CRIME

# 2024 Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth

JANUARY 18, 2024 | BY CHAINALYSIS TEAM

SHARE

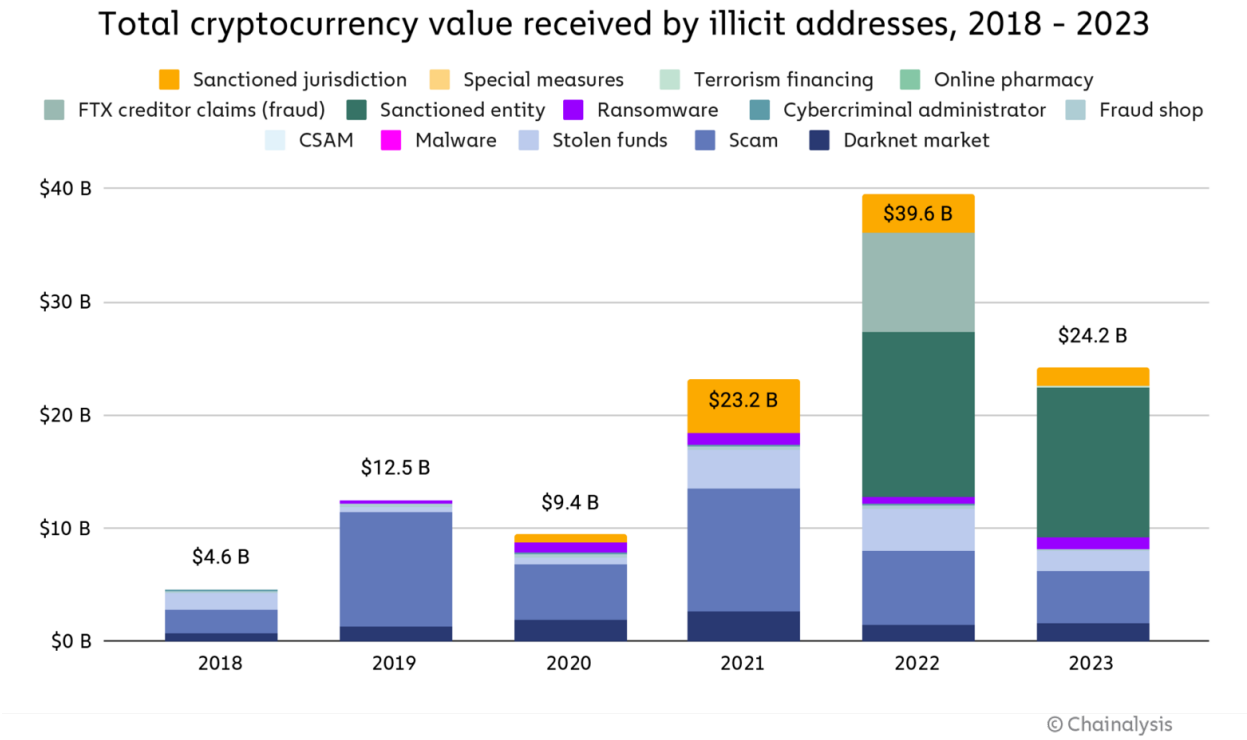
## The Chainalysis 2024 Crypto Crime Report

Coming soon

Reserve your copy

2023 was a year of recovery for cryptocurrency, as the industry rebounded from the scandals, blowups, and price declines of 2022. With crypto assets rebounding and market activity growing over the course of 2023, many believe that crypto winter is ending, and a new growth phase may soon be upon us.

But what did all of that mean for crypto crime? Let's look at the high-level trends.




2023 saw a significant drop in value received by illicit cryptocurrency addresses, to a total of $24.2 billion. As always, we have to caveat by saying that these figures are lower bound estimates based on inflows to the illicit addresses we've identified today. One year from now, these totals will almost certainly be higher, as we identify more illicit addresses and incorporate their historic activity into our estimates. For instance, when we published our Crypto Crime Report last year, we estimated $20.6 billion worth of illicit transaction volume for 2022. One year later, our updated estimate for 2022 is $39.6 billion. Much of that growth came from the identification of previously unknown, highly active addresses hosted by sanctioned services, as well as our addition of transaction volume associated with services in sanctioned jurisdictions to our illicit totals.

