Chainalysis

FEBRUARY 2025

The 2025 Crypto Crime Report

The rising role of cryptocurrency in all forms of crime and how its transparency is creating unique opportunities for investigation

Table of Contents

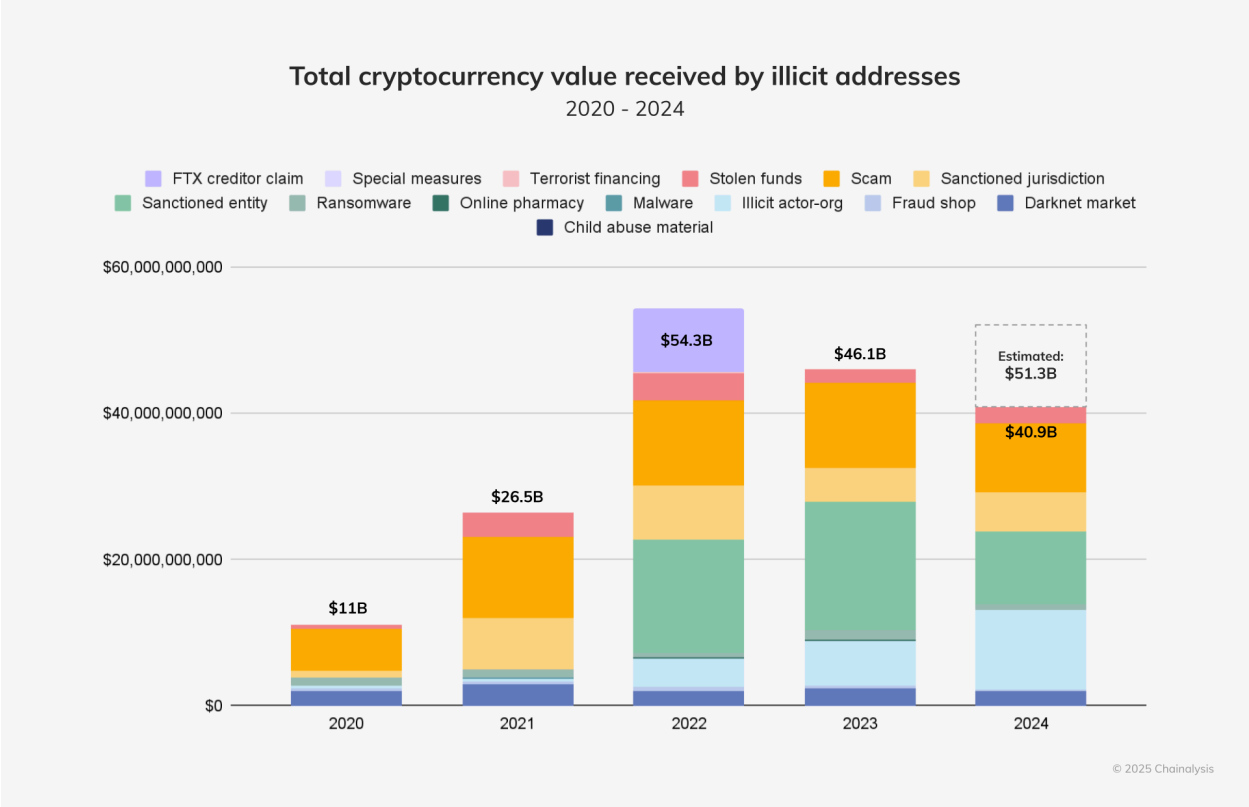
Introduction

Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized

In recent years, cryptocurrency has become increasingly mainstream. Although illicit activity on-chain previously revolved heavily around cybercrime, cryptocurrency is now also being used to fund and facilitate all kinds of threats, ranging from national security to consumer protection. As cryptocurrency has gained greater acceptance, illicit on-chain activity, too, has become more varied. For example, some illicit actors primarily operate off-chain, but move funds on-chain for laundering.

We report on certain defined categories — stolen funds, darknet markets, and ransomware, to name a few — on an annual basis. However, with the diversification of crypto crime to include all types of crime, the on-chain illicit ecosystem has witnessed increasing professionalization, with a broadening array of illicit actor organizations and networks using cryptocurrency, as well as increased complexity in their operations. In particular, we have seen the emergence of large-scale on-chain services that provide infrastructure for numerous types of illicit actors to help them launder their ill-gotten crypto.

How are these developments playing out on-chain? Let's take a look at the data and high-level trends.



According to our metrics today, it looks like 2024 saw a drop in value received by illicit cryptocurrency addresses to a total of $40.9 billion. However, 2024 was likely a record year for inflows to illicit actors as these figures are lower-bound estimates based on inflows to the illicit addresses we've identified up to today.

A year from now, these totals will be higher, as we identify more illicit addresses and incorporate their historic activity into our estimates. For instance, when we published last year's Crypto Crime Report, we reported $24.2 billion for 2023. One year later, our updated estimate for 2023 is $46.1 billion. Much of that growth came from various types of illicit actor organizations, such as vendors operating through Huione, which provide on-chain infrastructure and laundering services for high-risk and illicit actors.

It stands to reason that 2024's illicit cryptocurrency volume will exceed that of 2023. Since 2020, our annual estimates of illicit activity — which include both evidentiary attributions and Chainalysis Signals data — have grown by an average of 25% between annual reporting periods. Assuming a similar growth rate between now and next year's Crypto Crime Report, our annual totals for 2024 could surpass the $51 billion threshold.

In general, our totals exclude revenue from non-crypto-native crime, such as traditional drug trafficking and other crimes in which crypto may be used as a means of payment or laundering. Such transactions are virtually indistinguishable from licit transactions in on-chain data, although law enforcement with off-chain information can still investigate these crimes using Chainalysis solutions. In cases where we're able to confirm such information, we count the transactions as illicit in our data. For example, since the conviction of FTX's former CEO of fraud, our 2022 figures have included the $8.7 billion in creditor claims against the exchange. However, there are almost certainly many instances where we do not have such confirmation, and therefore the numbers would not be reflected in our totals.

How big was crypto crime in 2024?

$40B

received by illicit addresses known today, but we estimate the total may be closer to $51 billion given historical trends

0.14%

of total on-chain transaction volume

Estimates of illicit transaction activity DO include:

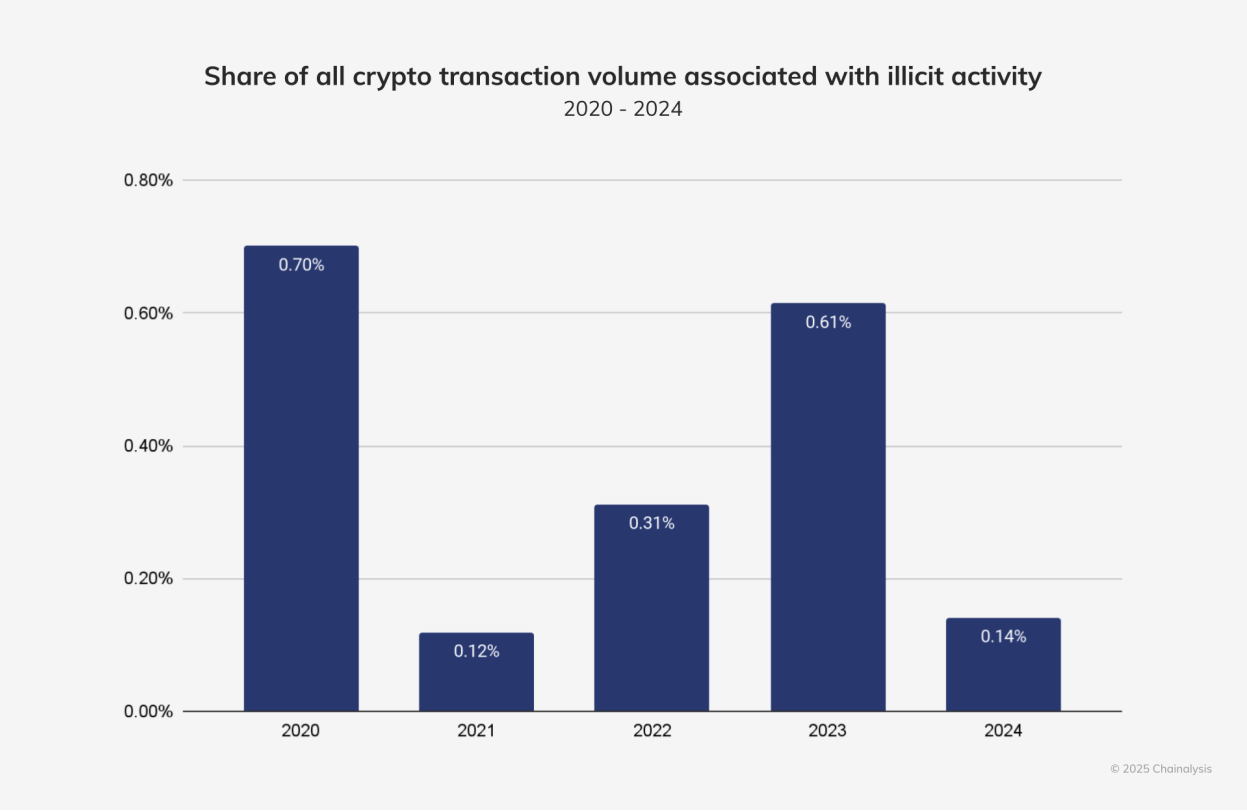
- ✓ Funds sent to addresses we've identified as illicit
- ✓ Funds stolen in crypto hacks

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 validate as illicit without more information.
- ✗ Funds associated with extremist groups. **Why?** Because the definition of what constitutes extremism is often subject to interpretation and inconsistent across jurisdictions.
- ✗ Funds associated with crypto platforms accused of fraud, absent convictions in court. **Why?** Because only a judge and jury can make that determination.
- ✗ Transaction volumes 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.

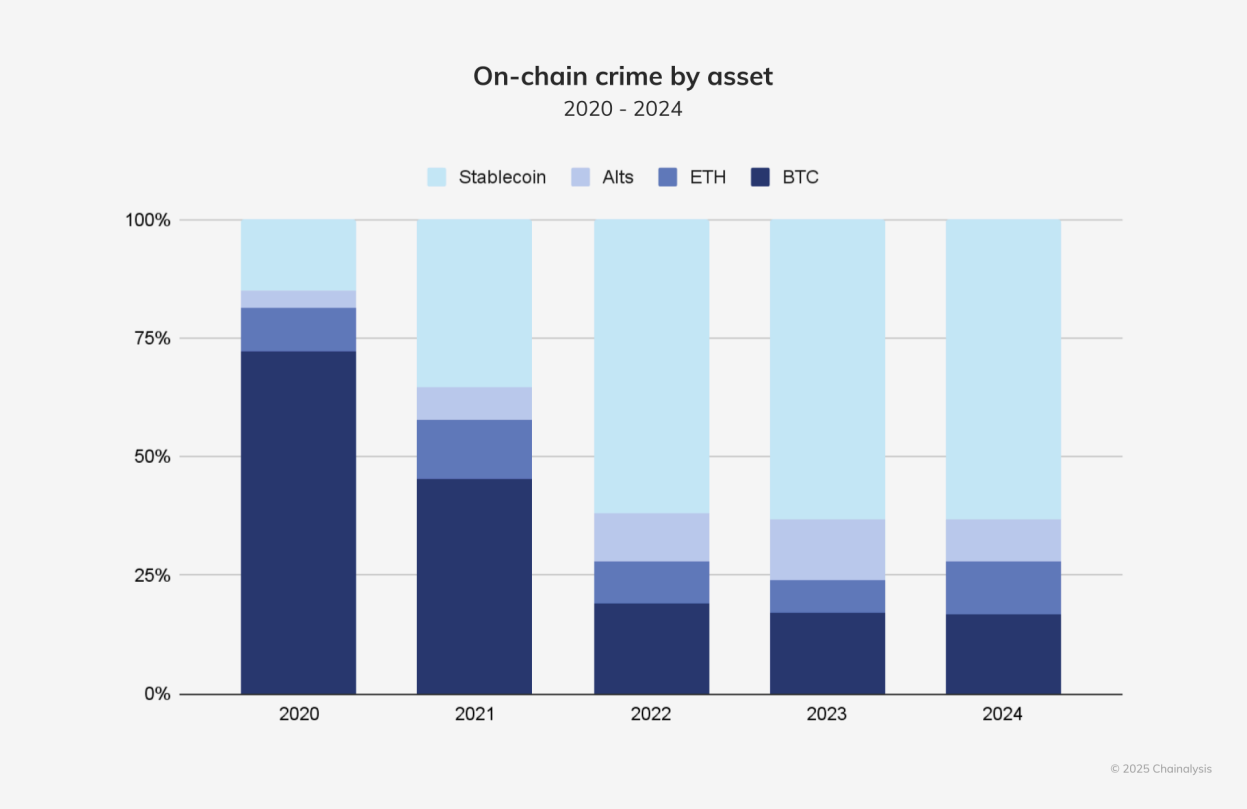
At the time of this publication, we see a reduction in absolute value of illicit activity year-over-year (YoY); however, based on historical growth rates, we suspect that this number will eventually exceed last year's total as our data attributions improve. In addition, our estimate for the share of all attributed crypto transaction volume associated with illicit activity, depicted below, also fell to 0.14% from 0.61% in 2023.[1] Similarly, we expect this share to rise over time, although historically these rates consistently remain below 1%.

As we initially shared in our mid-year crypto crime update, another important update this year is that we've begun to factor suspected illicit activity into our total estimates for certain crime types, based on Signals data. Previously, our estimates included only totals tied to addresses for which we had supporting documentation demonstrating that they belong to a certain illicit entity. Signals leverages on-chain data and heuristics to identify the suspected category for a particular unknown address or cluster of addresses, with confidence levels ranging from likely to almost certain. The introduction of Signals not only grows our estimates of certain illicit activity categories over time, but also enables us to refine previous years' estimates, given more time has passed to collect inputs and understand on-chain patterns of suspicious activity. As bad actors continue to evolve their tactics, so too will our methods of detecting and disrupting them.



[1] ***Transaction volume*** is a measure of all attributed economic activity, a proxy for funds changing hands. We have tweaked our methodology this year to include only transactions involving at least one attributed entity, while removing peel chains, internal service transactions, transactions between two personal wallets, change, and any other type of transaction that would not count as an economic transaction between distinct economic actors.

We are also seeing a continued trend vis-à-vis the types of assets involved in crypto crime.



Through 2021, BTC was unequivocally the cryptocurrency of choice among cybercriminals, likely due to its high liquidity. Since then, however, we have observed a steady diversification away from BTC, with stablecoins now occupying the majority of all illicit transaction volume (63% of all illicit transactions). This new reality is part of a broader ecosystem trend in which stablecoins also occupy a sizable percentage of all crypto activity, demonstrated by total growth YoY in stablecoin activity around 77%. In our 2024 Geography of Cryptocurrency report, we covered the wide array of practical use cases for stablecoins in a range of markets, such as storing value, sending remittances, facilitating cross-border payments, and international trade. Additionally, stablecoin issuers often freeze funds if they are made aware of their use by illicit actors. For example, Tether has frozen addresses of concern linked to scams, terrorist financing, and sanctions evasion, which can make stablecoins a poor tool for the transfer of value by illicit actors.

Nonetheless, despite these ecosystem-wide trends, some forms of crypto crime, such as ransomware and darknet market (DNM) sales, remain BTC-dominated. The popular privacy coin Monero, although an increasingly important part of the DNM ecosystem, is not included in the analysis for this report. Other illicit activity, such as scamming or laundering stolen funds, often take a more eclectic approach and spread out across all asset types. Others, such as transactions associated with sanctioned entities, have shifted primarily to stablecoins. Sanctioned entities, including individuals operating in sanctioned jurisdictions, often have a greater incentive to use stablecoins due to challenges otherwise accessing the U.S. dollar through traditional means amid a desire to benefit from its stability

Below, we'll take a closer look at three key trends that defined crypto crime in 2024 and will be important to watch going forward.

.

Stolen funds and scams still prolific

Stolen funds increased by approximately 21% YoY to $2.2 billion. Although the largest share of stolen funds was robbed from decentralized finance (DeFi) services, centralized services were the most targeted in Q2 and Q3. Private key compromises accounted for the largest share (43.8%) of stolen crypto in 2024, with North Korean hackers stealing more from crypto platforms than ever before: $1.34 billion, representing 61% of the total amount stolen for the year. Some of these events appear to be linked to North Korean IT workers, who have been increasingly infiltrating crypto and web3 companies, compromising their networks, and using sophisticated tactics, techniques, and procedures (TTPs).

