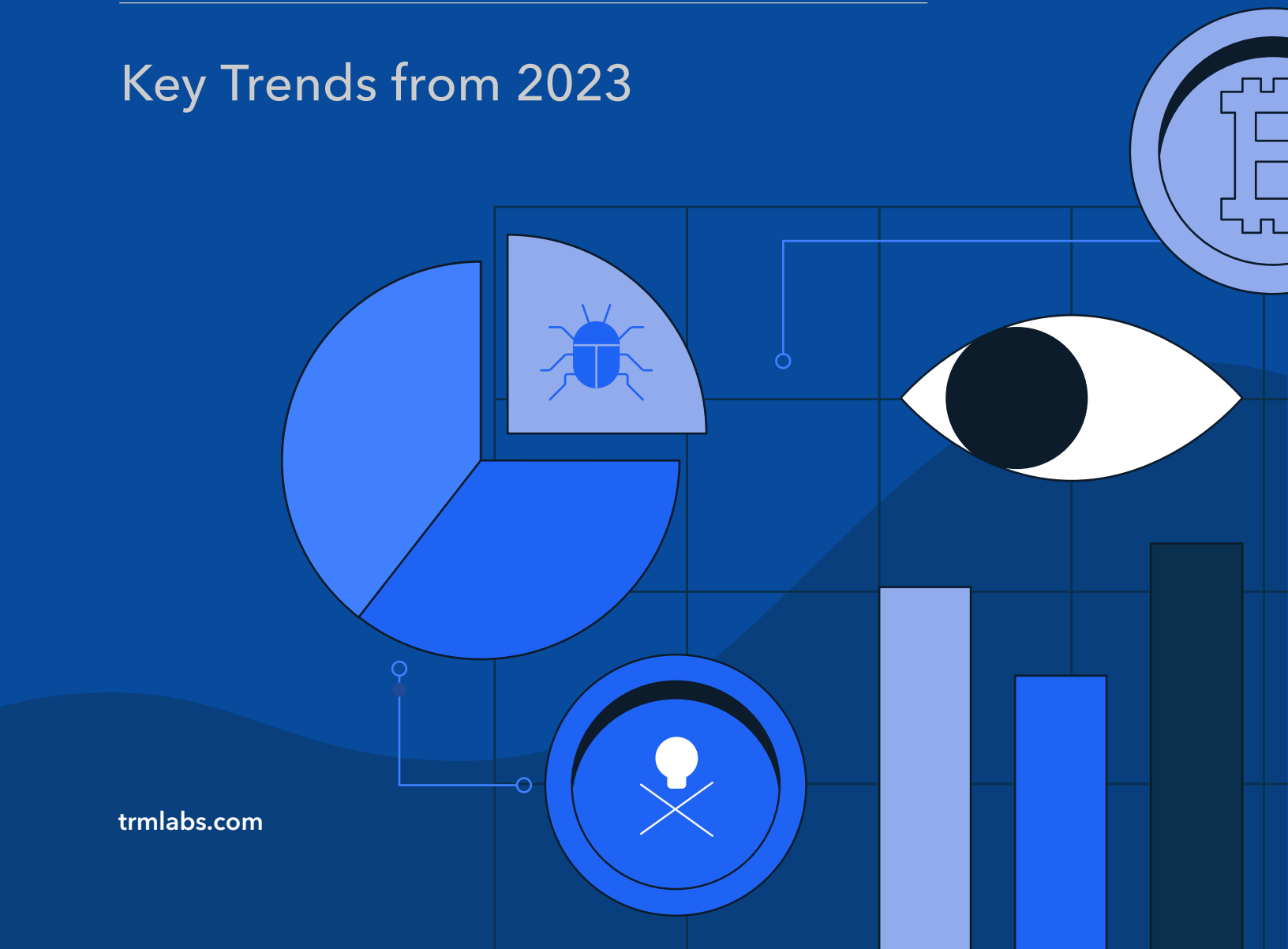
TRM

The Illicit Crypto Economy

Key Trends from 2023



trmlabs.com

Executive Summary

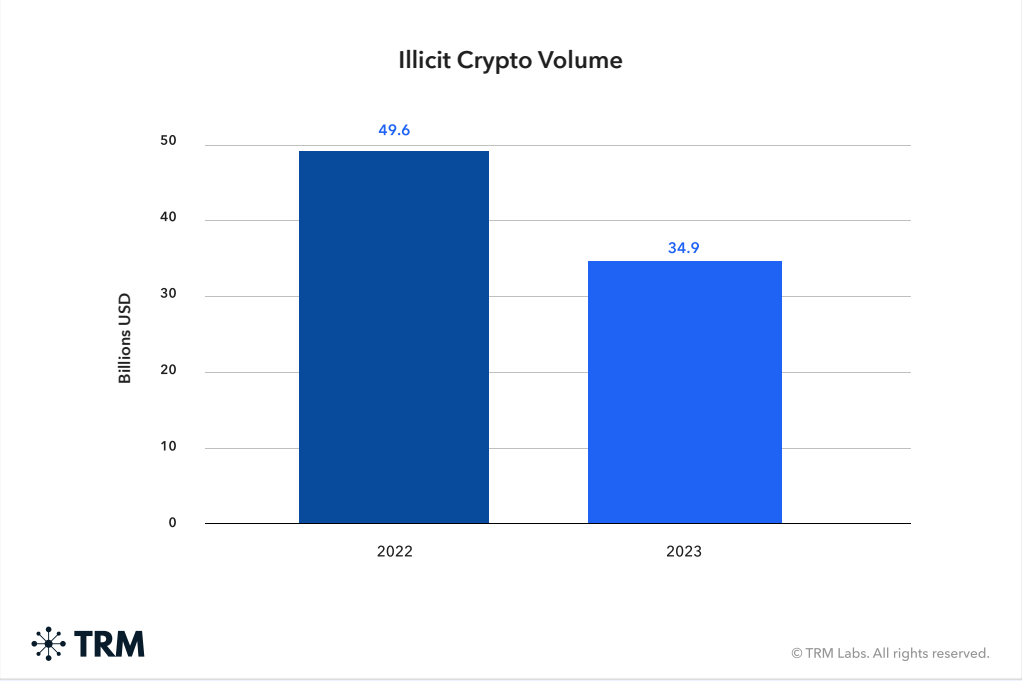
Scams and frauds accounted for approximately a third of all crypto crime in 2023, according to TRM Labs data. Despite the overall proportion of total illicit funds in the crypto ecosystem shrinking by 9% year-on-year, criminals still handled over USD 34 billion worth of cryptocurrencies.

