially inflate the value of its crYUSD to ~$3B. $2B of this was withdrawn in order to repay the attacker's outstanding flash loans, while the remaining $1B was used to drain all of Cream's assets available for lending ($130M).
Vulcan Forged	$103 million	DeFi platform	Security Breach	Attacker gained access to the private keys of 96 addresses and sent their contents to hacker-controlled wallets.
Undisclosed	$91 million	DeFi platform	Code Exploit	Attacker used the platform's content delivery network (CDN) to respond to queries with malicious code that stole user assets
Undisclosed	$91 million	Exchange	Security Breach	Attacker gained access to the private keys of the service's internet-connected hot wallets.

2021 in cryptocurrency theft: A cautionary tale for DeFi developers

As the total value locked in DeFi climbs to ever-greater all-time highs—$256 billion at last peak—so too does the risk of exploitation. If there's one takeaway from the meteoric rise of thefts from DeFi platforms, it's the need for smart contract security and price oracle accuracy. Code audits, decentralized oracle providers, and an altogether more rigorous approach to platform security could be the ideal means to that end.

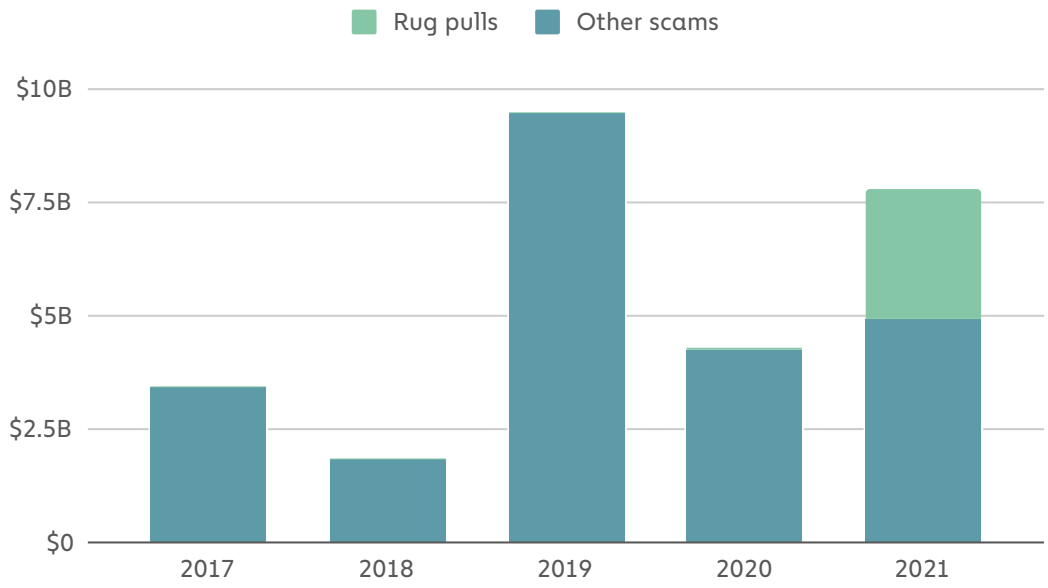
Fortunately, even when these functions do fail and cryptocurrencies are stolen, blockchain analysis can help. Investigators with a full picture of the movement of funds from address to address can take advantage of opportunities to halt assets in transit, stopping bad actors before they cash out.

Scams

The Biggest Threat to Trust in Cryptocurrency: Rug Pulls Put 2021 Scam Revenue Close to All-time Highs

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

Total yearly cryptocurrency value received by scammers | 2017–2021



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

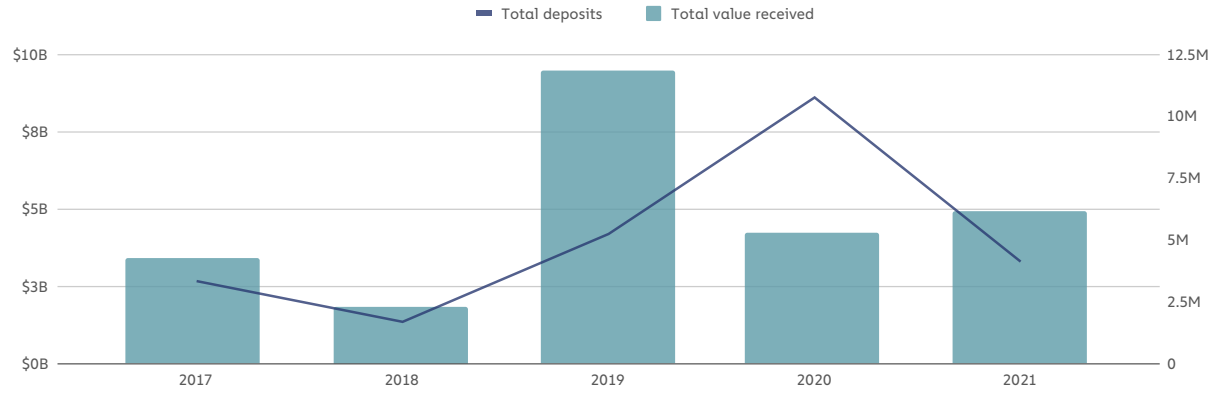
Another change that contributed to 2021's increase in scam revenue: the emergence of rug pulls, a relatively new scam type particularly common in the DeFi ecosystem, in which the developers of a cryptocurrency project — typically a new token — abandon it unexpectedly, taking users' funds with them. We'll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

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

Investment scams in 2021: More scams, shorter lifespans

While total scam revenue increased significantly in 2021, it stayed flat if we remove rug pulls and limit our analysis to financial scams — even with the emergence of Finiko. At the same time though, the number of deposits to scam addresses fell from just under 10.7 million to 4.1 million, which we can assume means there were fewer individual scam victims.

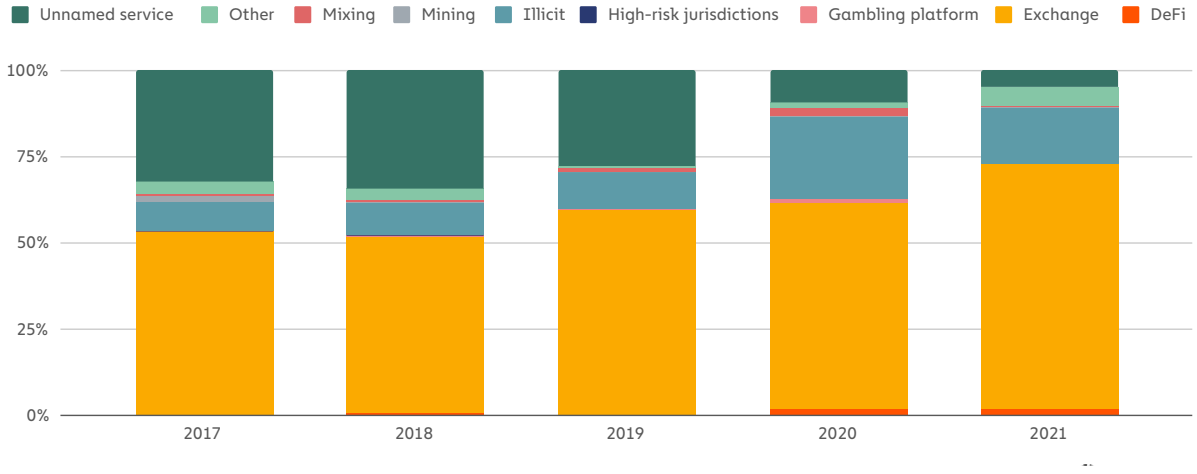
Total yearly cryptocurrency value received by investment scams | 2017–2021



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

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

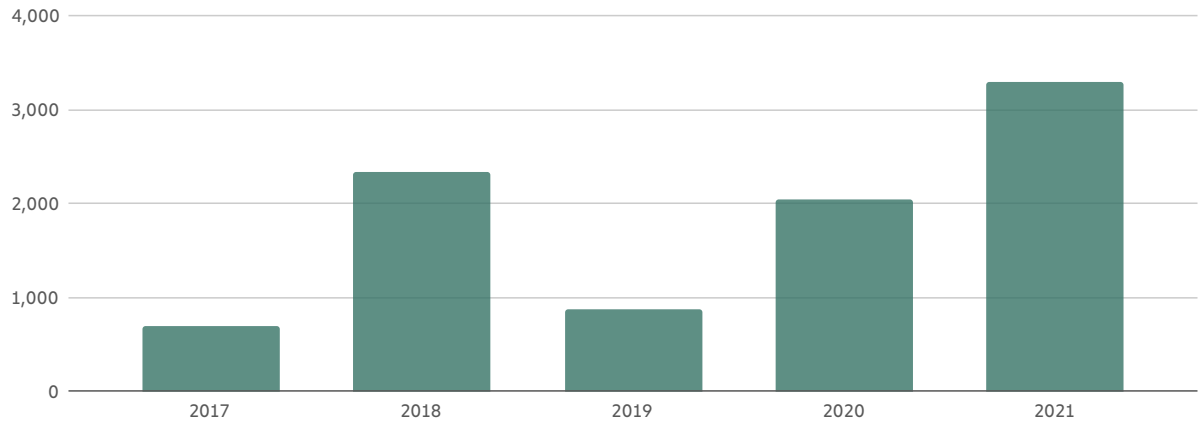
Destination of funds leaving investment scam addresses by year | 2017–2021



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

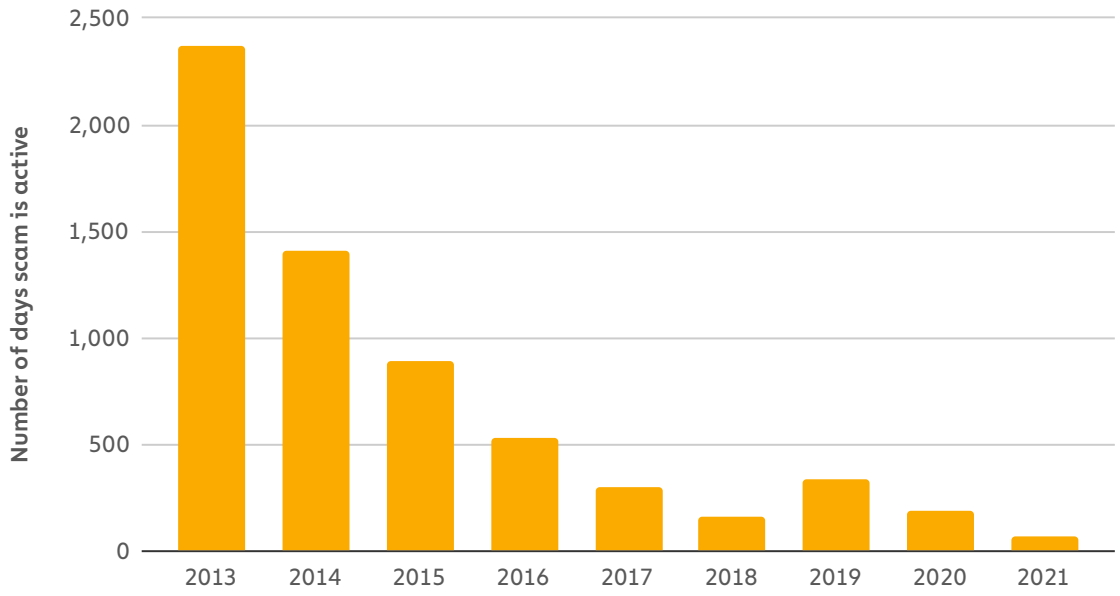
The number of financial scams active at any point in the year — active meaning their addresses were receiving funds — also rose significantly in 2021, from 2,052 in 2020 to 3,300.

Total number of unique active investment scams by year | 2017–2021



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

Lifespan of average scam by year | 2013–2021



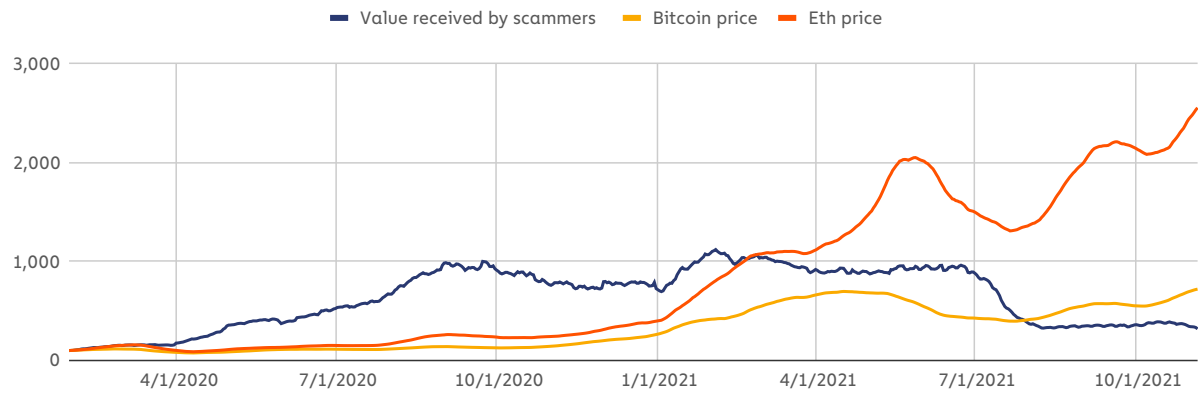
The average financial scam was active for just 70 days in 2021, down from 192 in 2020. Looking back further, the average cryptocurrency scam was active for 2,369 days, and the figure has trended steadily downwards since then. One reason for this could be that investigators are getting better at investigating and prosecuting scams. For instance, in

September 2021, the CFTC filed charges against 14 investment scams touting themselves as providing compliant cryptocurrency derivative trading services — a common scam typology in the space — whereas in reality they had failed to register with the CFTC as futures commission merchants. Previously, these scams may have been able to continue operating for longer. As scammers become aware of these actions, they may feel more pressure to close up shop before drawing the attention of regulators and law enforcement.

At the same time, we're seeing the end of a long-standing statistical relationship between cryptocurrency asset prices and scamming activity. Scams typically come in waves corresponding with sustained price growth in popular cryptocurrencies like Bitcoin and Ethereum, which typically also lead to influxes of new users. We see this reflected in the chart below — scamming activity spiked following bull runs in 2017 and 2020.

This isn't all that surprising. New, less savvy users attracted by cryptocurrency's growth are more likely to fall for scams than more seasoned users. However, the relationship between asset prices and scamming activity now appears to be disappearing.

Index: Total value received by scams vs. ETH and BTC price, 30-day moving average
Index: Jan 2020 = 100 | JAN 2020– NOV 2021

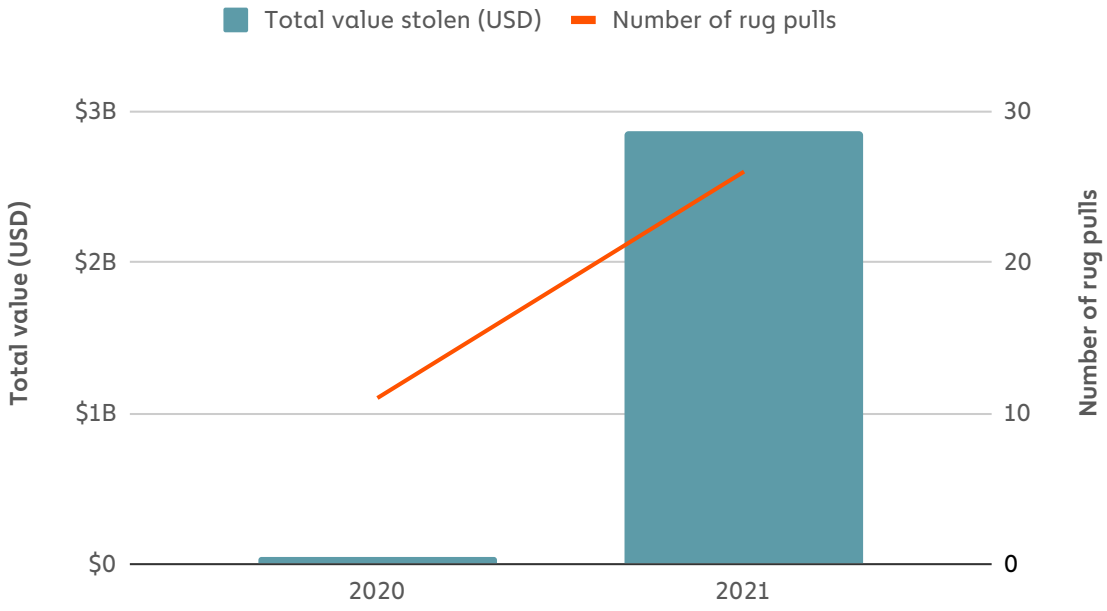


Above, we see scam activity rise in concert with Bitcoin and Ethereum prices until 2021, when scamming activity stays flat and even begins to drop regardless of whether prices rise or fall.

Rug pulls are the latest innovation in scamming

Rug pulls have emerged as the go-to scam of the DeFi ecosystem, accounting for 37% of all cryptocurrency scam revenue in 2021, versus just 1% in 2020.

