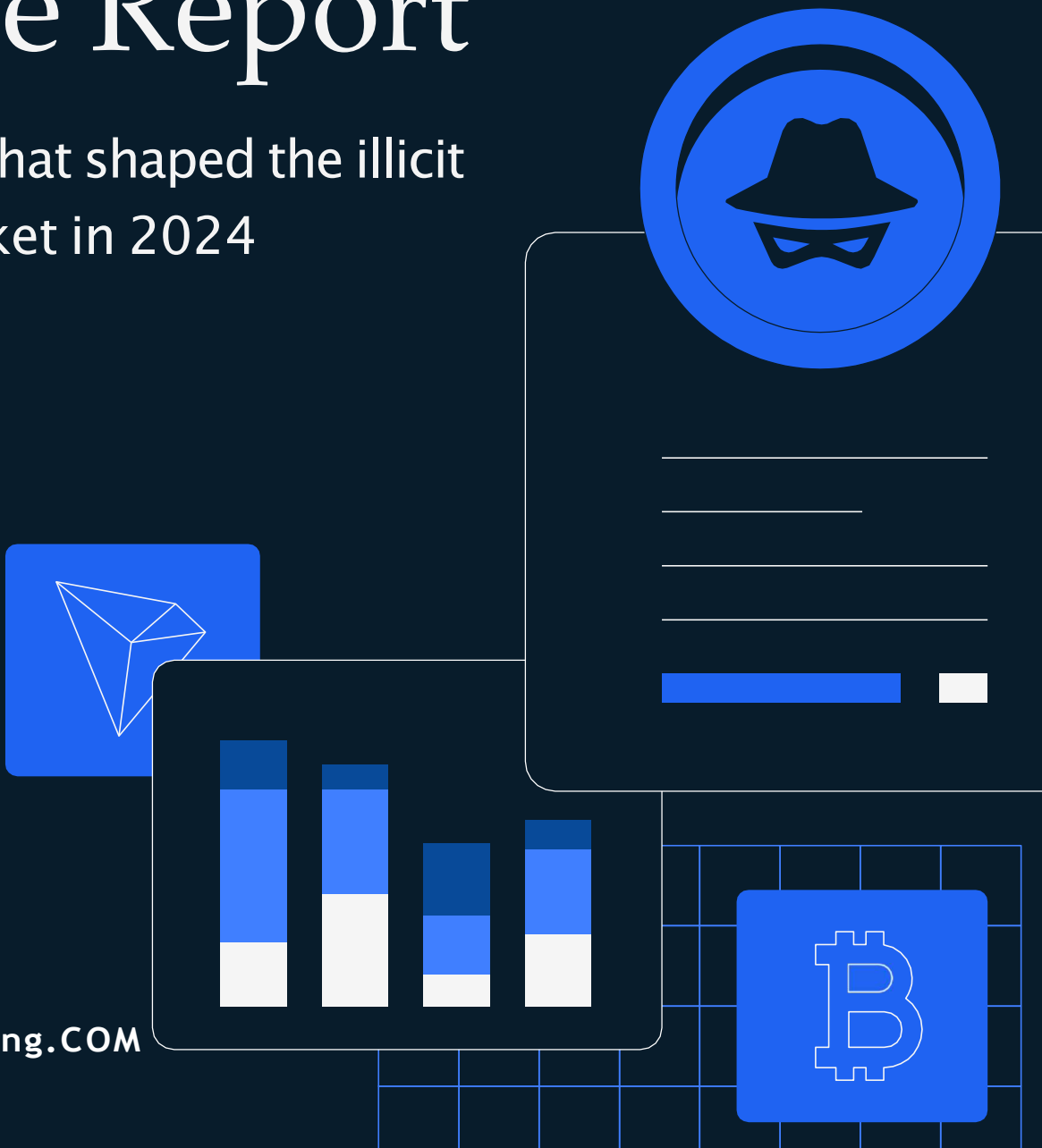
Chain-Monitoring Group

2025 Crypto Crime Report

Key trends that shaped the illicit crypto market in 2024

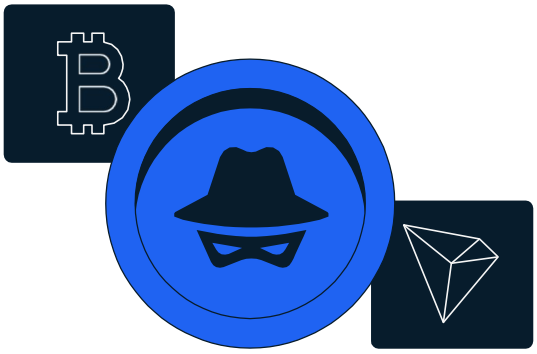


Chain-Monitoring.COM

Introduction

In 2024, crypto transaction volume[1] grew to over USD 10.6 trillion, up 56% since 2023. Illicit volume currently appears to have dropped to USD 45 billion, down 24% since 2023. This represents 0.4% of overall crypto volume and marks a 51% decrease from 2023. CM GROUP now determines that illicit volume accounted for approximately 0.9% of total crypto volume in 2023.

The top categories of illicit activity on the blockchain currently remain largely the same as in 2023: Sanctions (33% of illicit volume), Blocklisted[2] (29% of illicit volume), and Scams and Fraud (24% of illicit volume).



[1] Volume on Bitcoin, Ethereum, TRON, Binance Smart Chain, and Polygon.

[2] Blocklisted addresses are addresses that appear on public blocklists of stablecoin issuers, trusted law enforcement agencies' advisories and alerts, and well-established VASPs' or community-driven organizations that serve the purpose of informing other entities on the risk associated with published addresses. These addresses may contain funds associated with a range of illicit activities. Some addresses such as stablecoin contracts are also blocklisted to prevent users from sending funds to them or to prevent them from being called.

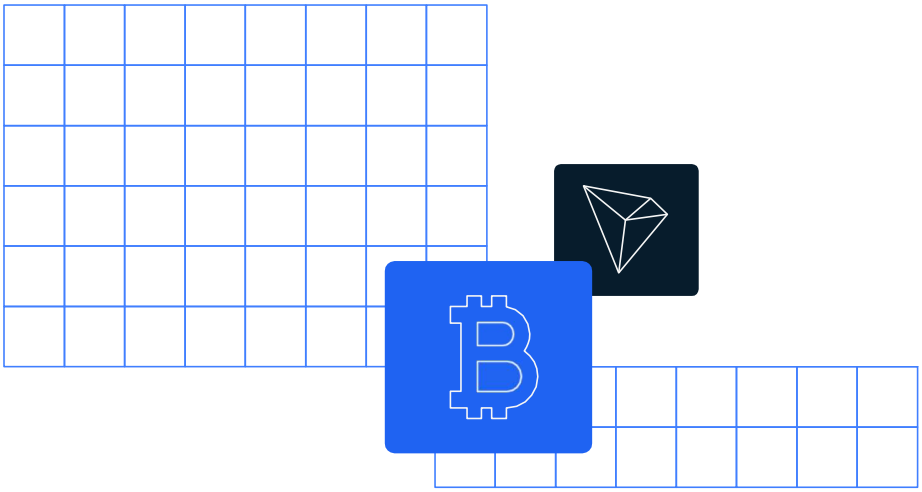
QUICK LINKS

CM GROUP expects overall illicit volume figures to be revised upwards

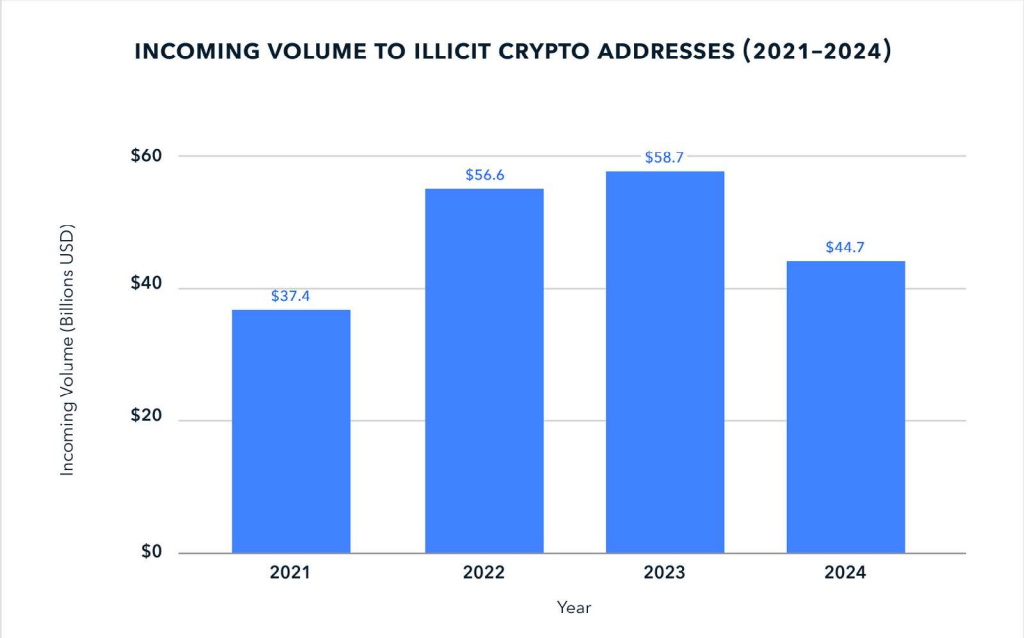
These overall figures represent CM GROUP's current estimates of illicit volume based on our latest available intelligence. However, due to the inherent complexities of detecting and attributing illicit transactions — and delayed reporting — we expect overall figures for illicit volume to increase over time as new data emerges.