While some crime categories, such as darknet drugs sales, remained buoyant, the volumes of hacked and sanctions-exposed funds posted significant declines; fentanyl sales posted lower growth than in 2022. Those downward trends were accompanied by increased pressure from governments and law enforcement bodies: for example, the US alone tripled the number of crypto crime-linked entities and individuals subject to sanctions.

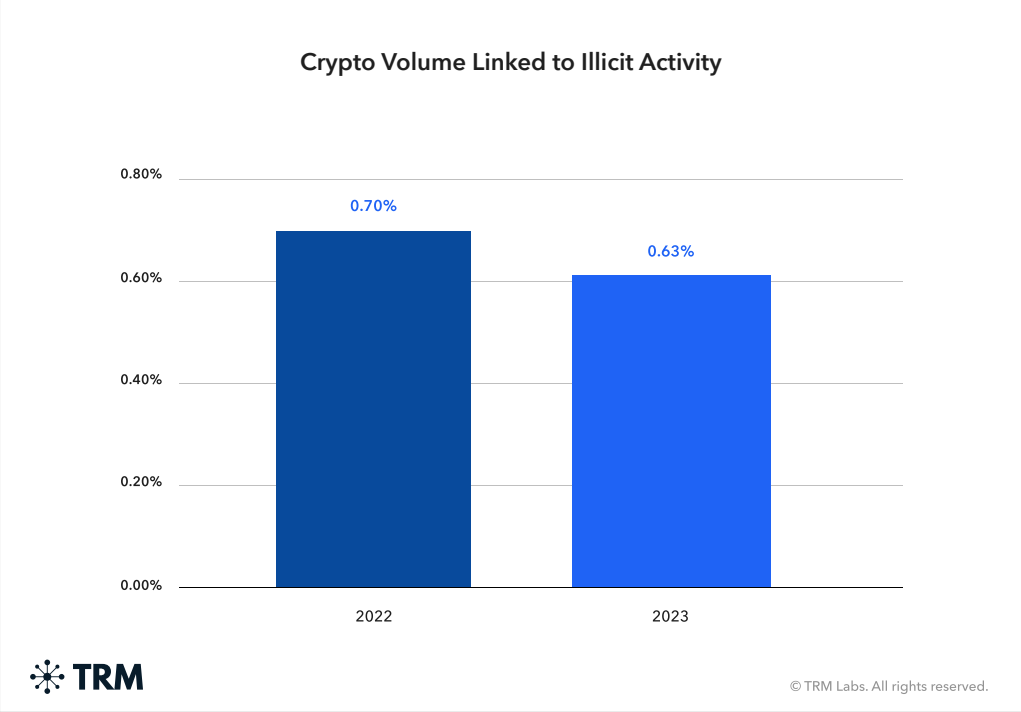
Here are the eight key trends that shaped that the illicit crypto economy in 2023, according to TRM's blockchain intelligence team:

1. Total Illicit Volumes Down

In 2023, the volume of illicit funds within the cryptocurrency ecosystem experienced a significant reduction, decreasing by nearly one-third from USD 49.5 billion in 2022 to USD 34.9 billion. This decline of illicit fund volumes outpaced the 22% reduction seen in the overall cryptocurrency transaction volume during the same period.



The share of illicit funds as a proportion of all crypto value also fell, to 0.63 from 0.70% in 2022. Both figures are higher than existing industry estimates, reflecting that TRM Labs captures more illicit volume, especially linked to sanctions and investment fraud, and captures illicit activity across a greater number of blockchains such as Polygon and BNB Smart Chain (BSC); unverified crowdsourced reports of crypto crime were not included in the data.



2. Sanctioned Volumes Plummeted

The total value of funds sent to sanctioned addresses and entities fell to USD 16.2 billion in 2023 from USD 25.4 billion in 2022.

Sanctions designations rose three-fold, from 11 designation events in 2022 to 33 in 2023. Among the targets were twelve ransomware groups, six high risk exchanges and a cryptocurrency mixing service.

3. Hacks Proceeds Halved

Hack proceeds fell by over 50% to USD 1.8 billion from USD 3.7 billion in 2022. Actors linked to North Korea, responsible for nearly a third of all funds stolen in crypto attacks, made off with 30% less than they did in 2022.

4. Scams and Fraud Declined

Scams and fraud volumes - the total payments into addresses that TRM has connected to fraud or scams - dropped to USD 12.5 billion from USD 13.9 billion in 2022.

5. Fentanyl Growth Rates Dropped 150%

The growth rate of sales by online crypto-denominated vendors specializing in fentanyl and its precursor materials dropped by 150% in volume over 2023 from 2022. Despite the slowdown in growth, however, overall vendor sales volumes still increased by over 97% year-on-year, from USD 16 million to USD 33 million.

6. Illicit Drug Sales Remained Robust

Sales of illicit drugs on darknet marketplaces (DNMs) grew to USD 1.6 billion, from USD 1.3 billion recorded in 2022. Individual vendor shops operating outside DNMs rose to USD 310 million from USD 271 million in 2022.

7. Almost Half of All Illicit Crypto Volume Occurred on the TRON Blockchain

Approximately 45% of crypto illicit volume occurred on the TRON (TRX) blockchain, up from 41% in 2022, followed by Ethereum at 24% and Bitcoin at 18%.

Tether (USDT) was the stablecoin with the largest amount of illicit volume, at USD 19.3 billion. Approximately 1.63% of Tether (USDT) volume was linked by TRM to illicit activity, compared to 0.05% of USDC.

8. Tether Dominated Terrorist Financing

Hamas and other groups announced moratoriums on crypto donations over 2023, likely in response to greater international law enforcement scrutiny. This became particularly acute in the wake of the Hamas attacks on Israel in October 2023, which spurred leading exchanges and cryptocurrency companies to freeze assets linked to Hamas and its sympathizers.