Total cryptocurrency value stolen in rug pulls versus number of rug pulls | 2020 VS. 2021



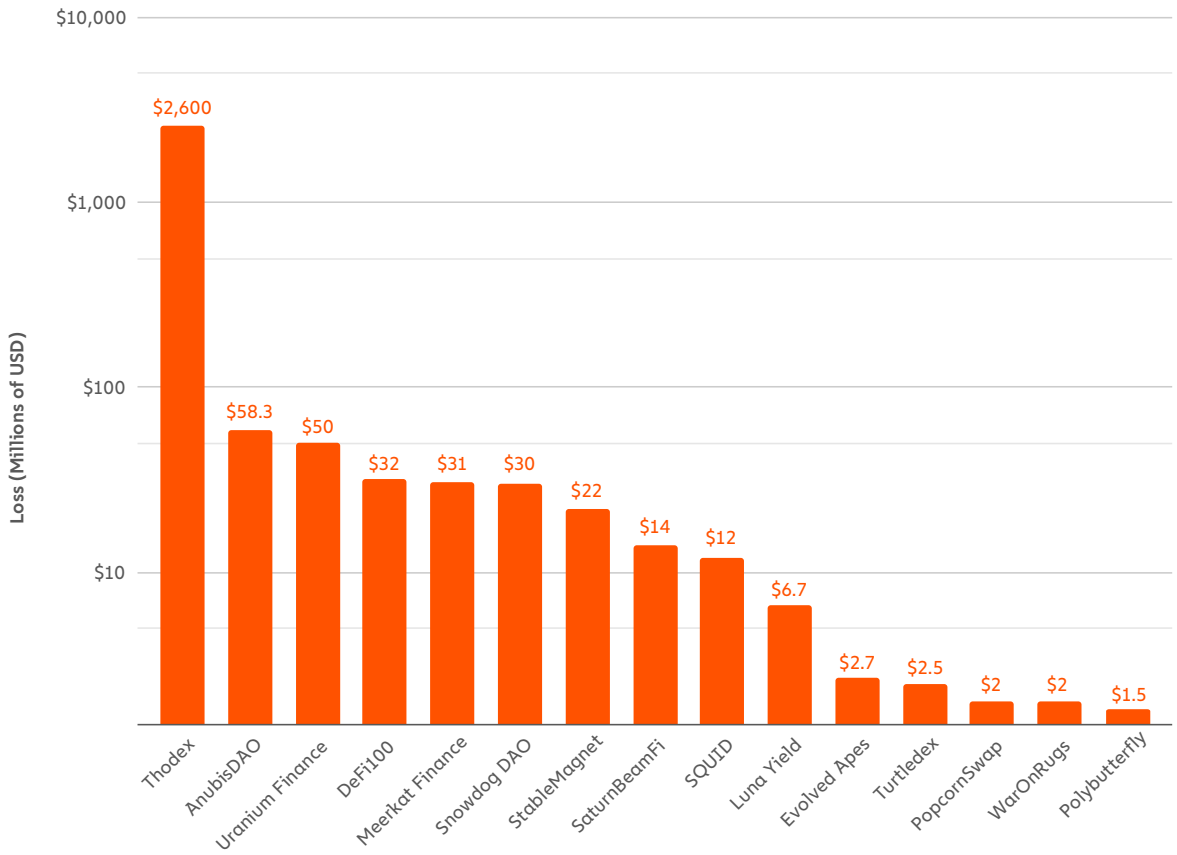
All in all, rug pulls took in more than $2.8 billion worth of cryptocurrency from victims in 2021.

As is the case with much of the emerging terminology in cryptocurrency, the definition of "rug pull" isn't set in stone, but we generally use it to refer to cases in which developers build out what appear to be legitimate cryptocurrency projects — meaning they do more than simply set up wallets to receive cryptocurrency for, say, fraudulent investing opportunities — before taking investors' money and disappearing.

Rug pulls are most commonly seen in DeFi. More specifically, most rug pulls entail developers creating new tokens and promoting them to investors, who trade for the new token in the hopes the token will rise in value, which also provides liquidity to the project — that's how most DeFi projects start. In rug pulls, however, the developers eventually drain the funds from the liquidity pool, sending the token's value to zero, and disappear. Rug pulls are prevalent in DeFi because with the right technical know-how, it's cheap and easy to create new tokens on the Ethereum blockchain or others and get them listed on decentralized exchanges (DEXes) without a code audit. That last point is crucial — decentralized tokens are meant to be designed in such a way that investors holding governance tokens can vote on things like how assets in the liquidity pool are used, which would make it impossible for the developers to drain the pool's funds. While code audits that would catch these vulnerabilities are common in the space, they're not required in order to list on most DEXes, hence why we see so many rug pulls.

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

2021 Top 15 rug pulls by cryptocurrency value stolen | 2021

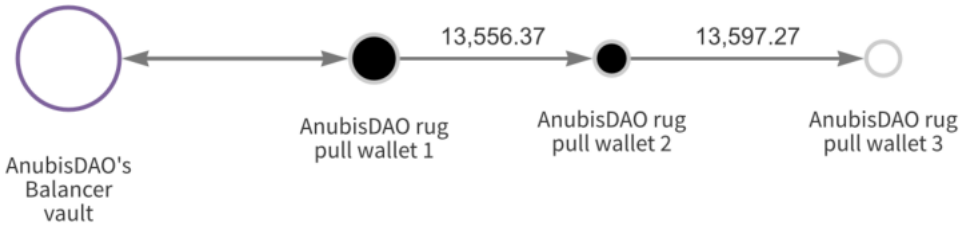


It's important to remember that not all rug pulls start as DeFi projects. In fact, the biggest rug pull of the year centered on Thodex, a large Turkish centralized exchange whose CEO disappeared soon after the exchange halted users' ability to withdraw funds. In all, users lost over $2 billion worth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

AnubisDAO, the second-biggest rug pull of 2021 at over $58 million worth of cryptocurrency stolen, provides an excellent example of how rug pulls in DeFi work.

AnubisDAO's Twitter banner. Credit CryptoHubK

AnubisDAO launched on Thursday, October 28, 2021, claiming it planned to provide a decentralized, free-floating currency backed by a basket of assets. With little more than a DOGE-inspired logo — the project had no website or white paper, and all of its developers went by pseudonyms — AnubisDAO raised nearly $60 million from investors practically overnight, all of whom received the project's ANKH token in exchange for funding the project's liquidity pool. But a mere 20 hours later, all the funds raised, primarily held in wrapped Ethereum, disappeared from AnubisDAO's liquidity pool, moving to a series of new addresses.



We can see these transactions on the graph above. AnubisDAO used contracts created through Balancer's Liquidity Bootstrapping Protocol to receive and hold the wrapped Ethereum investors sent to their liquidity pool in exchange for ANKH tokens. However, the address that deployed the liquidity pool contract was already in possession of the vast majority of the liquidity provider (LP) tokens for that pool. 20 hours after the sale began, the address that created the pool cashed out it's massive holdings of LP tokens, allowing

them to make off with nearly all the wrapped Ethereum and ANKH tokens in the pool. The thief then moved that wrapped Ethereum through a series of intermediary wallets. Soon after this, the Twitter account that had acted as the public face of AnubisDAO went offline, and ANKH's value plummeted to zero.

Since the theft, there's been a great deal of finger pointing and conflicting explanations. One of the project's pseudonymous founding developers claims another founder, who had access to AnubisDAO's liquidity pool, is solely responsible for the rug pull, while that founder claims to have fallen victim to a phishing attack that compromised the pool's private keys — the evidence that founder has supplied doesn't support that theory, however. At this time, all signs point to a standard rug pull, but it's unclear whether or not all of the developers were in on it.

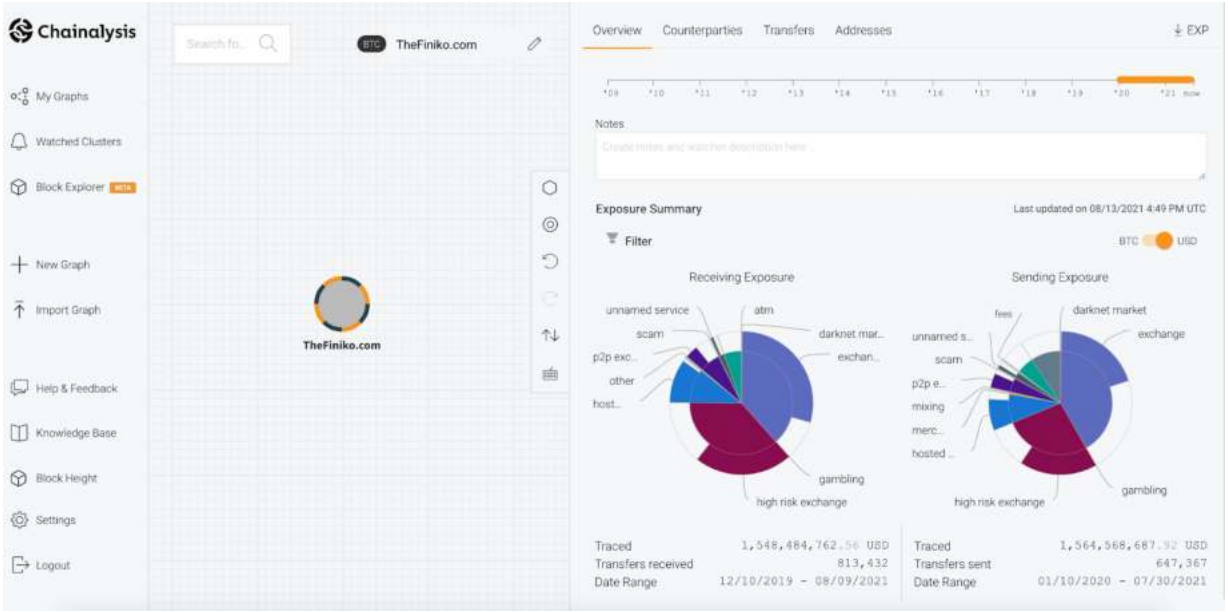
AnubisDAO should serve as a cautionary tale to investors evaluating similar opportunities. The most important takeaway is to avoid new tokens that haven't undergone a code audit. Code audits are a process by which a third-party firm analyzes the code of the smart contract behind a new token or other DeFi project, and publicly confirms that the contract's governance rules are iron clad and contain no mechanisms that would allow for the developers to make off with investors' funds. They can also check for security vulnerabilities that could be exploited by hackers. OpenZeppelin is one example of a firm that provides code audits, but there are several others that are also considered trustworthy. Investors may also want to be wary of tokens that lack the public-facing materials one would expect from a legitimate project, such as a website or white paper, as well as tokens created by individuals not using their real names.

DeFi is one of the most exciting, innovative areas of the cryptocurrency ecosystem, and there are clearly big opportunities for early adopters. But the newness of the space and relative inexperience of many investors provides a prime landscape for scamming opportunities by bad actors. It'll be difficult for DeFi's growth to continue if potential new users don't feel they can trust new projects, so it's important that trusted information sources in cryptocurrency — whether they're influencers, media outlets, or project participants — help new users understand how to spot shady projects to avoid.

Finiko: 2021's billion dollar Ponzi scheme

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

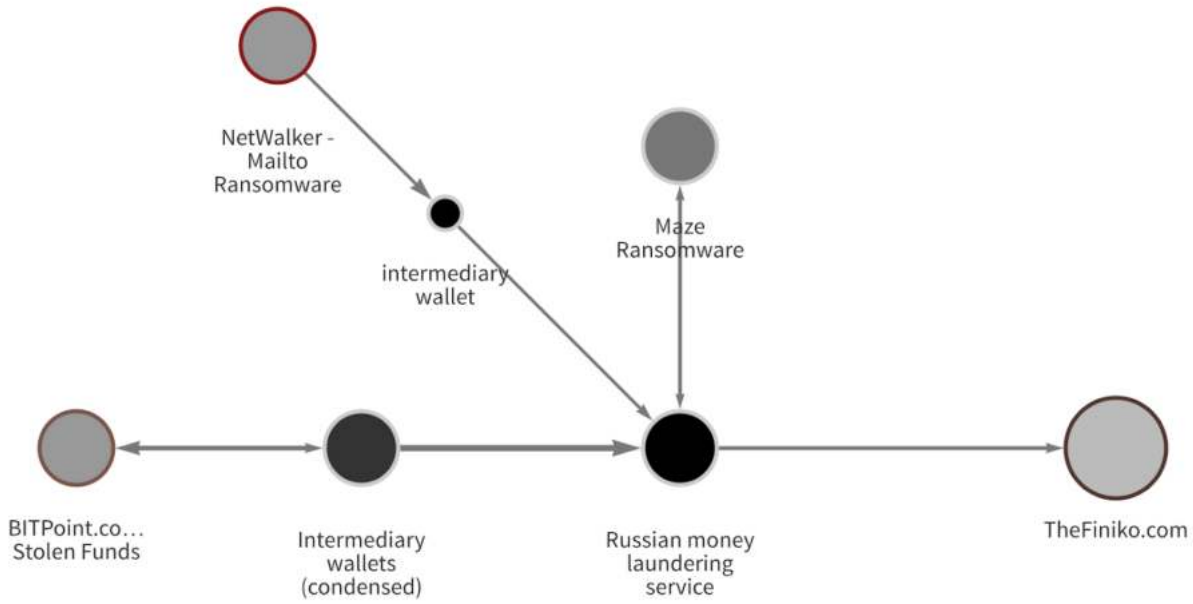
According to the Moscow Times, Finiko was headed up by Kirill Doronin, a popular Instagram influencer who has been associated with other Ponzi schemes. The article notes that Finiko was able to take advantage of difficult economic conditions in Russia exacerbated by the Covid pandemic, attracting users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



During the roughly 19 months it remained active, Finiko received over $1.5 billion worth of Bitcoin in over 800,000 separate deposits. While it's unclear how many individual victims were responsible for those deposits or how much of that $1.5 billion was paid

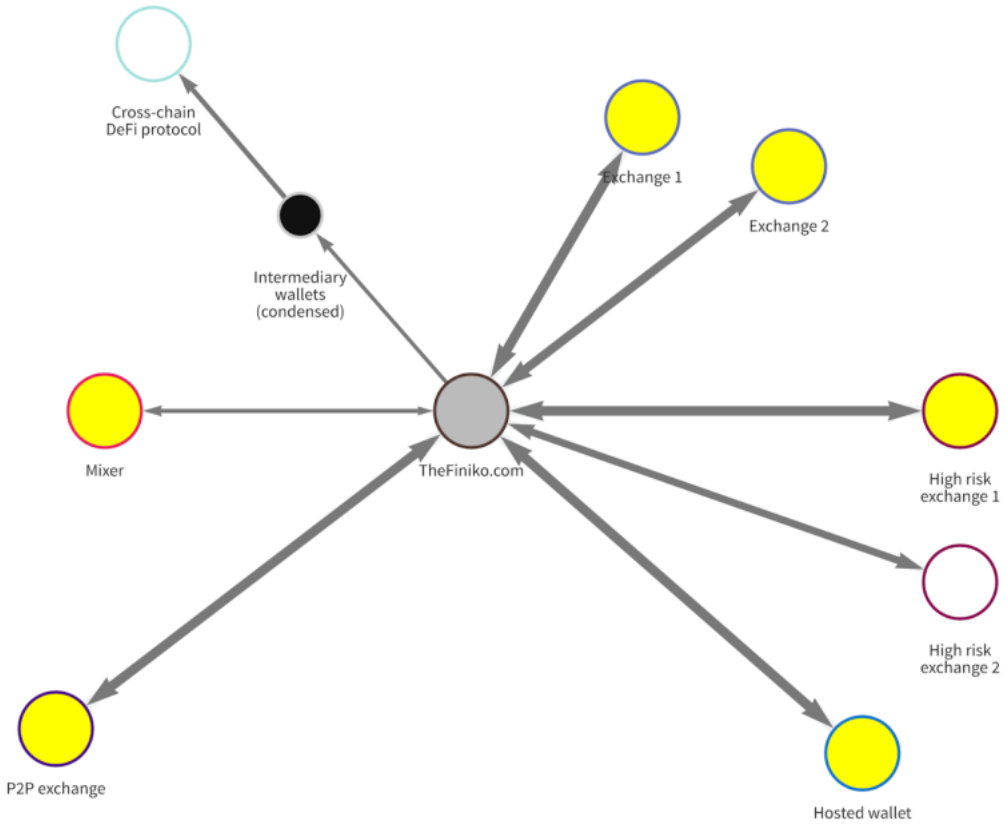
out to investors to keep the Ponzi scheme going, it's clear that Finiko represents a massive fraud perpetrated against Eastern European cryptocurrency users, predominantly in Russia and Ukraine.

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



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

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



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

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

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

How one cryptocurrency platform is saving users from scams

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

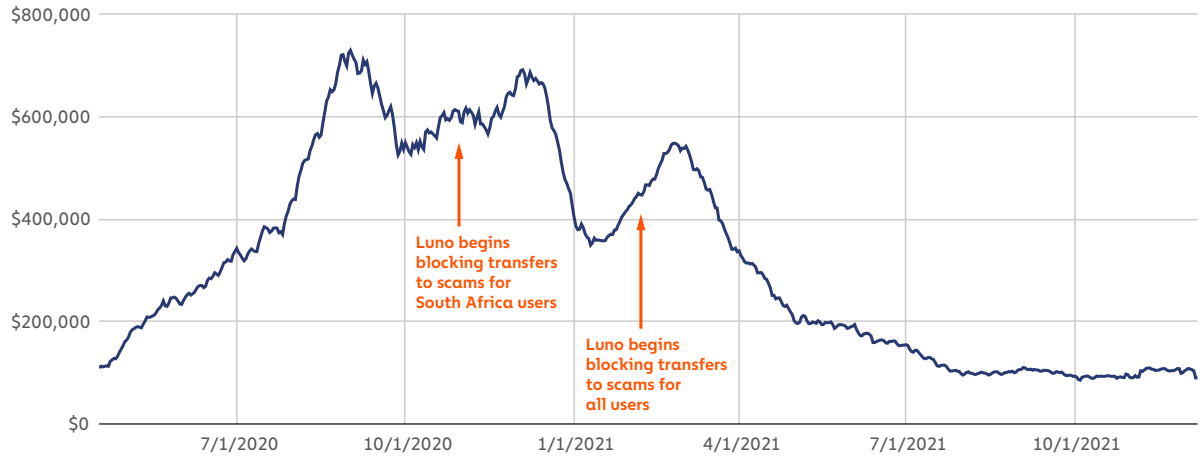
Luno is a leading cryptocurrency platform operating in over 40 countries, with an especially heavy presence in South Africa. In 2020, a major scam was targeting South African cryptocurrency users, promising outlandishly large investment returns. Knowing that its users were at risk, Luno decided to take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

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

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

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

Daily value received by scams from Luno, 30-day moving average



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

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

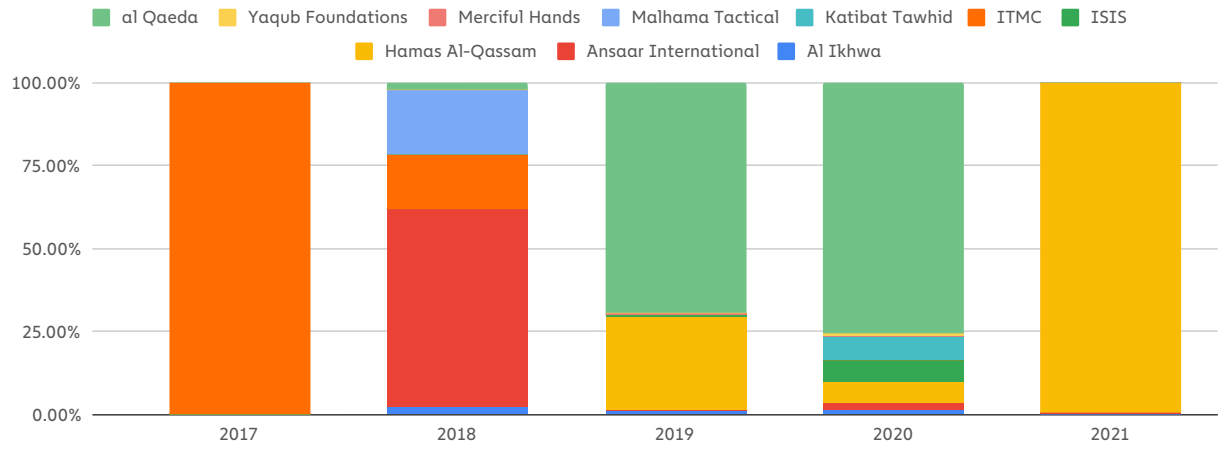
Terrorism Financing

Al-Qaeda, ISIS, and Hamas Among Terrorist Groups Fundraising in Cryptocurrency—With Government Seizures Close Behind

By the end of 2021, we've identified a number of terrorist organizations that have attempted to finance their operations with cryptocurrency. What's harder to find, however, is a group that has gotten away with it.