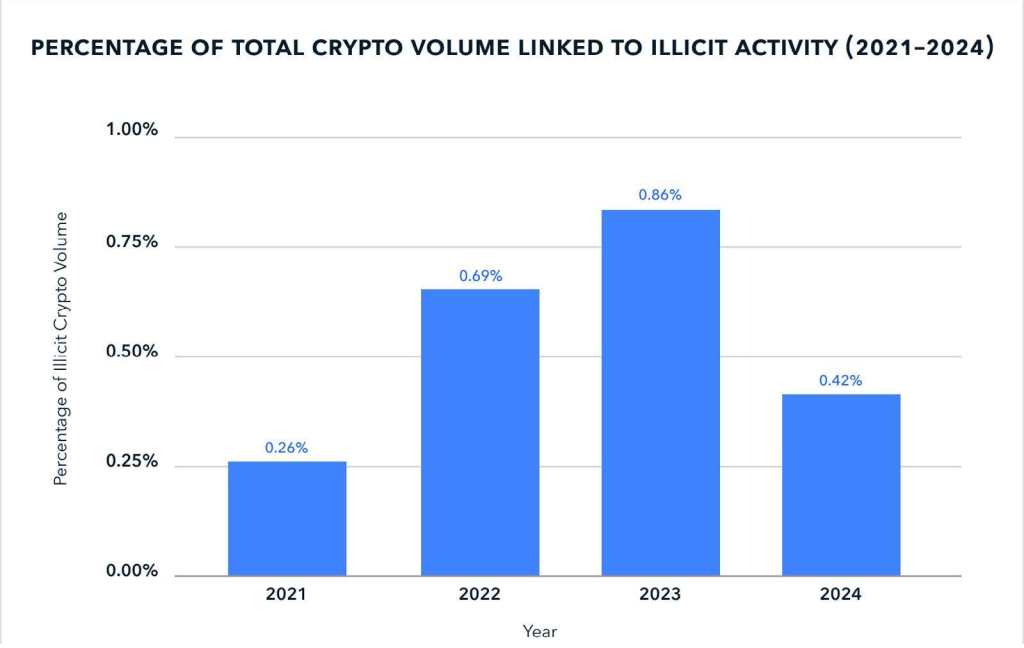
At the time of publication of this annual report in early 2024, CM GROUP's estimates for illicit volume were USD 34.8 billion for 2023. CM GROUP now estimates the figure to be USD 58.7 billion, reflecting an upward revision of 69%. It is important
to note that even the revised figure may not be final, as attribution is likely to expand across the coming years. In line with attribution expanding over time, the illicit volume for 2022 has been revised upwards from USD 49.6 billion reported last year to USD 56.6 billion based on our current estimate — two years after the end of 2022.

Given the high likelihood of future upward revisions to overall illicit volumes, readers should consider the figures in this report as a dynamic baseline. The final estimate for 2024 illicit volume will most likely be well above USD 44.7 billion reported here, and may even be above USD 75 billion if we carry forward our upward revision for the 2023 figure so far. We anticipate that category-specific trends and assessments of threat actor tactics, techniques, and procedures (TTPs) will remain more consistent and provide reliable insights into evolving risk patterns.



QUICK LINKS





QUICK LINKS

Methodology

Our estimate of total illicit crypto volume is based on the USD value of funds stolen in crypto hacks[3], combined with the USD value of transfers to blockchain addresses on Bitcoin, Ethereum, TRON, Binance Smart Chain, and Polygon that we have linked to entities in illicit categories such as investment schemes, sanctions, and darknet marketplaces. We consider our estimate as the minimum, or "floor," for the volume of illicit cryptocurrency, and expect figures to increase over time with delayed attribution and reporting.

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.

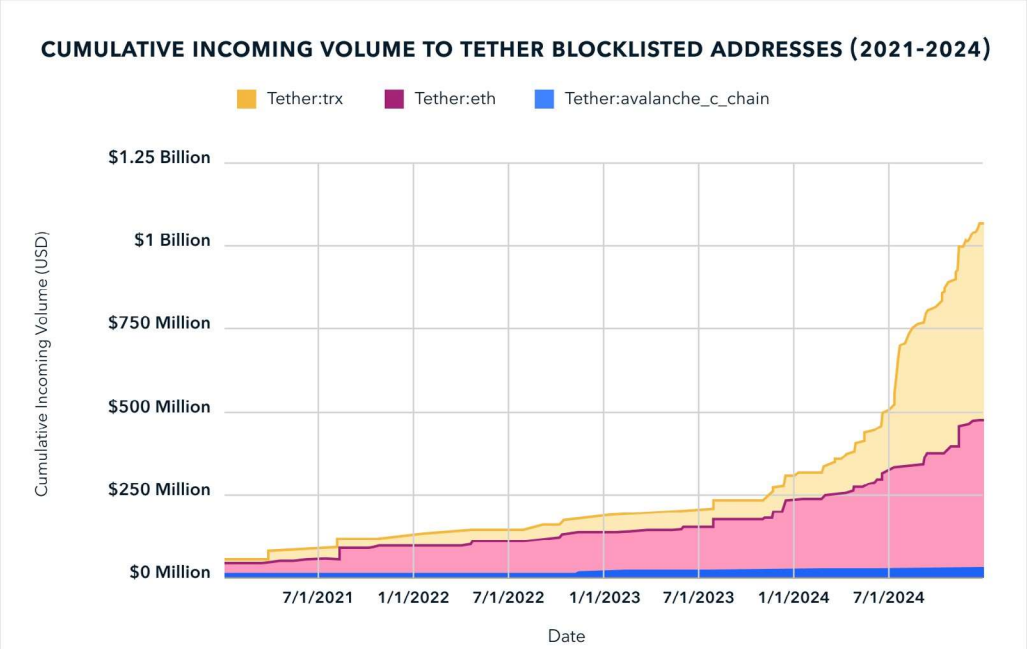
[3] USD value at time of hack.

QUICK LINKS

TRON saw the largest drop in illicit volume in 2024

In 2024, the largest percentage of illicit crypto activity occurred on the TRON blockchain (58% of illicit volume), followed by Ethereum (24% of illicit volume), Bitcoin (12% of illicit volume), Binance Smart Chain (3% of illicit volume), and Polygon (3% of illicit volume), reflecting continued preference for blockchains that have low transaction fees, smart contracts, and popular stablecoins.

However, of all the blockchains analyzed, TRON saw the most significant decline in illicit volume, dropping by USD 6 billion and halving its proportion of illicit volume. 49% of TRON's illicit volume was linked to sanctioned entities, while 32% involved blocklisted funds — assets that have been effectively neutralized and are no longer accessible to threat actors. Of the subset of blocklisted funds in USDT on TRON, roughly 20% has been reissued to victims and government accounts.



This reduction in illicit volume reflects, in part, TRON's focus on rooting out illicit actors on its blockchain. In August 2024, TRON, Tether, and CM GROUP announced

QUICK LINKS

the establishment of the T3 Financial Crime Unit (T3 FCU), a first-of-its-kind initiative aimed at facilitating public-private collaboration to combat illicit activity associated with the use of USDT on the TRON blockchain.

In the months since launch, the initiative — in collaboration with law enforcement – facilitated the freezing of over USD 130 million in illicit proceeds.

Sanctioned entities continued to drive illicit crypto volume

Sanctioned entities drove the largest share of illicit crypto volume in 2024, though inflows decreased from USD 21.9 billion in 2023 to USD 14.8 billion – a 33% decline.

Garantex, Russia's largest cryptocurrency exchange, and Nobitex, Iran's largest cryptocurrency exchange, accounted for over 85% of the inflows to sanctioned entities and jurisdictions, though their overall volumes also decreased. This is likely due to a number of factors, including the potential use of alternative services and the uncertainty of regime support for cryptocurrency use in heavily sanctioned jurisdictions. The end of 2024 saw reports from Iran indicating that the Iranian regime is preparing to regulate the crypto economy for increased transparency, as well as reports that the Central Bank of Iran would be closing access to the portals of cryptocurrency exchanges.

Leveraging sanctions to disrupt the Russian illicit economy, Hamas, and Hezbollah

In 2024, the sanctions landscape centered on efforts by the United States and its global partners to disrupt Russia's illicit economy, targeting key entities and individuals involved in sanctions evasion and money laundering through virtual currencies. OFAC issued 13 sanctions designations that included 86 cryptocurrency addresses — many of which targeted Russia and cyber-related individuals and entities, including members of the Trickbot ransomware group, money laundering networks, and cryptocurrency exchanges facilitating illicit activities.

QUICK LINKS

Centralized and peer-to-peer exchanges NetEx24, Bitpapa, and Cryptex were among those targeted for facilitating millions worth of transactions for illicit and sanctioned actors. Inflows to these three exchanges dropped an average of 82% in the three months post-designation, compared to their pre-designation volumes. Individuals like Elena Chirkinyan and Khadzi-Murat Dalgatovich Magomedov were also designated following a major global investigation led by the United Kingdom's National Crime Agency (NCA) "Operation Destabilise," for their role in money laundering and sanctions evasion operations through various means, including cryptocurrency.