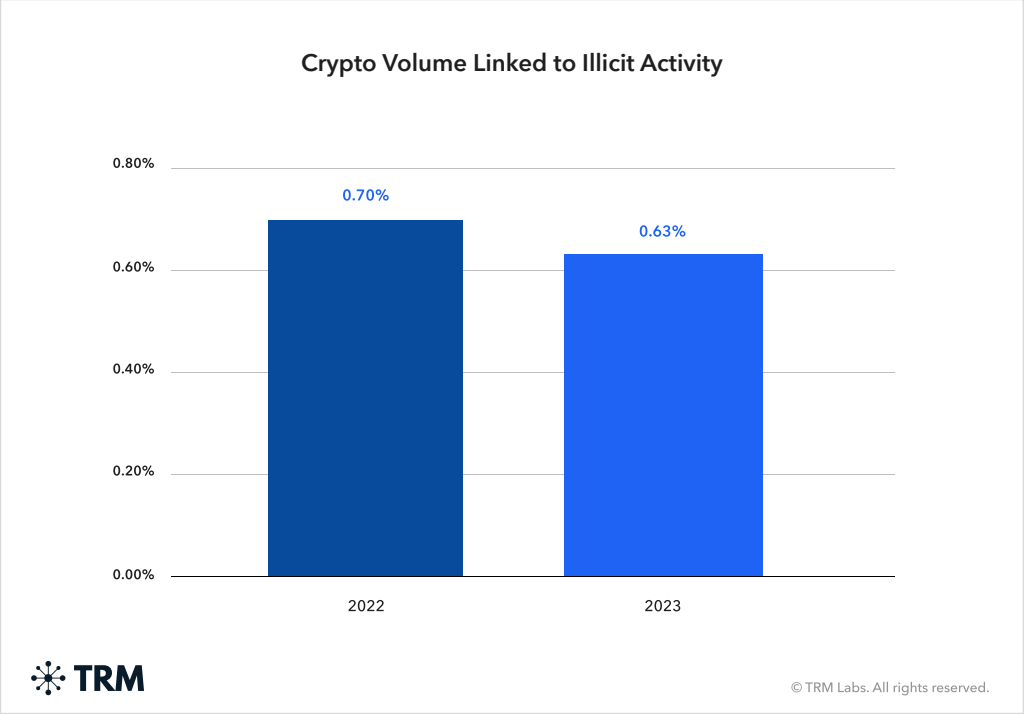
Yet among those terror financing campaigns that continued to accept cryptocurrency, the number of unique TRON addresses that received Tether (USDT) rose by 125%.

The Illicit Crypto Economy: Key Trends from 2023

Introduction

Scams and fraud worth USD 12.5 billion accounted for a third of all illicit funds in the crypto ecosystem in 2023, according to TRM Labs data. As with all the numbers in this report, this figure is likely to change as more information is gathered over time.

The total proportion of illicit funds on the blockchain fell by 9%, from 0.70% in 2022 to 0.63% in 2023. And while still massive, at USD 34.8 billion, the volume of illicit funds was 30% lower than the USD 49.5 billion recorded in 2022.



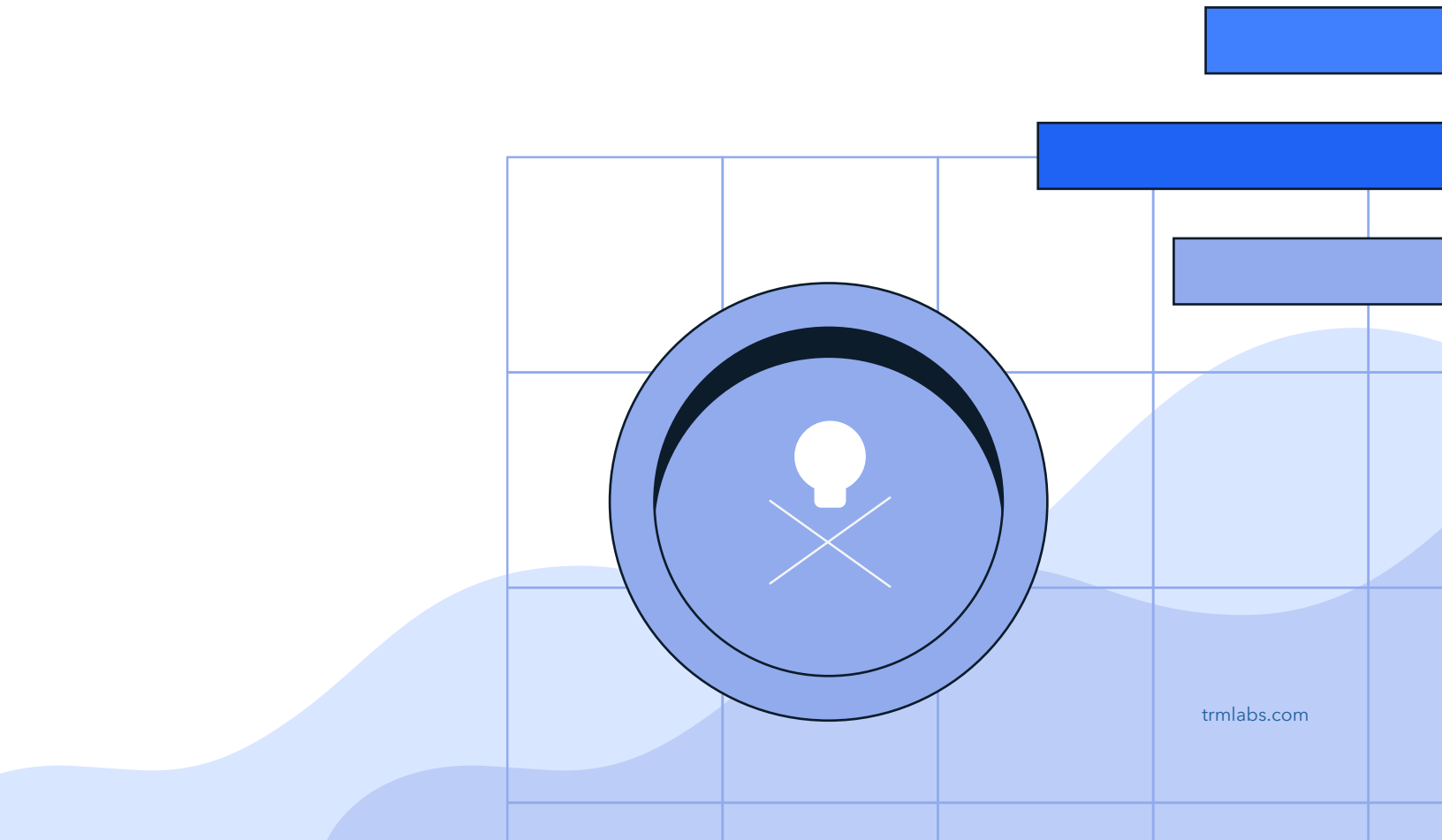
Yet the story is not clear cut, with some of the largest crime typologies experiencing decreases while others remained stable or even grew. The largest driver of the overall decline was a 30% fall in sanctions volume, from USD 25.3 billion in 2022 to USD 16.2 billion in 2023. Hacks fell from USD 3.7 billion in 2022 to USD 1.8 billion in 2023.