- In 2019 and 2020, al-Qaeda raised cryptocurrency through Telegram channels and Facebook groups. Thanks to the FBI, HSI, and IRS-CI, more than $1 million was seized from a money service business (MSB) operator who facilitated some of these transactions.
- In early Spring of 2021, al-Qassam Brigades, Hamas' military wing, collected more than $100,000 in donations. In July, the Israeli government seized much of it from associated MSBs.

Share of total terrorism financing activity by organization | 2017–2021



In the following section, we isolate three cases from 2021—one in June, one in July, and another in December—that showcase governments' recent successes in the fight against cryptocurrency-financed terrorism.

Case 1: Israeli Government Seizes Cryptocurrency Addresses Associated with Hamas Donation Campaigns

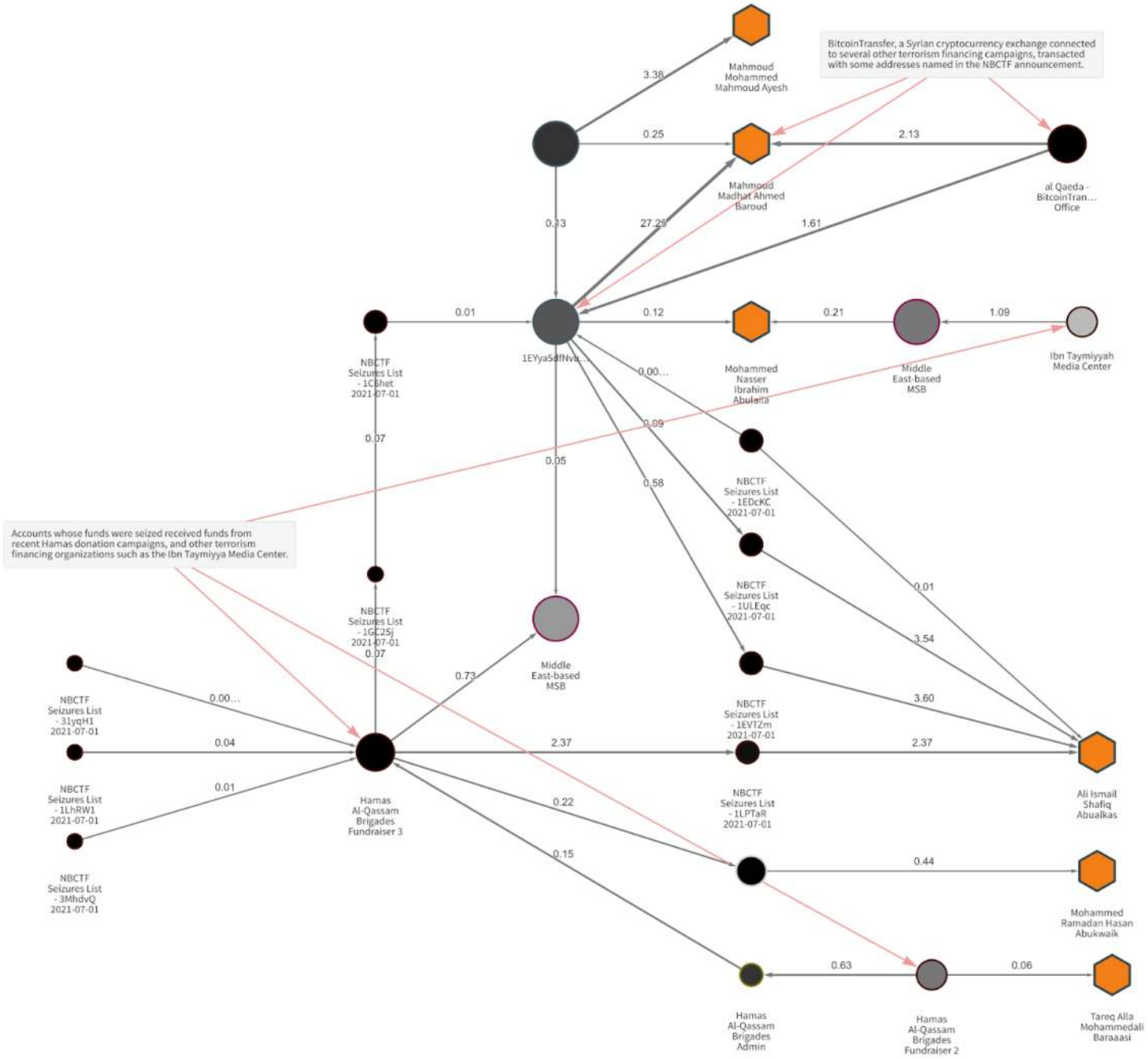
On June 30th, Israel's National Bureau for Counter Terror Financing (NBCTF) announced the seizure of cryptocurrency held by several wallets associated with donation campaigns carried out by Hamas. The action came after a sizable growth in cryptocurrency donations to al-Qassam Brigades in May following increased fighting between the group and Israeli forces.

Notably, this is the first terrorism financing-related cryptocurrency seizure to include such a wide variety of digital currencies. NBCTF seized not only Bitcoin, but Ether, Tether, XRP, and more. The seizure was made possible through an investigation of open-source intelligence (OSINT) and blockchain data.

Below, we examine how the second of these—the analysis of blockchain data—contributed to the case.

How funds moved from donation addresses to exchanges

The Chainalysis Reactor graph below shows the Bitcoin portion of the transactions carried out by many of the addresses listed in the NBCTF announcement. Many of these addresses have been attributed to individuals connected to the donation campaigns.



The orange hexagons represent deposit addresses hosted at large, mainstream cryptocurrency exchanges that are controlled by individuals named in the NBCTF announcement. As we can see, the funds often passed through intermediary wallets, high-risk cryptocurrency exchanges, and money services businesses (MSBs) before reaching the exchanges from which the named individuals likely hoped to cash out.

Interestingly, we can see that two donation addresses named in the announcement received funds from addresses associated with the Idlib office of BitcoinTransfer (top right of graph), a Syrian cryptocurrency exchange connected to previous terrorism financing cases. Another received funds from a Middle East-based MSB that had previously received funds from the Ibn Taymiyya Media Center (directly beneath the BitcoinTransfer cluster), an organization that has also been associated with terrorism financing in the past.

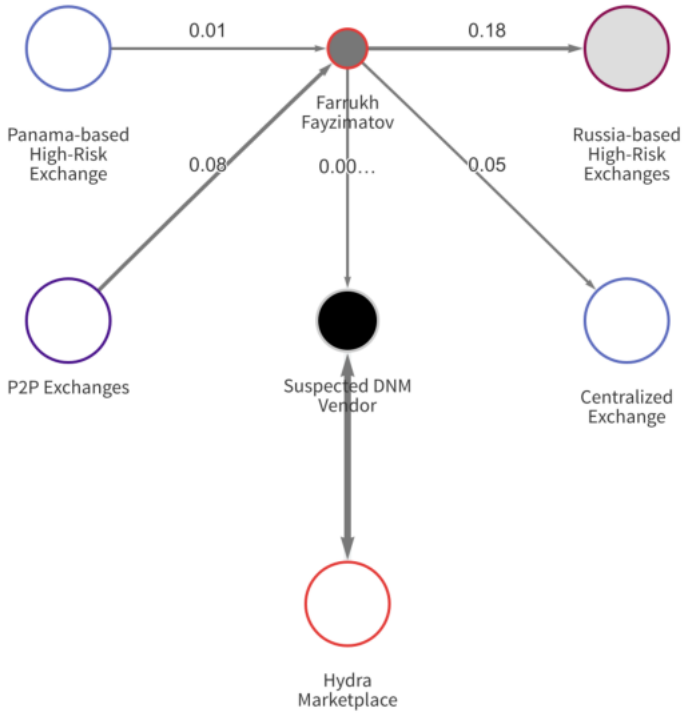
The value of blockchain analysis in conjunction with other data sources

This investigation is a perfect example of the value of blockchain analysis, especially when used in conjunction with other open source data. Israeli authorities analyzed OSINT to find Hamas' donation addresses and, with blockchain analysis tools, were able to follow the funds to find consolidation addresses and uncover the names of individuals associated with the campaigns. Up-to-date transaction data across several blockchains was crucial in this case as agents tracked and seized funds of several different cryptocurrencies, not just one. We applaud the Israeli authorities for a successful operation and look forward to providing valuable tools that facilitate more such successes for our government customers around the world.

Case 2: Terrorist Financier designated by the U.S. Office of Foreign Assets Control (OFAC)

On July 28, 2021, OFAC sanctioned Farrukh Furkatovitch Fayzimatov for having materially assisted and supported Hay'et Tahrir al-Sham (HTS), a militant group involved in the Syrian Civil War. Fayzimatov utilized social media to post propaganda, recruit new members, and solicit donations to purchase equipment for the benefit of HTS.

His fundraising efforts have been linked to an address tracked by Chainalysis, the details of which are depicted in the graph below.



On the left side of the graph, we find that Fayzimatov received funds directly from centralized and P2P exchanges that did not collect know-your-customer information. This indicates that the individuals sending bitcoin to Fayzimatov intended to keep their activity anonymous. On the right, we observe that Fayzimatov sent funds to high-risk exchanges based in Russia, one centralized exchange that did collect KYC information, and a small sum to a suspected vendor at Hydra Marketplace, a Russian darknet market.

Following the OFAC designation, Fayzimatov's on-chain activity ceased.

Case 3: Wales-based convicted terrorist caught using darknet market 'Bypass Shop'

In December, a 29-year-old man was sentenced to 16 months in jail for Bitcoin transactions made on the Bypass Shop, a darknet market for stolen credit card information.

The transactions were made from the man's wallet at an exchange, which prompted the company to issue a suspicious activity report. From there, police identified the man as Khuram Iqbal of Cardiff, and arranged for his arrest.

This was not Iqbal's first run-in with the law. Iqbal had been jailed in 2014 for possessing terrorist information and disseminating terrorist publications under the pseudonym Abu Irhaab—Arabic for "father of terrorism." In total, Iqbal possessed nine copies of the al-Qaeda magazine "Inspire," and published more than 800 links to extremist material on Facebook.

Before then, Iqbal made two attempts to join the jihadi cause by flying to Kenya and Turkey. He was deported on both occasions.

Blockchain analysis: Governments' best tool in the fight against cryptocurrency-financed terrorism

As terrorist organizations adopt further blockchain technologies and cryptocurrency fundraising techniques, it's critical for governments to keep up. Our 2021 findings indicate that many agencies have, and the rewards have been considerable.

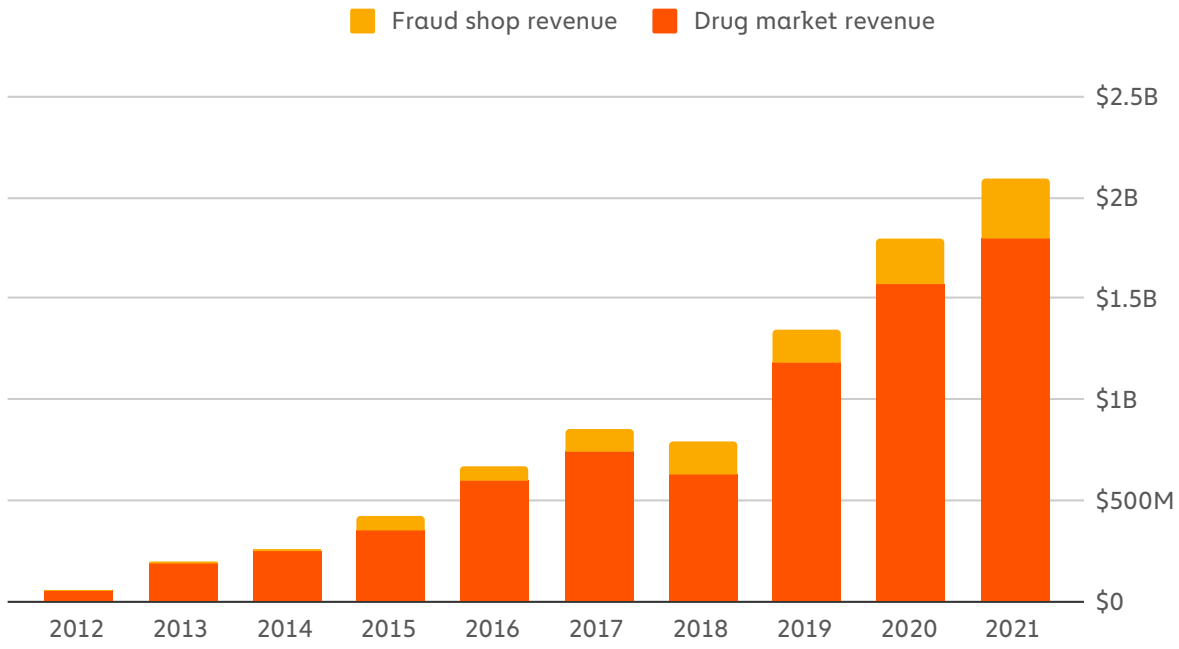
Governments that have embraced blockchain analysis have seized millions of dollars in cryptocurrency and stopped a number of terrorist financiers—further evidence that with the proper tools, investigators can cut terrorist organizations off from the funds that enable their rise.

Darknet Markets

Darknet Markets Hit All-time High in Revenue, Eclipsing $2 Billion, Despite Their Decline in Overall Number

Darknet markets set a new revenue record in 2021, bringing in a total of $2.1 billion in cryptocurrency. Roughly $300 million of this total was generated by fraud shops, which brokered the sale of stolen logins, credit cards, exploit kits, and more. The rest—more than $1.8 billion—was generated by drug-focused markets.

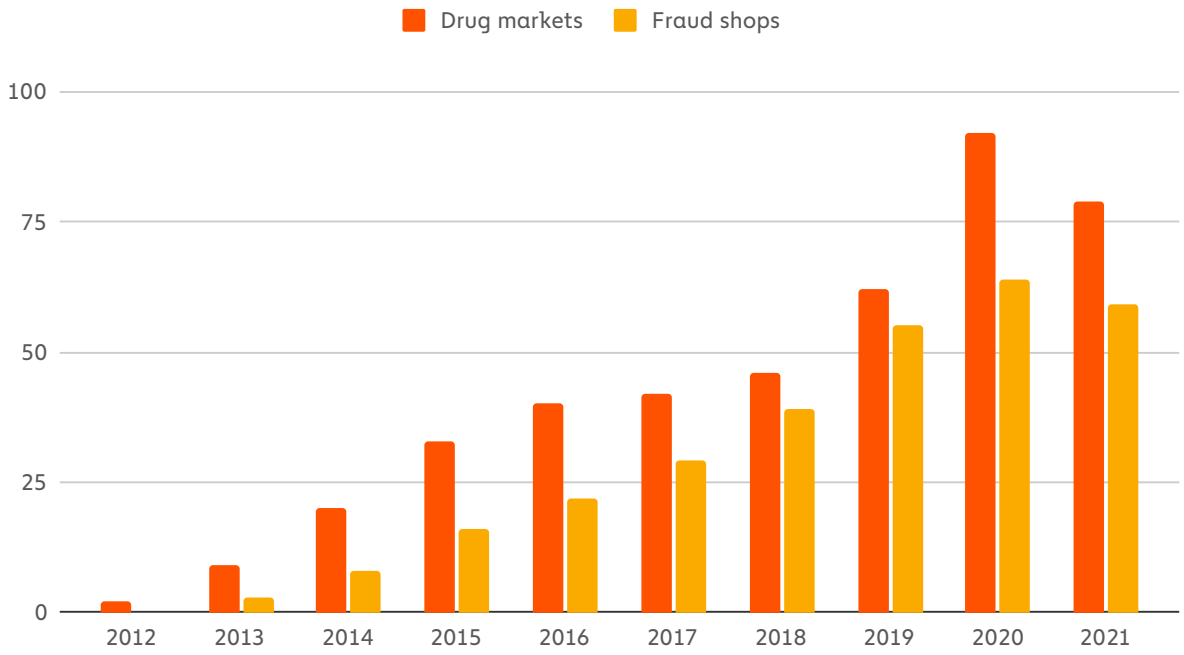
Darknet market revenue by market category | 2012-2021



We also identified an additional $112 million (not included above) in revenues for these categories from direct buyer-to-vendor sales, meaning sales that didn't use a darknet market as an intermediary. We discuss this trend in greater detail later in this section.

Despite this illicit industry's continued revenue growth, the number of active markets actually fell this year. By the end of 2021, there were five fewer fraud shops and 13 fewer drug-focused markets than at the end of 2020.

Number of active drug markets and fraud shops | 2012-2021



Interestingly, many of the market closures in 2021 were planned, with administrators giving users the opportunity to withdraw their funds in advance. This is unusual; in the past, market administrators closing shop often ran off with users' funds in what is known as an exit scam. But more recently, perhaps to avoid the unwanted investigations of upset users, the primary administrative approach has changed.

As is typical, law enforcement investigations also contributed to or directly caused many shutdowns. For instance, less than a month before Joker's Stash announced the fraud shop's voluntary closure, the FBI and Interpol seized four of its blockchain domains—.bazar, .lib, .emc, and .coin. Later, in June, a multinational operation seized the infrastructure of Slil_PP, one of the largest fraud shops for stolen username-password combinations. And in October, the Department of Justice announced the results of Dark HunTor, an operation that resulted in the arrest of 150 drug traffickers and the closure of two drug markets. Still other darknet markets, such as DarkMarket, Monopoly, and CanadianHeadquarters, have shuttered after being caught in similar precarious situations this year.