High- and low-tech fraud and scams were prolific in 2024, with high-yield investment scams and pig butchering representing the most successful fraud and scam types. We have also observed the increasing use of artificial intelligence (AI) in the fraud and scams space, such as in highly personalized sextortion attacks. This use of AI is consistent with a broader trend across a range of illicit cybercrimes, as services have emerged that leverage AI to bypass know-your-customer (KYC) requirements. Fraud and scam operators are also leveraging guarantee services such as Huione (discussed below), while crypto ATM scams are a growing concern, especially as they relate to elder fraud.

Ransomware still front and center, darknet markets and fraud shop volumes on the decline

Ransomware has continued to see revenues in the hundreds of millions of dollars, but a number of large, multilateral law enforcement disruptions coupled with decreased victim appetite to pay ransoms have made a dent in the ecosystem. 2024 has nonetheless been a productive year, as attack volume was relatively sustained and some ransomware groups have still managed to eke out payments — albeit in lower amounts.

DNMs received $2 billion as opposed to close to $2.3 billion in 2023, while fraud shop volume is down by slightly more than half at $220.1 million. This marked decline for fraud shops is due in part to a large U.S.-Dutch takedown of Universal Anonymous Payment System (UAPS), a crypto payment processor that facilitated transactions for hundreds of fraud shops, including Brian Dumps and Faceless.

Crypto crime landscape increasingly diverse and professionalized

An array of illicit actors, including transnational organized crime groups, are increasingly leveraging cryptocurrency for traditional crime types, such as drug trafficking, gambling, intellectual property theft, money laundering, human and wildlife trafficking, and violent crime. Furthermore, some criminal networks are resorting to crypto to facilitate polycrime, or multiple crime types. Indeed, of the total $40.9 billion received by illicit crypto addresses in 2024, $10.8 billion was received by "illicit-actor org," our catch-all term for wallets of services and individuals both directly committing cybercrime like hacking, extortion,

trafficking, or scams, as well as those facilitating this activity by selling the underlying infrastructure, tools, and services needed to commit crime and profit, including laundering-as-a-service.

Perhaps no entity better illustrates the professionalization of the crypto crime ecosystem than the online marketplace Huione Guarantee. As we highlighted in our 2024 mid-year crypto crime update, Huione and all vendors operating on their platform have processed more than $70 billion in crypto transactions since 2021. This platform has provided infrastructure which facilitates the sale of scam technology and processed on-chain transactions for pig butchering and other fraud and scams, addresses reported as stolen funds, sanctioned entities such as the Russian exchange Garantex, fraud shops, child sexual abuse material, and Chinese-language gambling sites and casinos, among others.

Ransomware

35% Year-over-Year Decrease in Ransomware Payments, Less than Half of Recorded Incidents Resulted in Victim Payments

The ransomware landscape experienced significant changes in 2024, with cryptocurrency continuing to play a central role in extortion. However, the total volume of ransom payments decreased year-over-year (YoY) by approximately 35%, driven by increased law enforcement actions, improved international collaboration, and a growing refusal by victims to pay.

In response, many attackers shifted tactics, with new ransomware strains emerging from rebranded, leaked, or purchased code, reflecting a more adaptive and agile threat environment. Ransomware operations have also become faster, with negotiations often beginning within hours of data exfiltration. Attackers range from nation-state actors to ransomware-as-a-service (RaaS) operations, lone operators, and data theft extortion groups, such as those who extorted and stole data from Snowflake, a cloud service provider.

In this chapter, we'll explore these developments and their implications, including a variety of case studies — LockBit, Iranian ransomware strains, Akira/Fog, and INC/Lynx — that exemplify this year's trends.

Ransomware activity shifts halfway through the year

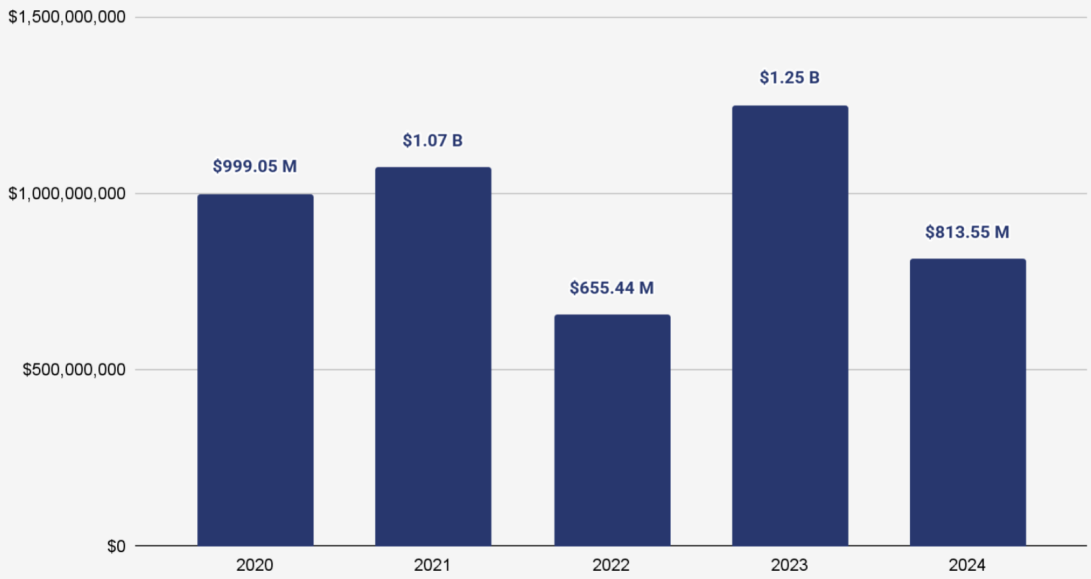
In 2024, ransomware attackers received approximately $813.55 million in payments from victims, a 35% decrease from 2023's record-setting year of $1.25 billion, and for the first time since 2022, ransomware revenues declined.

As we noted in our mid-year crime update, value extorted by ransomware attackers between January and June 2024 had reached $459.8 million, approximately 2.38% higher than the value extorted over the same time period in 2023. H1 2024 also saw a few exceptionally large payments, such as the record-breaking $75 million payment to Dark Angels.

Despite its small half-over-half (HoH) increase, we expected 2024 to surpass 2023's totals by the end of the year. Fortunately, however, payment activity slowed after July 2024 by approximately 34.9%. This slowdown is similar to the HoH decline in ransom payments since 2021 and the overall decline during H2 2024 in some types of crypto-related crime, such as stolen funds. Notably, the decline this year is more pronounced than in the last three years.

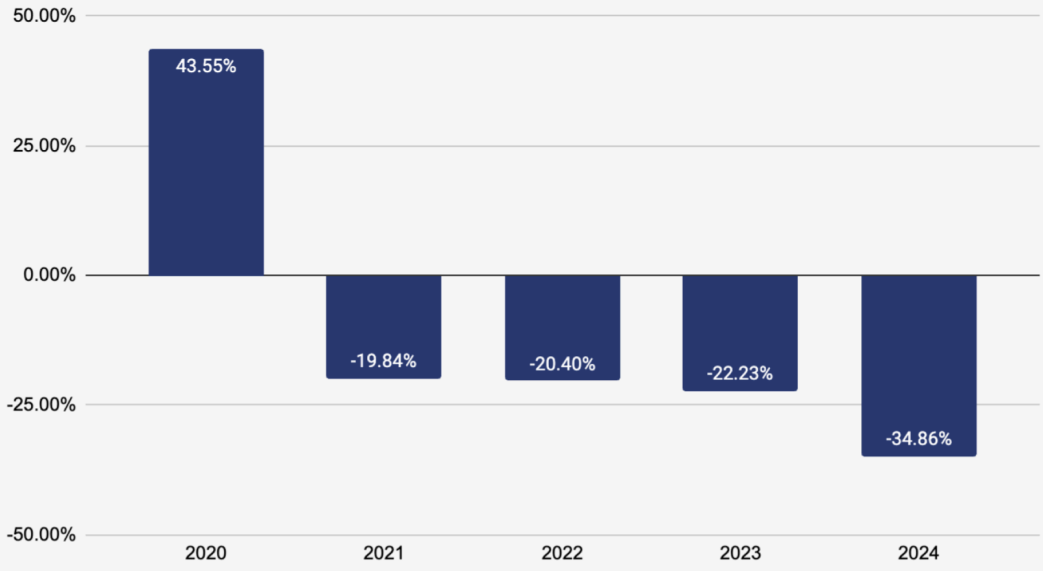
Annual ransomware payment totals

2020 - 2024



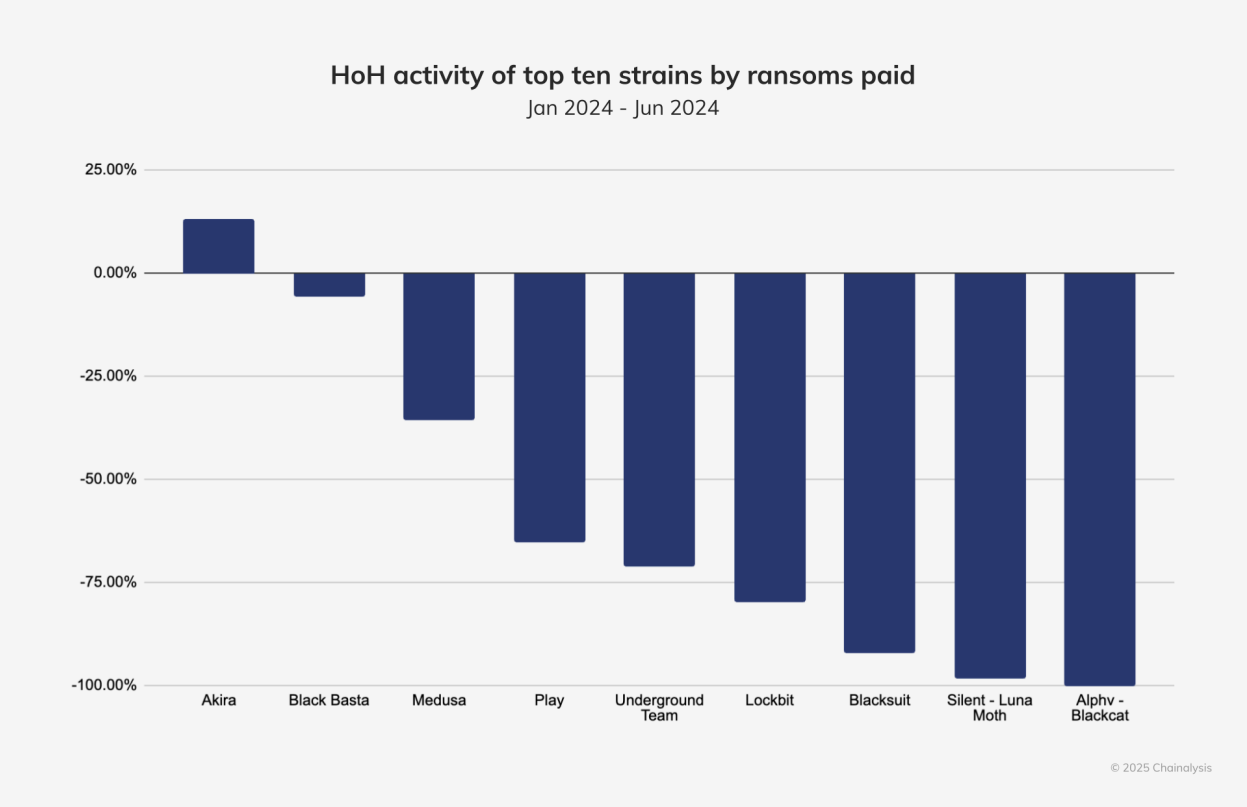
Percent change in ransom payments from H1 to H2 by year

2020 - 2024

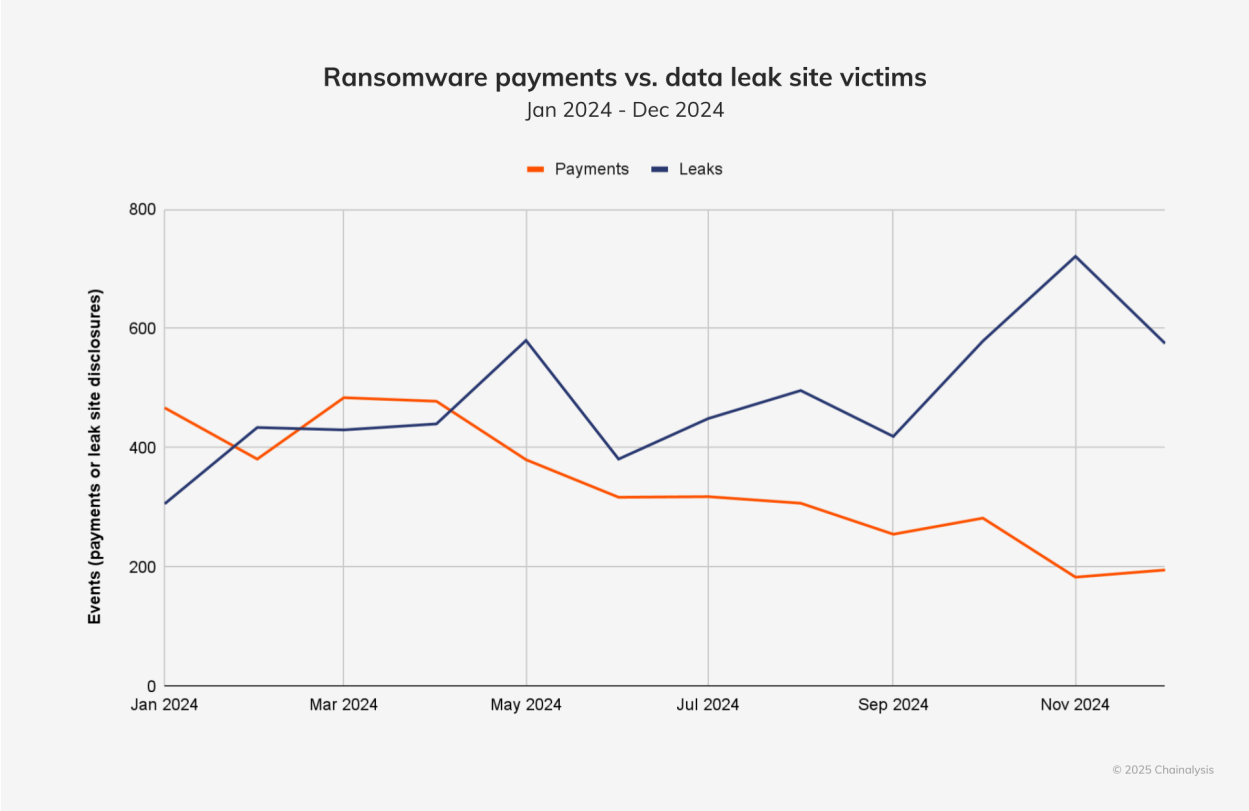


A closer examination of the top 10 ransomware strains in terms of H1 revenue provides valuable insights into the groups driving these HoH trends. As we see in the below chart, Akira, which has targeted more than 250 entities since March 2023, is the only H1 top 10 ransomware strain to have ramped up its efforts in H2 2024. LockBit, which was disrupted by the United Kingdom's National Crime Agency (NCA) and the U.S. Federal Bureau of Investigation (FBI) in early 2024, saw H2 payments decrease by approximately 79%, showcasing the effectiveness of international law enforcement collaboration. ALPHV/BlackCat, which had been among 2023's top grossing strains, exit scammed in January 2024, leaving a void in H2.

As Lizzie Cookson, Senior Director of Incident Response at Coveware, a ransomware incident response firm, told us, "The market never returned to the previous status quo following the collapse of LockBit and BlackCat/ALPHV. We saw a rise in lone actors, but we did not see any group(s) swiftly absorb their market share, as we had seen happen after prior high profile takedowns and closures. The current ransomware ecosystem is infused with a lot of newcomers who tend to focus efforts on the small- to mid-size markets, which in turn are associated with more modest ransom demands."



To further contextualize what may have driven H2's decrease in ransomware payment activity, we first looked at data leak sites, which could be a proxy for ransomware events. In the below chart, we can see that the number of ransomware events increased into H2, but on-chain payments declined, suggesting that more victims were targeted, but fewer paid.



Source: ecrime.ch

Data leak sites posted more victims in 2024 than in any year prior. Not only were there more alleged victims, but, according to Allan Liska, Threat Intelligence Analyst at Recorded Future, there were 56 new data leak sites in 2024 — more than double the number Recorded Future identified in 2023. However, there are some caveats to consider with data leak site information and what it suggests about the ransomware ecosystem.