Scams and frauds also declined, while another potentially significant reversal was observed in crypto-denominated fentanyl sales: in 2023, growth rates slowed to their lowest levels in two years.

Bucking the downward trend were online drug sales, which retained their buoyancy despite the shutdown of several high profile darknet marketplaces. Even here, however, there appeared to be signs that sanctions and enforcement actions correlated with diminished sales volumes - albeit in the short term.

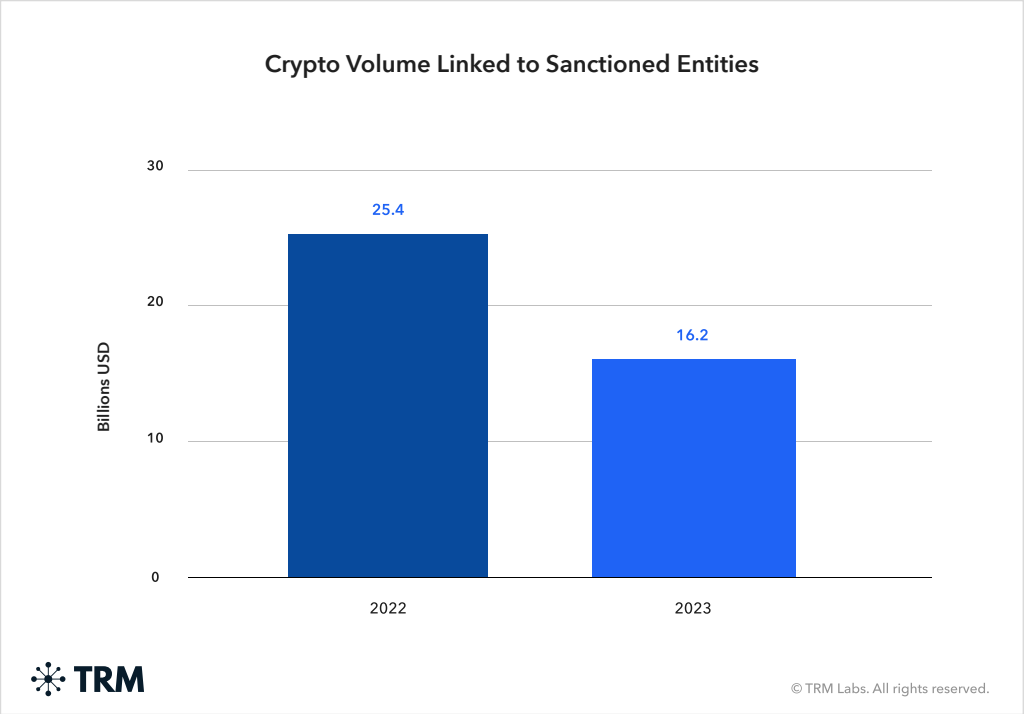
Many factors are likely to have contributed to the dent in crypto crime over 2023, including increased vigilance from businesses, fraud awareness among the general public, and pure chance. Sophisticated criminals may also have become better at avoiding detection. Most notably, three times as many crypto-related entities and individuals were sanctioned by the US government in 2023 than in 2022, in addition to several major crackdowns on crypto-denominated illicit drugs marketplaces by European police.

While no one leading cause can be singled out, the uptick in aggressive law enforcement efforts from authorities in the US, Europe and other significant crypto markets undoubtedly created a more hostile environment for crypto criminals.



Sanctions

Sanctions provided the biggest driver of the fall in illicit crypto funds over 2023. The value of cryptoassets linked to sanctioned entities fell by a third, from USD 25.4 billion in 2022 to USD 16.2 billion in 2023. This suggests that the amount of funds that pass through or interact with sanctioned entities has decreased as more entities are sanctioned.



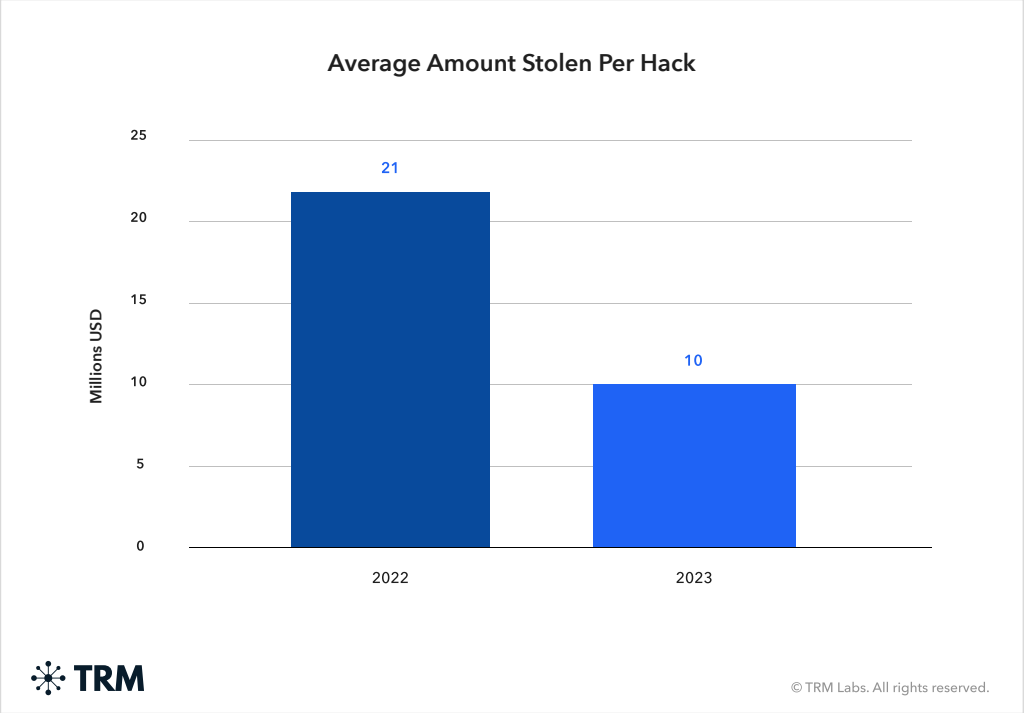
Indeed, last year also saw a three-fold rise in sanctions against crypto-related businesses and individuals. Twelve ransomware groups, six high risk exchanges and a cryptocurrency mixing service featured among the 33 OFAC designations.