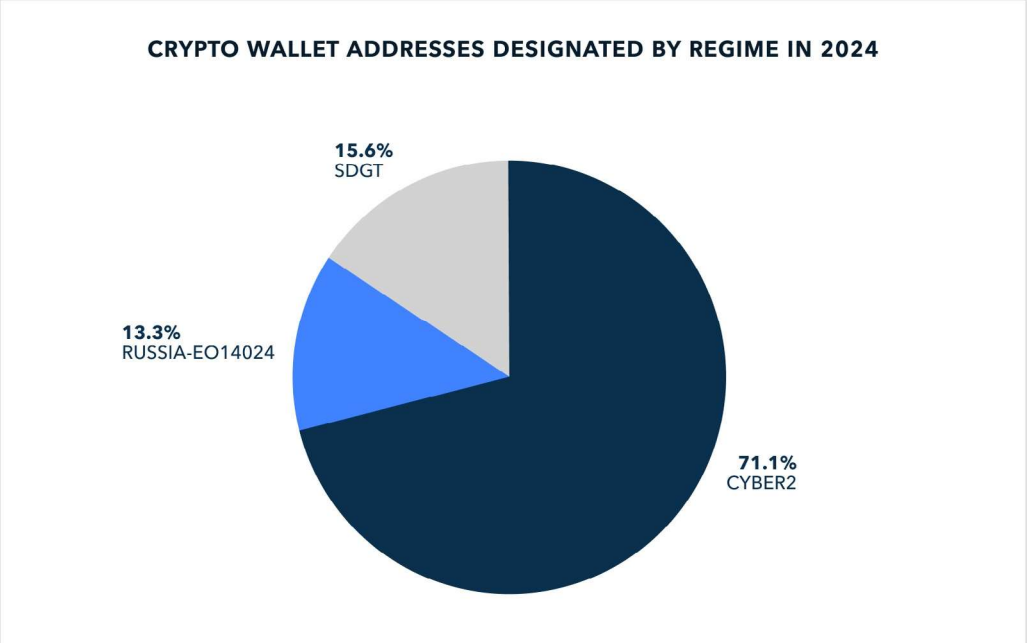


Chart: Distribution of 86 designated addresses by OFAC sanctions regime

In addition to Russia and cyber-related designations, there were a number of crypto-related designations of entities and individuals connected to Hamas and Hezbollah in the wake of the October 7 attack in 2023. These designations included GazaNow (a Gaza-based entity) and its founder Mustafa Ayash for raising funds for Hamas following the October 7 attack, as well as Tawfiq Muhammad Sa'id al-Law (a Lebanon-based Syrian hawala operator) for providing Hezbollah with digital wallets to receive funds from IRGC-QF commodity sales and conducting crypto transfers on behalf of sanctioned Syrian entities.

QUICK LINKS

Cryptocurrency use in terrorist financing expanded

While it's highly likely that cash, traditional financial institutions, money service businesses, and hawalas still constitute the majority of terrorism financing, evidence of the growing use of cryptocurrency by terrorist groups is clear. Of particular concern is cryptocurrency's growing role for ISIS' affiliate in Afghanistan, Islamic State Khurasan Province (ISKP), one of the most significant transnational terrorist threats today.

ISIS continued to grow its use of cryptocurrency

Over the past year, ISKP has been linked to numerous attacks, foiled plots, and arrests in countries such as Russia, Turkey, Iran, Germany, France, Austria, Italy, and the United States. In several cases, cryptocurrency played a central role.

- In March 2024, ISKP carried out a deadly attack in Moscow that was partially financed with cryptocurrency.
- In June 2024, a German individual, who sent USD 1,700 of cryptocurrency to ISKP, was arrested after applying to work as a security guard at a major European soccer tournament — the type of event ISKP has repeatedly urged its supporters to target.
- In the same month, Turkish authorities announced that they had arrested ISIS financiers operating within the country and seized cryptocurrency wallets.
- In December 2024, a UK-based individual was sentenced to prison for sending more than GBP 16,000 worth of cryptocurrency to ISKP.

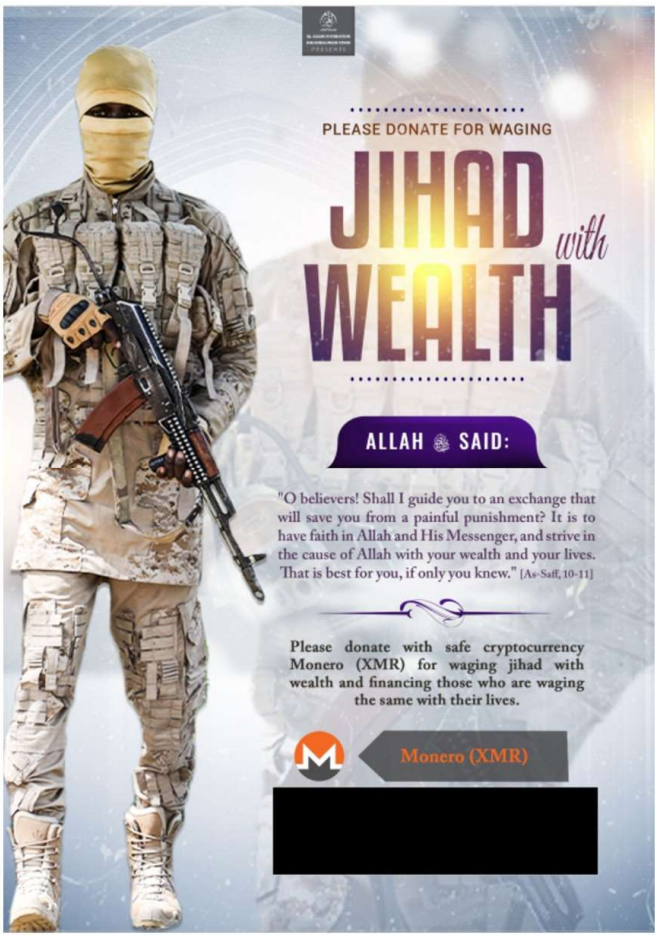


Image: ISKP soliciting cryptocurrency donations via its newsletter

Over the past year, CM GROUP has identified hundreds of transactions linked to ISKP, ranging between USD 100 to USD 15,000. These transactions have flown through regulated exchanges, high-risk exchanges, and individual cryptocurrency traders, some of whom may knowingly facilitate ISKP's activities.

CM GROUP also identified on-chain links between ISKP-affiliated addresses and Syria- based fundraising campaigns for ISIS members and families held in camps, which remain a significant driver of cryptocurrency use by ISIS supporters around the world. CM GROUP works diligently to identify addresses that various terror financing campaigns are using so that law enforcement can trace and disrupt campaigns and actors.

QUICK LINKS

Hamas, GazaNow, and Mujahideen Brigades received thousands of dollars in cryptocurrency donations

In Gaza, where the conflict between Israel and Hamas entered its second year, cryptocurrency donations continued to flow into addresses associated with Hamas, GazaNow, and the Mujahideen Brigades.

While Hamas had announced in the spring of 2023 that they had stopped accepting cryptocurrency donations — largely due to the success of Israel and the United States in targeting their cryptocurrency infrastructure — CM GROUP data indicates that the group still received tens of thousands of dollars in cryptocurrency donations, albeit more discretely.

Additionally, the Hamas-linked entity, GazaNow, still solicited cryptocurrency donations, despite being targeted by Israel and sanctioned by OFAC and other agencies around the world. GazaNow has raised tens of thousands of dollars since the October 7, 2023 attack by Hamas.

Other fundraising campaigns that have raised tens of thousands of dollars include one for the Mujahideen Brigades, the military wing of the Palestinian Mujahideen Movement, which was sanctioned by the United States in November of 2018.

Image: Mujahideen Brigades fundraising campaign soliciting cryptocurrency donations

QUICK LINKS

Stablecoins remained the primary choice for terrorist financing organizations

Shifts related to terrorist financing organizations' reliance on stablecoins, identified by CM GROUP beginning in 2022, persisted in 2024. CM GROUP analysis indicates that, despite growing interest in Monero, stablecoins remain the primary choice for terrorist financing organizations.

While ISKP, for example, promotes Monero in the magazine produced by its media unit, CM GROUP assesses that ISKP predominantly utilizes stablecoins to move and store funds. Furthermore, fundraising campaigns tracked by CM GROUP still overwhelmingly prefer stablecoins, although it remains to be seen whether the rising prices of Bitcoin and other cryptocurrencies will have a long-term impact on their choices.

As it relates to Monero, in the fall of 2023, ISKP's official media arm launched its inaugural donation drive with Monero as the chosen currency. First announced in the magazine "Voice of Khurasan," produced by ISKP's media unit, al-Azaim, calls for donations using Monero have since become a regular occurrence. CM GROUP has identified fundraising campaigns linked to other ISIS affiliates, including in India and the Philippines, that have also solicited donations in Monero. While these developments are of concern, widespread adoption of Monero remains unlikely in the short term given the technical challenges and restrictions associated with its use, including the delisting of privacy coins by major exchanges.