Corsin Camichel, Threat Researcher at eCrime, shared more information on the legitimacy of leaks. "We have observed leak site posts claiming organizations, only to fail on a deeper analysis. For example, we have seen claims for multinational organizations, but in reality, only a smaller subsidiary was impacted. More than 100 organizations got listed on two or more data leak sites in 2024. The 'MEOW' leak site plays a big role in this, seeming to compromise websites and list data taken from web servers or databases." Another reason for the inverse relationship between ransomware payments and data leak site victims shown above could be that threat actors have been caught overstating or lying about victims or reposting claims by old victims. "The LockBit operators played games to pretend to stay relevant and active after a law enforcement action called 'Operation Cronos,' as they re-posted many previously listed claims again or added attacks that happened a long time ago, some even over one year ago," Camichel added.

Liska also shared with us information about illegitimate victims posted to data leak sites, stating, “This is especially true of LockBit, which, in a bid to remain relevant after being ostracized by much of the underground community post law enforcement action, has published as high as 68% repeat or straight up fabricated victims on its data leak site.”

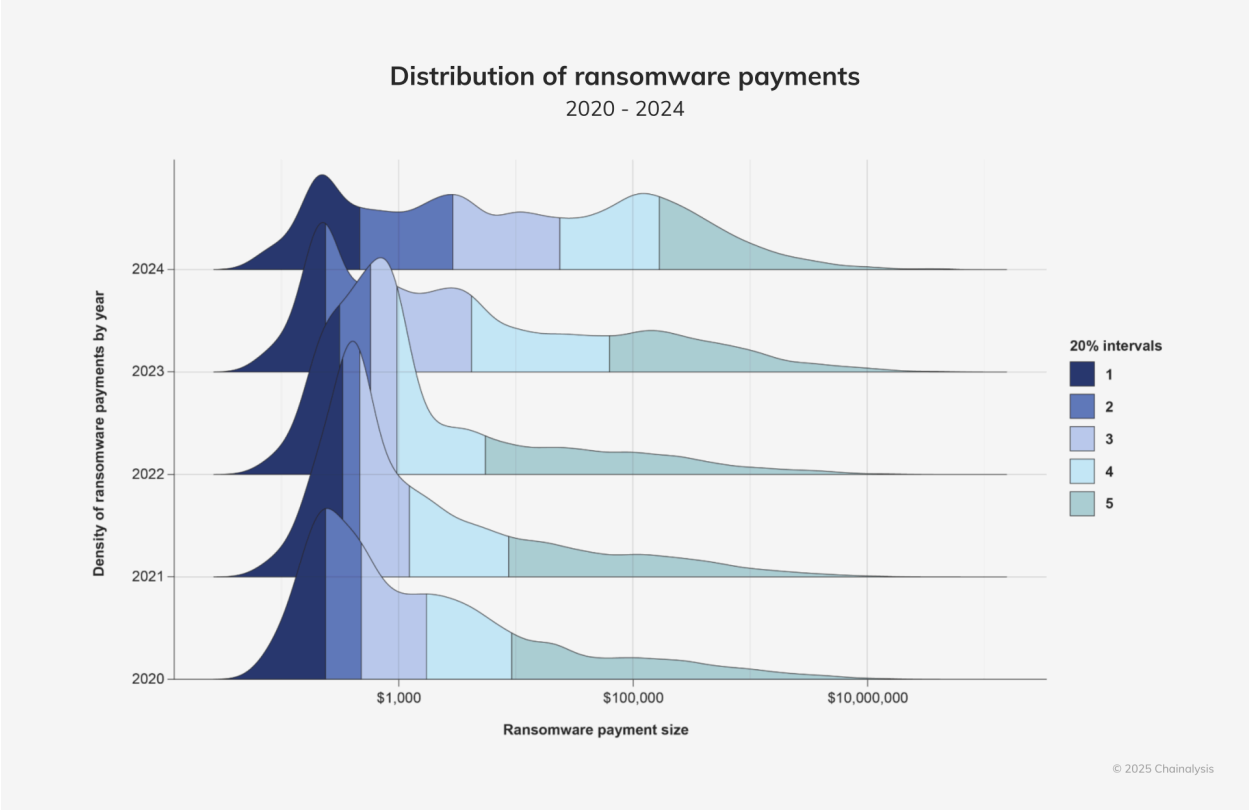
In the aftermath of the LockBit disruption and BlackCat’s exit scam, another interesting phenomenon has been the rise of RansomHub RaaS, which absorbed a lot of the displaced operators from LockBit and BlackCat. RansomHub posted the highest number of victims in 2024, according to Camichel, and despite only emerging in February 2024, ranked in the top 10 strains for 2024, according to on-chain data.

Incident response data show that the gap between the amounts demanded and paid continues to increase; in H2 2024, there was a 53% difference between the two factors. Reporting from incident response firms suggests a majority of clients opt not to pay altogether, which means the actual gap is larger than the below numbers suggest.

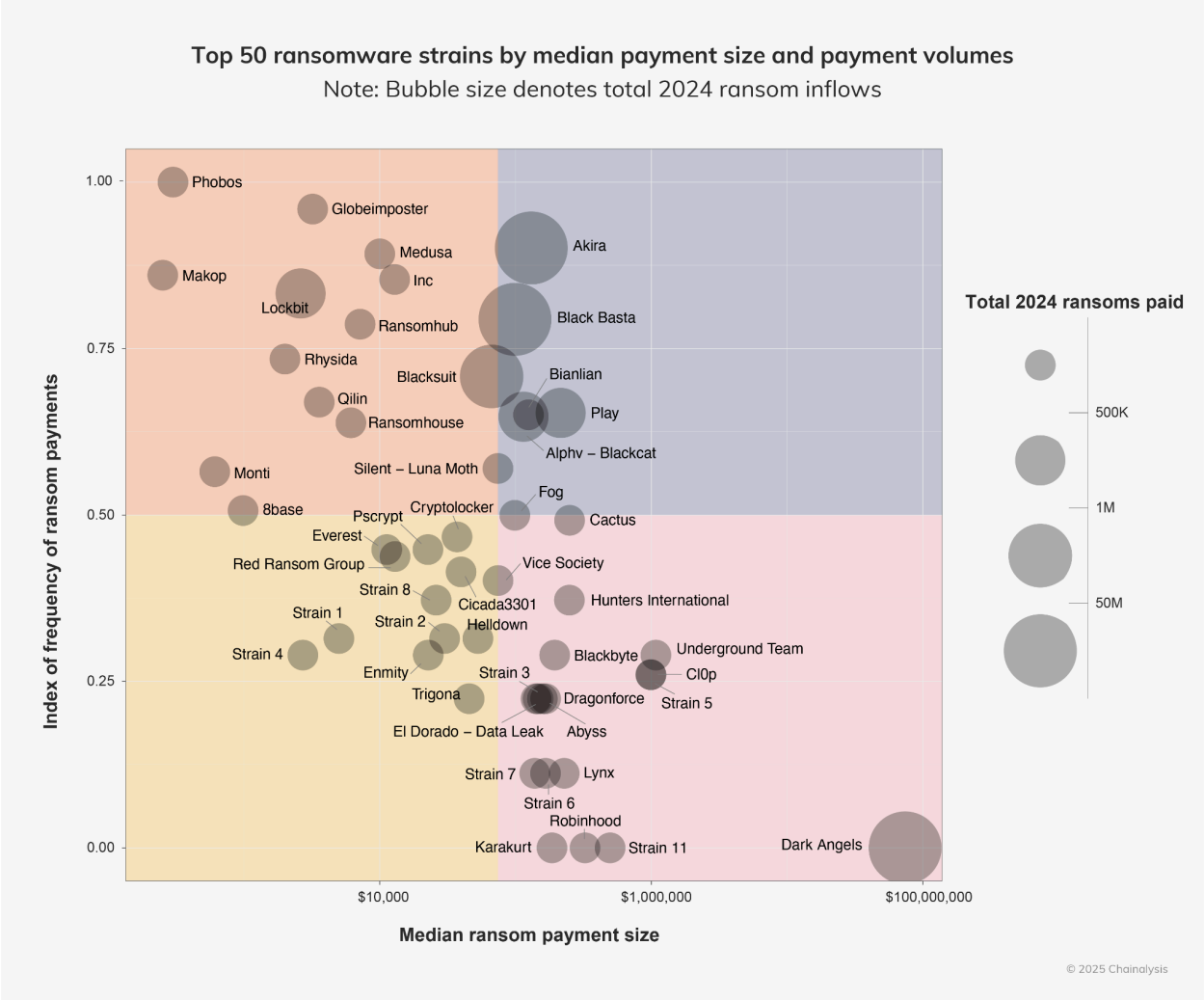
We spoke to Dan Saunders, Director, Incident Response, EMEA at Kivu Consulting, a cybersecurity incident response firm, to learn more about this victim resilience. “According to our data, around 30% of negotiations actually lead to payments or the victims deciding to pay the ransoms. Generally, these decisions are made based on the perceived value of data that’s specifically been compromised,” he stated. Similarly, Cookson noted that, thanks to improved cyber hygiene and overall resiliency, victims are increasingly able to resist demands and explore multiple options to recover from an attack. “They may ultimately determine that a decryption tool is their best option and negotiate to reduce the final payment, but more often, they find that restoring from recent backups is the faster and more cost-effective path,” she added. Final payment amounts typically ranged from $150,000 to $250,000, regardless of initial demands.

When looking at the figure below, we can see the evolution of ransomware payment distributions into 2024. In 2020, there was a long tail but a single hump to ransomware payments, but in 2024, there were three classes of ransomware actors. Some, such as Phobos, have average payments clustering at less than $500 – $1,000. There is another cluster around $10,000 and a third with payments north of $100,000, some of which reached $1 million. We also see more events at the higher end of the distribution, meaning proportionately greater attacks in excess of $1 million.

This segmentation reflects the shift in the ransomware actor landscape that Cookson observed, with smaller groups dominating low- and mid-value payments, while the outlier 7-8 figure ransoms push the distribution rightward toward the third class of payments.



In the below chart, we can see which strains were the worst in terms of total value extorted (bubble size), median payment size (X axis), and an index of extortion events (Y axis).



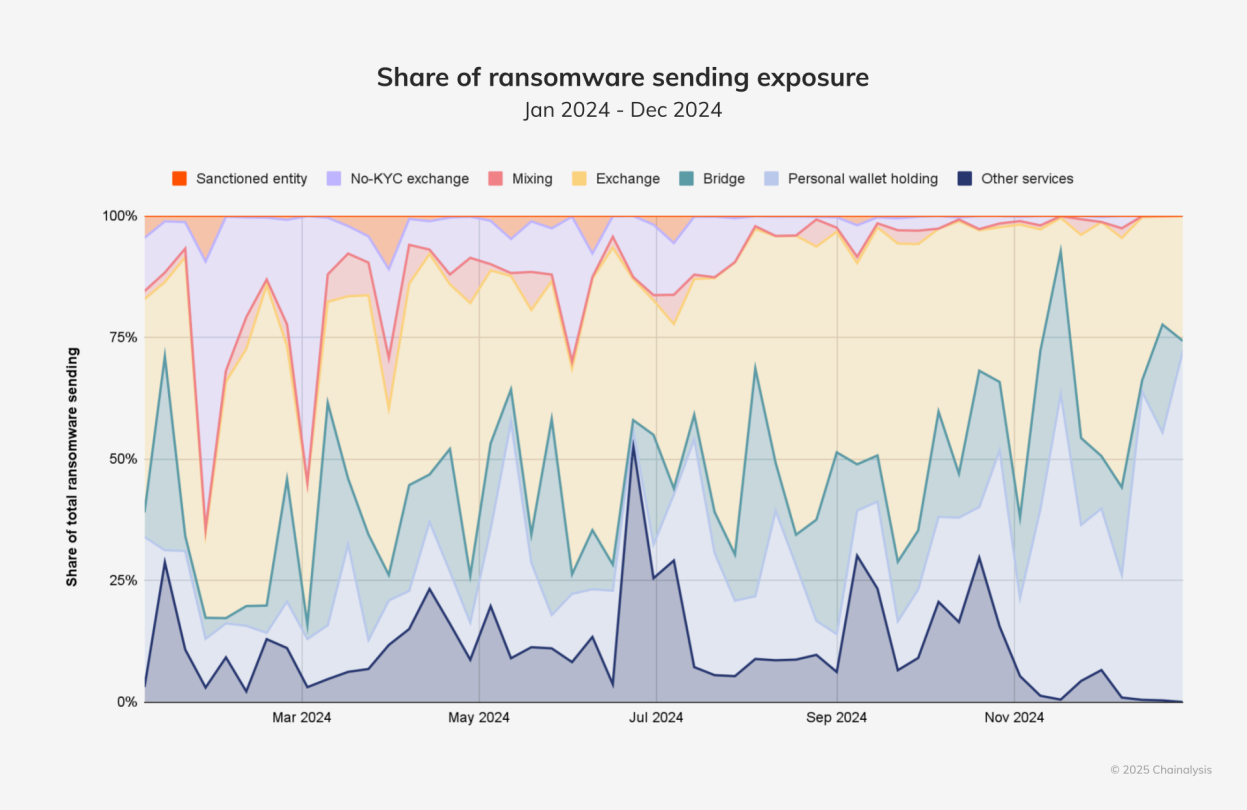
Ransomware off-ramping: Where do the funds go?

Understanding ransomware laundering methods offers critical insights into post-exploit threat actor behavior, enabling law enforcement to respond more efficiently and, in some cases, anticipate future actions based on established patterns.

In the below chart, we see that ransom funds primarily flowed through centralized exchanges (CEXs) (used to off-ramp funds), personal wallets (to hold funds), and bridges (to attempt to obscure the movement of funds). We note a substantial decline in the use of mixers in 2024. Historically, mixing services routinely captured between 10% and 15% of ransomware quarterly money laundering flows. The decline of mixing among ransomware actors over the years is very interesting and a testament to the disruptive impact of

sanctions and law enforcement actions, such as those against Chipmixer, Tornado Cash, and Sinbad. In place of mixers, we have noted ransomware actors increasingly rely on cross-chain bridges to facilitate their off-ramping. In contrast, CEXs continue to be a mainstay of the ransomware offramping playbook, with 2024 seeing a slightly above-average reliance on these types of services (39% versus 37% for the period between 2020 and 2024).

It's worth calling out the substantial volumes of funds being held in personal wallets. Curiously, ransomware operators, a primarily financially motivated group, are abstaining from cashing out more than ever. We attribute this largely to increased caution and uncertainty amid what is probably perceived as law enforcement's unpredictable and decisive actions targeting individuals and services participating in or facilitating ransomware laundering, resulting in insecurity among threat actors about where they can safely put their funds.