Such aggressive tactics may have impacted at least some forms of crypto crime. For example, dips in crypto-denominated fentanyl sales were found to correlate closely with OFAC sanctions and enforcement actions against Chinese precursor manufacturers. North Korea's laundering of stolen funds are also likely to have been affected by actions against its preferred cryptocurrency mixers.

Hacks and Exploits

Last year saw a dramatic reduction in the amount of crypto lost to hacks around the world. While the number of hacks remained roughly unchanged, volumes fell by around 50% to USD 1.8 billion, down from USD 3.7 billion in 2022.

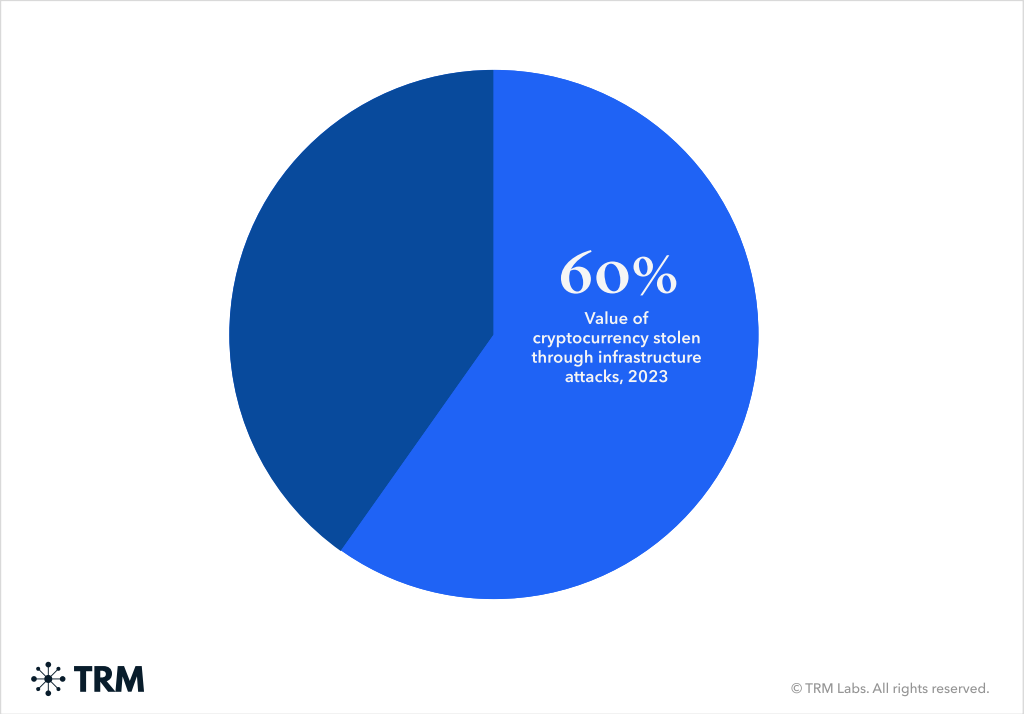
On average, USD 10 million was stolen per attack in 2023, against USD 21 million in 2022. Even North Korea, responsible for almost a third of all crypto attack volumes, stole 30% less than it did in 2022.



There is likely to have been no single, definitive reason for the decrease in attack volumes. Rather, a combination of improved security measures, intensified law enforcement actions, and enhanced coordination among industry participants may have helped to curb the efficacy of hacking attempts.

Infrastructure Attacks Were the Most Lucrative

Nearly 60% of the cryptocurrency stolen in 2023 was stolen through infrastructure attacks such as private key theft or seed phrase compromise, up from about 35% in 2022. Each such attack resulted in an average loss of USD 30 million. The next largest attack typologies - protocol attacks and code exploits - accounted for a fifth of hack volumes.

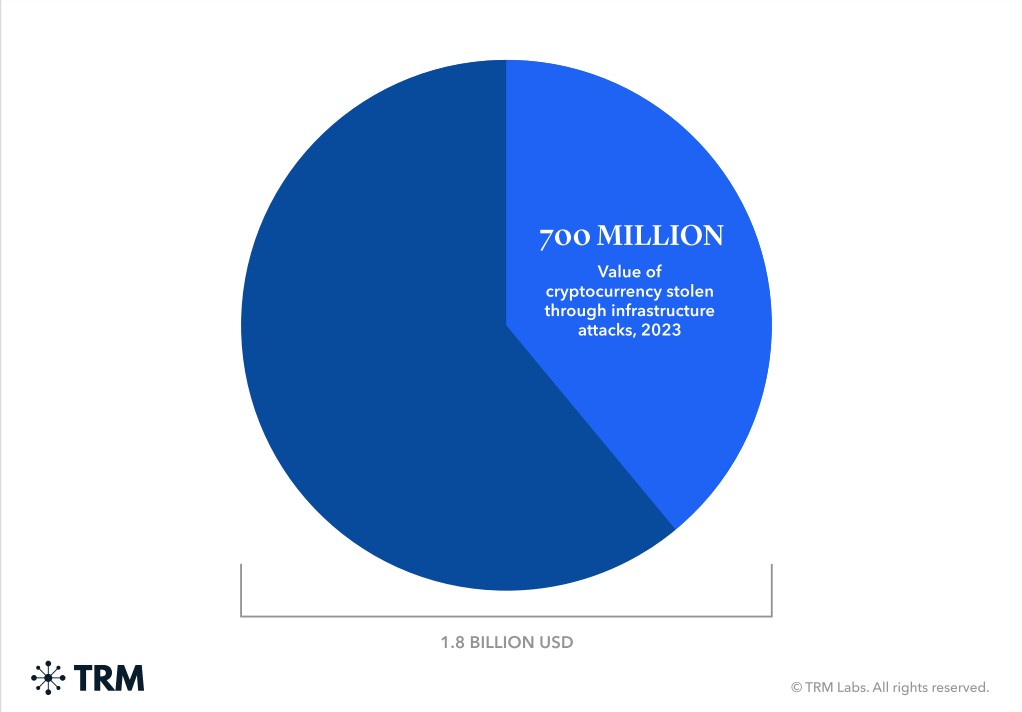


The Top 10 Attacks Netted 70% of All Stolen Funds

The ten largest hacks accounted for almost 70% of all funds stolen in 2023. Several individual hacks exceeded USD 100 million, among them attacks against Euler Finance (March), Multichain (July), Mixin Network (September) and Poloniex (November).