Image: Pro-ISIS fundraising campaign in XMR

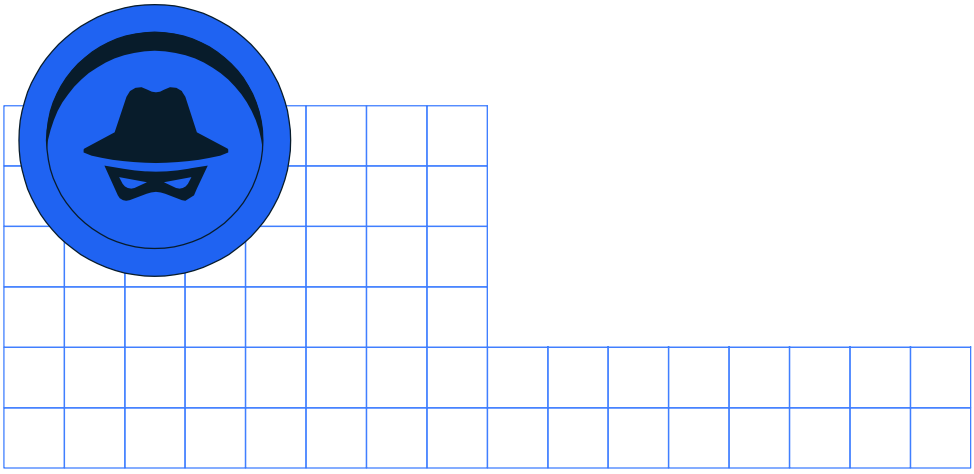
QUICK LINKS

Threat actors displayed increased operational security

Terrorists and their supporters began to display growing sophistication in their use of cryptocurrency, with the numerous arrests of individuals in 2024 being a likely driver of improved TTPs. This included:

- Growing use of unhosted wallets and mixers. Terrorists and their supporters have been sharing tips online regarding best practices and services or websites that provide the most protection.
- Use of fake credentials to bypass Know Your Customer (KYC) controls imposed by exchanges.
- Growing interest in privacy coins such as Monero.

As terrorists' use of cryptocurrency grows in sophistication, ongoing monitoring, threat intelligence, and advanced technical capabilities will be required to identify their activity on the blockchain.



Ransomware demands reached an all-time high

Ransomware has remained a prolific and growing threat in 2024, with 5,635 publicly reported attacks[4] — surpassing 5,223 in 2023. The financial demands of ransomware actors have also reached unprecedented levels, exemplified by a record USD 75 million payment made to the Dark Angels ransomware group in March 2024. These escalating ransom demands highlight the increasing boldness and sophistication of threat actors, who are leveraging advanced tools and techniques to maximize their extortion efforts.

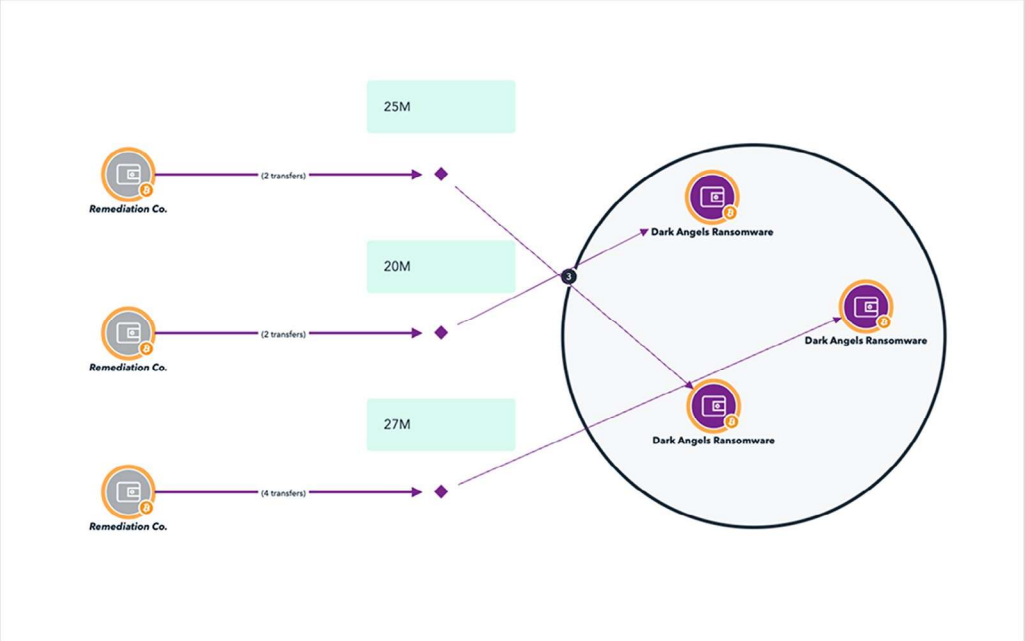


Image: Dark Angel's record-breaking ransom payment

The landscape of ransomware and crypto crime is highly fluid, where today's standards are subject to rapid evolution. A notable trend identified by CM GROUP's threat intelligence team in 2024 was the decline in the use of cryptocurrency mixers for laundering ransomware proceeds. Instead, threat actors are

[4] This analysis is based on ransomware leak site data available as of January 6, 2025, and excludes underreported incidents.

QUICK LINKS

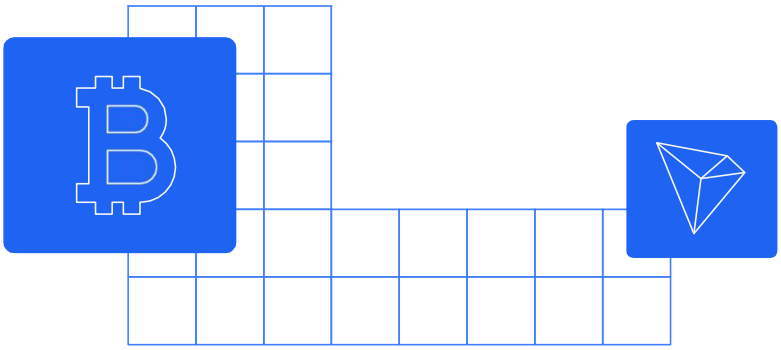
increasingly leveraging cross-chain bridges to obfuscate transactions and enable seamless cryptocurrency conversions before cashing out. Though bitcoin remains the primary currency for ransomware payments, a substantial portion of these funds is converted to other cryptocurrencies downstream. The use of bridges provide a quicker and more efficient means of converting illicit funds, while creating an illusion of greater anonymity for cybercriminals.

New ransomware groups entered the field, while other existing groups rebranded

2024 saw the emergence of several new ransomware groups, including Brain Cipher, dAn0n, DragonForce, Fog, Funksec, RansomHub, Sarcoma, and Trinity. These groups have quickly gained notoriety for their sophisticated tactics and successful attacks across various industries. For example, Trinity has been associated with targeting critical infrastructure such as healthcare and government organizations — including two healthcare providers based in the United Kingdom and United States.

In addition to new entrants, several prominent ransomware groups rebranded or shifted operations under new names to evade law enforcement scrutiny. Notable examples include the resurgence of groups like Lynx (aka INC), DennistheHitman (aka GlobeImposter), and Qilin (aka Agenda), which have adopted innovative extortion methods to enhance their effectiveness.

The Ransomware-as-a-Service (RaaS) model continues to dominate the ecosystem, empowering less-skilled actors to carry out high-impact attacks. Affiliates have become increasingly adaptable, often switching between platforms and groups, as evidenced by on-chain activity.



QUICK LINKS

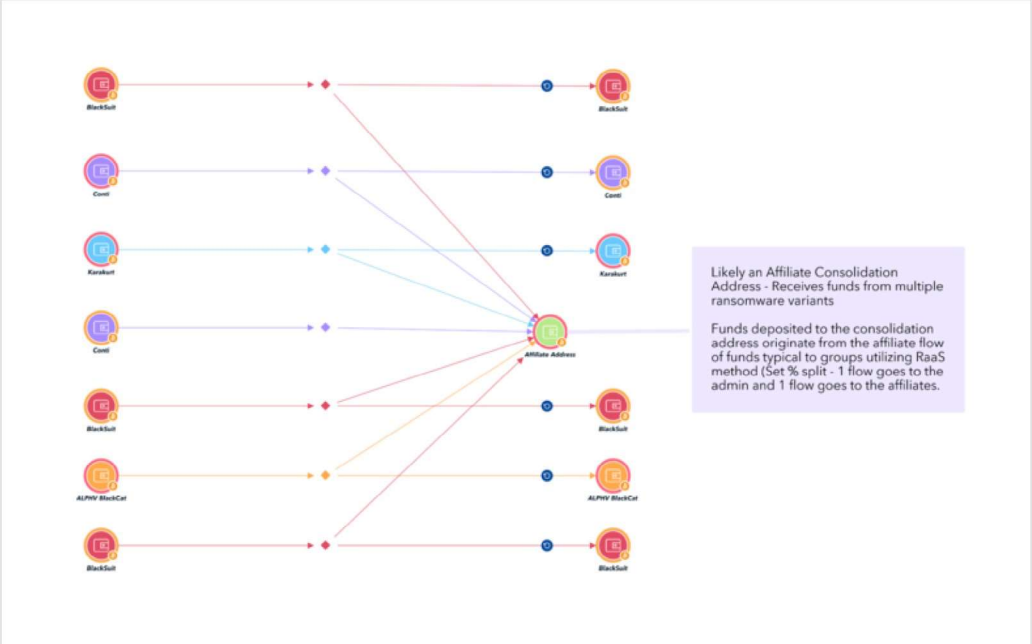


Image: Ransomware affiliate consolidation address receiving payments from multiple variants

While the ransomware landscape has traditionally been strongly associated with Russian-speaking actors, especially at the administrator level, it has diversified over the years. Groups are now incorporating affiliates from geographies around the world with a wide spectrum of language skills. For instance, DragonForce ransomware demonstrates this shift, with ties to Northern or Central Asia, as suggested by audio recordings of its associated actors on their TOR site.

Despite this change, Russian-speaking ransomware groups remain very active — with some of the most sophisticated actors in the cybercriminal landscape. Many of these groups are linked to high-profile attacks, leveraging advanced encryption techniques, innovative extortion tactics, and RaaS models to scale operations.

QUICK LINKS

Notable attacks in 2024 primarily targeted the technology, retail, and financial services sectors

Data leak sites have proliferated, serving as platforms for public shaming and extortion. These sites are increasingly used in multi-layered extortion strategies, adding pressure on victims to pay ransoms by posting victim names and company details.