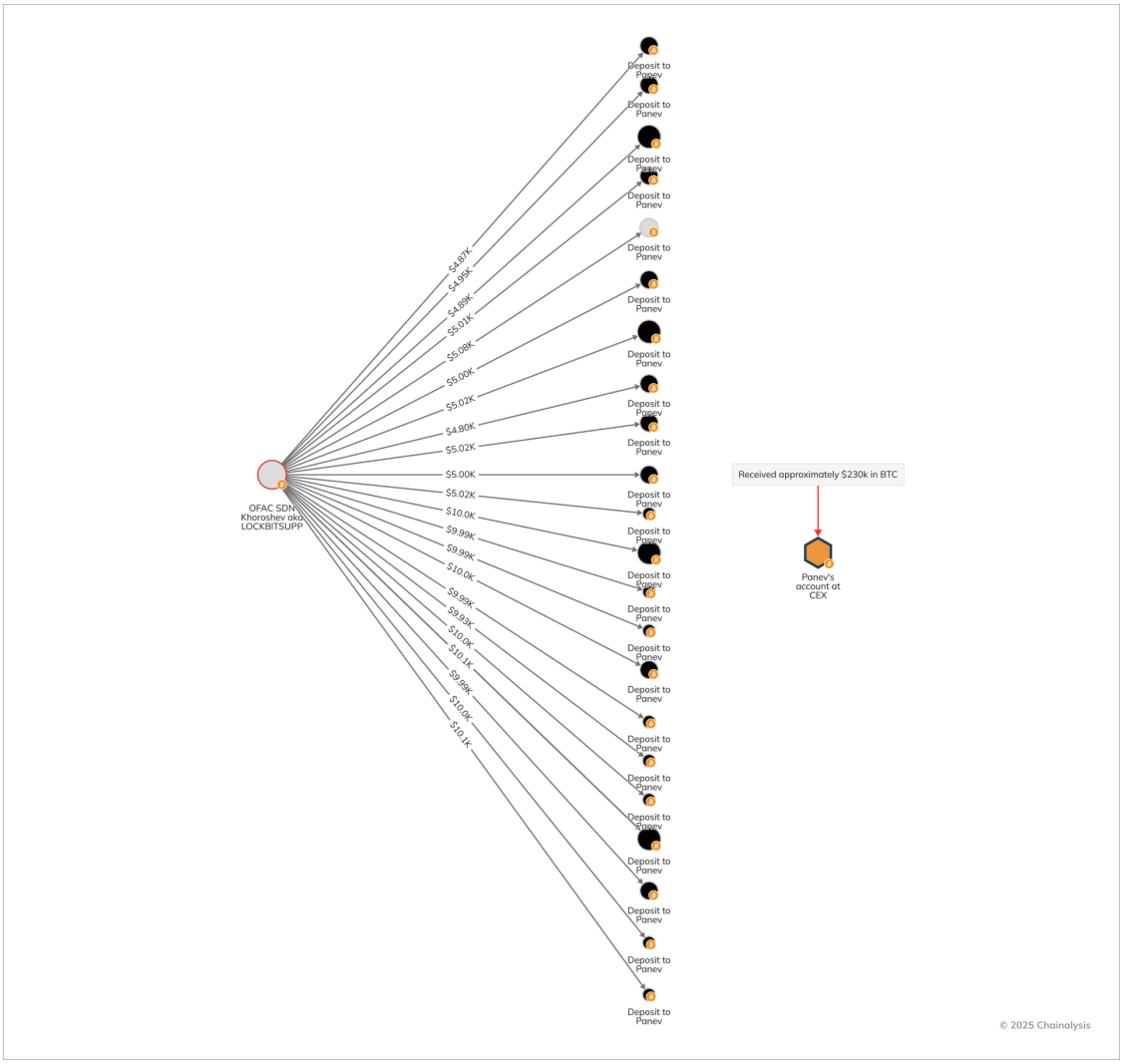
While numerous factors are likely behind any one of the trends visible in the chart above, the decline in the use of no-KYC exchanges since October 2024 may be attributed to the designation of Russia-based exchange Cryptex and the German Federal Criminal Police (BKA)'s seizure of 47 Russian language no-KYC crypto exchanges — both in September 2024. The timing of those enforcement actions, coupled with the period when ransomware inflows to no-KYC exchanges dwindled, is conspicuous.

Ransomware case studies

Panev's arrest and its impact on LockBit's operations

Between 2019 and 2024, Israeli-Russian dual citizen Rostislav Panev allegedly played a crucial role in supporting LockBit. He is accused of developing several tools for the group, including one that enabled attackers to print ransom notes from any printer connected to compromised systems, for which he was reportedly paid around $230,000 in bitcoin (BTC). While Russian nationals, including LockBit's administrator Dimitry Yuryevich Khoroshev, have previously faced sanctions for their roles in these attacks, it is important to recognize that ransomware is truly a global threat, involving actors from around the world. Panev is currently in Israel awaiting extradition to the United States, where he is wanted for conspiracy to commit fraud, cybercrime, wire fraud, and other offenses.

In the Reactor graph we can see, per the indictment, the transfer of roughly $5,000 in BTC from Khoroshev on a biweekly basis beginning in 2022. Then, from July 2023 through early 2024, approximately $10,000 in BTC was transferred to Khoroshev on a monthly basis.

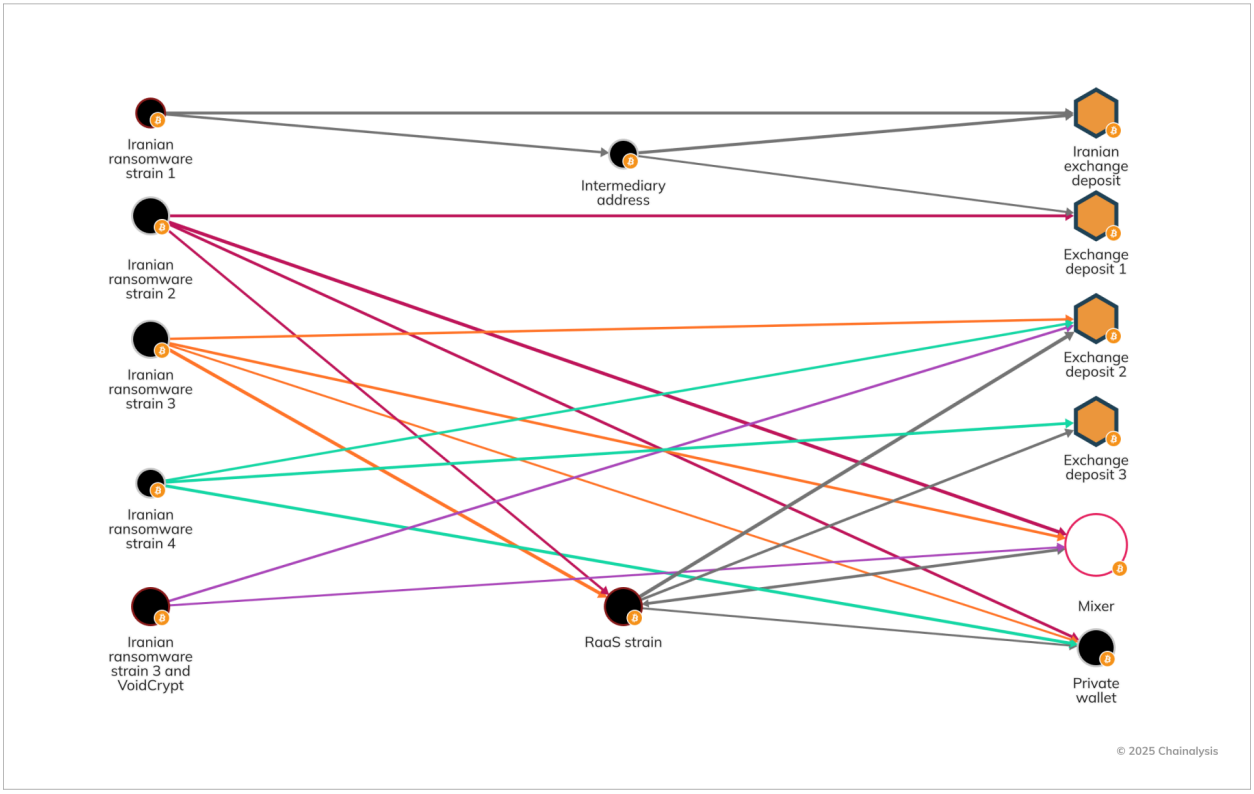


Panev's arrest potentially marked a significant blow to LockBit's ability to reconstitute, and highlighted that, even years after a crime has been committed, blockchain's transparent and immutable nature continues to empower law enforcement to trace illicit activities and disrupt transnational cybercrime syndicates. The LockBit takedown and Panev's arrest were major victories in 2024 and sparked a shift toward a more fragmented and less coordinated ecosystem.

Iranian ransomware involvement

In addition to Russian-speaking cybercriminals, within the past several years, Iranian nationals have also been sanctioned by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) for their involvement in facilitating and conducting ransomware attacks. We've also previously noted on-chain evidence of LockBit affiliates working with Iranian ransomware strains and depositing funds at an Iranian exchange.

Fortunately, through our on-chain analysis, we can identify Iranian actors as they rebrand or switch to a different RaaS. As we see in the below Chainalysis Reactor graph, we tied four different ransomware strains to the same Iranian threat actor, who likely also deployed a popular RaaS strain. We also see the reuse of deposit addresses at multiple global exchanges, connecting these seemingly disparate strains — not only to each other, but also confirming the operator's Iran ties.

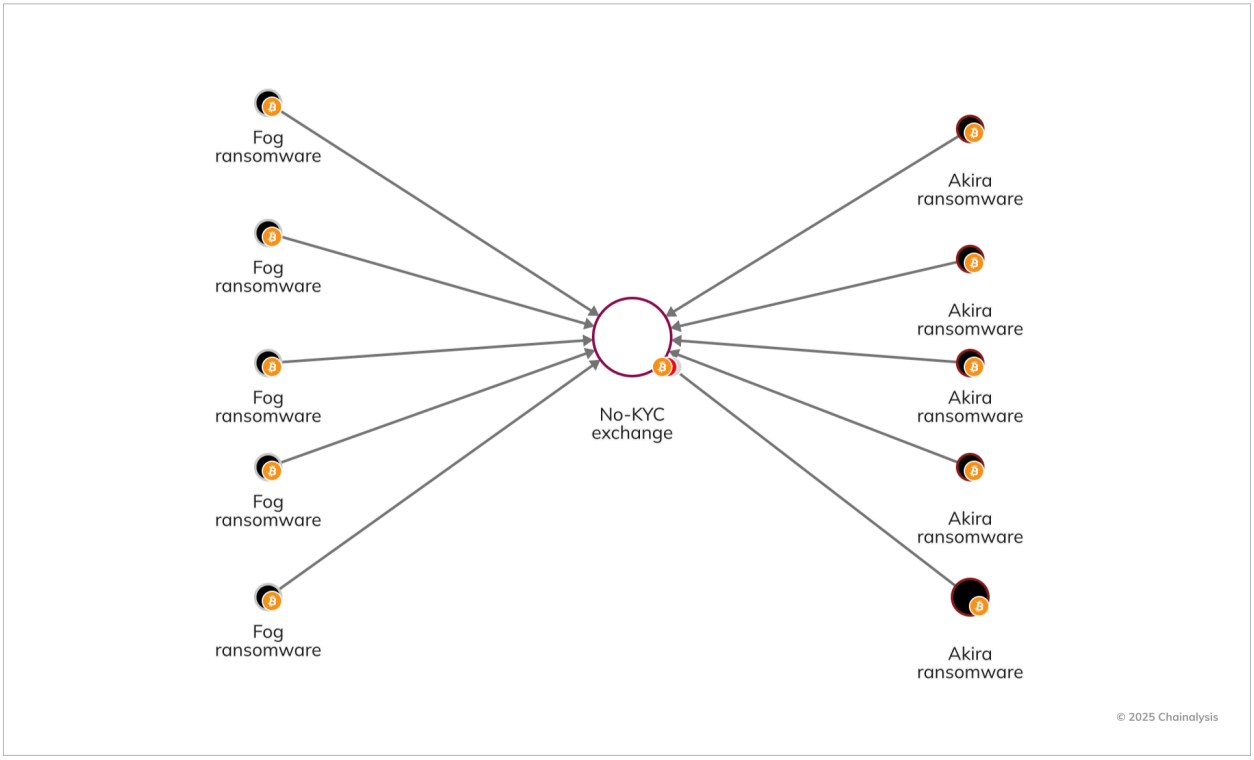


Major strains rebranding, launching offshoots

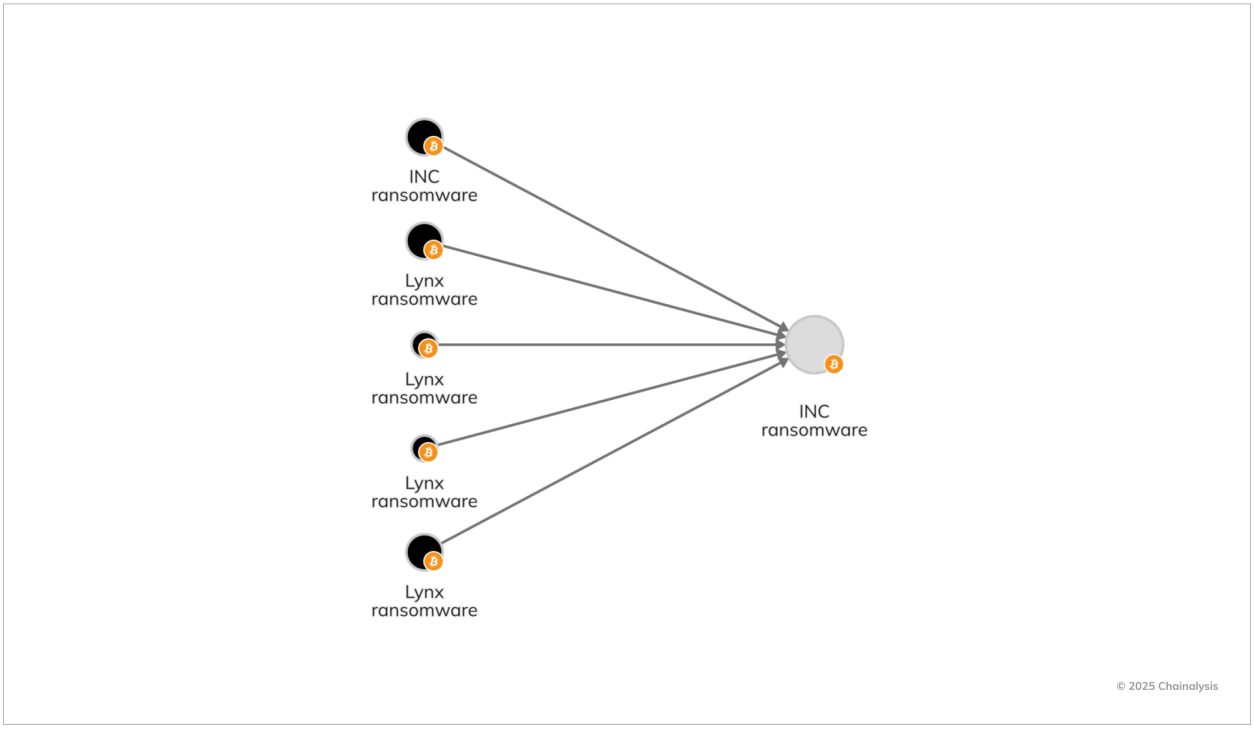
Since Akira's emergence, it has proven successful in exploiting vulnerabilities — particularly in enterprise environments — and has gained traction with a number of high-profile attacks. As we mentioned above, Akira is the only top 10 ransomware strain to have ramped up its efforts in H2 2024.

In September 2024, Fog, a new ransomware strain, entered the scene, and has since demonstrated an ability to target critical vulnerabilities, much like Akira. Both groups have primarily focused on exploiting VPN vulnerabilities, which allows them to gain unauthorized access to networks and consequently deploy their ransomware.

Both Akira and Fog have used identical money laundering methods, which are distinct from other ransomware strains, further supporting a connection between them. For instance, the following Chainalysis Reactor graph shows that several wallets operated by Akira and Fog have transferred funds to the same no-KYC exchange.



In addition to Akira's relationship to Fog, we have also discerned links between the INC and Lynx ransomware variants by examining similar on-chain behaviors. Cybersecurity researchers have also noted the two strains' shared source code.



These overlapping relationships illustrate a broader trend within the ransomware ecosystem: the continuous evolution of cybercriminal strategies in response to increased law enforcement scrutiny.