North Korean Hackers Stole 30% Less than in 2022

Hackers tied to North Korea stole approximately USD 700 million in cryptocurrency in 2023 - just over a third of all funds stolen in crypto attacks that year. However, the figure represented a 20% reduction from the USD 825 million embezzled in 2022. Despite the decrease in total volume, hacks perpetrated by North Korea remained on average ten times larger than those not linked to North Korea.



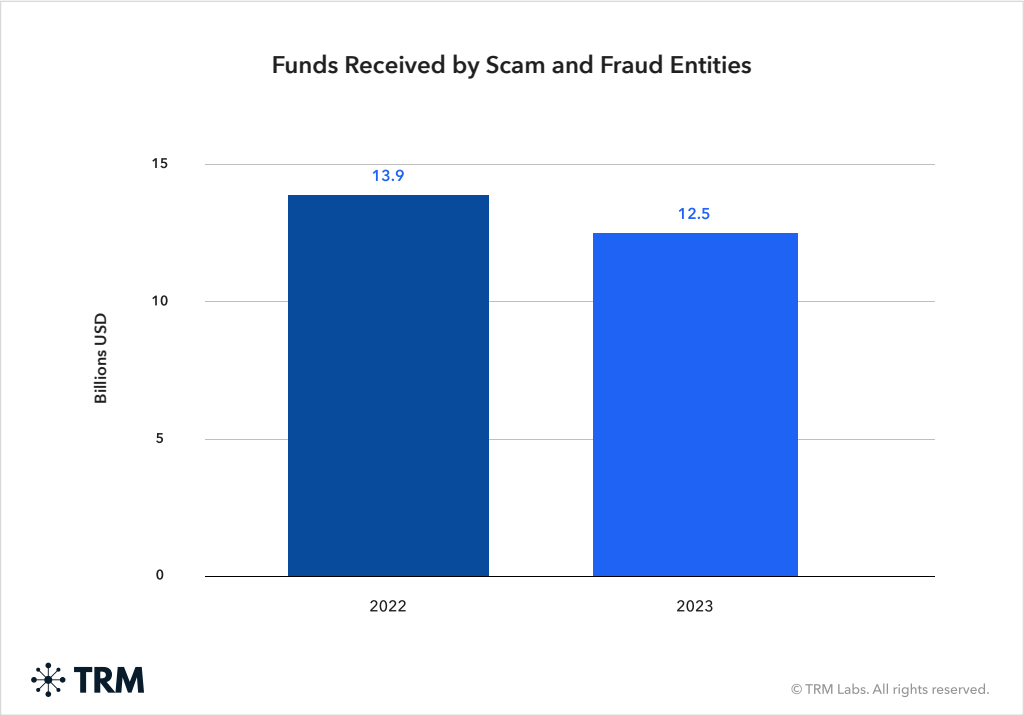
North Korea conducted nearly all its attacks by compromising private keys and seed phrases, which are critical security elements of digital wallets. Hackers transfer the victims' digital assets to wallet addresses controlled by North Korean operatives. They are then swapped mostly for USDT on TRON and converted to hard currency using high-volume OTC brokers.

Over 2023, the North Korea's money laundering methods continued to evolve to evade international law enforcement pressure. As US sanctions and enforcement actions targeted Tornado Cash and ChipMixer - its previous go-to obfuscation platforms - North Korea pivoted to another mixer it had already begun using, the BTC service Sinbad. After Sinbad was itself sanctioned by OFAC in November 2023, North Korea has continued exploring other emerging laundering mechanisms.

Scams and Fraud

According to TRM research, the amount of cryptocurrency sent to addresses linked to scam and fraud schemes decreased by USD 1.5 billion in 2023, falling 11% from USD 13.9 billion in 2022 to 12.5 billion in 2023. Apparent Ponzi and pyramid schemes were the largest subcategory of frauds, receiving around 6.6 billion over the course of the year.

Proceeds from apparent pig butchering, in which criminals use psychological manipulation to defraud victims through fake investment schemes, declined slightly from USD 4.7 billion in 2022 to USD 4.4 billion in 2023.



Illicit Drugs

Most illicit drugs sold for crypto online are bought on darknet markets, known as DNMs. In North America and Western Europe, purchased products are delivered by post, whereas Russian-speaking DNMs dominant in Eastern Europe and the former Soviet Union distribute their products through dead-drops in public places. Drugs are also sold on other platforms, such as individual shops that operate outside of DNMs, whether on the dark or surface web.