Another key reason the new total is so much higher, besides the identification of new illicit addresses: We're now counting the $8.7 billion in creditor claims against FTX in our 2022 figures. In last year's

report, we said that we would hold off on including transaction volumes associated with FTX and other firms that collapsed that year under allegedly fraudulent circumstances in our illicit totals until legal processes played out. Since then, a jury has convicted FTX's former CEO of fraud.

Typically, we only include measurable on-chain activity in our estimates for illicit activity. In the case of FTX, it is impossible to use on-chain data alone to measure the scope of the fraudulent activity, as there's no way to isolate illegitimate movements of user funds. As such, we believe the $8.7 billion in creditor claims against FTX is the best estimate to include. Given the size and impact of the FTX situation, we are treating it as an exception to our usual on-chain methodology. If courts convict in similar, ongoing cases, we plan to include their activity in our illicit transaction data as well in the future.

All other totals exclude revenue from non-crypto native crime, such as conventional drug trafficking in which crypto is used as a means of payment. Such transactions are virtually indistinguishable from licit transactions in on-chain data. Of course, law enforcement with off-chain context can still investigate these flows using Chainalysis solutions. In cases where we're able to confirm such information, we count the transactions as illicit in our data, but there are almost certainly many instances where that isn't the case, and therefore the numbers wouldn't be reflected in our totals.

**$24.2B**
received by illicit addresses

**0.34%**
of total on-chain transaction volume

### Estimates of illicit transaction activity DO include

- ✓ Funds sent to addresses we've identified as illicit
- ✓ Funds stolen in crypto hacks

### Estimates of illicit transaction activity DO NOT include

- ✗ Funds sent to addresses we have not yet identified as illicit. **Why?** Because we don't know that they're illicit yet. But we update our numbers on a rolling basis as we make more identifications.
- ✗ Funds derived from non-crypto native crime, except for cases brought to our attention by customers. **Why?** Because these transactions are impossible to identify as illicit without more information.
- ✗ Funds associated with crypto platforms accused of fraud, absent convictions in court. **Why?** Because only a judge and jury can make that determination.
- ✗ Transaction volume associated with potential market manipulation. **Why?** Because our research heuristics are designed to catch suspected instances of market manipulation based on on-chain behavior, but aren't definitive.
- ✗ Funds associated with crypto money laundering. **Why?** Because our goal here is to calculate total revenue from illicit activity, based on inflows to illicit addresses. We share the total value laundered on-chain in the report's money laundering section, calculated based on the value sent from illicit addresses to off-ramping services. Including money laundering totals here based on outflows would effectively be double counting, and artificially inflate our estimates of on-chain criminal activity.



In addition to the reduction in absolute value of illicit activity, our

estimate for the share of all crypto transaction volume associated with illicit activity also fell, to 0.34% from 0.42% in 2022. [1]

We're also seeing a shift in the types of assets involved in cryptocurrency-based crime.

Through 2021, Bitcoin reigned supreme as the cryptocurrency of

choice among cybercriminals, likely due to its high liquidity. But that's changed over the last two years, with stablecoins now accounting for the majority of all illicit transaction volume. This change also comes alongside recent growth in stablecoins' share of all crypto activity overall, including legitimate activity. However, stablecoin dominance isn't the case for all forms of cryptocurrency-based crime.

Some forms of illicit cryptocurrency activity, such as darknet market sales and ransomware extortion, still take place predominantly in Bitcoin. [2] Others, like scamming and transactions associated with sanctioned entities, have shifted to stablecoins. Those also happen to be the biggest forms of crypto crime by transaction volume, thereby driving the larger trend. Sanctioned entities, as well as those operating in sanctioned jurisdictions or involved with terrorism financing, also have a greater incentive to use stablecoins, as they may face more challenges accessing the U.S. dollar through traditional means, but still want to benefit from the stability it provides. However, stablecoin issuers can freeze funds when they become aware of their

illicit use, as Tether recently did with addresses linked to terrorism and warfare in Israel and Ukraine.

Below, we'll look at three key trends that defined crypto crime in 2023 and will be important to watch moving forward.

## Scamming and Stolen Funds down big

Crypto scamming and hacking revenue both fell significantly in 2023, with total illicit revenue for each down 29.2% and 54.3% respectively.