Navigating an evolving threat landscape

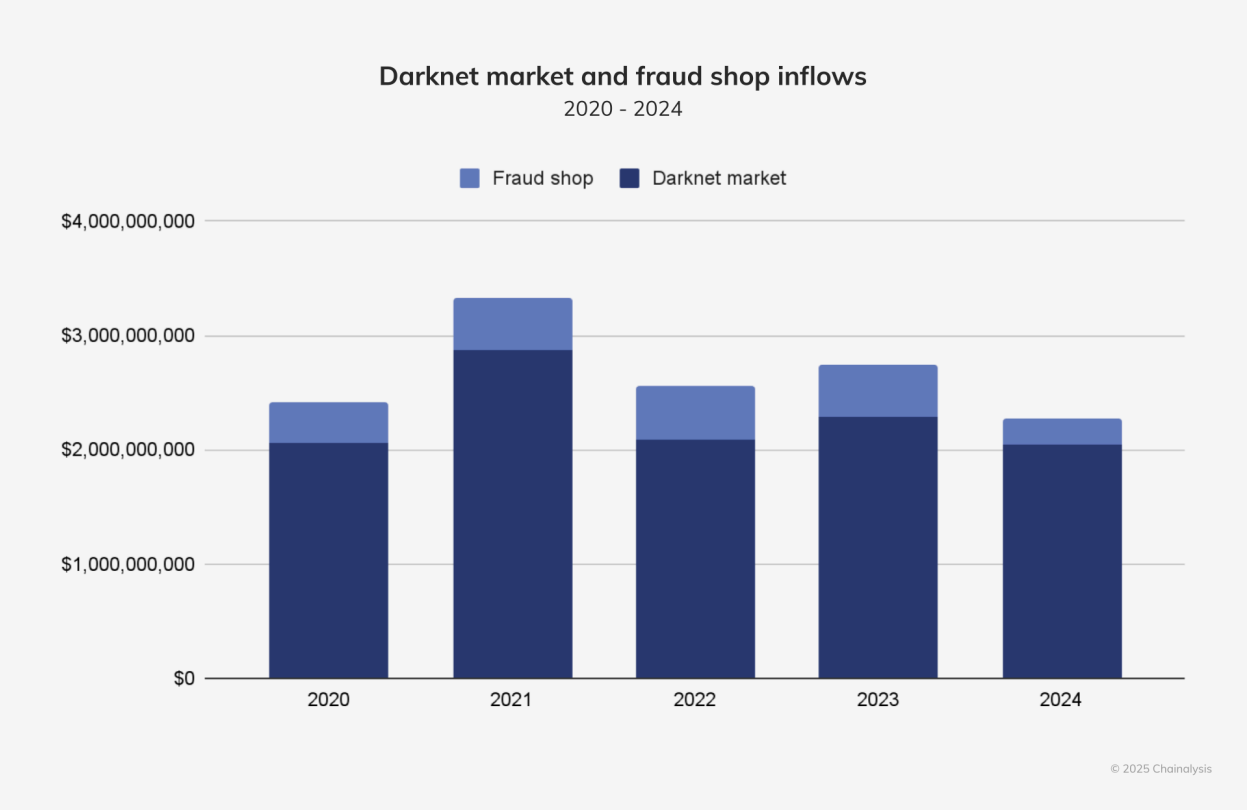
Ransomware in 2024 reflected shifts driven by law enforcement action, improved victim resilience, and emerging attack trends. Crackdowns and collaboration with incident response firms and blockchain experts helped disrupt many ransomware groups, reducing their profitability. Victims also demonstrated greater resistance to ransom demands, widening the gap between demands and payments.

Financial strategies continue to adapt under law enforcement pressure, although malicious actors face increasing difficulties laundering payments from victims. Sustained collaboration and innovative defenses will remain critical to building on the progress made in 2024.

Darknet Markets

Darknet market and fraud shop BTC revenues decline amid years-long international law enforcement disruption

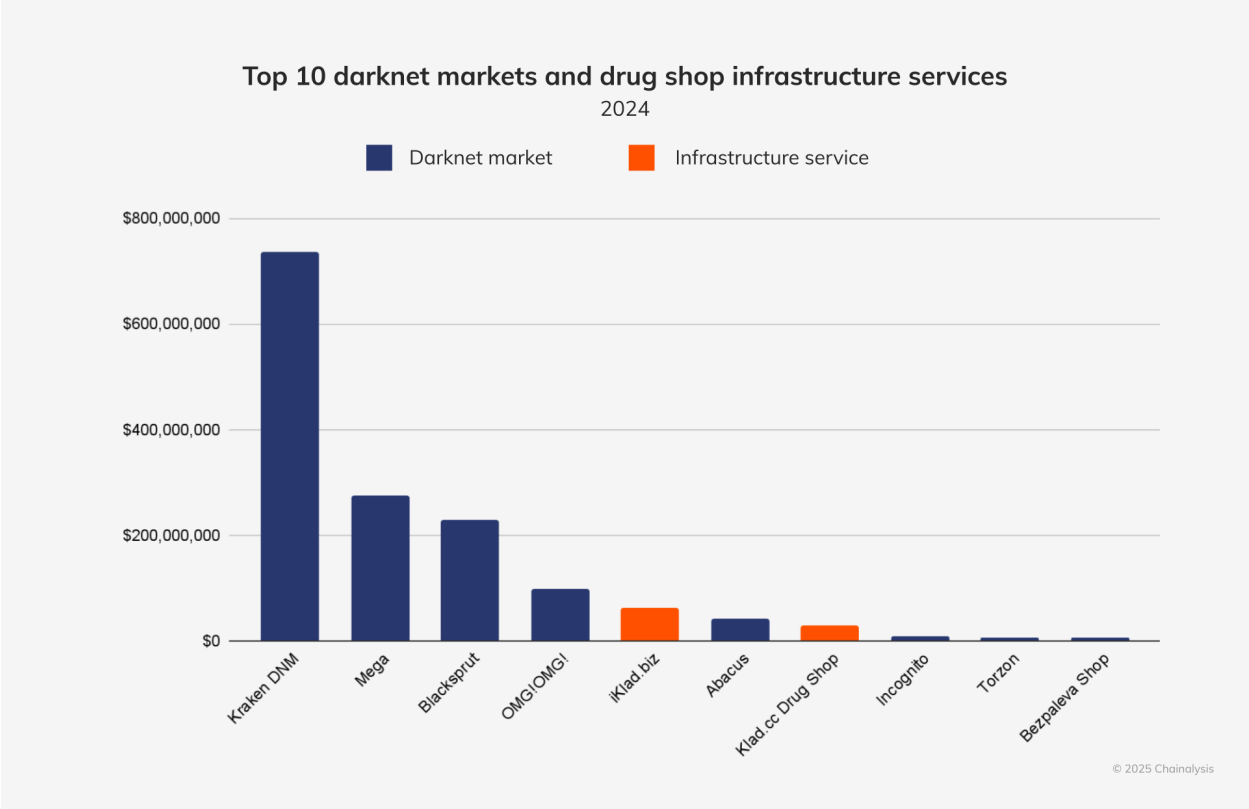
A series of law enforcement takedowns in the last few years have shaped the 2024 drug and fraud ecosystems. While 2024 was likely a record year for crypto crime revenue overall, darknet market (DNM) and fraud shop inflows fell, with DNMs receiving just over $2 billion in BTC on-chain, and fraud shops $225 million.



Historically, DNMs have been known for the illicit drug trade, but in recent years have differentiated themselves with unique service offerings. This trend, however, is not universal. For example, in Russia-based DNMs, the illicit drug trade remains predominant. Since last year's Crypto Crime Report, the top performing Russia-based DNMs have held steady, but Kraken DNM overtook Mega as the leading DNM by annual revenue in 2024.

While Mega's inflows declined by more than 50% year-over-year (YoY), Kraken DNM's rose nearly 68% YoY. Kraken DNM, which billed itself as Hydra's Market's successor, received $737 million on-chain in 2024.

Blacksprut, which rose to prominence with Mega in the wake of Hydra's 2022 sanctions designation, law enforcement seizure, and subsequent collapse, came in third with 13.6% less revenue YoY.



As reported last year, some drug shops have been outsourcing services like website hosting and payment processing. iKlad.biz and Klad.cc, shown in the chart above, are examples of those infrastructure providers. While these outfits are not traditional DNMs, their success highlights how drug vendors are scaling their operations throughout Russian-speaking countries. In spite of Hydra Market's disruption in 2022, former Hydra affiliates still found operating in today's DNMs rely heavily on these infrastructure providers. Last December, a Russian court imposed a life sentence on Stanislav Moiseyev, Hydra Market's suspected founder and operator, although the Moscow prosecutor's office did not publicly tie the guilty verdict to Hydra. The court also sentenced fifteen accomplices to anywhere from eight to 23 years in maximum-security penal colonies.

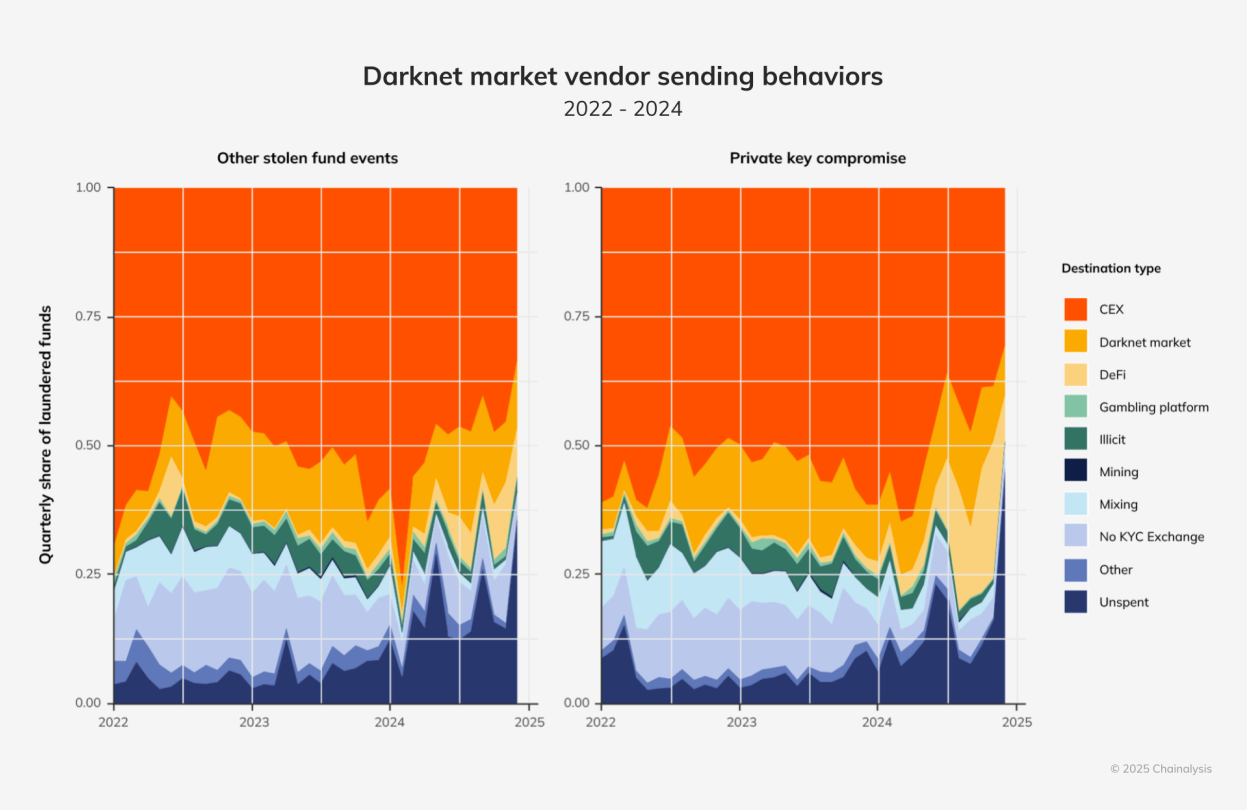
Besides Hydra operators, other DNM administrators faced criminal prosecution in 2024. In March, Incognito Market's administrators conducted an exit scam. The FBI tied Taiwanese national Rui-Siang Lin, Incognito's operator, to the DNM's website by tracing crypto transfers to an exchange account in Lin's name. Lin was charged with a host of crimes, and by May, federal authorities in New York had arrested him.

Nemesis Market also saw its demise in March, when German authorities seized its infrastructure, along with $102,000 in cryptocurrency.

As international authorities have disrupted DNMs large and small in the last few years, cybercriminals and drug dealers have learned firsthand the consequences of running BTC-accepting DNMs given the currency's inherent transparency. Many operators have since moved to accepting only Monero (XMR), a privacy coin with features designed to boost anonymity and reduce traceability. XMR activity falls outside the scope of this report.

Darknet market vendors evolve their on-chain behavior

Historically, DNMs have usually cashed out their funds at centralized exchanges (CEXs). Although CEXs remain a stable destination in the DNM ecosystem, the pattern of sending funds to them shifted in 2024, as illustrated in the chart below. Last year, DNM vendors sent a significantly higher portion of their funds to DeFi than they did historically. This trend is notable since DNMs operate largely in BTC or privacy coins. Throughout 2024, DNM vendors also sent far more value to personal wallets and stored funds on-chain. Retail vendors appear to be holding a greater portion of their proceeds on-chain than wholesale vendors, while wholesale vendors (those who distribute drugs in large quantities) are making greater use of DeFi.

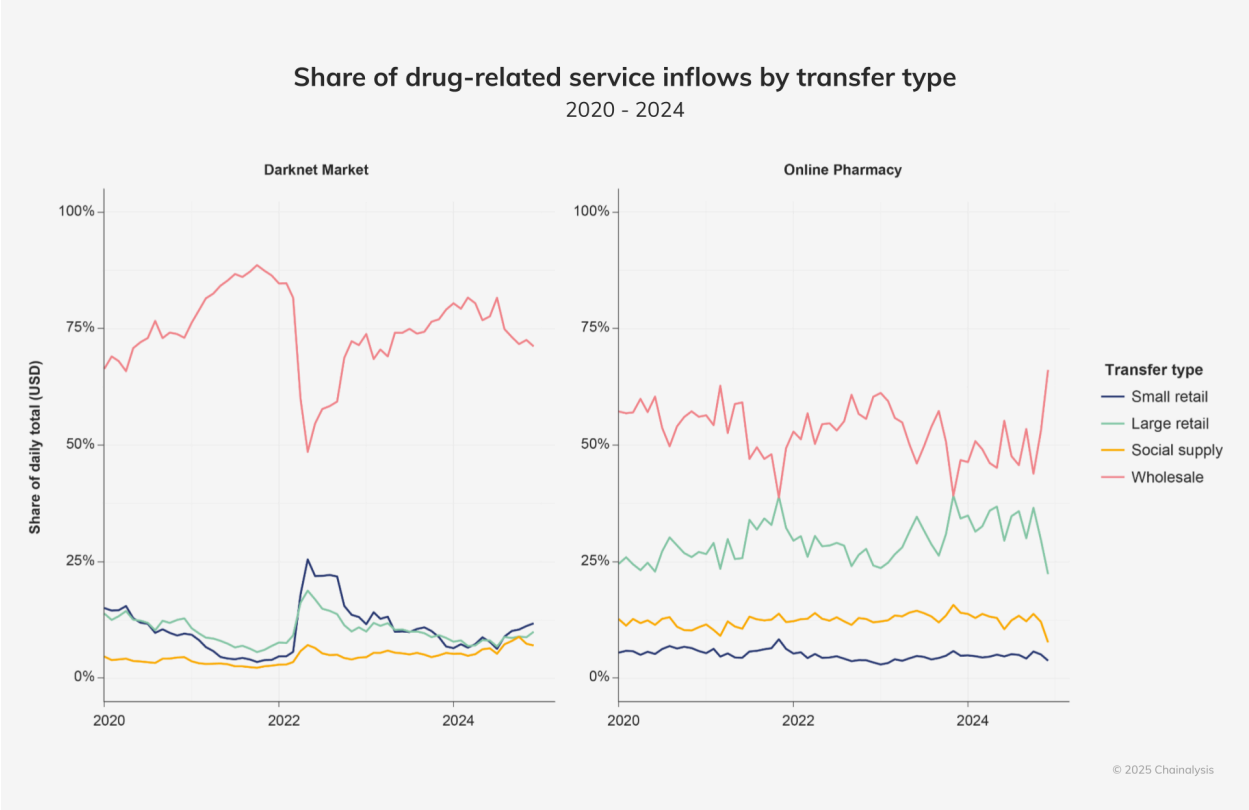


Darknet market and online pharmacy inflows according to drug-purchasing behaviors

When looking at crypto inflows to DNMs in 2024, the data indicate that wholesale drug purchases were dominant, averaging between 71 and 81% of this year's total market share. For online pharmacies, wholesale purchases led in 2024, followed by large retail.

Below are definitions for DNM purchase categories, based on purchase sizes, from which we infer buyer intent:

- **Small retail.** Less than $100, likely made for personal consumption.
- **Large retail.** Between $100 and $500, also likely made for personal consumption.
- **Social supply.** Between $500 and $1,000, indicating customers may be sharing drugs with third parties in social settings.
- **Potential wholesale.** Over $1,000, more likely made by drug sellers and distributors.