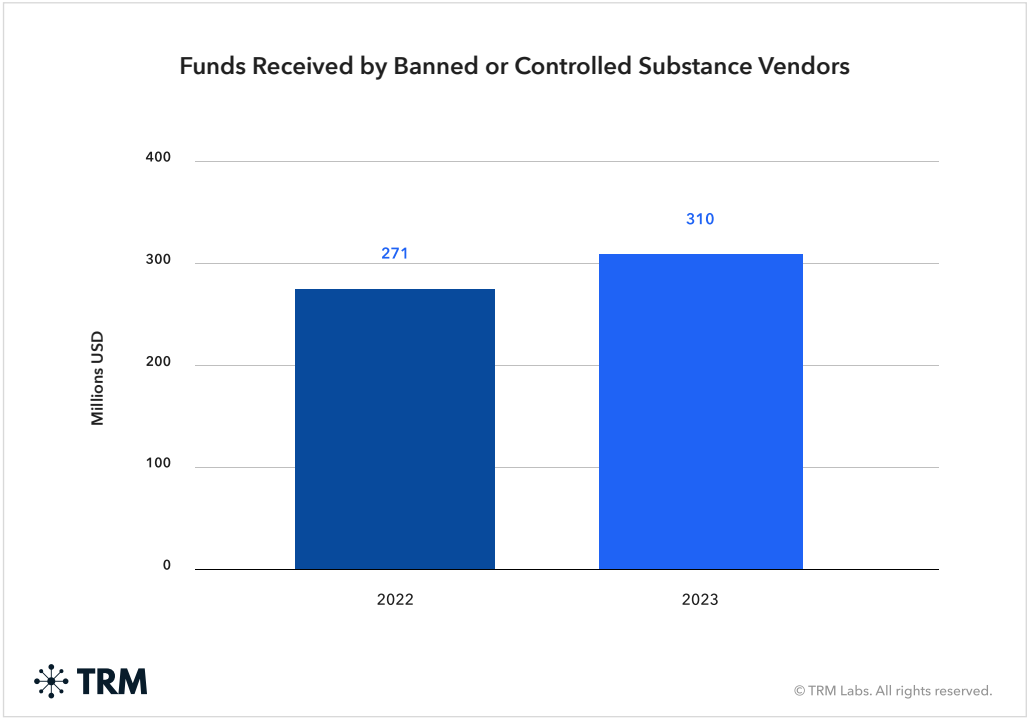
Darknet Markets (DNMs) Remained Buoyant…

Illicit drug sales on the dark web appeared to be unaffected by the general crypto crime downturn. In 2023, DNM volumes grew to USD 1.6 billion, from USD 1.3 billion recorded in 2022.

…As Did Vendors Operating Outside DNMs…

Sales of banned and controlled substances in individual vendor shops monitored by TRM Labs grew 15% to USD 310 million in 2023 from USD 271 million in 2022. These vendors included peer-to-peer (P2P) dealers using encrypted email; communication apps such as Telegram, Wickr and WhatsApp; sites on the dark and surface web; and so-called "autoshops" - automated sales bots operated by vendors on encrypted communication apps.

While Bitcoin remained dominant, the volume of drug sales that used the TRON blockchain more than quadrupled from the year before.



…but Fentanyl Sellers' Sales Growth Halved

Last year also delivered a reversal to a long-term trend in the international fentanyl trade - at least when it comes to the crypto space. The growth rate in crypto-denominated sales by online vendors specializing in fentanyl and its precursor materials dropped by about 150 percentage points in 2023.

Despite the slowdown in growth, total volumes of fentanyl precursor sales tracked by TRM still grew by over 97% over 2023 from USD 16 million to USD 33 million. Moreover, such crypto-denominated sales likely represent a fraction of the total market for fentanyl and fentanyl precursors, most of which continue to be traded using traditional currency. Although Bitcoin comprised the lion's share of online fentanyl sales, the highest growth was recorded by TRX, which saw a nearly ten-fold increase in volume from 2022.

The decrease in the growth rates appeared to correlate with significant sanctions and enforcement events: the US Treasury's Office of Foreign Assets Control (OFAC) sanctioned 135 individuals and entities linked to fentanyl production and distribution across 12 designation events. That followed a steady increase in designation activity since 2018, with five individuals and entities designated in 2019, seven in 2020, 15 in 2021 and 17 in 2022.

Cross-Chain Crime

The distribution of crime across blockchains remained largely steady from 2022. Approximately 45% of crypto illicit volume occurred on the TRON (TRX) blockchain, up from 41% in 2022. Ethereum was the next largest, at 24%, a decline from 32% the previous year. Bitcoin contributed 18% (16% in 2022), followed by Binance Smart Chain (BSC) with 10% (2022: 9%) and Polygon with 4% - a doubling of its 2% figure from 2022.

Generally, TRM has observed a trend of both licit and illicit volumes shifting to open blockchains that have low transaction fees, smart contracts, and popular stablecoins. These factors likely contributed to the shift from Bitcoin to blockchains such as Ethereum and TRON. As new blockchains continue to emerge with these properties, the distribution of illicit volume across chains will likely continue to evolve.*

TRM found USDT to be the stablecoin with the largest amount of illicit volume, at USD 19.3 billion. That is 1.63% of its total volume. By contrast, the other leading international stablecoin, USDC, has only USD 428.9 million in illicit volume, or 0.05% of its total volume.

*Report updated April 1, 2024 to include additional context about the drivers of the distribution of illicit volume across chains.

Terrorist Financing

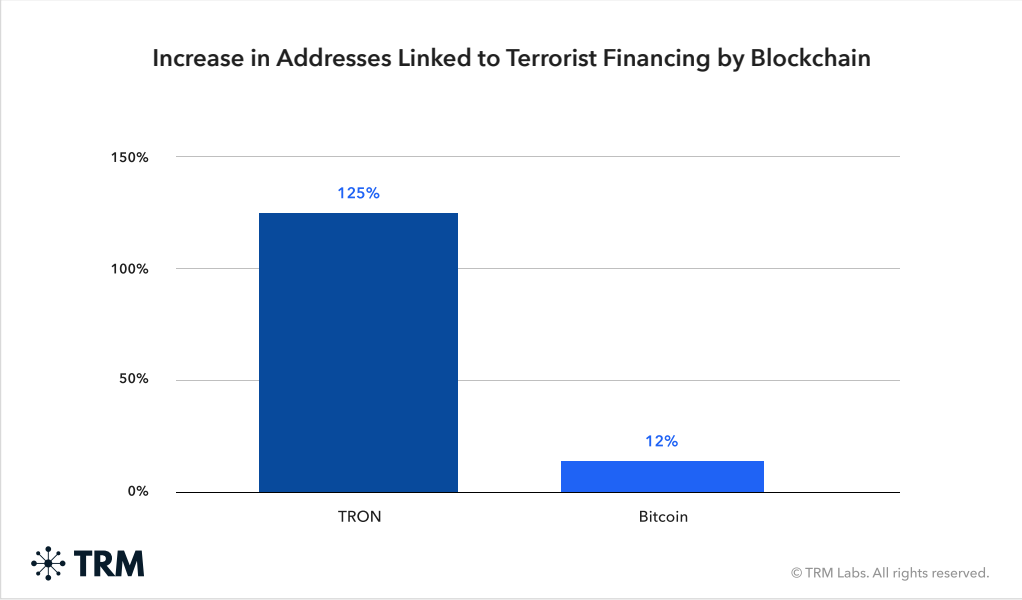
While cash, hawala and even traditional money services remain the default tools for terrorism financing, TRM research found a growing interest in and use of crypto by terrorist groups and their supporters to solicit donations and conduct cross-border payments.