For the darknet markets that remain, competition is fiercer than ever, and competitors aren't afraid to play dirty. Data leaks, DDoS attacks, and doxxes are common occurrences in the space, according to Flashpoint's Senior Director of Research Ian Gray. For example, shortly after the relaunch of AlphaBay in August 2021, a DDoS attack was allegedly conducted on the marketplace by "mr_white," the administrator of the since-shuttered White House Market. Another DDoS attack, this one unattributed, took Cannazon, a

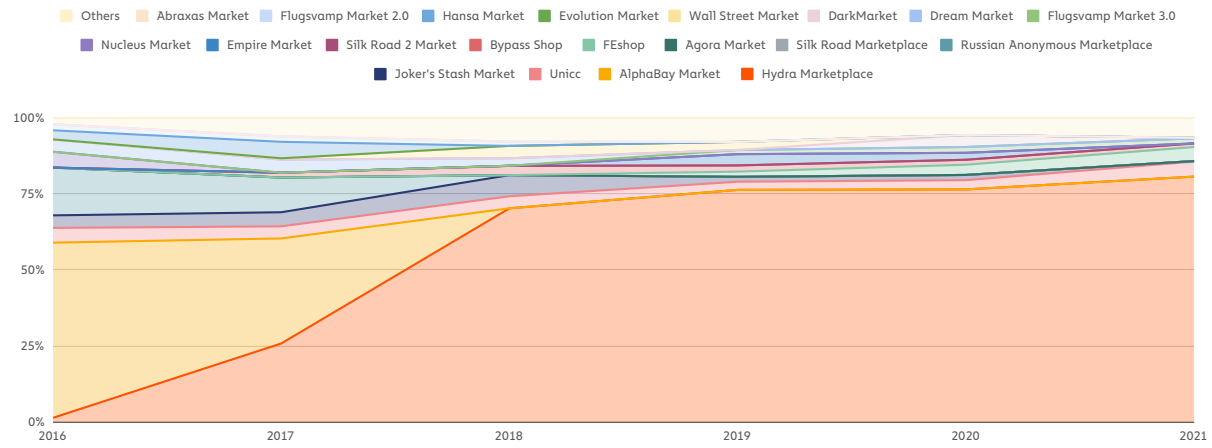
marijuana-focused market, permanently offline. A third action, an alleged dox of Hydra market's administrators, was published on the hydra[.]expert domain in February.

These competitive threats, alongside other barriers to entry like finding a hosting provider and retaining vendors, have made opening and operating a darknet market too difficult for many would-be administrators—another explanation for the decline.

The Russia-based Hydra Market continues to dominate by total revenue, but other markets outside of Eastern Europe also thrive

Hydra, a market that serves only Russian-speaking countries, remains the largest darknet market by far. In 2021, Hydra accounted for 80% of darknet market revenue worldwide.

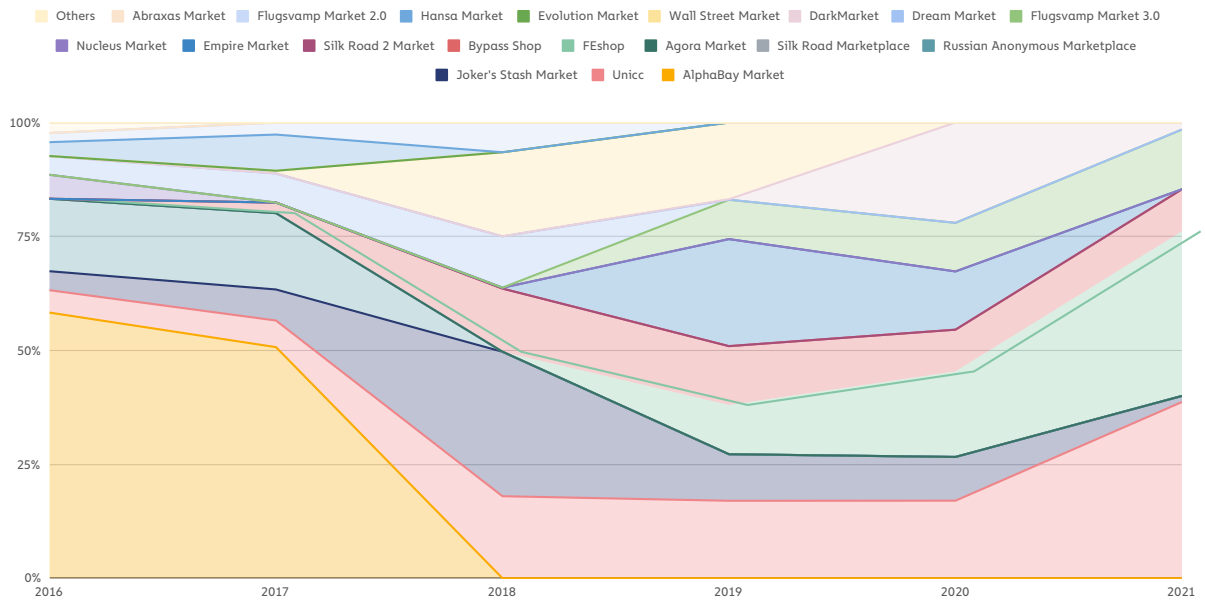
Darknet markets by share of total market | 2016-2021



Hydra is distinct for its size, Russian focus, and variety of offerings: users of Hydra can purchase both drugs and fraud-related goods and services on the website, though drugs account for the majority of its sales. However, Hydra is so large that it can prevent our data visualizations from showing the important role of other, more global markets.

Below, we exclude Hydra activity and find that the remaining markets are in much closer competition.

Darknet markets by share of total market (excluding Hydra) | 2016-2021

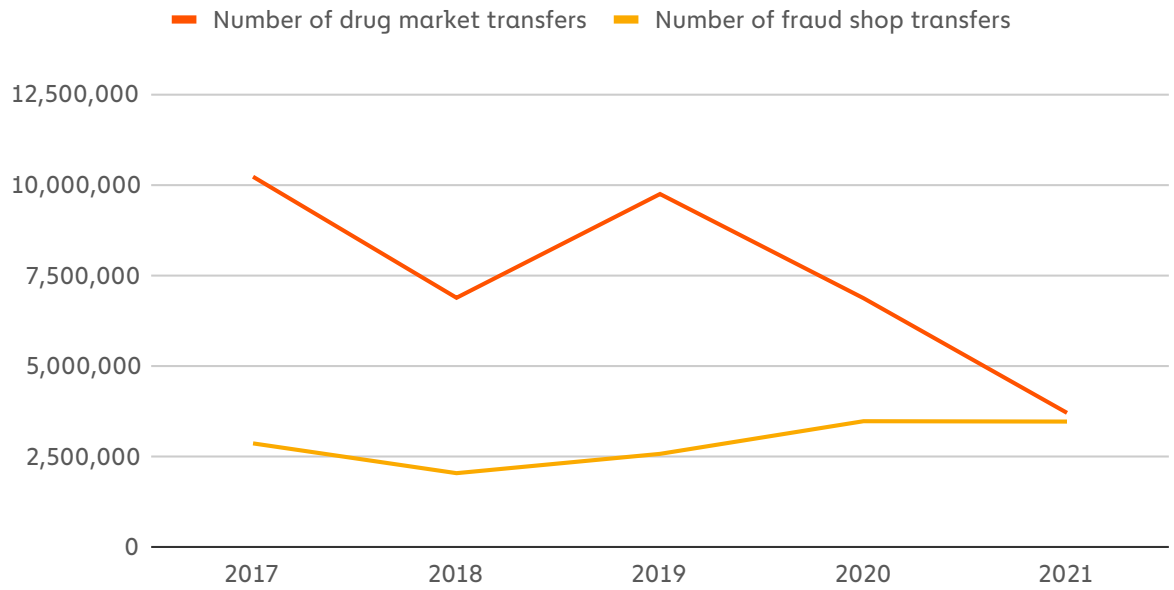


The five largest markets other than Hydra this year were, in descending order of revenue: UniCC, FEshop, Flugsvamp Market, Bypass Shop, and DarkMarket. Of these five markets, three were fraud shops (UniCC, FEshop, Bypass shop), two were drug markets (Flugsvamp Market, DarkMarket), and two were taken down by law enforcement (UniCC and DarkMarket). All of these markets serve customers worldwide, with the exception of Flugsvamp, which serves only Swedish users.

As the number of transfers to drug markets and their user counts dwindle, growing payment sizes more than compensate

Curiously, the number of transfers to drug-focused markets has fallen considerably over the past five years, from 11.7 million in 2016 to just 3.7 million this year.

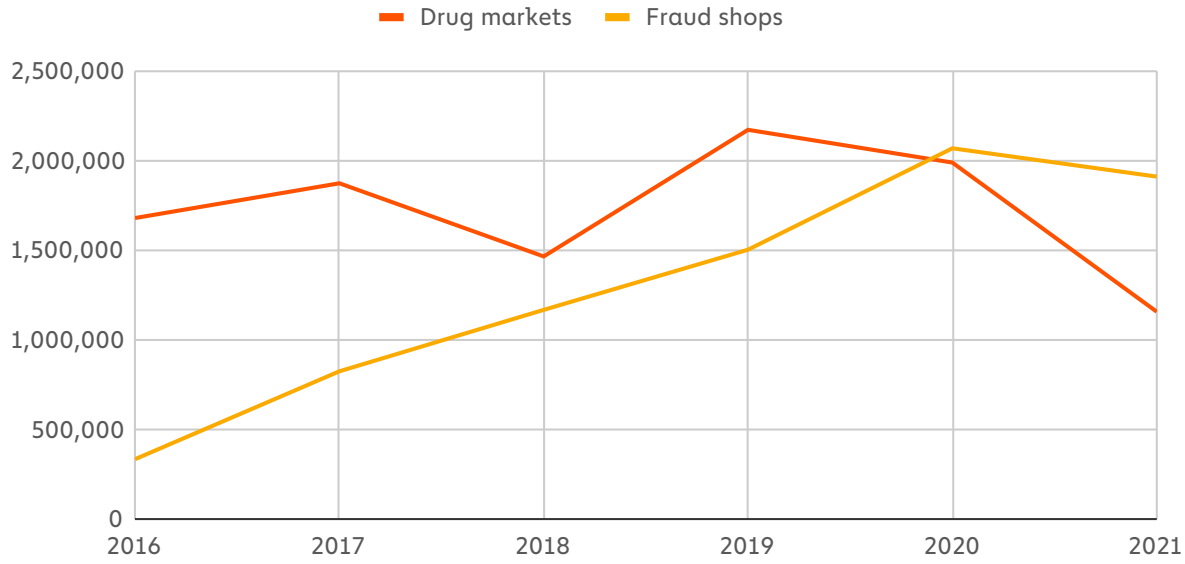
Number of transfers to drug markets and fraud shops | 2016-2021



An "active user" is defined as any wallet that has sent or received more than $5 worth of cryptocurrency to/from darknet markets during the year

The number of active users on drug markets has also undergone a decline, shrinking from almost 1.7 million in 2016 to 1.2 million in 2021.

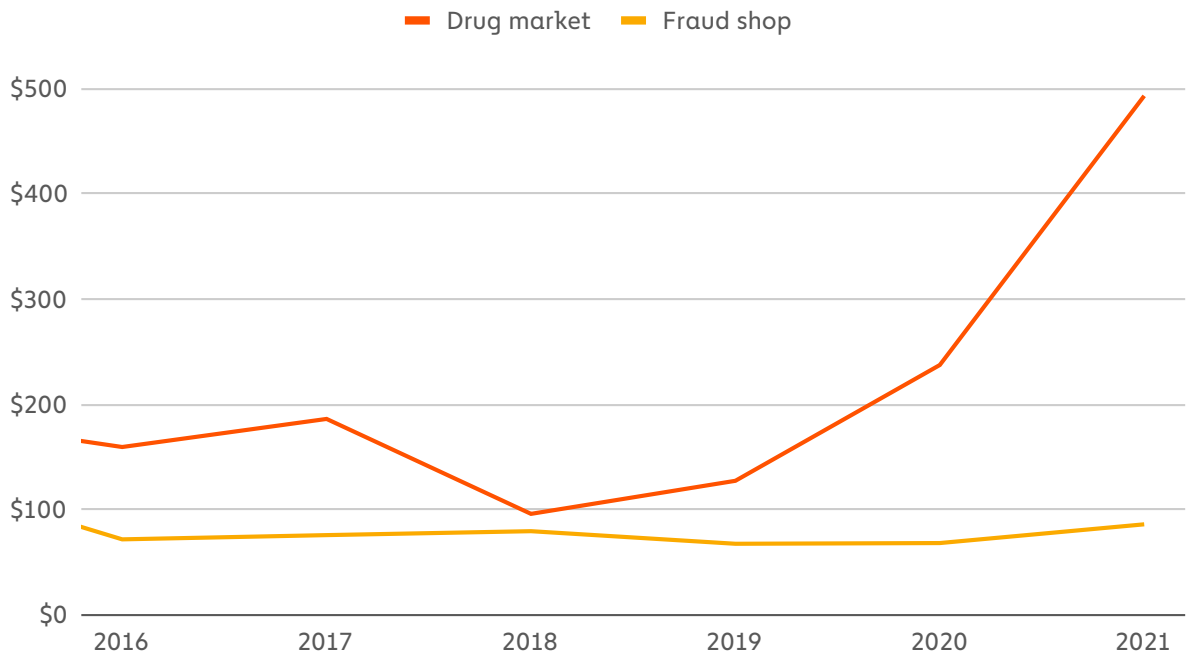
Number of active users of drug markets and fraud shops | 2016-2021



With drug market declines like these, one would expect overall drug market revenues to fall, but in fact they've done the opposite. From 2016 to 2021, drug market revenue growth averaged 35.7 percent per year. So if more users and more transfers aren't behind this growth, what is?

Our finding: bigger payments. From 2016 to 2021, the average payment size has leapt from $160 to $493 worth of cryptocurrency.

Average payment size to drug markets and fraud shops



Interestingly, this trend has only played out with drug-focused markets, as the average purchase price for fraud shops has remained flat. But there are several possible explanations for drug markets' payment size rise. It could be the case that drug vendors are now selling more to drug distributors than just drug users, or that some users who once bought small quantities are now buying much more. But it could also be explained by per unit price increases—it's difficult to know for sure, as we can't tell exactly what users are ordering, or how much.

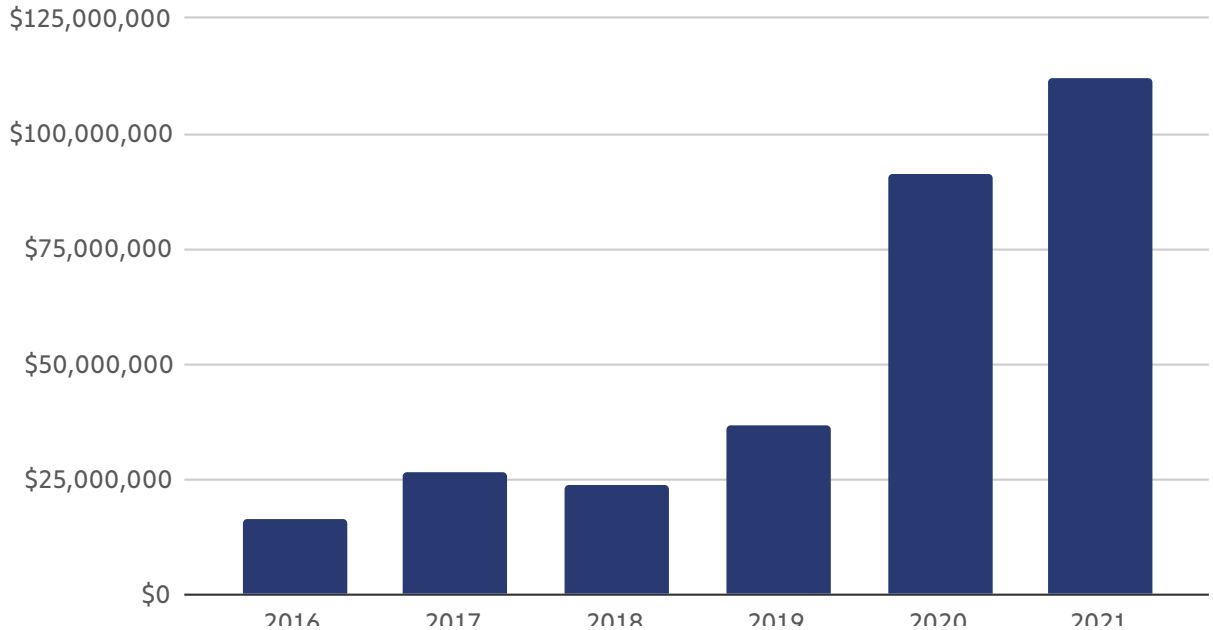
Whatever the explanation may be, it's clear that the nature of darknet markets are changing. Direct buyer-to-vendor sales, anonymous postage services, and privacy coins are cases in point.

Darknet market buyers and vendors transact directly more than ever

Direct buyer-to-vendor sales—transactions that take place without going through a darknet market—have been on the rise since 2019. We suspect that many of these buyer-vendor relationships were initially established on darknet markets, but that after a series of successful purchases, the buyers and vendors then arranged to transact off-market going forward.

Sales of this kind reached $112 million this year, equivalent to approximately 5% of total darknet market revenues.

Total value sent directly from darknet market buyers to vendors | 2016-2021



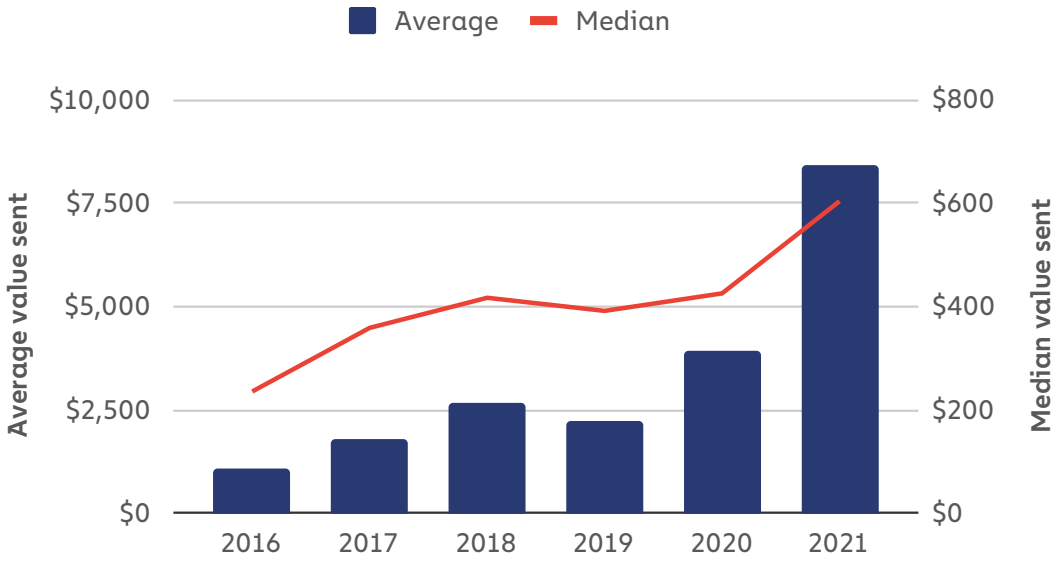
A user is considered a vendor if they have received more than $5,000 in cryptocurrency from darknet markets (DNMs) and are a net receiver of funds from DNMs. A user is considered a buyer if they have sent more than $100 in cryptocurrency to darknet markets and are a net sender of funds to DNMs.