When examining drug-purchasing habits from DNMs spanning 2020 to 2024, some patterns emerge, in particular about wholesale activity, that is, purchases likely made by organizations with the intent to redistribute. First, the major drawdown in DNM wholesale revenue in 2022 can be attributed to the Hydra Market takedown. Second, while wholesale drug purchasing revenues have steadily climbed since that drop, they have yet to regain their former highs. This could indicate that:

1. No DNM since Hydra has established itself as the premier destination for wholesale drug purchases.

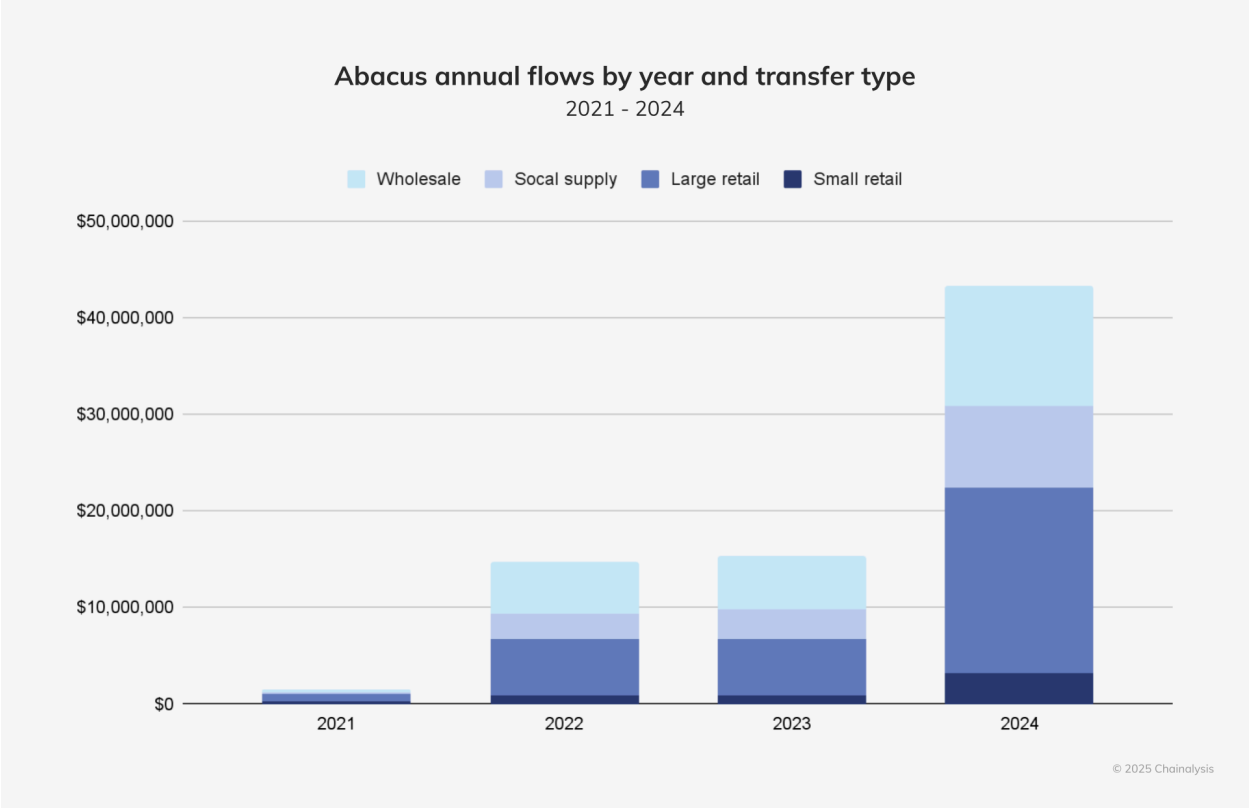
2. Global law enforcement operations are becoming increasingly effective in disrupting markets that cater to these purchasers.

3. Sellers and vendors are resorting to other channels, like instant messaging platforms, and/or payment methods for illicit drug trade.

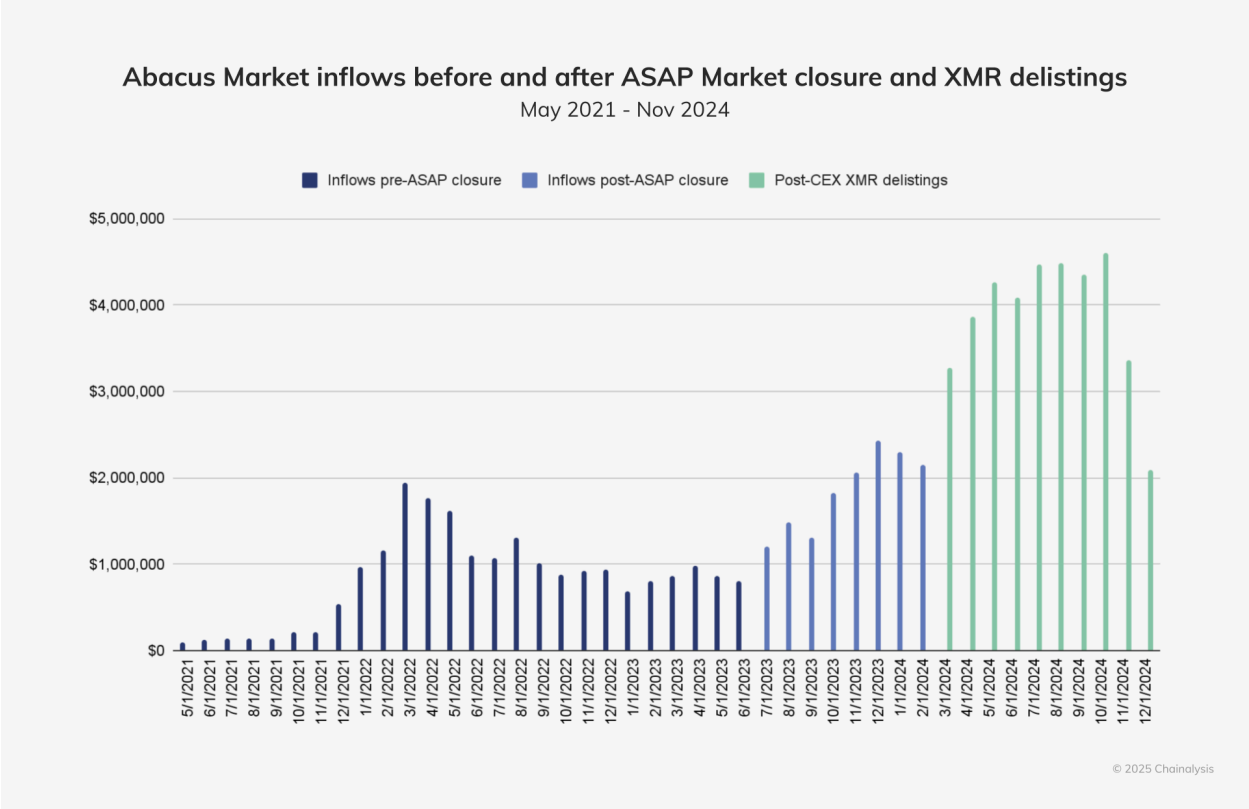
As for online pharmacies, these have predominantly catered to wholesale and large retail customers in the last several years, and 2024 saw growth in wholesale purchases toward the end of last year. Like DNMs, online pharmacies receive most of their revenues from larger drug resellers.

Abacus Market: Facilitating illicit drug trade

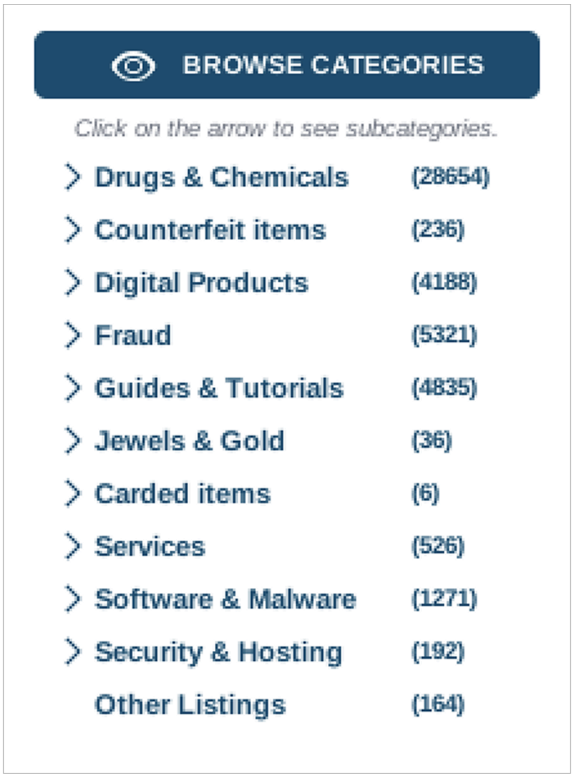
In 2024, Abacus Market was the highest-earning DNM serving Western customers. Last year, Abacus Market received $43.3 million on-chain.



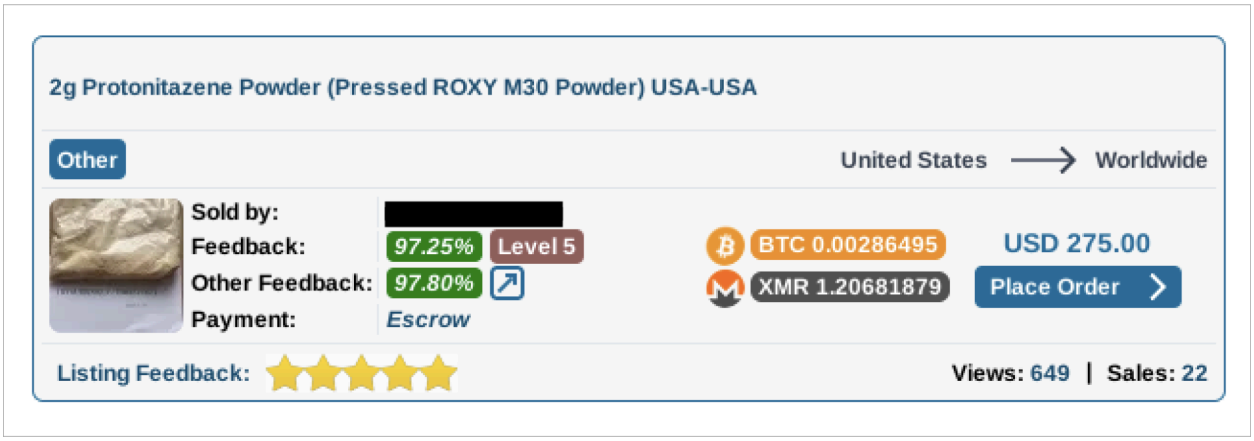
Since 2021, Abacus Market's revenue has increased substantially, and in 2024, it more than doubled, growing by 183.2% YoY. This increase may be due in part to the closures of top DNMs, the shift to the exclusive acceptance of XMR by other active markets, and delistings of XMR by popular centralized exchanges. The below graph shows an increase in Abacus sales (in BTC) following the closure of ASAP Market in July 2023, and a further increase following some CEXs delisting XMR.



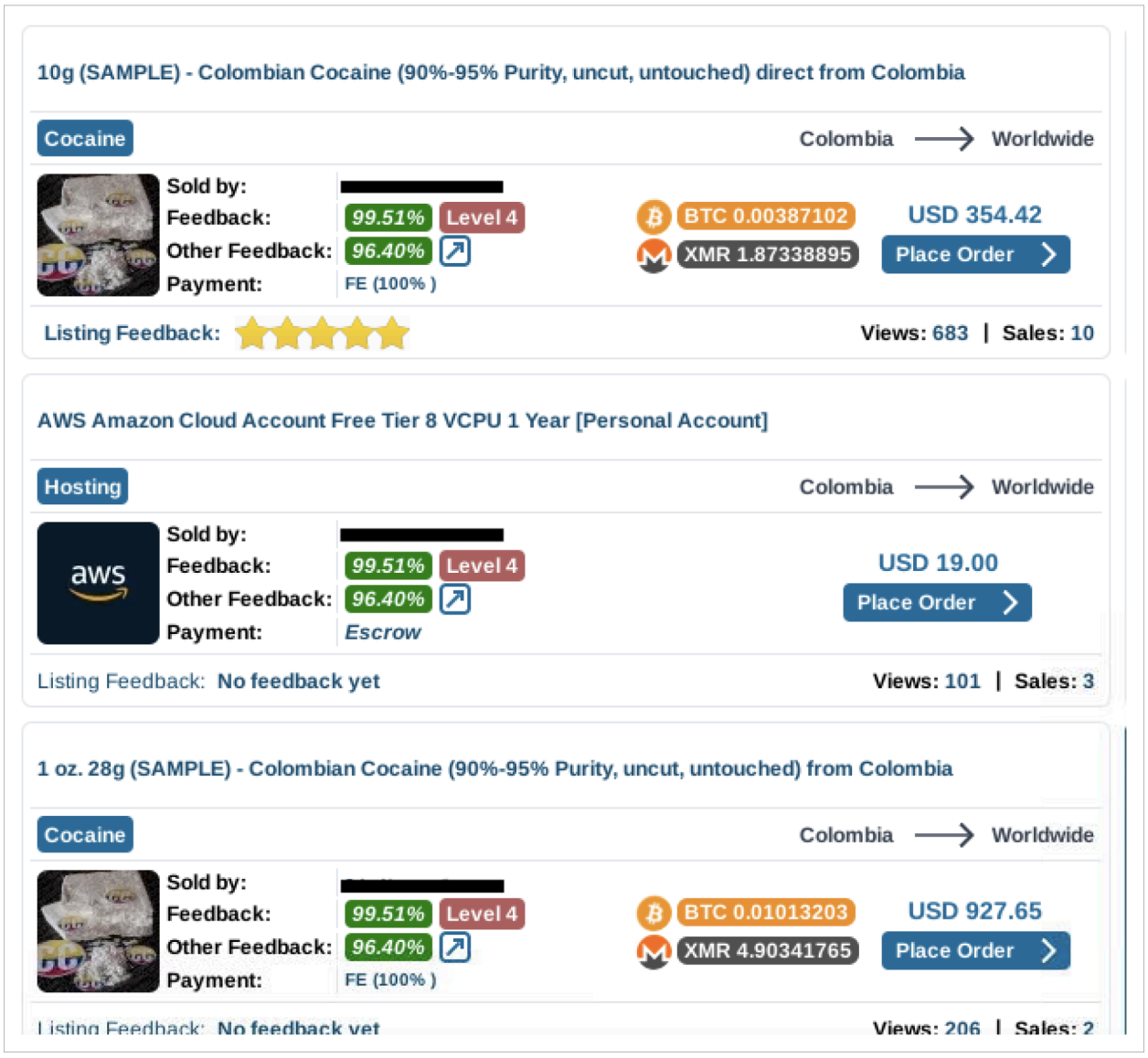
Abacus Market has a global presence and broad product offering. Below is a screenshot from the Abacus Market website showing the range of items it sells, with drugs and chemicals representing the overwhelming majority of its products.



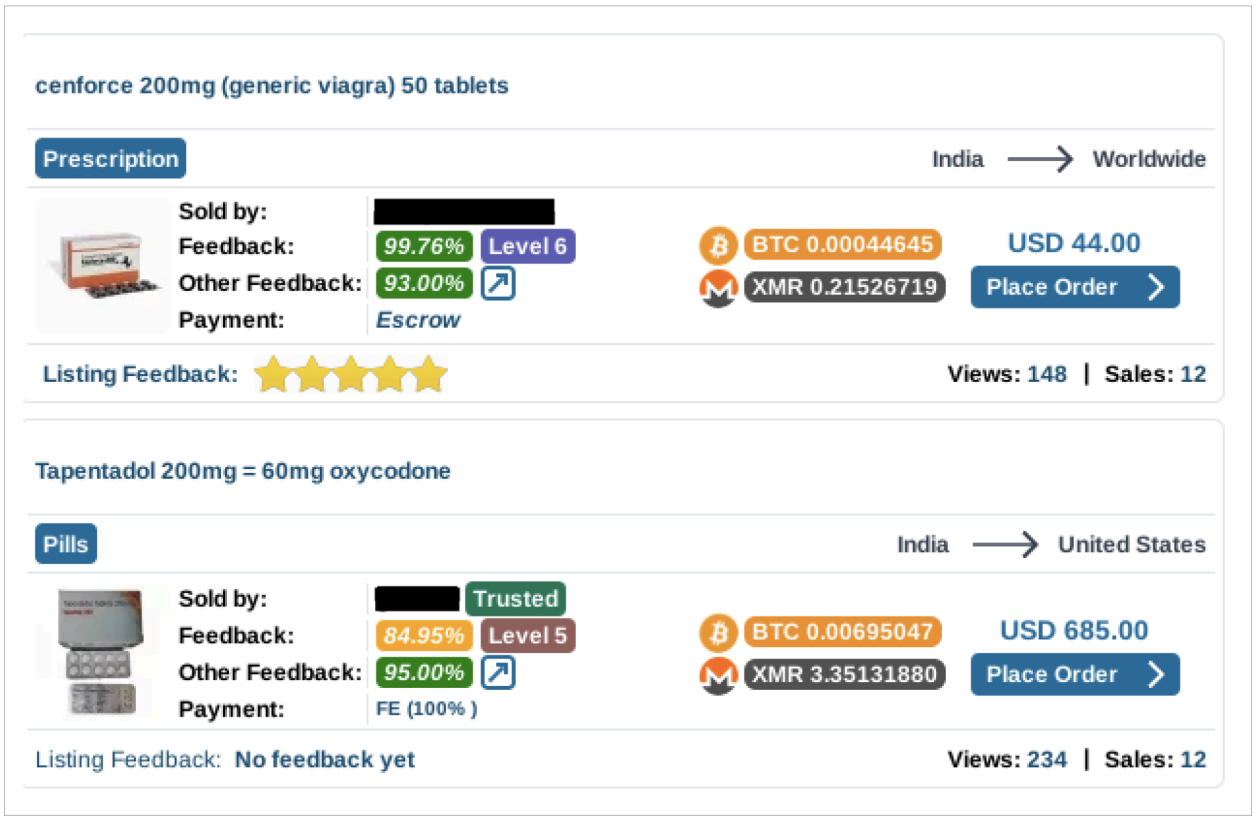
On Abacus Market, the US, Canada, Germany, Australia, and the UK have the highest number of listings. In the US, there's a large diversity in the types of products sold, including counterfeit pills. For example, in the screenshot below, an American vendor lists protonitazene powder, and advertises its uses as a counterfeit for oxycodone, also referred to as "M30" (i.e. 30 mg).