Ransomware attacks in 2024 continued to target critical sectors, causing widespread disruption — with the top three sectors being technology, manufacturing, and professional services[5]. Trends leading into 2025 suggest ransomware groups will continue to target healthcare and critical infrastructure, supply chain vulnerabilities, and cloud service providers to maximize their efficiency and impact.

- Healthcare and critical infrastructure: Healthcare systems remain a prime target, with attacks causing significant disruptions to patient care and operations. Attacks against organizations like Change Healthcare and PIH Health underscore the vulnerability of critical services to cyber threats.
- Supply chain compromises: Attackers have increasingly focused on vendors and service providers like CDK Global and Blue Yonder to maximize downstream impacts. This tactic has been particularly disruptive in the technology and manufacturing sectors, where dependencies are high.
- Cloud service providers: High-profile attacks have targeted cloud service providers, resulting in the exposure of sensitive data and global service disruptions. In June 2024, data theft attacks targeted customers of the cloud data platform Snowflake, leading to breaches at companies like AT&T, Ticketmaster, and Santander Bank. Attackers obtained login credentials through infostealer malware, compromising sensitive customer data.

International collaboration is critical in disrupting ransomware actors

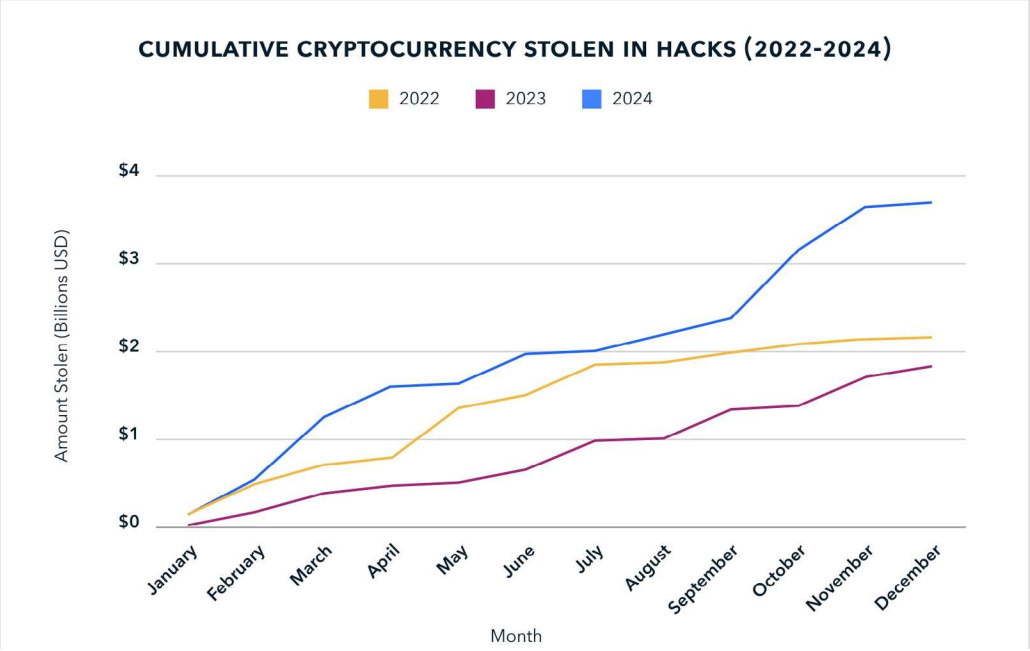
In 2024, global efforts to combat ransomware included major international collaborations like Operation Cronos, which disrupted LockBit's infrastructure, and Operation Endgame, targeting ransomware networks across Europe. The Counter Ransomware Initiative (CRI) gathered 68 nations to enhance strategies against ransomware, while sanctions targeted key figures in groups like Evil Corp. Increased collaboration between public and private entities has been instrumental in these successes. Real-time intelligence-sharing and joint

[5] This analysis is based on ransomware leak site data available as of January 6, 2025, and excludes underreported incidents.

operations have expanded resources and allowed for the timely disruption of ongoing attacks, highlighting the importance of strong partnerships in combating ransomware.

USD 2.2 billion was stolen in crypto-related hacks

In 2024, USD 2.2 billion was stolen in hacks and exploits — a 17% increase from 2023 — bringing the three-year total to over USD 7.7 billion. The crypto space continues to grapple with evolving threats, with decentralized finance (DeFi) protocols remaining prime targets. The average hack size stood at USD 14 million, reflecting both the sophistication and scale of modern breaches.



Infrastructure attacks (primarily private key and seed phrase compromises) accounted for nearly 70% of stolen funds in 2024. These compromises are common because private keys and seed phrases serve as the foundational access credentials for crypto wallets and platforms. Hackers exploit poor storage

QUICK LINKS

practices, conduct phishing campaigns, and deploy malware to gain access to these sensitive credentials. Once the private key is stolen, the thief typically transfers the funds to their own wallet — often obfuscating the trail using mixers, tumblers, or other money-laundering techniques to evade detection.

The surge in hacking activity in 2024 highlights the evolving threat landscape in the crypto space. With a 17% year-over-year increase in stolen funds and North Korea's outsized role in these attacks, the industry faces mounting pressure to implement stronger security measures. The scale of North Korean operations, combined with their reliance on private key and seed phrase theft, underscores the need for innovation in securing digital assets and mitigating state-sponsored cyber threats.

North Korea stole nearly USD 800 million of cryptocurrency

North Korea accounted for approximately 35% of all stolen funds in 2024, approaching nearly USD 800 million in stolen cryptocurrency (including only attacks for which CM GROUP has moderate or higher confidence). On average, North Korean attacks were nearly 5 times larger than those by other actors,
underscoring their emphasis on high-impact operations. Their primary method — stealing private keys and seed phrases — highlights the urgent need for robust key management solutions.

Pressure from US and international law enforcement on the crypto mixing industry led to the shutdown of key services like Samourai Wallet and Wasabi's original coordinator. In their place, North Korea has turned to smaller services like JoinMarket, Mixero, and the new, independent coordinators for Wasabi's protocol.

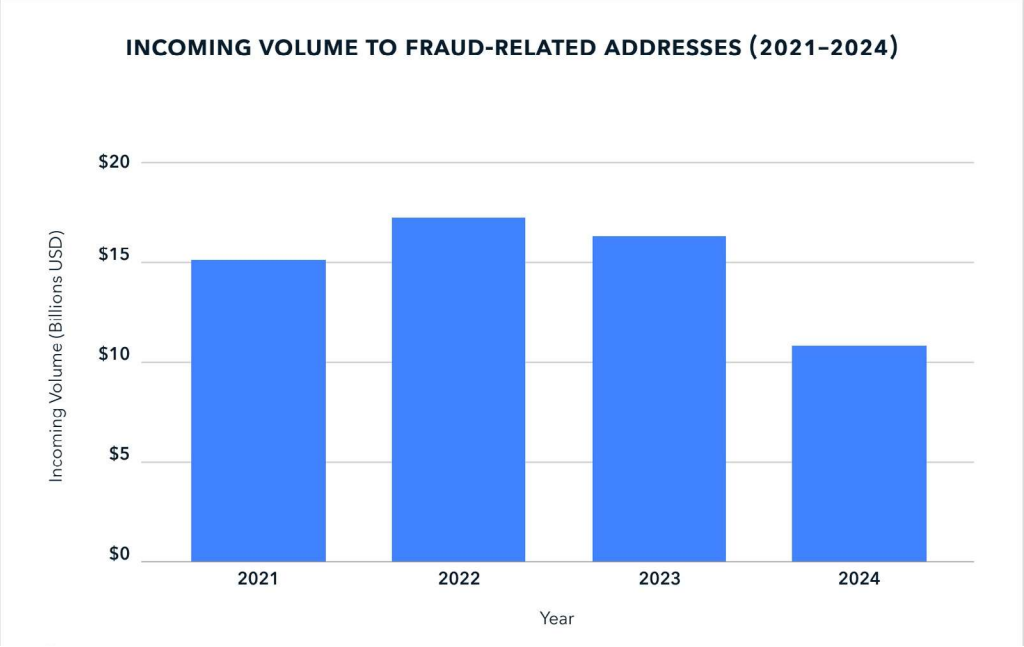
Law enforcement continues to face steep hurdles blocking and recovering stolen funds. North Korea, and the laundering groups it works with, have increased and diversified the number of bridges and blockchains they use to move crypto assets. Many of these services are truly decentralized and incapable of freezing stolen funds as they transit their protocols. The movement of many of these funds from theft addresses to ultimate disposition with likely brokers, mostly on the TRON blockchain, often occurs within the space of hours. The speed and efficiency of these transfers make freezes by law enforcement extremely challenging; CM GROUP's analysis of recent thefts suggests frictional losses to freezes or other interdictions by government remain small.

QUICK LINKS

Scam and fraud volumes declined, but remain a significant threat in the cryptosphere

In 2024, funds sent to fraud amounted to at least USD 10.7 billion, representing a 40% decrease from 2023. This continued the decline from 2022, a year when funds sent to Ponzi schemes and financial grooming schemes (commonly referred to as "pig butchering" scams) reached an all-time high of about USD 16.8 billion.

As with all types of crypto crime discussed in this report, CM GROUP's coverage of fraud in 2024 will rise over time as more instances are found. Fraud numbers appear to be much more affected than other crimes, likely due to delayed fraud reporting by victims. Accordingly, CM GROUP assesses that fraud volumes likely still declined in 2024, but not nearly as sharply as the data currently shows.