This growth in direct sales volume might be explained by a deepening trust between long-time buyers and vendors, a growing distrust of darknet markets, a wish to avoid DNM fees, a desire to avoid being linked to known illicit activity, or some combination of these.

On average, these direct sales channels are substantial in terms of dollar amount: the average buyer sent a total of $8,441 worth of cryptocurrency to their preferred vendor during 2021. Sums this considerable may be indicative of large-scale illicit activity, whether it be attributed to drug trafficking or the sale of troves of financial data acquired through fraud.

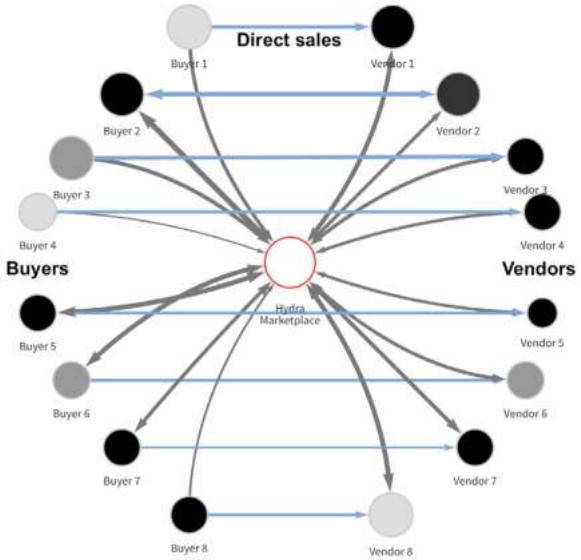
The median buyer, however, sent a total of just $603 to their preferred vendor this year.

Average and median value sent from each buyer to vendor per year | 2016-2021



This suggests that while massive direct sales account for a large majority of total volume, direct sales relationships exist at every size. In fact, this implies that more than half of all buyer-to-vendor relationships likely operate at a retail level, with the buyer sending less than $603 worth of cryptocurrency to the vendor during the year.

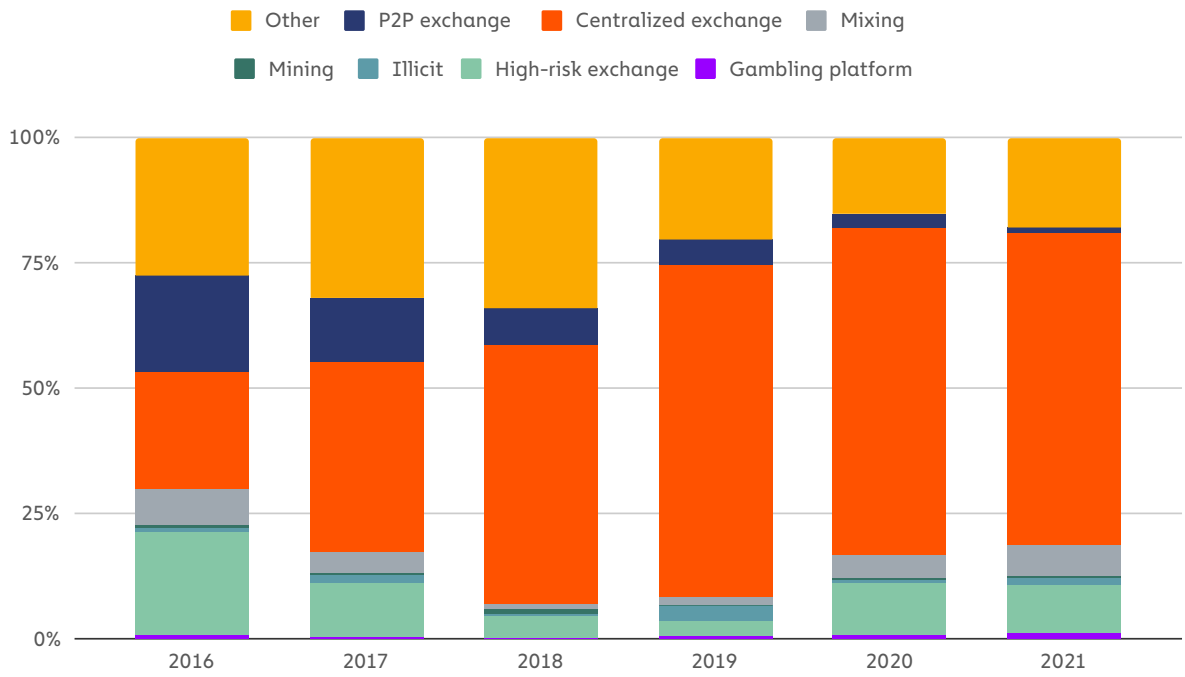
Nonetheless, the upper outliers are worth observing. Below, we visualize the eight largest buyer-to-vendor relationships by total value sent in 2021.



Each of these top buyers and vendors dealing directly have previously transacted through Hydra, presumably with one another (though we can't know for sure), as denoted by the grey lines. The blue lines, on the other hand, show direct transactions between the two without Hydra as an intermediary. On average, each buyer in this relationship has sent more than $3.1 million worth of cryptocurrency to their preferred vendor in 2021. This aligns with our hypothesis that the biggest direct relationships have ties to large-scale illicit activity.

We can analyze the transaction history of vendors like those shown above to better understand their money laundering strategy, based on the types of services to which they send funds.

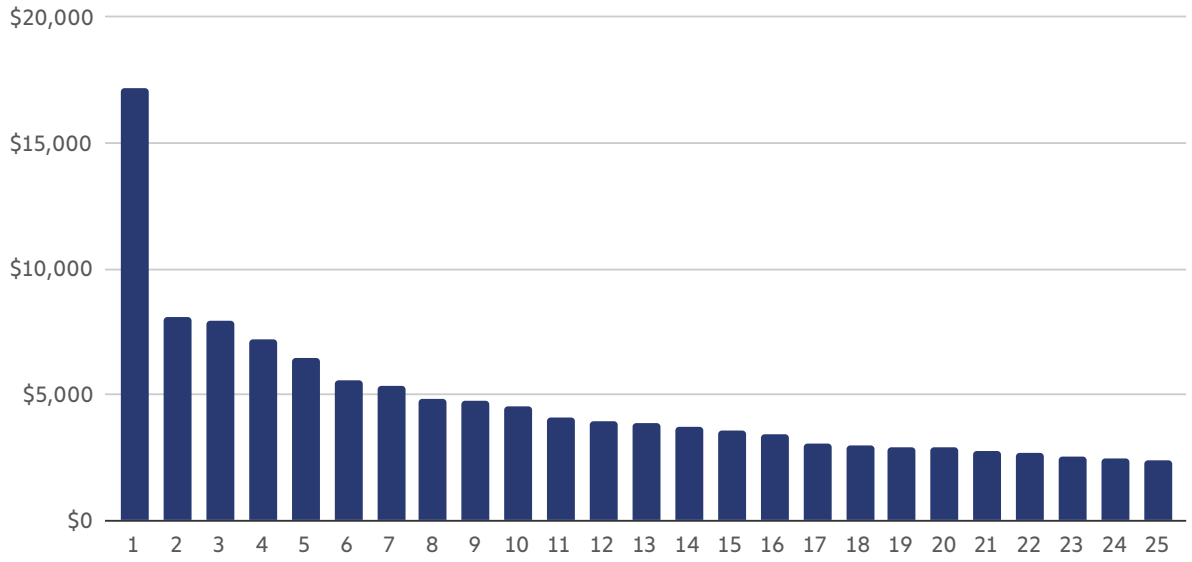
Destination of funds leaving darknet market vendor addresses | 2016-2021



Mainstream centralized exchanges are the most common destination, with high-risk exchanges and mixers also receiving a significant share.

Of course, not all funds sent from darknet market vendors indicate money laundering. Vendors often use cryptocurrency to purchase products and services necessary for their operations. Postage products and services — stamps, boxes, shipping labels, and the like — are a perfect example, as drug vendors typically mail their products to buyers. Chainalysis tracks several postage providers who accept payments in cryptocurrency, and has identified several darknet market vendors sending those providers significant sums.

Top darknet market vendors by value sent to postage providers | 2021



The most prolific of these vendors purchased over $17,000 worth of postage services this year, all using cryptocurrency. Ten other vendors each spent more than $4,000. And in aggregate, 322 vendors sent a combined $207,000 worth of cryptocurrency to these services this year, underscoring the important role a seemingly niche service plays in cryptocurrency-based crime.

Monero sees increased adoption as a darknet market payment method

Monero is seeing increased adoption among darknet markets this year, with the number of markets supporting it growing from 45% last year to 67% in 2021. In fact, a few markets, namely Archetyp, the revamped Alphabay, and the since-closed White House Market, exclusively support Monero. Bitcoin still dominates the darknet market space, however, with support from 93% of all markets.

Consolidation, competition, and caution defined darknet markets in 2021

Even as the demand for drugs and stolen credentials has continued to move online, competitors' black hat tactics and law enforcement takedowns have driven many more markets offline. In an abundance of caution, several markets have even closed voluntarily, while the markets that have opened in their place have embraced privacy-enhanced designs. Meanwhile, vendors have taken more steps than ever to enhance their shipping anonymity, and buyers have begun to transact with these vendors directly. All of these trends point to a darknet market industry that is fast maturing.

To solve cases that interface with darknet markets, investigators should be aware of these trends and have access to the proper tools to address them. Chainalysis Reactor's extensive attributions, graphing capabilities, and investigation teams can provide just that—the expertise and tooling needed to turn this blockchain data into actionable leads.

High-risk Jurisdictions & Sanctions

High-risk Jurisdictions & Sanctions

North Korea

North Korean Hackers Have Prolific Year as Their Total Unlaundered Cryptocurrency Holdings Reach All-time High

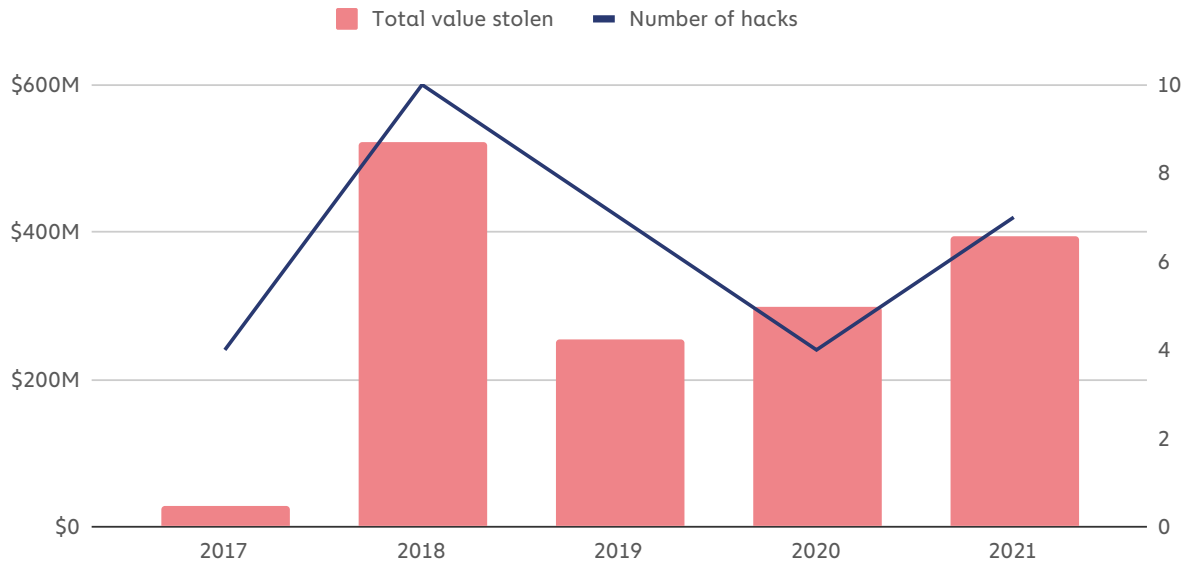
North Korean cybercriminals had a banner year in 2021, launching at least seven attacks on cryptocurrency platforms that extracted nearly $400 million worth of digital assets last year. These attacks targeted primarily investment firms and centralized exchanges, and made use of phishing lures, code exploits, malware, and advanced social engineering to siphon funds out of these organizations' internet-connected "hot" wallets into DPRK-controlled addresses. Once North Korea gained custody of the funds, they began a careful laundering process to cover up and cash out.

These complex tactics and techniques have led many security researchers to characterize cyber actors for the Democratic People's Republic of Korea (DPRK) as advanced persistent threats (APTs). This is especially true for APT 38, also known as "Lazarus Group," which is led by DPRK's primary intelligence agency, the US- and UN-sanctioned Reconnaissance General Bureau. While we will refer to the attackers as North Korean-linked hackers more generally, many of these attacks were carried out by the Lazarus Group in particular.

Lazarus Group first gained notoriety from its Sony Pictures and WannaCry cyberattacks, but it has since concentrated its efforts on cryptocurrency crime—a strategy that has proven immensely profitable. From 2018 on, the group has stolen and laundered massive sums of virtual currencies every year, typically in excess of $200 million. The most successful individual hacks, one on KuCoin and another on an unnamed cryptocurrency exchange, each netted more than $250 million alone. And according to the UN security council, the revenue generated from these hacks goes to support North Korea's WMD and ballistic missile programs.

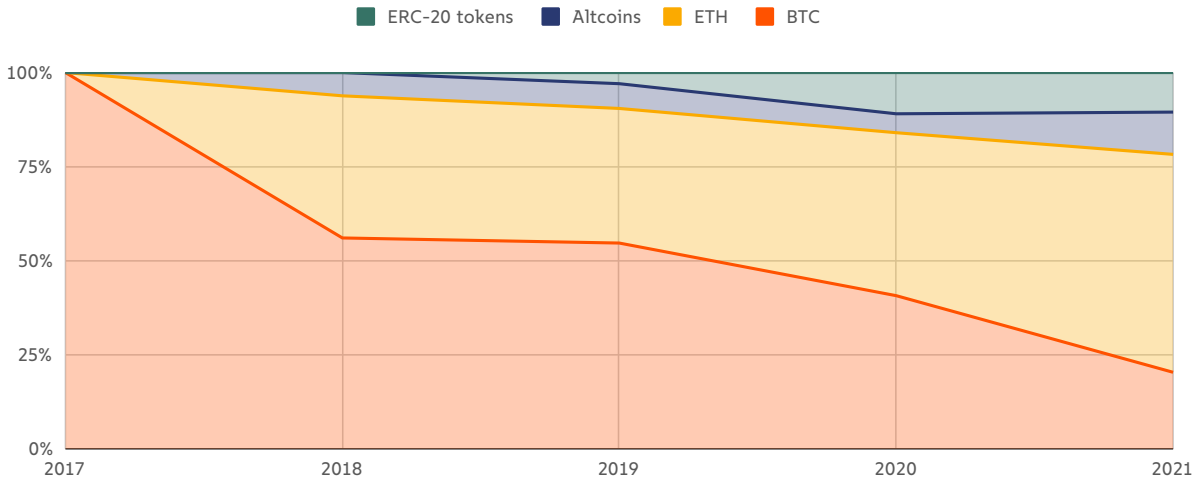
In 2021, North Korean hacking activity was on the rise once again. From 2020 to 2021, the number of North Korean-linked hacks jumped from four to seven, and the value extracted from these hacks grew by 40%.

North Korean-linked hacks by total value stolen and total number of hacks | 2017–2021



Interestingly, in terms of dollar value, Bitcoin now accounts for less than one fourth of the cryptocurrencies stolen by DPRK. In 2021, only 20% of the stolen funds were Bitcoin, whereas 22% were either ERC-20 tokens or altcoins. And for the first time ever, Ether accounted for a majority of the funds stolen at 58%.

Share of funds stolen by DPRK by coin type | 2017–2021

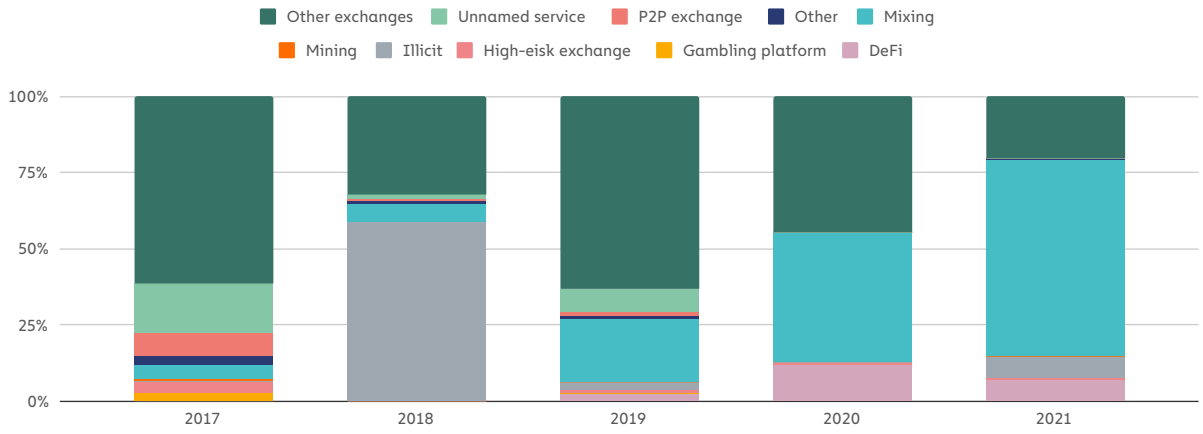


The growing variety of cryptocurrencies stolen has necessarily increased the complexity of DPRK's cryptocurrency laundering operation. Today, DPRK's typical laundering process is as follows:

1. ERC-20 tokens and altcoins are swapped for Ether via decentralized exchange (DEX)
2. Ether is mixed
3. Mixed Ether is swapped for Bitcoin via DEX
4. Bitcoin is mixed
5. Mixed Bitcoin is consolidated into new wallets
6. Bitcoin is sent to deposit addresses at crypto-to-fiat exchanges based in Asia —potential cash-out points

In fact, we observed a massive increase in the use of mixers among DPRK-linked actors in 2021.

Laundering mechanisms used by DPRK | 2017–2021



More than 65% of DPRK's stolen funds were laundered through mixers this year, up from 42% in 2020 and 21% in 2019, suggesting that these threat actors have taken a more cautious approach with each passing year.

Why mixers? DPRK is a systematic money launderer, and their use of multiple mixers —software tools that pool and scramble cryptocurrencies from thousands of addresses—is a calculated attempt to obscure the origins of their ill-gotten cryptocurrencies while offramping into fiat.