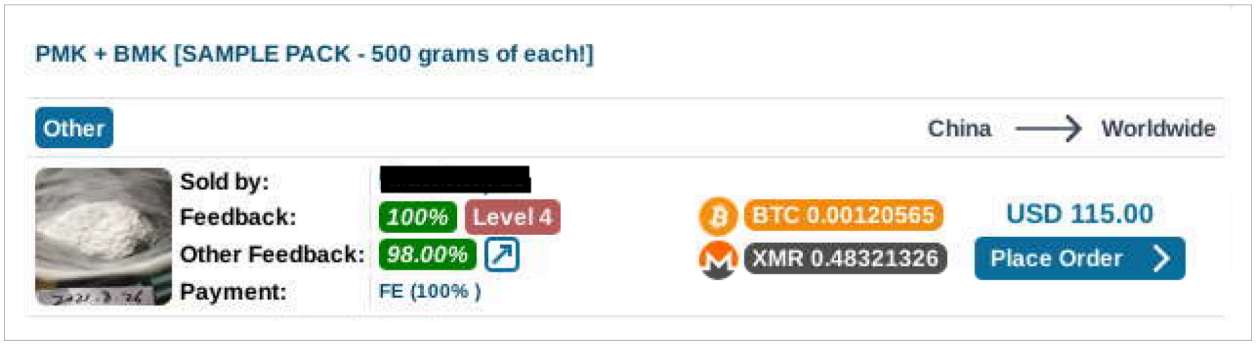
While the US market is best characterized by its diverse product offerings, other countries offer regional specialties. In Colombia, for instance, many of the vendor listings are for cocaine or Infrastructure-as-a-Service, as seen in the screenshot below.



Some countries have just one or a few vendors with a loyal customer base and a wider selection of goods. For example, in India, one of the most frequent listings is for generic medication, which mostly comes from the first vendor shown below.



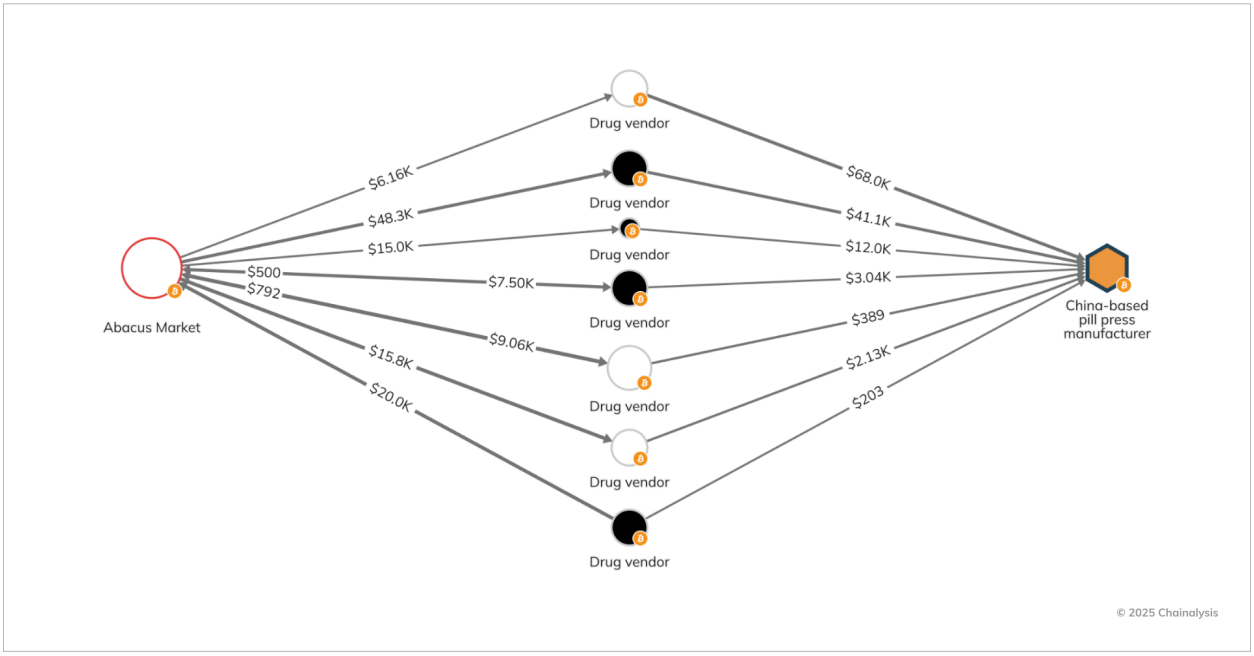
China-based Abacus vendors have many listings for research chemicals. They also sell PMK and BMK, which are precursors to MDMA and methamphetamine, respectively.



Darknet market connection to Chinese pill press manufacturers

While China-based vendors are frequently referenced as the source of precursors for dangerous synthetic drugs, their involvement in machinery sales is also an important aspect of the drug supply chain. One

China-based pill press manufacturer which advertises on clearnet business-to-business (B2B) websites has on-chain ties to drug vendors on Abacus Market. Along with its listings for large pill press machines, the vendor does not hide the sale of Oxycontin and Xanax TDP die kits, which are used to press counterfeit pills. The vendor accepts BTC and XMR, and analyzing its on-chain exposure to regional CEXs and DNMs reveals that it serves customers worldwide, including in the United States, Canada, Sweden, and Russia. The Reactor graph below shows this vendor's connection with drug vendors on Abacus Market.



While not all are pictured above, in total, we found 16 vendors either selling or sourcing drug material from Abacus and purchasing production supplies from this China-based vendor.

China-based vendors and novel synthetic opioids

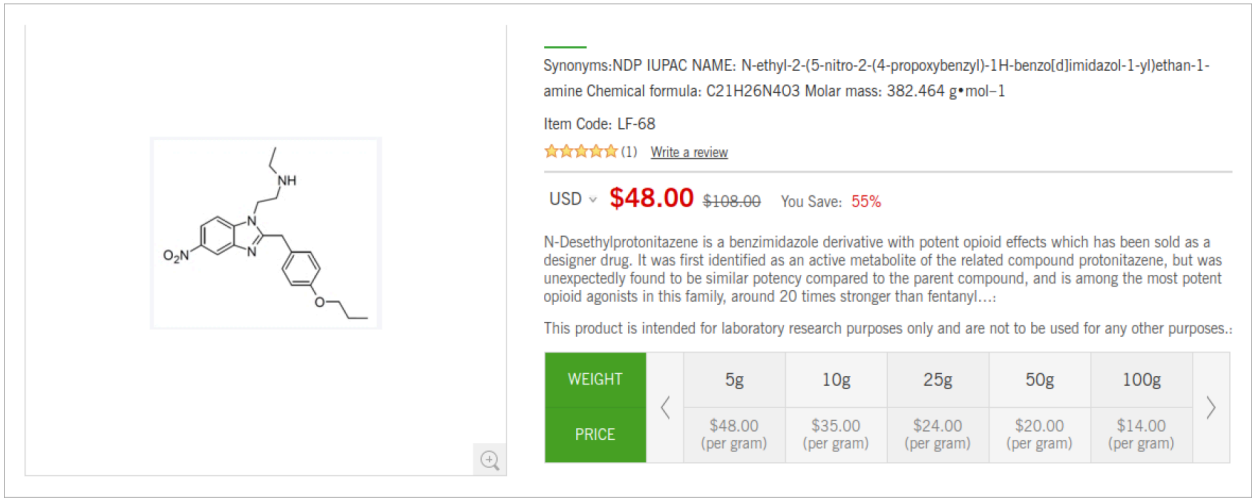
China-based precursor manufacturers mark the beginning of the synthetic drug supply chain. In years past, these organizations were more overt in their display of such products, openly advertising on mainstream B2B websites. Depending on the severity of the chemical, some manufacturers still follow this practice.

In 2024, however, many vendors of reagents and precursors have turned to criminal forums to advertise their product offerings, or have delisted (at least publicly) chemicals related to fentanyl synthesis. This could be in response to increasing pressure from the United States and China, and the crackdown on the websites selling these products. The organized crime section of this report, which discusses the nexus between Mexican cartels and Chinese fentanyl precursor manufacturers, indicates that this corridor still exists, although overall inflows to these manufacturers have seen a dip.

In addition to fentanyl, the presence of nitazenes in the global supply of dangerous synthetic opioids has increased, and China-based vendors have established themselves as the initial source. Nitazenes are a type of synthetic opioid with a similar potency to fentanyl. The US and Europe have seen an increase in

nitazine-related overdose deaths in recent years, perhaps due to the halt in the heroin supply following the Taliban's crackdown. Due to the novelty of these substances (and the fact that many are analogs) the true number of overdoses in Europe could be higher, as forensic drug testing may lag behind the pace of the crisis.

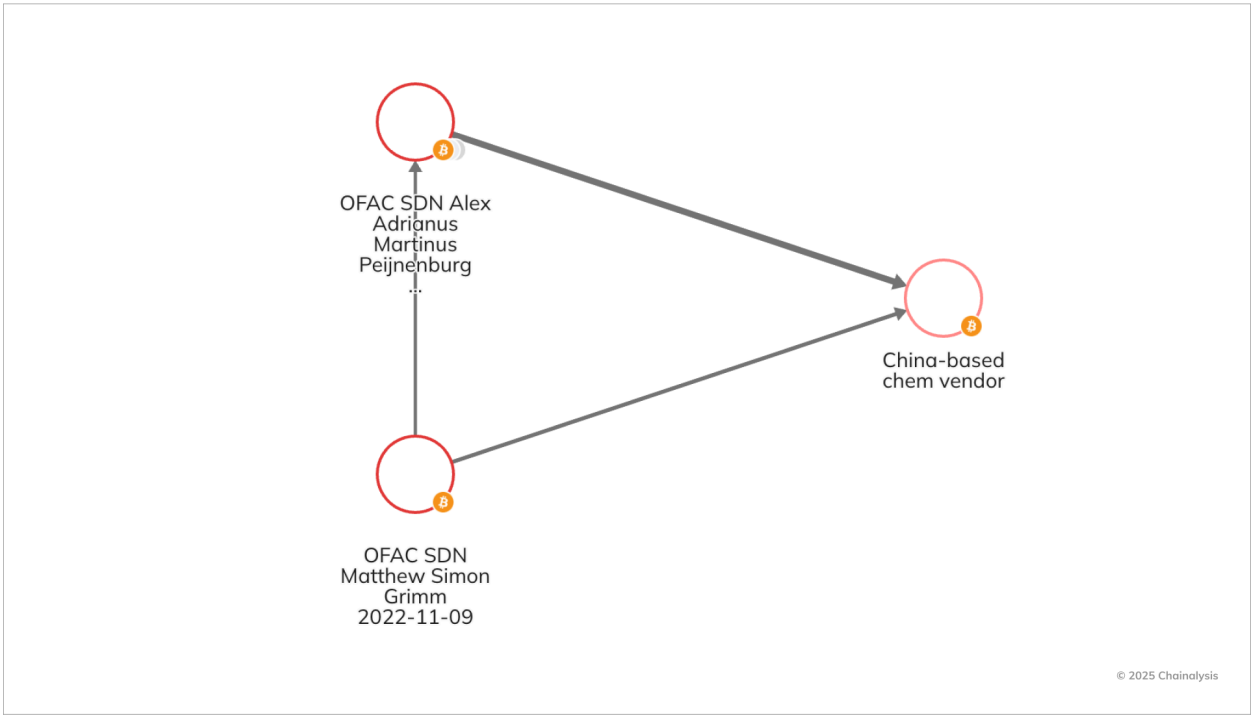
In addition to various benzodiazepines, stimulants, and psychedelics, one longstanding China-based research chemical manufacturer also sells nitazenes. The vendor's listing of a protonitazene analog boldly states that the compound has a potency 20x greater than that of fentanyl, as seen below. In this listing, the vendor offers free shipping to the US. Once received by the buyer, the compound could be pressed into counterfeit pills, like M30s, and further distributed to end consumers.



Screenshot from a China-based research chemical manufacturer's website

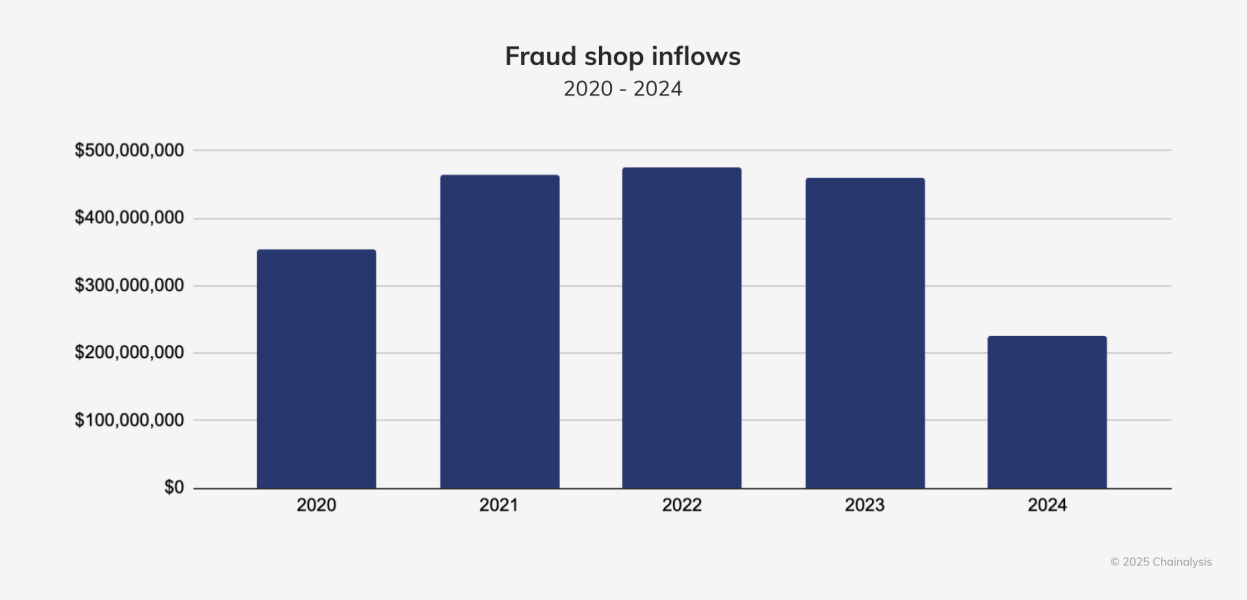
This vendor is known for supplying chemicals in bulk. Deposits span from the hundreds to the tens of thousands of dollars, and the average deposit amount in 2024 was over $2,000. On-chain data indicates the vendor supplies these drugs to other Chainalysis-identified online pharmacies and DNM vendors, all while maintaining a far-reaching global customer base throughout North America, Europe, Australia, and South America.

Interestingly, this vendor has also been a trusted supplier for OFAC-designated fentanyl traffickers Alex Adrianus Martinus Peijnenburg and Matthew Simon Grimm, having received close to $1.5 million in purchases from them.



Fraud shop revenues decline in 2024

Fraud shops are services found mainly on the dark web that sell stolen data and personally identifiable information (PII), which cybercriminals use for scams, identity theft, and ransomware attacks. In 2024, fraud shop inflows declined by 50% YoY, a sharp downturn from the last three years.