QUICK LINKS

Fewer Ponzi and pyramid schemes received over USD 100 million

Approximately 45% of the decrease in 2024 fraud volume appears to be driven by a decrease in flows to apparent Ponzi and pyramid schemes. These schemes received a total of USD 4.3 billion in funds from victims, marking a 37% decrease from 2023 inflows. While this fraud typology remains popular, and hundreds are still being created every month (targeting victims in diverse regions such as the United States, Argentina, South Korea, the United Kingdom, Italy, Cyprus, and the Philippines), CM GROUP did not see as many large schemes receiving over USD 100 million as in previous years (six in 2024 vs. 14 in 2023), which had volumes disproportionately driven by a handful of massive schemes.

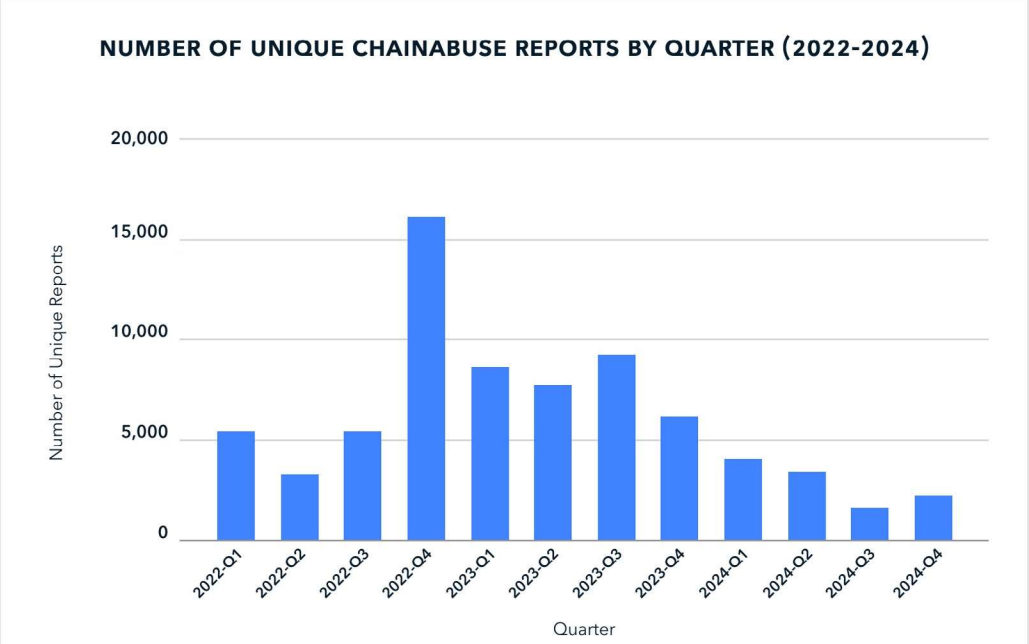
Ponzi and pyramid schemes rely on word-of-mouth, marketing, and social networks in order to become popular and yield large losses. They can obtain a level of virality similar to other types of social media activity via both off- and online methods that can supercharge a scheme — taking it from a scheme that receives USD 5 million in inflows to one receiving hundreds of millions of dollars.

This does not appear to have happened as often in 2024 as in previous years. Much like determining why particular social media posts "go viral" and others don't, it is difficult to say why no schemes appear to have "gone as viral" in 2024 as in previous years. It could be that people are more aware of such fraudulent schemes and did not fall for them as much. Or, recruitment into and marketing of these schemes could have moved offline or to private messaging, making them more difficult to find and track.

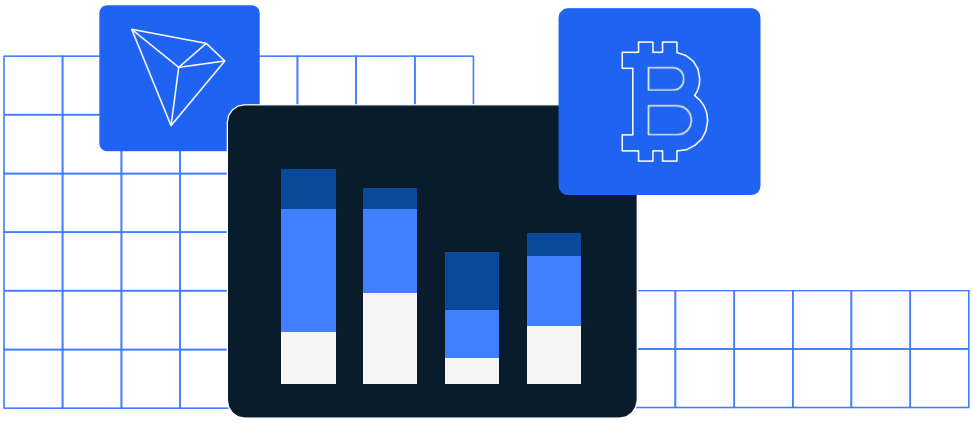
Self-reported instances of fraud remain high

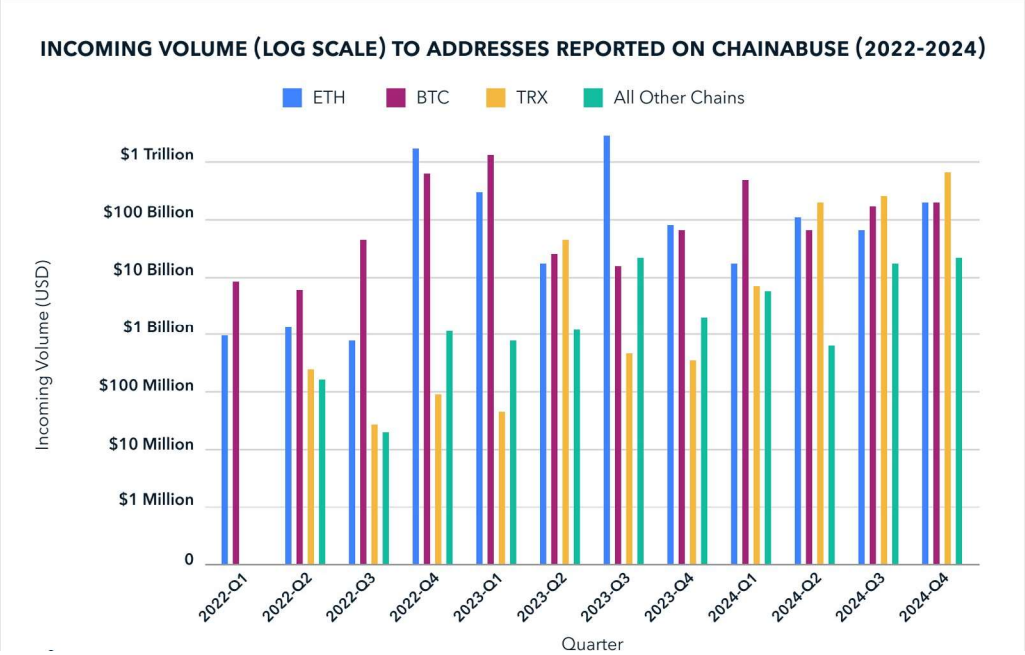
Though the overall volume for fraud dipped, CM GROUP still saw thousands of new investment scam and phishing websites being deployed each month, and received thousands of reports from Chainabuse, the largest publicly available reporting platform for illicit crypto activity.

QUICK LINKS

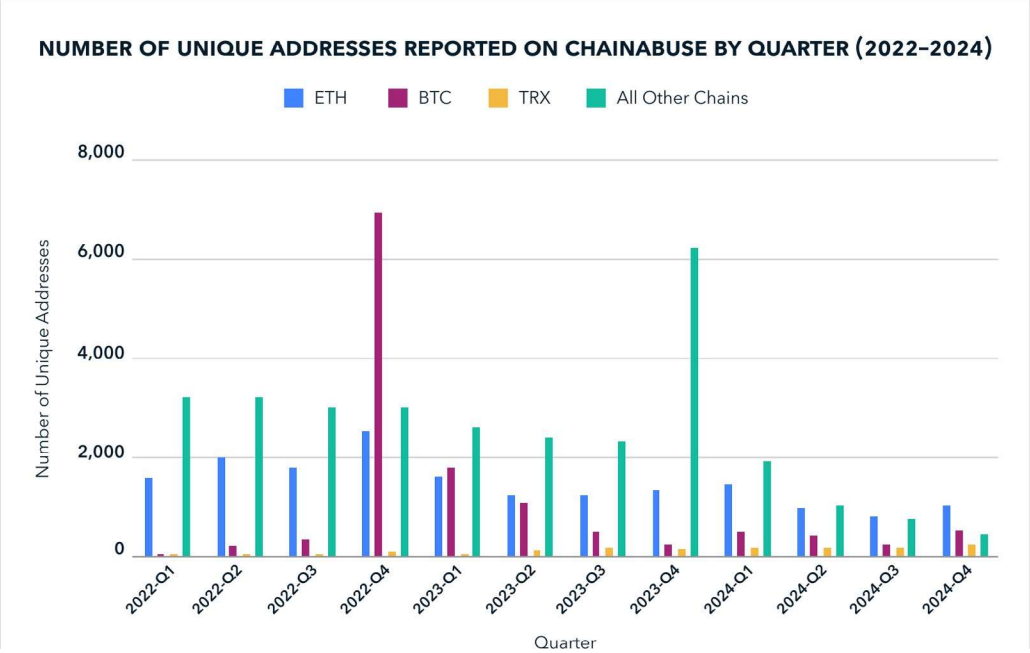


Incoming volume to addresses reported on Chainabuse appeared to remain steady in 2024 — and at relatively high volumes compared to earlier years.