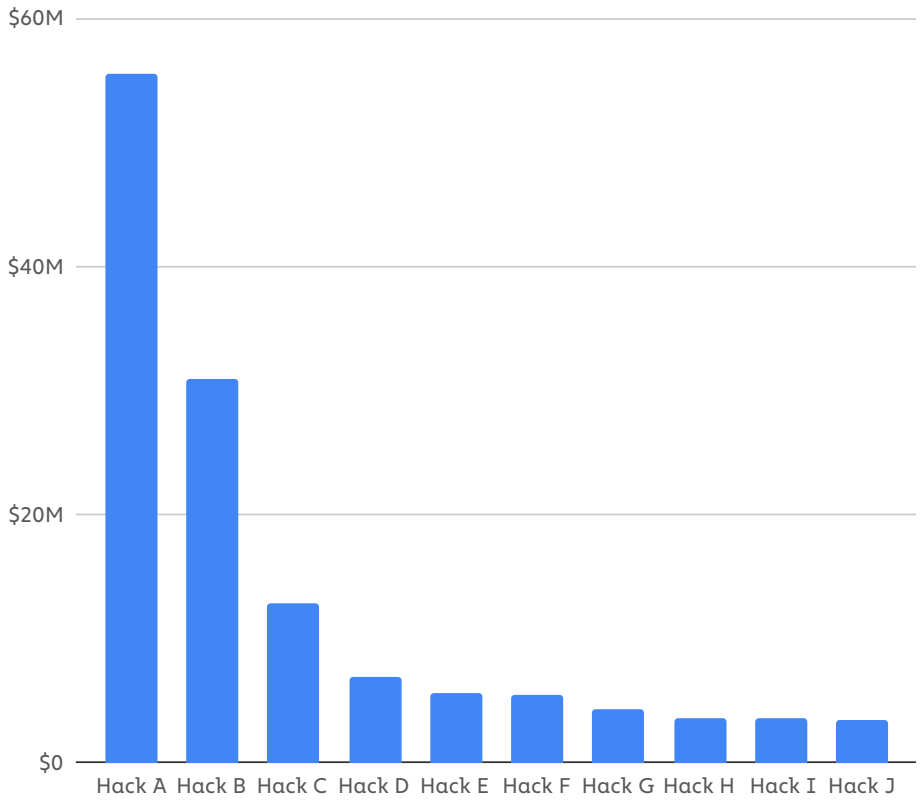
Why DeFi? DeFi platforms like DEXs provide liquidity for a wide range of ERC-20 tokens and altcoins that may not otherwise be convertible into cash. When DPRK swaps these coins for ETH or BTC they become much more liquid, and a larger variety of mixers and

exchanges become usable. What's more, DeFi platforms don't take custody of user funds and many do not collect know-your-customer (KYC) information, meaning that cybercriminals can use these platforms without having their assets frozen or their identities exposed.

DPRK's stolen fund stockpile: $170 million worth of old, unlaundered cryptocurrency holdings

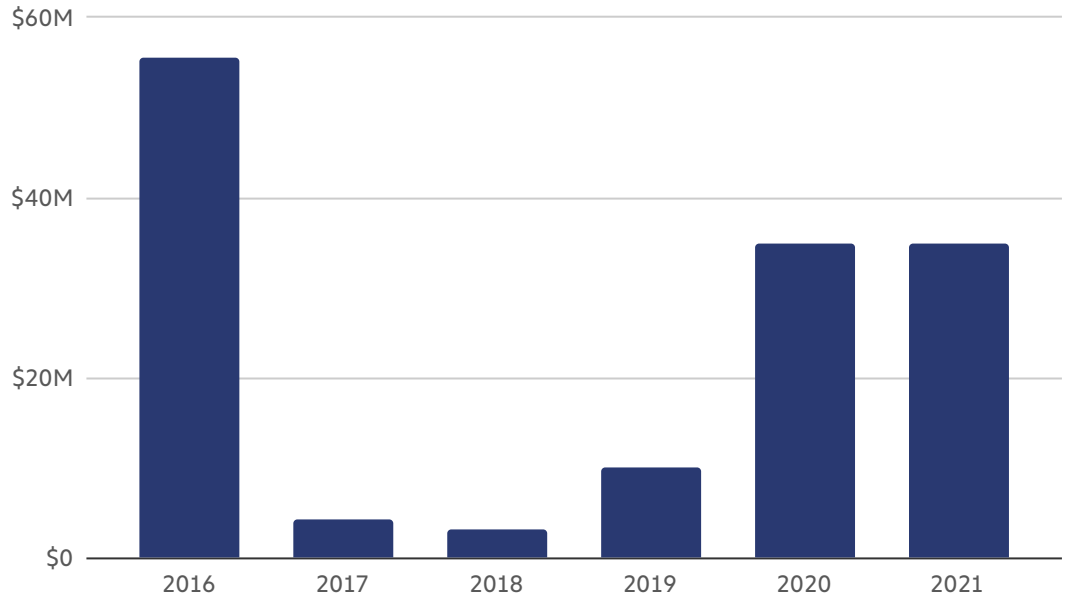
Chainalysis has identified $170 million in current balances—representing the stolen funds of 49 separate hacks spanning from 2017 to 2021—that are controlled by North Korea but have yet to be laundered through services. The ten largest balances by dollar value are listed below.

North Korea's largest unlaundered cryptocurrency holdings by hack



Of DPRK's total holdings, roughly $35 million came from attacks in 2020 and 2021. By contrast, more than $55 million came from attacks carried out in 2016—meaning that DPRK has massive unlaundered balances as much as six years old.

Total balances held by North Korean actors by date of attack | 2016–2021



This suggests that DPRK-linked hackers aren't always quick to move stolen cryptocurrencies through the laundering process. It's unclear why the hackers would still be sitting on these funds, but it could be that they are hoping law enforcement interest in the cases will die down, so they can cash out without being watched.

Whatever the reason may be, the length of time that DPRK is willing to hold on to these funds is illuminating, because it suggests a careful plan, not a desperate and hasty one.

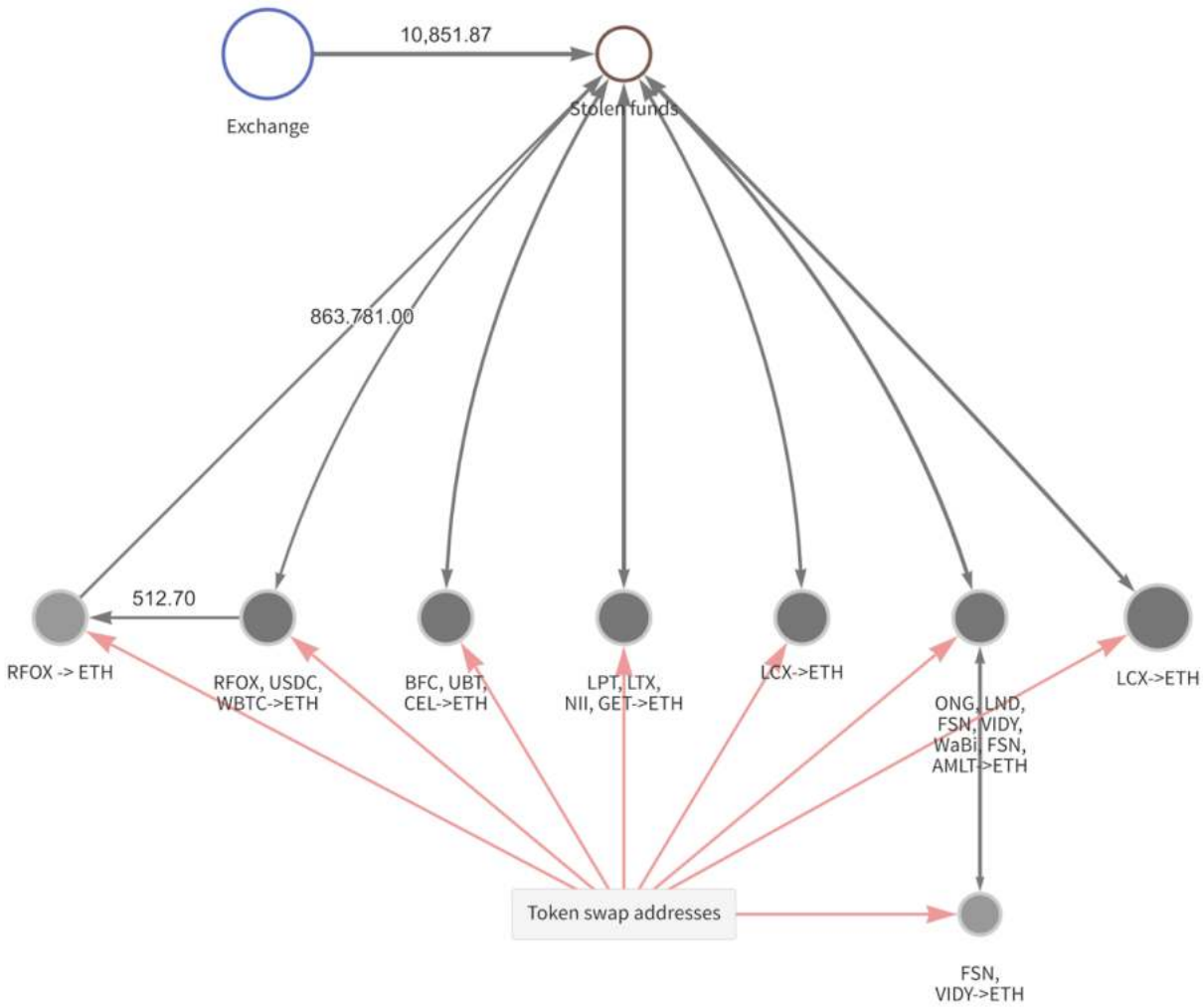
Coinswap, mix, consolidate, cash out: How North Korea-linked hackers laundered $91 million after an exchange hack

In August, a cryptocurrency exchange announced that an unauthorized user had gained access to some of the wallets it managed. The night before, 67 different ERC-20 tokens, along with large quantities of Ether and Bitcoin, had been moved from these wallets to addresses controlled by a party working on behalf of DPRK.

The attacker then used decentralized protocols to swap the various ERC-20 tokens for Ether. From there, they mixed the Ether, swapped the mixed Ether for Bitcoin, mixed the Bitcoin, consolidated the mixed Bitcoin into new wallets, and then deposited the funds into crypto-to-fiat exchanges based in Asia. As a result, approximately $91.35M in cryptoassets was laundered.

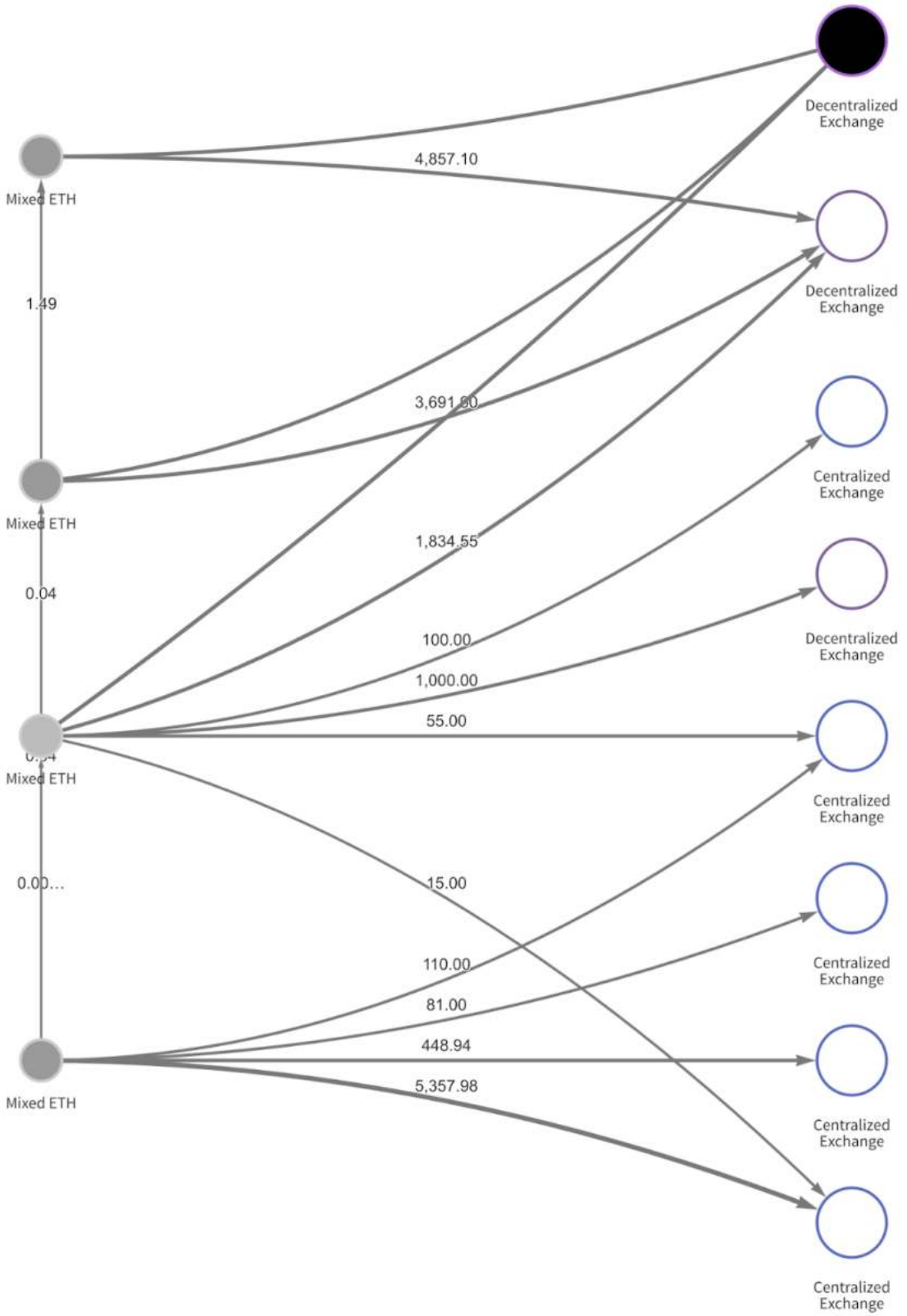
Below, we've visualized each stage of the laundering process in Chainalysis Reactor.

Stage 1: Stolen ERC-20 tokens swapped for Ether at DEXs:

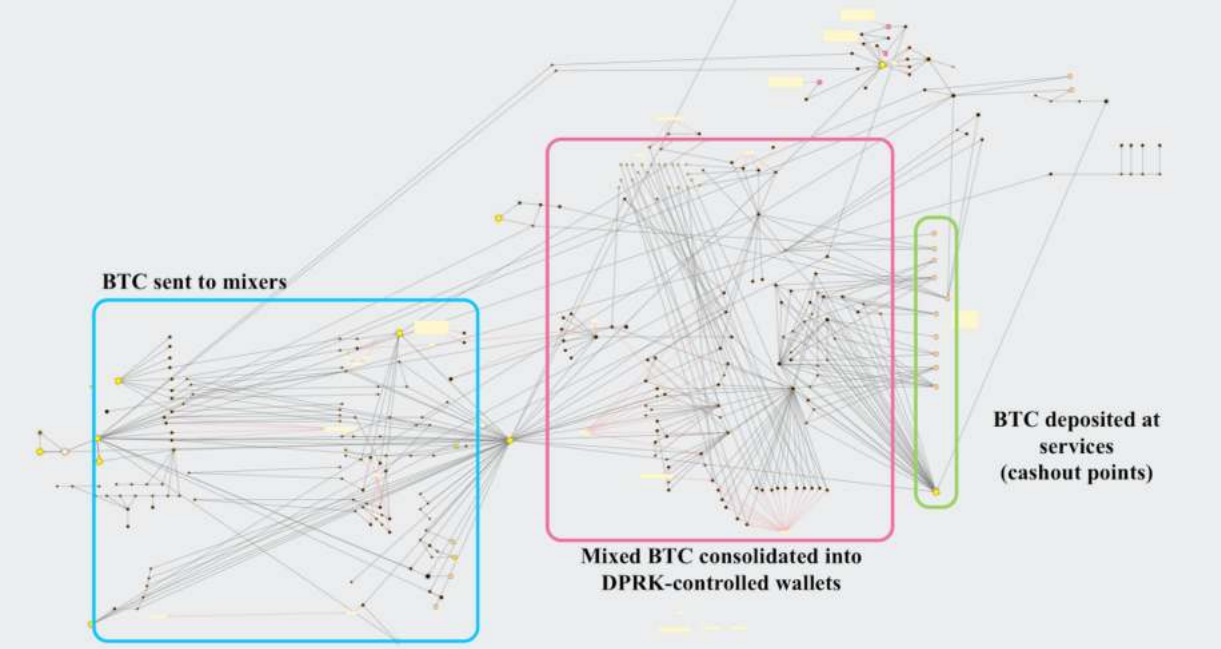


Next, the newly acquired Ether was mixed, and then swapped again.

Stage 2: Mixed Ether deposited at DEXs and CEXs to swap for Bitcoin



Stage 3: Movement of stolen funds after being swapped for BTC



At the end of this process, the attackers move the Bitcoin to centralized, primarily Asia-based exchanges, where it's likely swapped for a fiat currency like China's Renminbi, allowing them to finally access the cash gained from the hack.

DPRK: An advanced persistent threat to the cryptocurrency industry

These behaviors, put together, paint a portrait of a nation that supports cryptocurrency-enabled crime on a massive scale. Systematic and sophisticated, North Korea's government—be it through the Lazarus Group or its other criminal syndicates—has cemented itself as an advanced persistent threat to the cryptocurrency industry in 2021.

Nonetheless, the inherent transparency of many cryptocurrencies presents a way forward. With blockchain analysis tools, compliance teams, criminal investigators, and hack victims can follow the movement of stolen funds, jump on opportunities to freeze or seize assets, and hold bad actors accountable for their crimes.

High-risk Jurisdictions & Sanctions

Russia

Russian Cybercriminals Drive Significant Ransomware and Cryptocurrency-based Money Laundering Activity

Russia is a leading country in cryptocurrency adoption, placing 18th overall on our Global Crypto Adoption Index. But the story of Russia's cryptocurrency usage isn't entirely positive. Individuals and groups based in Russia — some of whom have been sanctioned by the United States in recent years — account for a disproportionate share of activity in several forms of cryptocurrency-based crime.

In this section, we'll delve into two intertwined areas of Russia's crypto crime ecosystem that, together, have serious implications for cybersecurity, compliance, and national security: ransomware and money laundering.