This includes ISIS and its affiliates in multiple countries around the world, as well as Iranian-backed groups like Hamas and Palestinian Islamic Jihad (PIJ), which have received hundreds of thousands of dollars' in cryptocurrency over the past few years. Nevertheless, to date cryptocurrency use (especially as it relates to fundraising campaigns) appears to be primarily confined to small-scale transactions.

Particularly following the Hamas attacks on Israel in October 2023, the use of cryptocurrency by international terrorist groups has taken on renewed urgency among governments, policymakers and researchers. Binance and Tether froze accounts belonging to Hamas and pro-Hamas fundraising campaigns following the October attacks. By that point, Hamas had already announced that it would no longer accept cryptocurrency donations, citing concern for the safety of donors.

Tether Remains the Currency of Choice…

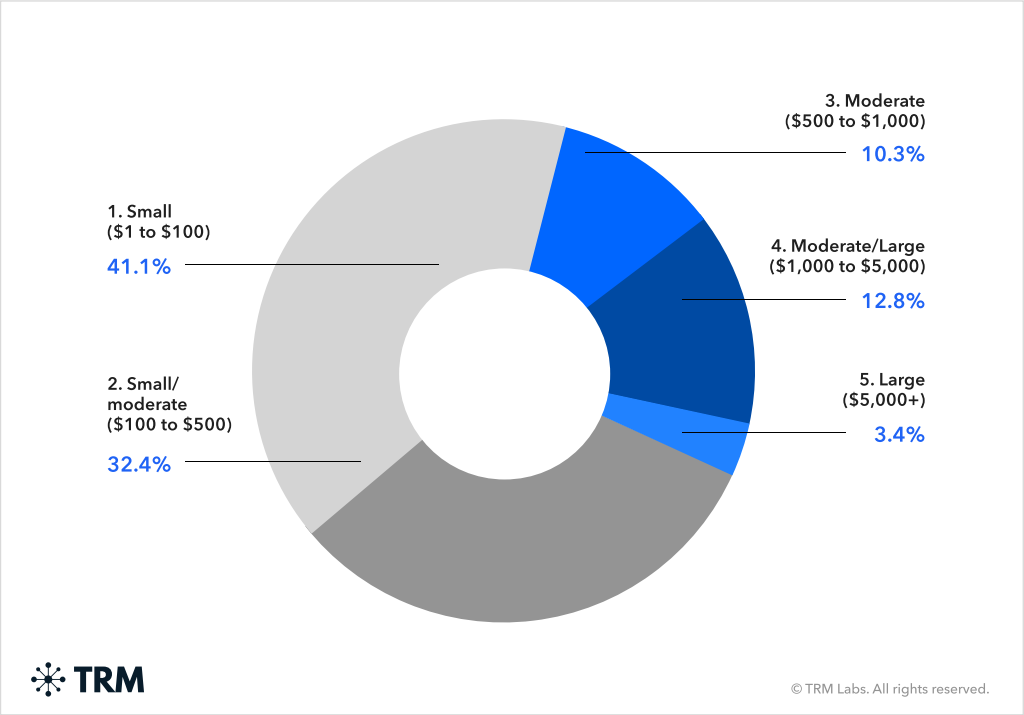
In 2023, Tether (USDT) on the TRON blockchain cemented its position as the currency of choice for use by terrorist financing entities. Among cryptocurrency addresses linked to terror financing campaigns, the year saw a 125% increase in TRON addresses, compared to a 12% increase in Bitcoin addresses.



There are several potential reasons for the apparent preference for Tether on TRON among terrorist financing entities. They include the currency's relatively low gas fees, minimal price fluctuations and a residual - but outdated - perception that it is more difficult to trace.

…With Most Donations Under USD 500

Three-quarters of donations to terrorist fundraising campaigns were under USD 500, with around 40% at USD 100 or less.



Illicit Volume Methodology

Our estimate of total illicit crypto volume is based on the USD value of funds stolen in crypto hacks, combined with the USD value of transfers to blockchain addresses that we have linked to illicit entities such as fraud schemes, sanctioned entities, and darknet marketplaces. We consider our estimate as the minimum, or "floor," for the volume of illicit cryptocurrency.

The following are excluded from our estimate of illicit cryptocurrency volume:

1. Proceeds from crimes initially conducted in fiat currency and subsequently converted into cryptocurrency. These proceeds are typically converted into crypto through on-ramp services and are challenging to identify with on-chain data alone. Accurately assessing the value of these proceeds would require additional data from virtual asset service providers and national financial intelligence units.

2. Transfers to blockchain addresses that have not been linked to illicit activities. We estimate the potential maximum volume of such transfers by analyzing transactions with unattributed addresses that do not appear to represent internal transfers within a single entity.

3. Transfers related to the laundering of illicit crypto proceeds. Our figure of illicit crypto USD volume estimates the crypto revenue generated by illicit entities; it excludes the laundering of these proceeds. In calculating illicit crypto volume as a percentage of total crypto volume, we only consider incoming transaction volume linked to attributed entities, excluding transfers that appear to be internal to entities such as peeling chains and certain swaps on decentralized exchanges.

Conclusion

The reductions observed in many crypto crime categories over 2023 was welcome news for those working to make the financial system safer for the billions of people who use cryptocurrency. Significantly, the decline in illicit fund volumes surpassed the shrinkage of total value in the crypto ecosystem during the bear market.

However, while the share of illicit funds as a proportion of all crypto value fell over 2023, TRM found it to be substantially higher than existing industry estimates. Looking ahead, with the prices of Bitcoin and other cryptocurrencies racing to reach and possibly surpass previous peaks, criminals may find greater incentives to take advantage of the re-energised marketplace. Meanwhile, increasing geopolitical tensions in the Middle East, Asia and the former Soviet Union are likely to embolden hackers and other threat actors.

Against this background, vigilance and cooperation among crypto businesses, blockchain analytics companies, governments and international bodies is more essential than ever to understanding and combating crypto crime.