Finally, reported fraudulent activity on Chainabuse matches CM GROUP internal data showing that bitcoin is the most common payment method requested by scammers — though its dominance has decreased over time.



QUICK LINKS

Financial grooming, or "pig butchering" scams, received more than USD 2.5 billion in 2024

Financial grooming scams, also known as "pig butchering," experienced a significant decline in 2024. Addresses associated with this fraud typology received at least an estimated USD 2.5 billion, a possible 58% decrease from 2023. This total is very likely an undercount of the true number, as many victims do not report their losses — and even fewer report their experiences publicly.

CM GROUP attributes this reduction, in part, to heightened law enforcement efforts worldwide. For example, the number of freezes of USDT (historically the cryptocurrency of choice for financial groomers) increased substantially in late 2023 and continued in 2024.

CM GROUP analysis also revealed fewer high-volume financial grooming entities active in 2024 compared to 2023. This decline is likely a combination of the aforementioned enforcement actions, along with increased awareness, delayed reporting, and shifts in fraudsters' tactics.

- Increased awareness: News media and social media users have been publishing stories relating to victims' large losses, the method of the scam, and its connection to transnational organized crime and human trafficking all throughout 2023 and 2024. The more people are aware of this scheme, the harder it is for the scammers to find victims.
- Delayed reporting: It frequently takes time — often many months — for victims to report scam losses, if they report at all. CM GROUP will continue to attribute more volume to specific typologies over time as more known scam instances are found. For example, in CM GROUP's 2023 Illicit Crypto Economy report, our estimate for funds received by financial grooming addresses was approximately USD 4.4 billion. Today, we assess this 2023 figure to be approximately USD 6.0 billion.
- Shifting fraudster tactics: CM GROUP has observed that fraudsters' money movements have changed. Fraudsters appear to be using DAI more than they had in 2023, perhaps in response to more frequent USDT seizures. They also appear to be using more varied decentralized services and are bridging funds via decentralized services more often than in the past.

Unfortunately, the publicly-reported connection between financial grooming and forced scamming appears to still be live. Addresses known to be used for ransom payments facilitating the rescue of forced scamming victims continued to receive several million dollars of inflows in 2024.

QUICK LINKS

Threat actors increasingly leveraged AI to defraud victims

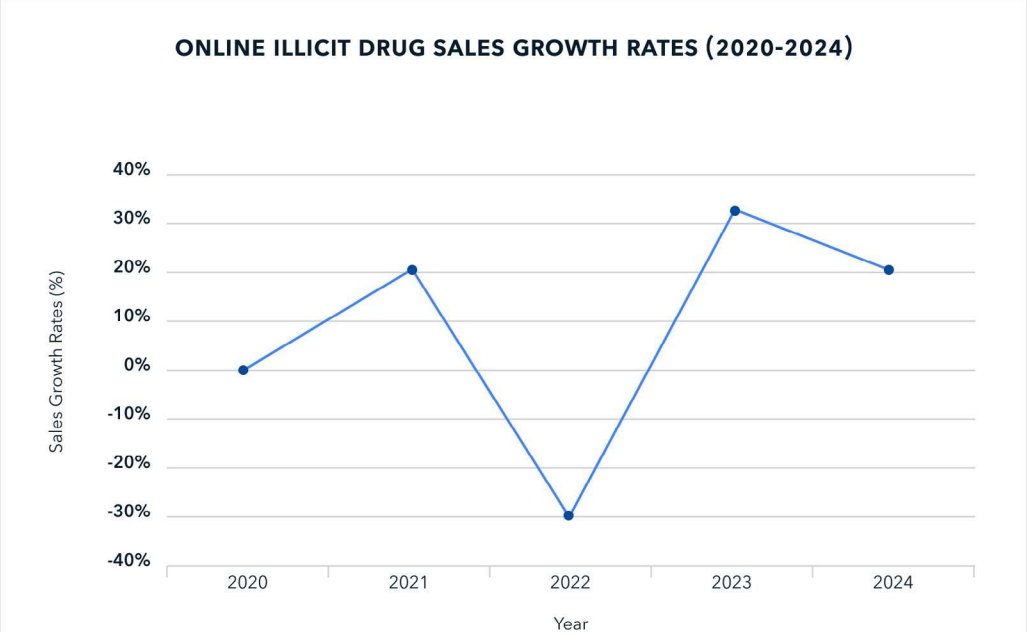
CM GROUP saw fraudsters use AI in multiple ways in 2024. Financial groomers and other scammers use large language models (LLMs) to:

- More easily create personas customized to the area in which their targeted victim resides, and to have more realistic conversations
- Create live voice and video deepfakes of famous individuals (or of victims' relatives or CEOs) to trick victims to invest money, pay an invoice, or make a hostage payment
- Send a higher quantity of (and better quality of) phishing messages
- Create pornographic images of individuals in order to extort them
- Create fake personas to bypass Know Your Customer (KYC) requirements

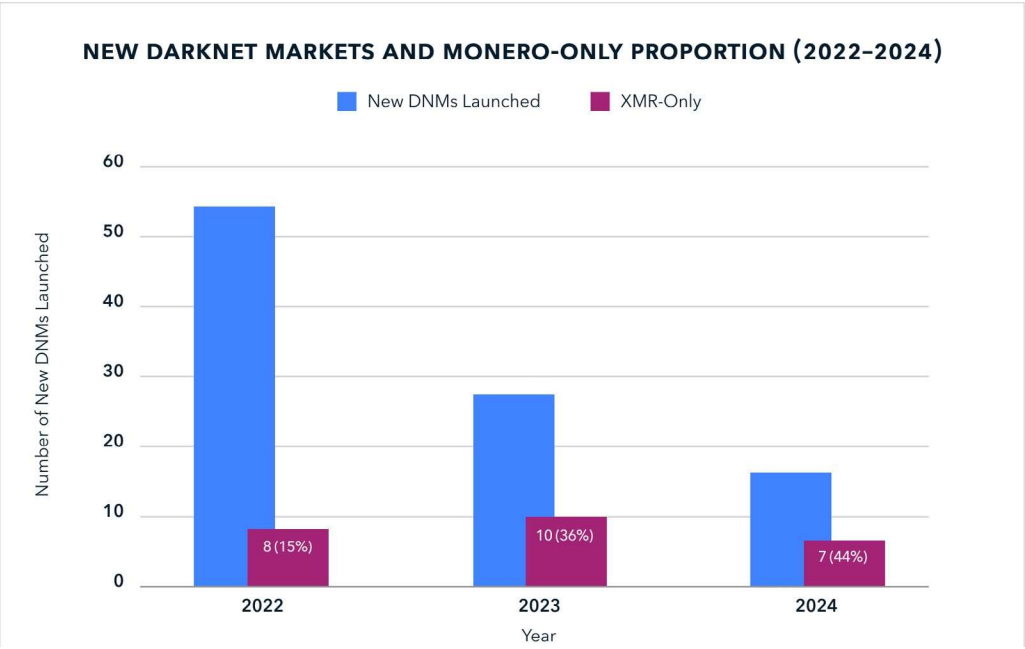
CM GROUP believes criminals of all kinds will heavily expand their use of AI in 2025, and is working to counter this grave threat.

Illicit drug sales continued to grow and expand outside of the darknet marketplace ecosystems

Cryptocurrency-enabled online sales of illicit drugs saw a year-on-year growth of over 19% between 2023 and 2024, nearing USD 2.4 billion.



2024 saw 42% fewer new darknet marketplaces (DNMs) launched year over year, with the proportion of Monero-only DNMs launched increasing from little more than a third in 2023 to nearly half in 2024.



QUICK LINKS

Drug sales are continuing to move to encrypted chat and social media platforms in the West

Over the last year, the online illicit drug trade has continued to decentralize away from darknet markets and towards encrypted chat and social media platforms. This trend, already prevalent in Western communities, has been increasingly seen in the Russian-language ecosystem as well.

Vendors today are choosing to establish vendor shops and engage in direct deals through a diverse array of encrypted communication applications and email. These platforms allow vendors to reach customers who are less technologically savvy, whilst also mitigating against market turbulence caused by darknet market exit scams or law enforcement takedowns. In this respect, the use of encrypted communication apps like Telegram and Signal have reduced the barriers to access for drug buyers to purchase products online, whilst also reducing fees that vendors pay to darknet markets for sales. This migration is further bolstered by the fact that the majority of new Western DNMs launched in 2024 have been characterized by poor design features or security issues.

The reduction in the quality and user numbers of Western DNMs stands in contrast to the Russian-language ecosystem, where fierce competition and high profits are driving innovation. Russian darknet market admins are now experimenting with developments including artificial intelligence-facilitated dispute resolution, closer integration with encrypted communication applications, incentive programs, harm reduction, UX customization, and aggressive marketing campaigns across digital and physical spaces.

Russian language darknet marketplaces continue to drive overall volume of illicit drug sales

Despite the many challenges faced by darknet marketplaces over the course of 2024, these platforms have nevertheless seen a slight increase of income compared to 2023, generating more than USD 1.7 billion.

Keeping to the trend witnessed in 2023, Russian-language darknet marketplaces continue to be responsible for the vast majority of revenue generated, contributing over 97% to the overall volume of illicit drug sales (up more than 1% from 2023) in bitcoin and TRON.