Russian cybercriminals set the pace for ransomware

Russia has long been home to some of the most skilled hackers in the world. According to cybersecurity investigators like Brian Krebs, this is largely due to the country's excellence in computer science education, combined with low economic prospects even for those who are skilled in the field. Given this background, it may not be surprising that Russia leads the way in ransomware. But the degree to which Russia-based ransomware strains dominate is quite shocking.

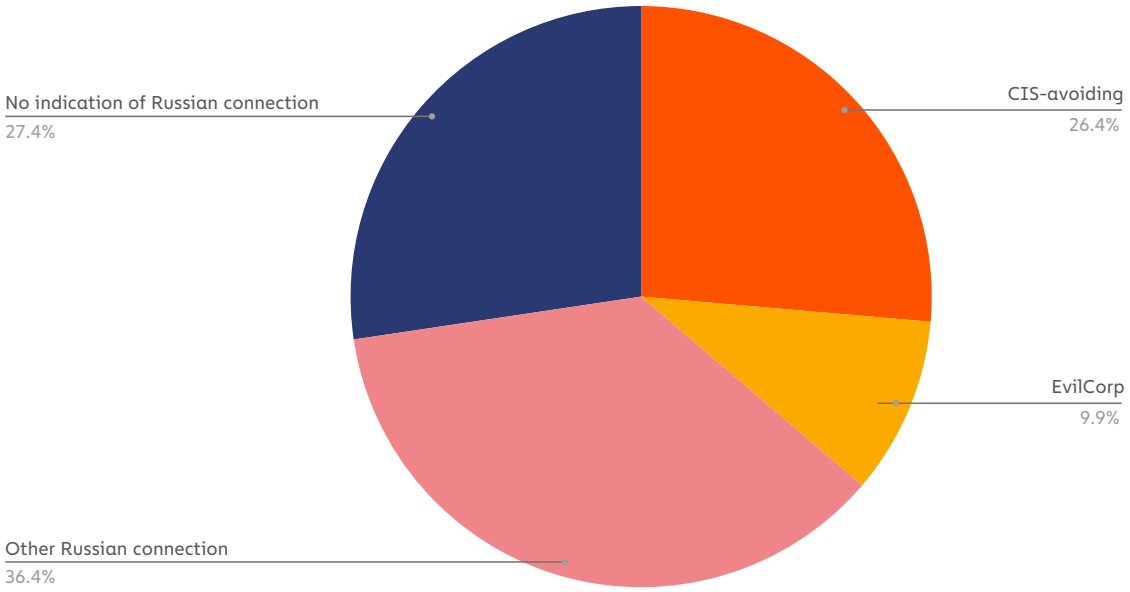
Before we dive into the data, a quick explainer — we generally tie specific ransomware strains to Russian cybercriminals based on one of three criteria:

- **Evil Corp.** Evil Corp is a Russia-based cybercriminal organization that has been prolific in ransomware, and whose leadership is believed to have ties to the Russian government.
- **Avoids CIS countries.** The Commonwealth of Independent States (CIS) is an intergovernmental organization of Russian-speaking, former Soviet countries. Many ransomware strains contain code that prevents the encryption of files if it detects the victim's operating system is located in a CIS country. In other cases, ransomware operators have even given over decryptors to return file access after learning they inadvertently targeted a Russian organization. We can attribute CIS-avoiding strains to Russian cybercriminals, though with a lesser degree of confidence, as some of them may be based in other CIS countries.
- **Other connections: language, affiliate location, etc.** There are several other ransomware characteristics that can indicate a strain is likely based in Russia. Examples include ransomware strains that share documents and announcements

in the Russian language, or whose affiliates are believed to be located in Russia with a high degree of confidence.

Using those three criteria, we show on the pie chart below the share of total ransomware revenue that went to strains affiliated with Russian organizations in 2021.

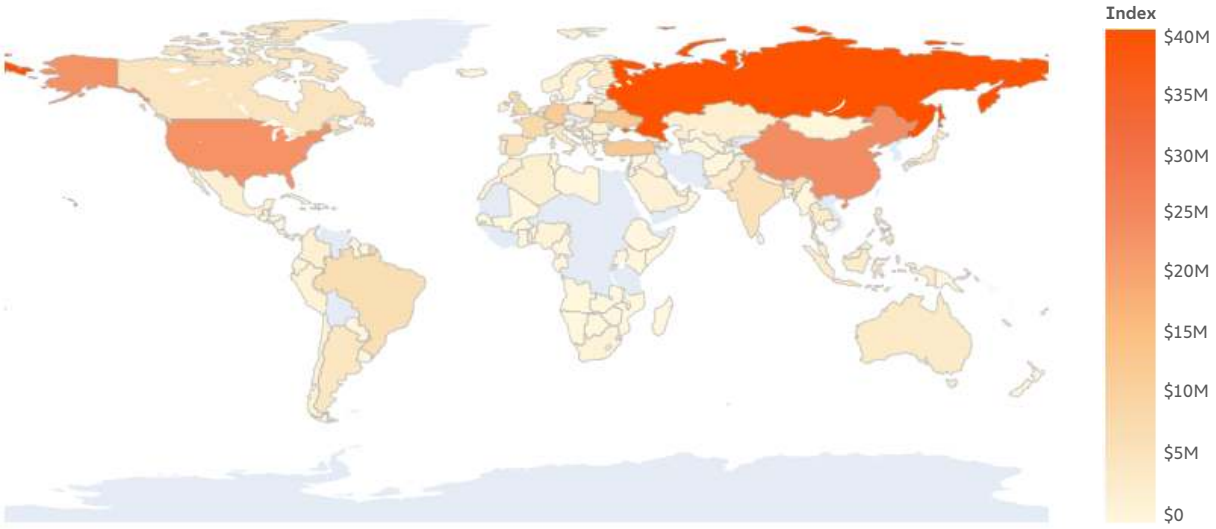
Share of 2021 ransomware revenue taken by Russia-affiliated strains | 2021



Overall, roughly 74% of ransomware revenue in 2021 — over $400 million worth of cryptocurrency — went to strains we can say are highly likely to be affiliated with Russia in some way.

Blockchain analysis combined with web traffic data also tells us that after ransomware attacks take place, most of the extorted funds are laundered through services primarily catering to Russian users.

Estimation of regional exposure to ransomware funds | 2021

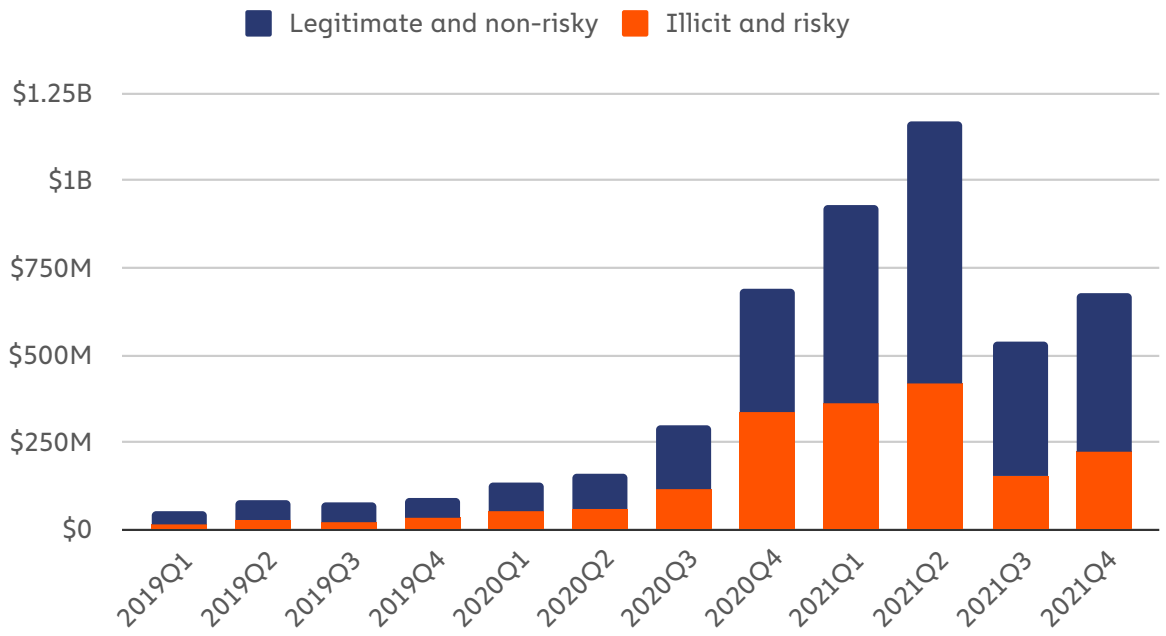


An estimated 13% of funds sent from ransomware addresses to services went to users estimated to be in Russia, more than any other region. That brings us to another point: A huge amount of cryptocurrency-based money laundering, not just of ransomware funds but of funds associated with other forms of cybercrime as well, goes through services with substantial operations in Russia.

Cryptocurrency-based money laundering in Moscow City

Russia is home to several cryptocurrency businesses that have processed substantial transaction volume from illicit addresses. In order to illustrate the scope of the problem, we thought it would be interesting to zoom in on businesses headquartered or with a significant presence in the capital's financial district, Moscow City. Chainalysis is tracking several dozen cryptocurrency businesses operating in Moscow City alone that facilitate significant amounts of money laundering.

Total value received by Moscow City cryptocurrency buinesses | 2019–2021

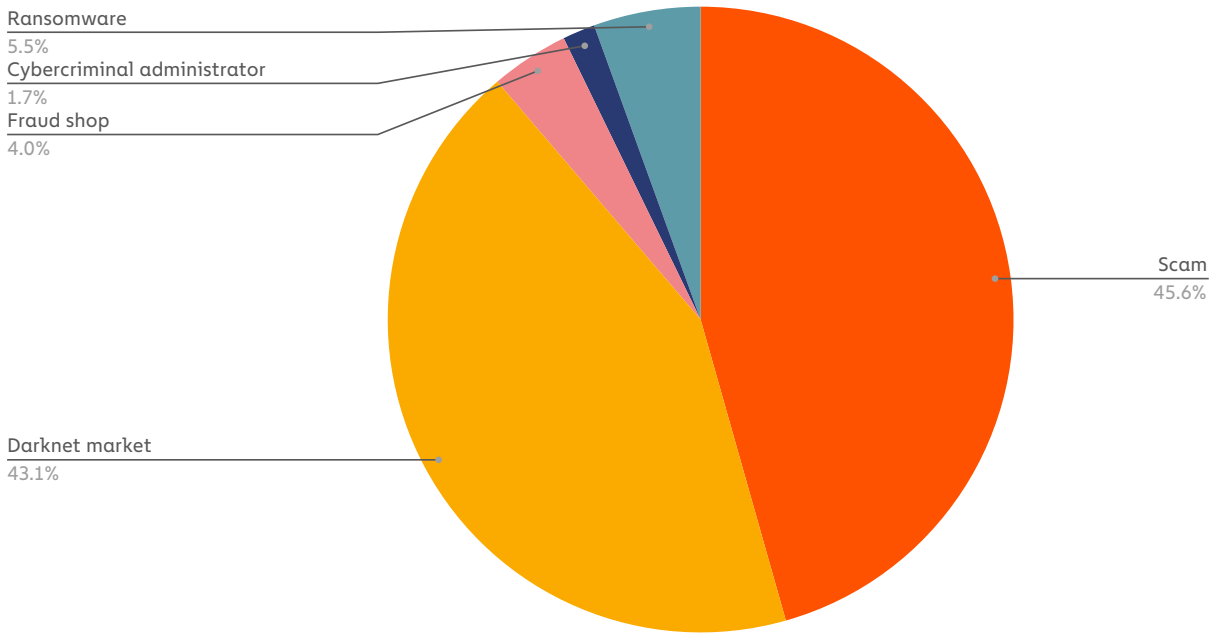


Note: The word "risky" here defines addresses connected to entities that, while not necessarily inherently criminal, are frequently linked to criminal activity, such as high-risk exchanges and mixers.

Collectively, these businesses receive hundreds of millions of dollars' worth of cryptocurrency per quarter, with totals peaking at nearly $1.2 billion in the second quarter of 2021. In any given quarter, the illicit and risky addresses account for between 29% and 48% of all funds received by Moscow City cryptocurrency businesses. In total, across the three-year period studied, these businesses have received nearly $700 million worth of cryptocurrency from addresses associated with explicitly criminal activity, which represents 13% of all value they've received in that time. Where do these illicit funds come from?

Illicit cryptocurrency moving to Moscow cryptocurrency businesses by crime type

| 2019–2021



Note: "Cybercriminal administrator" refers to addresses that have been attributed to individuals connected to a cybercriminal organization, such as a darknet market.

Scams at $313 million and darknet markets at $296 million make up the vast majority of illicit cryptocurrency sent to the Moscow City cryptocurrency businesses we track between 2019 and 2021. Ransomware is third at $38 million.

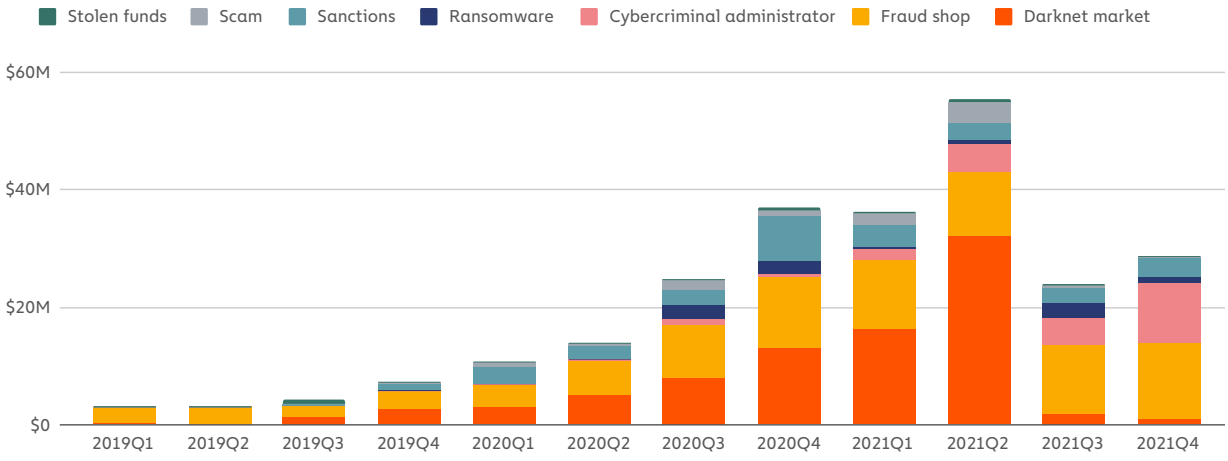
Overall, the Moscow City cryptocurrency businesses we track vary greatly in the role that money laundering plays in their overall business. Some of them are big enough that despite receiving millions of dollars' worth of funds from illicit addresses, those funds only represent 10% or less of all cryptocurrency they receive. Those instances could be attributed to the business's lack of knowledge, rather than purposeful criminal activity. But for other Moscow City cryptocurrency businesses, illicit funds make up as much as 30% or more of all cryptocurrency received, which suggests those businesses may be making a concerted effort to serve a cybercriminal clientele.

Interestingly, over half of the businesses described above have reportedly operated in the same Moscow City skyscraper: Federation Tower.

Credit: Mariano Mantel

Federation Tower, a two skyscraper complex in the heart of Moscow City, is one of the most prestigious buildings in all of Russia, with several prominent businesses headquartered there and residential units going for upwards of $36 million. However, as outlets like Bloomberg and the New York Times have reported, Federation Tower is home to several cryptocurrency businesses that have facilitated extensive money laundering, accepting funds from addresses involved in various forms of cryptocurrency-based crime — especially scams, darknet markets, and ransomware.

Illicit funds moving to Federation Tower cryptocurrency businesses | 2019–2021



Nothing is more emblematic of the growth of Russia's crypto crime ecosystem, and of cybercriminals' ability to operate with apparent impunity, than the presence of so many cryptocurrency businesses linked to money laundering in one of the capital city's most notable landmarks.

Below, we highlight some of the cryptocurrency businesses with a presence in Moscow City that have facilitated the most money laundering or are otherwise notable:

Analysis of a selection of Moscow City cryptocurrency businesses facilitating money-laundering | 2019–2021

Name	Total cryptocurrency value received (2019–2021)	Illicit and risky cryptocurrency value received (2019–2021)	Share of all value received coming from illicit and risky sources (2019–2021)	Notes
Garantex	$2,114,431,000	$645,223,700	31%	Has received over $10 million from ransomware strains including NetWalker, Phoenix Cryptolocker, and Conti.
Eggchange	$34,081,220	$3,705,827	11%	Has received hundreds of thousands of dollars' worth of cryptocurrency from darknet markets, scams, fraud shops, and ransomware operators. Founder Denis Dubnikov was arrested for his alleged role in helping Ryuk ransomware operators launder funds.
Cashbank	$45,400,600	$180,119	0.4%	While Cashbank's detected money laundering activity is relatively low in volume, it advertises on forums frequented by illicit actors and criminals.
Buy-bitcoin	$41,604,170	$11,374,910	27%	Has received $2.1 million from darknet markets, $400,000 in stolen funds, and $400,000 from ransomware attackers.
Tetchange	$21,903,700	$4,621,440	21%	Has received over $1 million from darknet markets and $600,000 from ransomware attackers.

Bitzlato	$2,000,077,000	$966,254,800	48%	Has received $206 million from darknet markets, $224.5 million from scams, and $9 million from ransomware attackers.
Suex	$426,189,500	$158,856,100	37%	Has received $24 million from scams, $20 million from darknet markets, and $12 million from ransomware. Sanctioned by OFAC in 2021.

What's next for crypto crime in Russia?

Looking ahead, change may be on the way for Russia's cryptocurrency ecosystem, especially as it relates to crime. In January 2022, Russian police arrested 14 affiliates of the REvil ransomware organization, marking one of the only times the local authorities have taken action against ransomware attackers operating within the country. However, analysts have speculated that the arrests were an act of diplomacy meant to cool tensions with the United States over Russia's troop buildup on Ukraine's borders, and may not indicate true commitment to fighting ransomware. At the same time, cryptocurrency's regulatory status in Russia appears to be in flux, with President Vladimir Putin defending cryptocurrency miners at the same time the country's national bank recommends an all-out ban on all cryptocurrency activity.

Regardless of what the future holds, it's important to understand where things stand now: Russian cybercriminal organizations are some of the biggest perpetrators of cryptocurrency-based crime — especially ransomware — and local cryptocurrency businesses provide money laundering services that enable this activity. 2021 saw positive momentum against this issue, from the seizure of funds from ransomware organization DarkSide to the sanctioning of Suex and Chatex. Chainalysis looks forward to working with law enforcement, regulators, and compliance professionals in 2022 to keep that momentum going.