As we discuss later in our scams section, many crypto scammers have now adopted romance scam tactics, targeting individuals and building relationships with them in order to pitch them on fraudulent investing opportunities, rather than advertising them far and wide, which often makes them more difficult to uncover. Although the FBI has published data showing that reports of crypto investment scams in the U.S. has been increasing year over year through 2022, our on-chain metrics suggest scamming revenues globally have been trending down since 2021. We believe this aligns with the long-standing trend that scamming is most successful when markets are up, exuberance is high, and people feel like they are missing out on an opportunity to get rich quickly. Of course, the impact of romance scams on individual victims is devastating and should not be understated. And while increased reporting – at least in the U.S. – is a good sign, we still believe insights into romance scams in particular suffer from underreporting. We hypothesize that the true damage of scamming is greater than what reporting to the FBI and our on-chain metrics show, but overall, scamming is down, given broader market dynamics.

Crypto hacking, on the other hand, is much more difficult for criminals

to hide, as industry observers can quickly spot the unusual outflows from a given service or protocol when a hack occurs. As we'll discuss later, the decline in stolen funds is driven largely by a sharp dropoff in DeFi hacking. That dropoff could represent the reversal of a disturbing, long-term trend, and may signify that DeFi protocols are improving their security practices. That said, stolen funds metrics are heavily outlier-driven, and one large hack could again shift the trend.

## Ransomware and darknet market activity on the rise

Ransomware and darknet markets, on the other hand, are two of the most prominent forms of crypto crime that saw revenues rise in 2023, in contrast with overall trends. The growth of ransomware revenue is disappointing following the sharp declines we covered last year, and suggests that perhaps ransomware attackers have adjusted to organizations' cybersecurity improvements, a trend we first reported earlier this year.

Similarly, this year's growth in darknet market revenue also comes after a 2022 decline in revenue. That decline was driven largely by the shutdown of Hydra, which was once the world's most dominant market by far, capturing over 90% of all darknet market revenue at its peak. While no single market has yet emerged to take its place, the sector as a whole is rebounding, with total revenue climbing back towards its 2021 highs.

## Transactions with sanctioned entities

## drive the vast majority of illicit activity

Perhaps the most obvious trend that emerges when looking at illicit transaction volume is the prominence of sanctions-related transactions. Sanctioned entities and jurisdictions together accounted for a combined $14.9 billion worth of transaction volume in 2023, which represents 61.5% of all illicit transaction volume we measured on the year. Most of this total is driven by cryptocurrency services that were sanctioned by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), or are located in sanctioned jurisdictions, and can continue to operate because they're in jurisdictions where U.S. sanctions are not enforced.

While those services can and have been used for nefarious purposes, it also means that some of that $14.9 billion in sanctions-related transaction volume includes activity from average crypto users who happen to reside in those jurisdictions. For example, Russia-based exchange Garantex, which was sanctioned by OFAC and OFSI in the U.K. for its facilitation of money laundering on behalf of ransomware attackers and other cybercriminals, was one of the biggest drivers of transaction volume associated with sanctioned entities in 2023. Garantex continues to operate because Russia does not enforce U.S. sanctions. So, does that mean all of Garantex's transaction volume is associated with ransomware and money laundering? No. Nevertheless, exposure to Garantex introduces serious sanctions risk for crypto platforms subject to U.S. or U.K. jurisdiction, which means those platforms must remain ever-more vigilant and screen for exposure to Garantex in order to be compliant.

## More crypto crime insights to come

Stay on the lookout for more research into cryptocurrency-based crime, as we continue to roll out insights on ransomware, hacking, crypto money laundering, and more. You can also click here to get the full 2024 Crypto Crime Report delivered to your inbox as soon as it's published.



**End notes:**

[1] Transaction volume is a measure of all economic activity, a proxy for funds changing hands. We remove peel chains, internal service transactions, change, and any other type of transaction that would not count as an economic transaction between distinct economic actors.

[2] These estimates do not include privacy coins like Monero.

*This material is for informational purposes only, and is not intended to provide legal, tax, financial, investment, regulatory or other professional advice, nor is it to be relied upon as a professional opinion. Recipients should consult their own advisors before making these types of decisions. Chainalysis does not guarantee or warrant the accuracy, completeness, timeliness, suitability or validity of the information herein. Chainalysis has no responsibility or liability for any*

*decision made or any other acts or omissions in connection with Recipient's use of this material.*

CRYPTO CRIME REPORT CYBERCRIME

DARKNET MARKETS RANSOMWARE SANCTIONS

SCAMS