QUICK LINKS

The lower threat of action from Russian law enforcement — coupled with the dead drop-based delivery model (read more here), focus on synthetic drugs (such as alpha-PVP and mephedrone, which can be produced locally), and the wide availability and low price of drug precursor chemicals typically imported from China — have enabled Russian-language darknet marketplaces to thrive.

Only four Russian-language DNMs left the approximately 20-strong ecosystem in 2024. The departure of market leaders such as Solaris Market — which ceased operations in autumn 2024 — is a rare occurrence. And while there have been no more successful law enforcement takedowns of Russian-language DNMs since the fall of Hydra Market in April 2022, the administrators of these platforms also avoid exit scams (typical of the Western DNM ecosystem), preferring instead to voluntarily cease operations and allow all users to withdraw their funds from the marketplace escrow.

Western darknet marketplaces struggled under sustained law enforcement action and exit scams

In contrast to Russian-language DNMs, Western darknet marketplaces continued to struggle throughout 2024 as a result of sustained law enforcement action, coupled with several high profile exit scams.

This has curtailed user confidence and stunted the ecosystem's growth, creating a climate of distrust that is reminiscent of the aftermath of Op. Onymous (the law enforcement takedown of the Silk Road 2.0 darknet marketplace together with a host of smaller DNMs in 2014) and Op. Bayonet/ GraveSac (the coordinated takedown of the AlphaBay and Hansa Market darknet marketplaces by US and European law enforcement in 2017), which left the Western DNM ecosystem reeling.

After the disappearance of Bohemia Market (a prolific Western DNM) and Cannabia Market (its sister market) in a suspected exit scam in January 2024 (later revealed by the Dutch authorities to have been under investigation), the community witnessed the exit scam of Incognito Market in March 2024. This incident also marked the never-before-seen attempt of its administrator, Pharoah (arrested in May 2024 and revealed to be 23 year-old Taiwanese national Rui-Siang Lin), to extort the marketplace's users.

QUICK LINKS

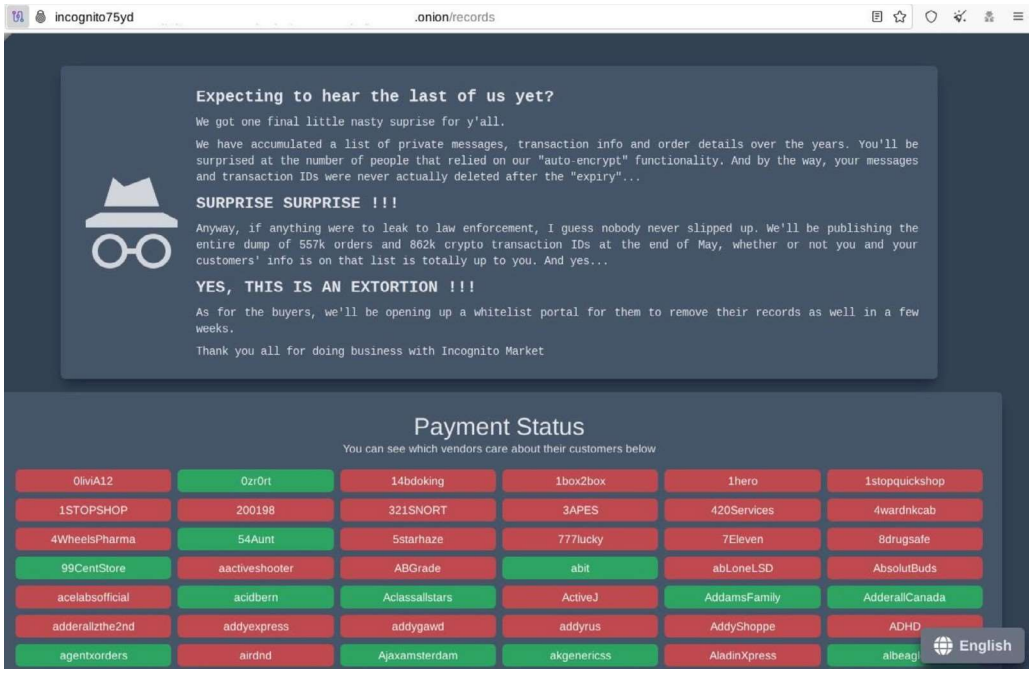


Image: Incognito admin Pharoah's extortion message addressed to vendors

This crisis was further compounded by the seizure of Nemesis Market by German law enforcement in March 2024, as well as the exits of other important and trusted players including Cypher Market (which disappeared in April 2024) and GoFish Market (September 2024), which had even been included in the Superlist of marketplaces trusted by the community.

Nevertheless, the Western DNM ecosystem experienced some innovation in spite of recent enforcement actions. Amongst the most notable was the first merger and acquisition between two marketplaces on the darknet — whereby the struggling SuperMarket was absorbed by the now-Superlisted DrugHub in an operation that lasted around one month. 2024 also saw the establishment of the first Telegram-only Western darknet marketplace, Si Market, which now hosts more than 40 vendors specializing in the sale of psychedelics, cannabis, and cannabis-related products.

QUICK LINKS

The use of crypto in vendor shop drug sales surged in 2024

The use of cryptocurrency in vendor shop drug sales saw a significant surge over the past year. Chain-Monitoring Group is the only blockchain intelligence provider with a specialist category unique to individual drug vendors — and this year, we saw incoming volumes sent to illicit vendor shops more than double. In 2023, these addresses received over USD 289 million. In 2024, this figure skyrocketed to over USD 600 million. This dramatic increase may reflect the decentralization
of the drug trade away from traditional darknet markets, as vendors grow more adept at operating across multiple platforms on both the clearnet and darknet — including e-commerce websites and social media platforms.

Arrest of Telegram founder sparks platform migrations for drug vendors

The arrest of Telegram's founder, Pavel Durov, in August 2024 triggered a notable shift in the operational dynamics of the platform's drug vendors.

Historically, Telegram has been a favored platform for selling drugs — due to its security and public perception of non-cooperation with law enforcement, as well as strict access controls for groups and channels. However, Durov's arrest has heightened fears that Telegram will now provide data on its users to law enforcement. Consequently, many vendors are migrating to alternative platforms, including Signal, Session, and WhatsApp. This exodus is expected to continue as Telegram enforces stricter measures to curtail criminal activities on its network and provide new opportunities for interdiction.

Chinese drug precursor manufacturers are adapting to intensified law enforcement efforts

Incoming crypto volumes to Chinese drug precursor manufacturers have seen a significant decline, from USD 27.6 million in 2023 to USD 17 million in 2024. This drop may be driven in part by stronger actions from the Chinese government following the Biden-Xi summit of November 2023. The summit resulted in the Chinese Communist Party (CCP) banning a range of fentanyl precursors and shutting down some suppliers, followed by a further ban of several nitazenes and analogs in July 2024. As a result, drug precursor manufacturers have begun to shift to new analogs and substances, while adopting alternative methods to cryptocurrency to obscure their financial footprints.

QUICK LINKS

Image: A Chinese drug precursor manufacturer advertises fentanyl precursors

CM GROUP has observed that these manufacturers have adapted their practices in response to intensified law enforcement efforts. Specifically, these manufacturers are becoming increasingly cautious about sharing cryptocurrency addresses in direct communications with buyers. This shift stems from the demonstrated efficacy of blockchain analysis in tracing illicit transactions and aiding investigations.

Looking ahead

The evolving landscape of crypto crime in 2024 highlights a complex interplay between advancing security measures and increasingly adaptive illicit actors. While efforts to curb illegal activities have shown promising results, threat actors continue to innovate — exploiting vulnerabilities within decentralized finance, blockchain infrastructure, and emerging technologies.

A key theme throughout the year has been the resilience and adaptability of illicit networks. Sanctioned entities, terrorist organizations, and ransomware groups have shifted tactics in response to global crackdowns, embracing new technologies and methods to obscure their activities. This adaptability underscores the need for constant evolution in enforcement strategies and international cooperation.

QUICK LINKS

The expanding use of cryptocurrencies by terrorist organizations and state-sponsored actors illustrates the dual-edged nature of technological innovations — providing both opportunity and risk. Ransomware actors and fraudsters are leveraging technological advancements, including cross-chain bridges and artificial intelligence, to bypass detection and scale their operations.

And the fragmentation of illicit markets, particularly in drug sales, signals a shift toward decentralization — with criminal enterprises moving away from traditional darknet marketplaces toward more agile and resilient platforms. This shift presents both new challenges and opportunities for disruption.

Ultimately, the fight against crypto crime requires a proactive, collaborative approach. Regulatory bodies, law enforcement agencies, and private sector partners must continue to adapt, innovate, and cooperate to outpace increasingly sophisticated threat actors. Central to this effort is the use of advanced blockchain intelligence tools, which provide critical insights for tracing illicit transactions, identifying threat actors, and supporting enforcement actions. The progress made in disrupting illicit networks demonstrates the impact of collective action, but sustained vigilance and adaptability — empowered by cutting-edge blockchain analytics — will be essential to securing the crypto ecosystem in the years ahead.

About Chain-Monitoring Group

Chain-Monitoring Group provides blockchain analytics solutions to help law enforcement and national security agencies, financial institutions, and cryptocurrency businesses detect, investigate, and disrupt crypto-related fraud and financial crime. CM group's blockchain intelligence platform includes solutions to trace the source and destination of funds, identify illicit activity, build cases, and construct an operating picture of threats. CMG is trusted by leading agencies and businesses worldwide who rely on CMG to enable a safer, more secure crypto ecosystem.
CMG is based in London, UK, and is hiring across engineering, product, sales, and data science.

To learn more, visit Chain-monitoring.com