Cryptocurrency Money Laundering in Moscow City

Together, these six Moscow City crypto services received $1.8 billion from addresses associated with illicit and risky activity.

Garantex
$645,223,700 recieved from illicit and risky sources

31% of all value received

Buy-bitcoin
$11,374,910 recieved from illicit and risky sources

27% of all value received

Bitzlato
$966,254,800 recieved from illicit and risky sources

48% of all value received

Eggchange
$3,705,827 recieved from illicit and risky sources

11% of all value received

Tetchange
$4,621,440 recieved from illicit and risky sources

21% of all value received

Suex
$158,856,100 recieved from illicit and risky sources

37% of all value received

High-risk Jurisdictions & Sanctions

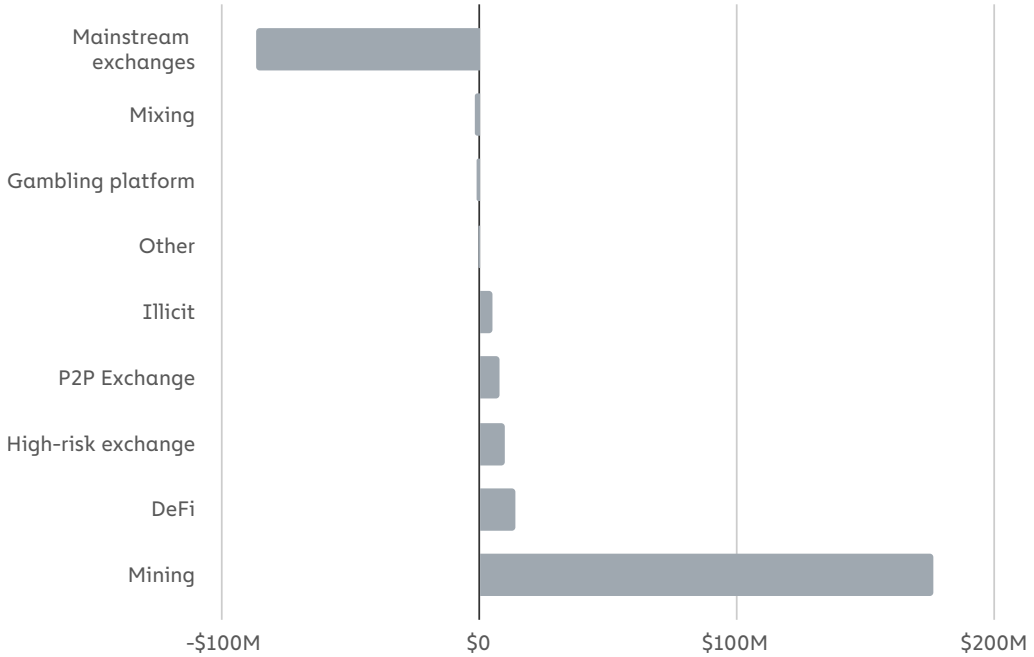
Iran

Bitcoin Mining Fuels Iran's Billion-Dollar Sanctions Evasions

Iran faces some of the most extensive U.S. sanctions of any country. Per the United States Treasury's Office of Foreign Assets Control (OFAC), U.S. businesses and individuals are effectively banned from transacting with Iranian businesses, including its biggest financial institutions and central bank. Some in the Iranian government have called for the country to use cryptocurrency to circumvent these sanctions, and Bitcoin mining may provide the perfect opportunity to do so. As one of the world's largest energy producers, Iran has the low-cost electricity needed to mine cryptocurrencies like Bitcoin cheaply, providing an injection of monetary value that sanctions can't stop.

Our research indicates Iranian Bitcoin mining is well underway at a surprisingly large scale. From 2015 to 2021, we found that Bitcoin mining funneled more than $186 million into Iranian services, most of it within the past year.

Net flows to and from Iranian services | 2015–2021



Iranian state actors are well aware of the opportunity. In 2019, the Iranian government created a licensing regime for cryptocurrency mining. And in March 2021, a think tank tied to the President's office released a report stressing its benefits.

But the costs have extended beyond just electricity. The Iranian government has had to ban Bitcoin mining twice this year due to frequent blackouts, many of which Iran's state

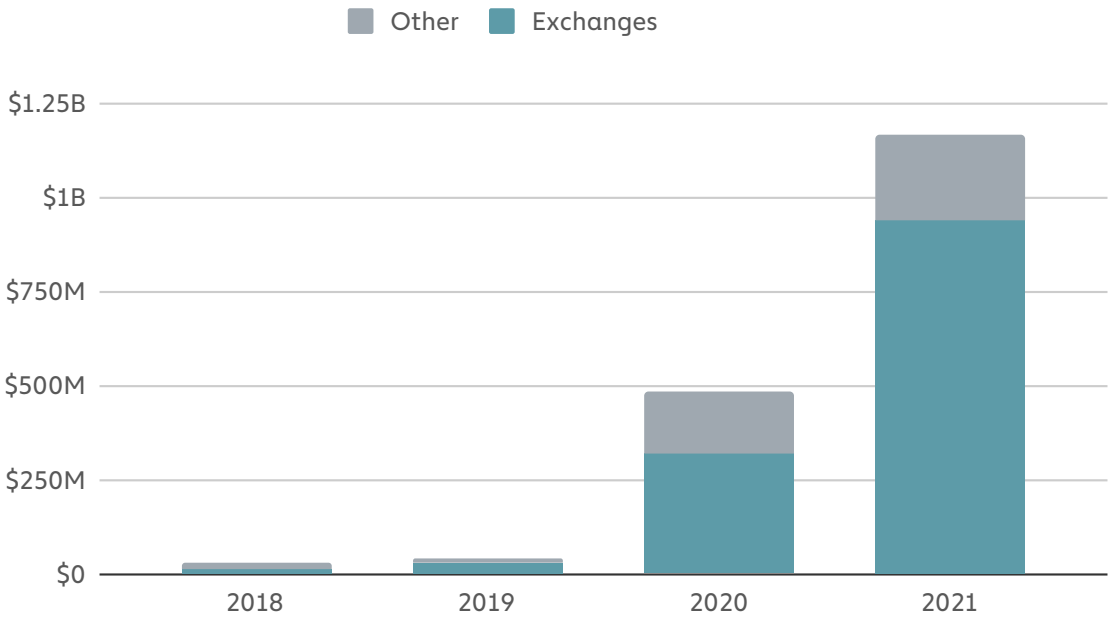
power agency has blamed on unlicensed Bitcoin mining. And unlicensed Bitcoin miners, for their part, allegedly account for "some 85%" of all activity in the country, per the Iranian president.

It has also opened up a new avenue of risk for cryptocurrency businesses. In theory, U.S. businesses could face penalties or even criminal prosecution if found in violation of OFAC sanctions, which prohibit U.S. persons or companies from servicing financial accounts belonging to Iranian persons or companies. That being said, businesses can monitor for exposure to Iranian miners to reduce this risk considerably.

It's also important to note that a nexus to sanctions is more attenuated at the transaction/mining fee level. If a U.S. business were to engage in a transaction and the fees paid from said transaction were received by an Iranian miner, the payer and payee would have had no say in who could receive these fees—the receiver of which is determined automatically by Bitcoin's proof-of-work protocol. To date, sanctions risk appears most prominent when a U.S. business transacts directly with the miner themselves.

Many exchanges operating in jurisdictions without active sanctions, however, continue to provide financial services to Iranian businesses. In fact, in 2021, services outside of Iran received $1.16 billion from Iranian services—more than double the value received last year.

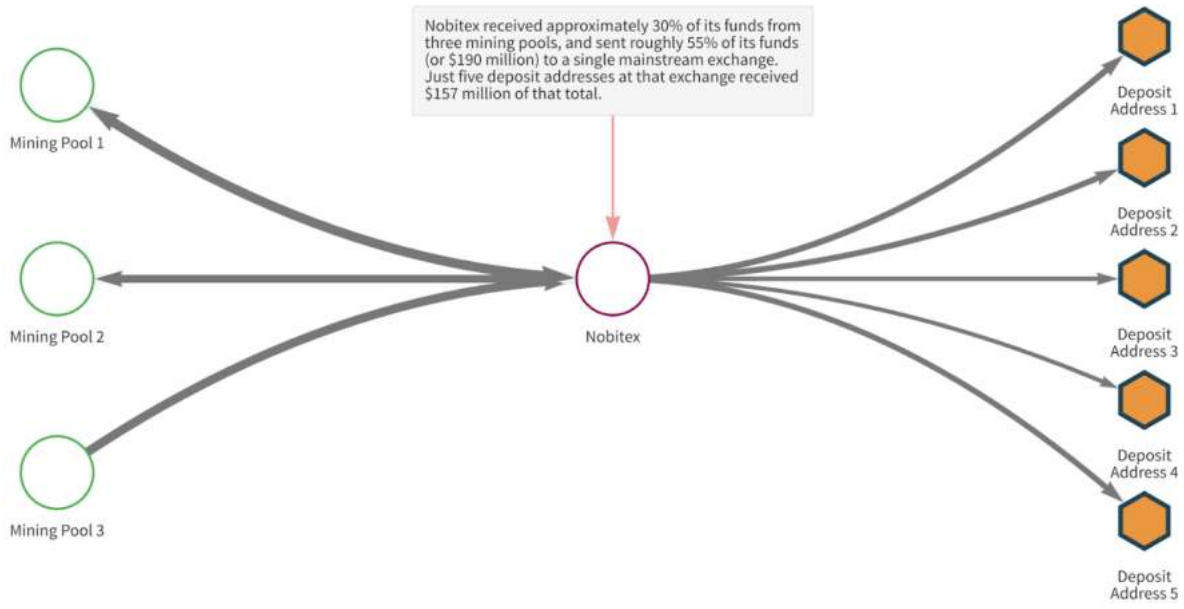
Total cryptocurrency value leaving Iranian services by destination | 2018–2021



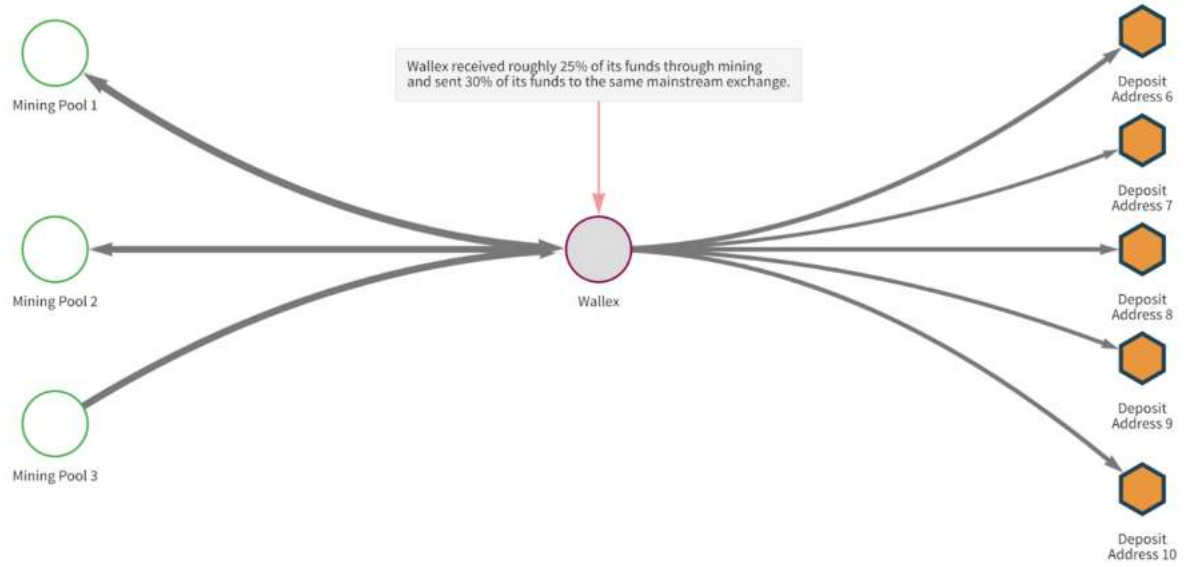
This transfer of funds from mining pools to Iranian services to services in the wider cryptocurrency ecosystem is a key corridor through which Iran evades sanctions. In the next section, we illustrate the most common paths to this end.

From mining pools to mainstream exchanges: Iran's sanctions evasion visualized

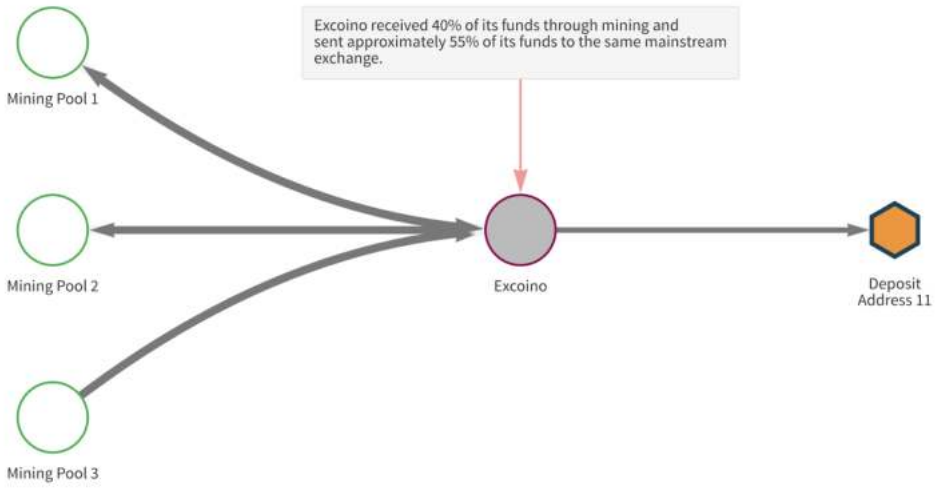
We can identify several of the services enabling Iran's sanctions evasion with blockchain analysis. Using Chainalysis Reactor, we visualize below the flow of funds from three mining pools to one mainstream exchange by way of Nobitex.ir, Iran's largest cryptocurrency exchange.



These same pools have similar degrees of exposure to Iran's second largest exchange, Wallex.ir.



And similar degrees of exposure to Iran's third largest exchange, Excoino.com.



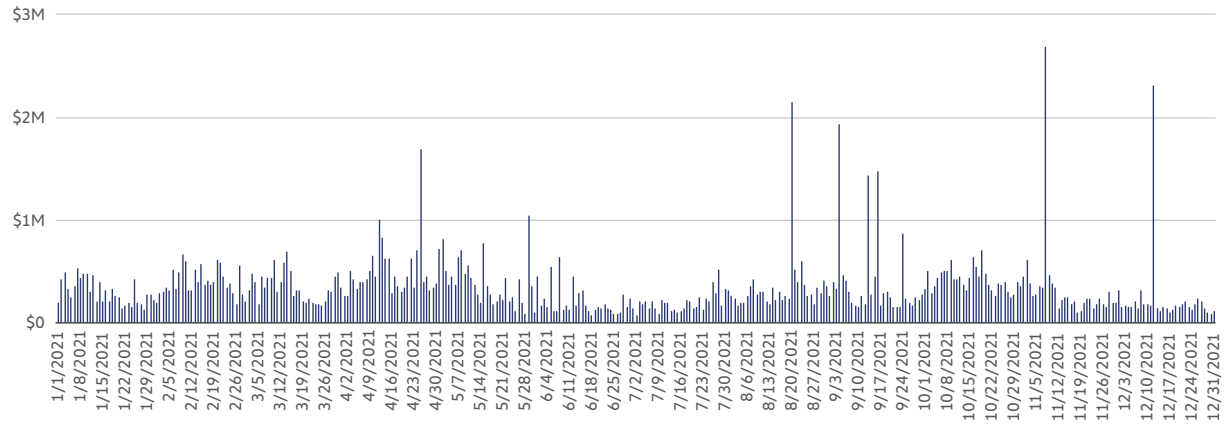
In spite of these large outflows, each mining pool above has a terms of service agreement explicitly disallowing Iranian users. On one of these mining pools' websites, the service states that by using the pool, the user guarantees that he/she is not subject to any economic sanctions, nor is he/she a citizen of Iran. On the two others, users are required to affirm that they are not a resident of Iran or any other jurisdiction where the services provided are restricted.

However, each mining pool above continues to send funds to Iranian services as of this report's release.

To get the complete picture of Iranian services' relationship with the mining world, we also measured the daily flows from *all* mining pools to *all* Iranian services in 2021—including those that don't mine Bitcoin.

We found that from January 1st to December 31st, outflows from mining pools to Iranian services averaged about $343,000 worth of cryptocurrency per day, approximately 80% of which was Bitcoin.

Daily cryptocurrency value received by Iranian services from mining pools | 2021



Interpreting these findings

Since our model captures only those mining pools with sending exposure to Iranian services in particular, $186 million likely underestimates Iran's total Bitcoin mining revenue from 2015 to 2021. In fact, other mining pools may support *much more* Iranian mining activity than the three pools we identify here—and given Iran's estimated 3.11% monthly share of the global hashrate, this is probably true. As such, this estimate should be considered a lower bound.

The implications for government agencies, financial institutions, and cryptocurrency businesses

With Iran embracing cryptocurrency, we advise interested government agencies to watch this situation closely. To avoid the risk of sanctions violations, we encourage U.S. cryptocurrency businesses and financial institutions to do the same. Businesses can automatically monitor for transactional exposure to Iranian entities with Chainalysis KYT, while government agencies can identify these transactions' counterparties with Reactor.

Thanks for reading the 2022 Crypto Crime Report

Chainalysis Authors

Kim Grauer
Director of Research

Will Kueshner
Content Marketer

Henry Updegrave
Senior Content Marketing Manager

Chainalysis

Check out more original Chainalysis research

Chainalysis Reports

> **Cryptocurrency Exchanges in 2021:** A Competitive Analysis

> **The 2021 NFT Market Report:** Everything You Need to Know About the NFT Market and Its Most Successful Collectors

VIEW ALL REPORTS

Chainalysis Insights

Data-driven content on cryptocurrency markets, regulation and developments

VISIT THE BLOG

Chainalysis

Chainalysis

Building trust in blockchains

About Chainalysis

Chainalysis is the blockchain analysis company providing data and analysis to government agencies, exchanges, and financial institutions across 40 countries. Our investigation and compliance tools, education, and support create transparency across blockchains so our customers can engage confidently with cryptocurrency. Backed by Accel, Benchmark, and other leading names in venture capital, Chainalysis builds trust in blockchains. For more information, visit www.chainalysis.com.

GET IN TOUCH
info@chainalysis.com

FOR MORE CONTENT
visit blog.chainalysis.com

FOLLOW US ON TWITTER
@chainalysis

FOLLOW US ON LINKED IN
linkedin.com/company/chainalysis