A few factors likely influenced this BTC revenue decline among fraud shops:

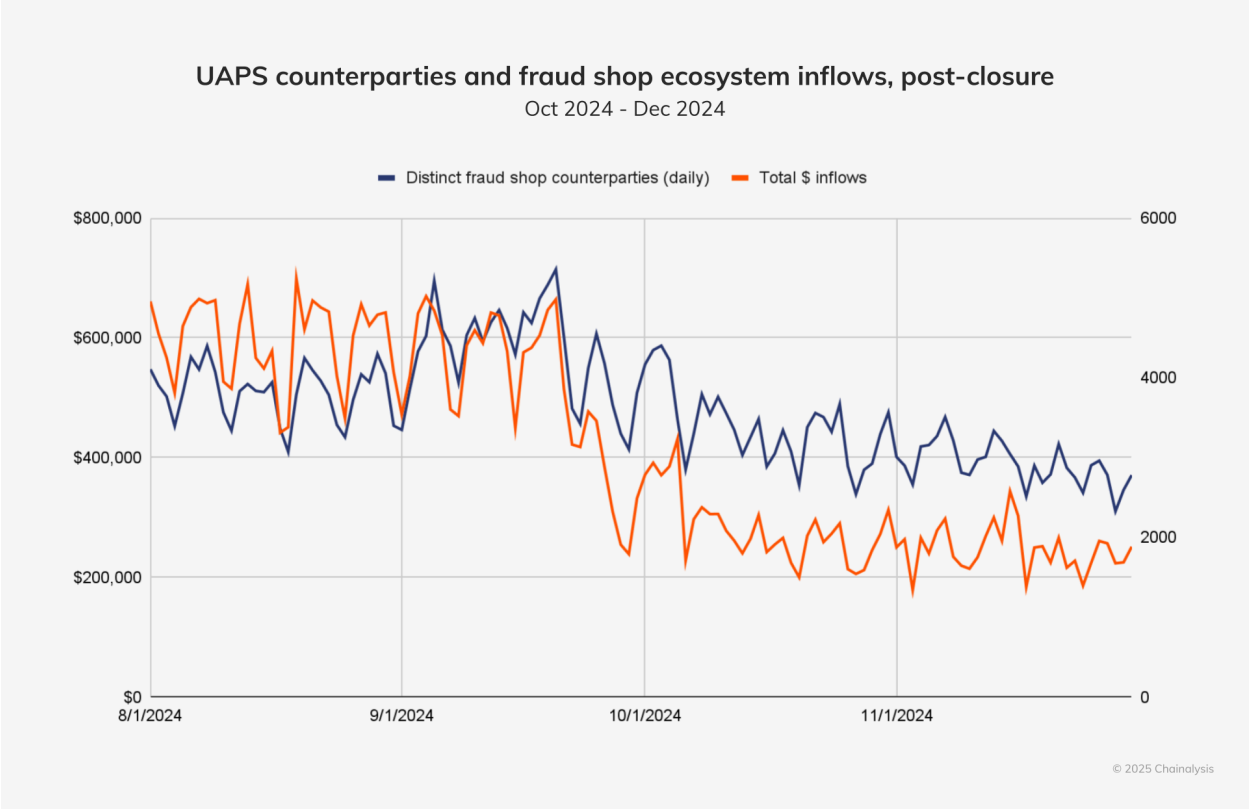
- The elimination of UAPS, a payment processor on which many fraud shops relied.
- US agencies and other international authorities prioritizing the takedown of fraud-related services.
- A migration away from BTC payments to XMR, as observed with DNMs.

UAPS: The takedown of a fraud shop payment processor and its impact on ecosystem

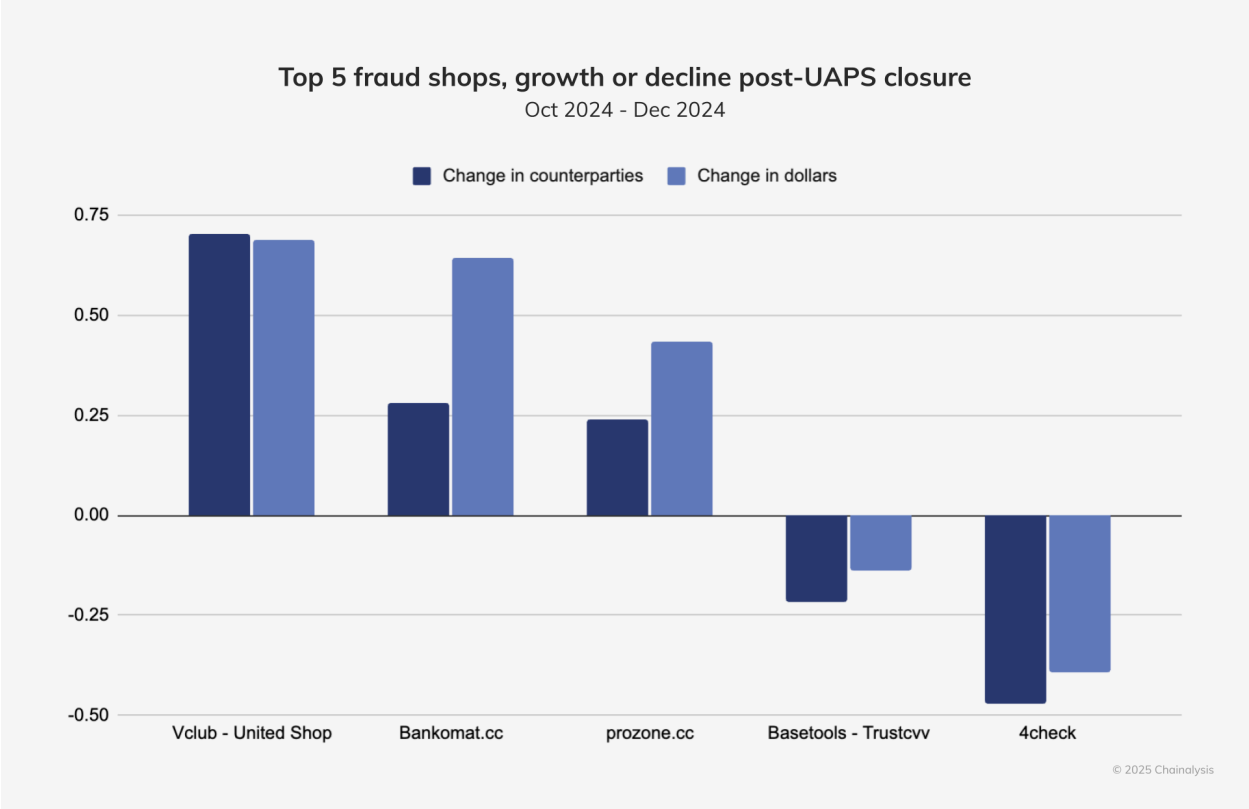
Last September, OFAC designated Sergey Sergeevich Ivanov, the alleged creator and operator of Universal Anonymous Payment System (UAPS), a payment processor used by many fraud shops, as well as PM2BTC, a Russian virtual currency exchanger associated with Ivanov, and Cryptex, a crypto exchange operating in Russia and registered in St. Vincent and the Grenadines.

These actions were part of a coordinated effort among US government agencies and foreign counterparts to combat Russian illicit finance. In September 2024, the US Secret Service's Cyber Investigative Section, Netherlands Police, and the Dutch Fiscal Intelligence and Investigation Service (FIOD) seized web domains and infrastructure linked to UAPS, PM2BTC, and Cryptex.

After the UAPS infrastructure takedown, we observed a swift decline in on-chain activity from UAPS counterparties, indicating that many fraud shops relied on this infrastructure to process customer payments. The chart below shows this counterparty decline, as well as a drop in crypto flows across the fraud shop ecosystem.



Conversely, some fraud shops saw an increase in activity and higher revenues on-chain. The chart below shows fraud shops that performed well after the UAPS takedown, indicating that the customer migration was swift, and favored longstanding, trusted fraud shops like Vclub and Bankomat.

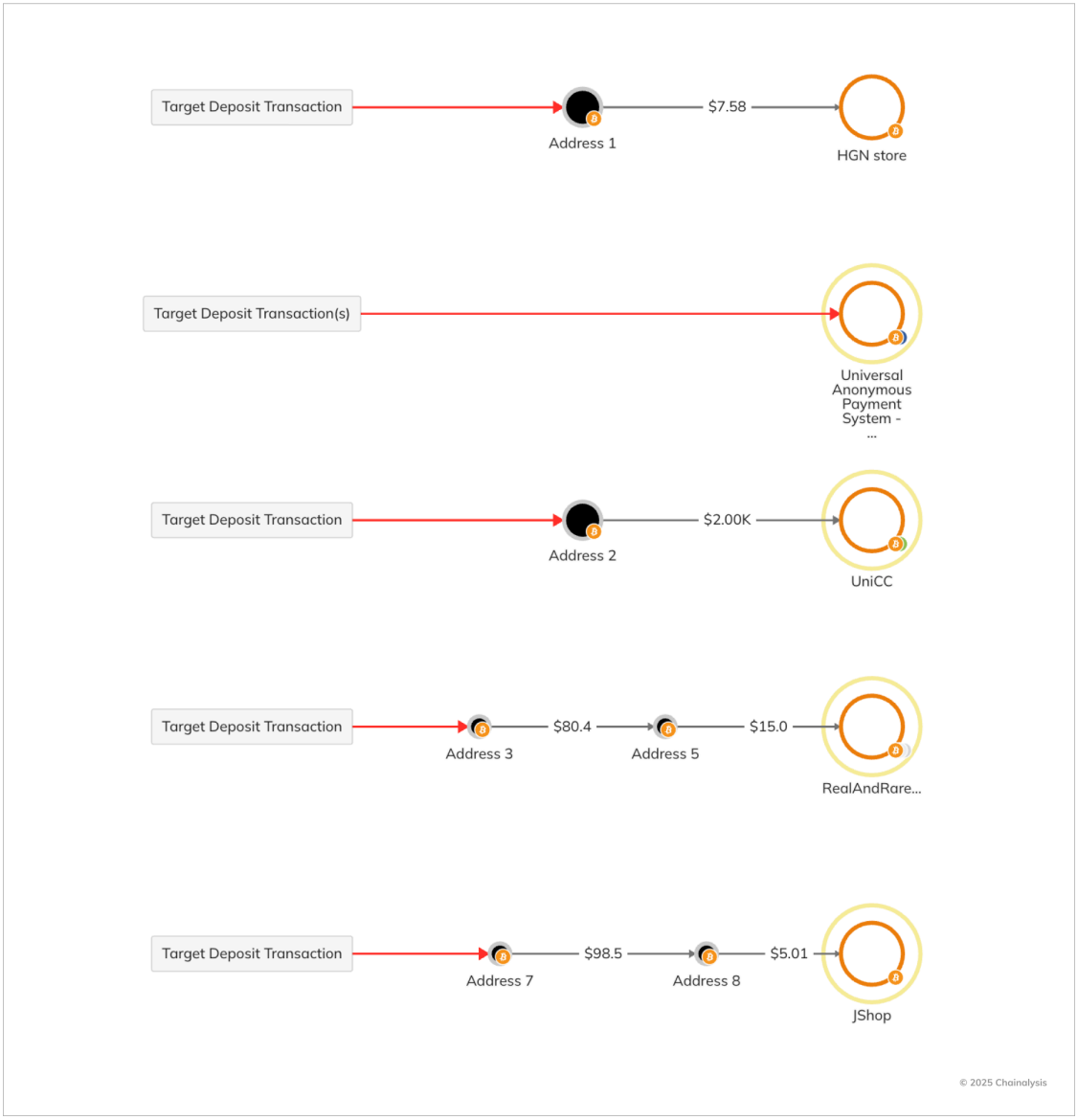


Revenues for the fraud shops on the right side of the chart declined, suggesting their dependence on UAPS for payment infrastructure.

The fraud shop-ghost gun connection: A case study

Ghost guns, assembled with prefabricated parts and without required serial numbers, are nearly always designed to be semi-automatic firearms, and are almost impossible to trace. Everytown, an organization that works to prevent gun violence in America, calls ghost guns a “weapon of choice for violent criminals” and extremists.

In 2023, the New York Police Department (NYPD) Intelligence Bureau, which predominantly handles counter terrorism cases, received a tip about two people in New York City involved in manufacturing and selling ghost guns. Using a series of search warrants and subpoenas, the NYPD found the suspects’ online raw material purchases, and uncovered a crypto dimension to the case, not publicly shared until now. Suspects were exchanging large sums of fiat for cryptocurrency by transferring cash into a mainstream CEX account and buying BTC, which they used to purchase stolen credit cards and identities from fraud shops on the dark web. The Reactor graph below shows five purchases made to fraud shops, four of which passed through intermediary addresses.



With these stolen credentials, the suspects purchased ghost gun parts and tools from a variety of legitimate websites, which they used to build ghost guns with a 3D printer, and sell for cash. A Manhattan district attorney successfully used this evidence to bring charges against one of the suspects.

Continued law enforcement efforts key to illicit market disruption

While DNM and fraud shop revenues declined in 2024 following years of concerted international law enforcement efforts, these platforms have managed to sustain their operations by adopting new tactics. In spite of disruptions to the dark web ecosystem, DNMs in particular continue to play a significant role in enabling the China-based synthetic drug production supply chain, highlighting the necessity for ongoing global cooperation to disrupt and dismantle illicit drug networks worldwide.

Market Manipulation

Suspected Wash Trading on Select Blockchains May Account for Up To $2.57 Billion in Trading Volume

In last year's report, we introduced a novel methodology for detecting suspicious trading patterns in crypto markets by analyzing on-chain data. We focused on decentralized finance (DeFi), given its transparency and the availability of on-chain information, which is not similarly available in centralized trading platforms. Our approach tracks patterns of behavior and not intent, which means that it is not by itself sufficient to prove market manipulation; however, it provides a valuable starting point for deeper investigations when combined with off-chain information. This focus on foundational insights is also why we do not estimate victim losses, as such calculations require significantly more data beyond on-chain analysis.

This chapter zeroes in on two prevalent forms of market manipulation: wash trading and pump-and-dump schemes. Wash trading involves artificially inflating trading volume by repeatedly buying and selling the same asset, creating a misleading perception of demand. Pump-and-dump schemes lure unsuspecting investors by driving up the price of an asset, often through coordinated hype, only for insiders to sell off their holdings at a peak, leaving unwitting holders of the asset with significant losses.

Keep reading as we delve into our methodologies for uncovering these suspicious patterns, providing a clearer view of how market manipulation manifests in the crypto space.

Heuristics enable identification of patterns of potential wash trashing, which show concentration in specific pools and among fewer actors

While there are subtle differences in the legal definitions of wash trading across jurisdictions, wash trades are generally understood to involve the near-simultaneous buying and selling of an asset without any change in beneficial interest, ownership, or market position.

Currently, most of the academic research on wash trading in crypto has been focused on centralized exchanges (CEXs), where possible motivations for inflating trade volumes include attracting users or climbing leaderboards. Unlike trading on CEXs, doing so on decentralized exchanges (DEXs) incurs gas fees, making wash trading potentially more expensive; nonetheless, such activity still exists.

Financial regulators around the world face challenges in identifying wash trading in traditional markets because collusion strategies vary and collusive transactions can be masked among normal trading activities. These challenges often take different forms in the crypto space, where pseudonymity, the use of decentralized platforms, and a lack of comprehensive regulatory oversight add complexity.

During our research, which primarily focuses on fungible tokens such as ERC-20 tokens and BEP-20 tokens, we encountered the following difficulties in identifying wash trading:

1. Maximal Extractable Value (MEV) bots and arbitragers share characteristics with wash trading, as they buy and sell the same token pairs in very short time intervals. However, this activity is not typically directed at driving up volumes, but rather at capturing arbitrage opportunities.
2. Most of the DEXs we studied are AMM-based (automatic market makers), rather than order book-based, as is common in most traditional financial markets. In order book-based markets, traders execute trades with a direct counterparty at a price set by one of the two parties to the transactions. In AMM-based markets, traders execute trades against a pool of assets supplied by liquidity providers at an algorithmically determined price. In the absence of a single trader sitting on both sides of a trade, it is more challenging to identify activity that would achieve a prearranged wash result. Additionally, because a trader lacks control over the quoted price for a transaction, it can also be challenging to determine whether the price is a result of an intentionally structured wash trade, rather than the price set algorithmically by the AMM.

Regardless, it is possible to look at on-chain activity to identify crypto addresses that exhibit patterns of potential wash trading activity, which we'll demonstrate with an analysis of two relevant heuristics.

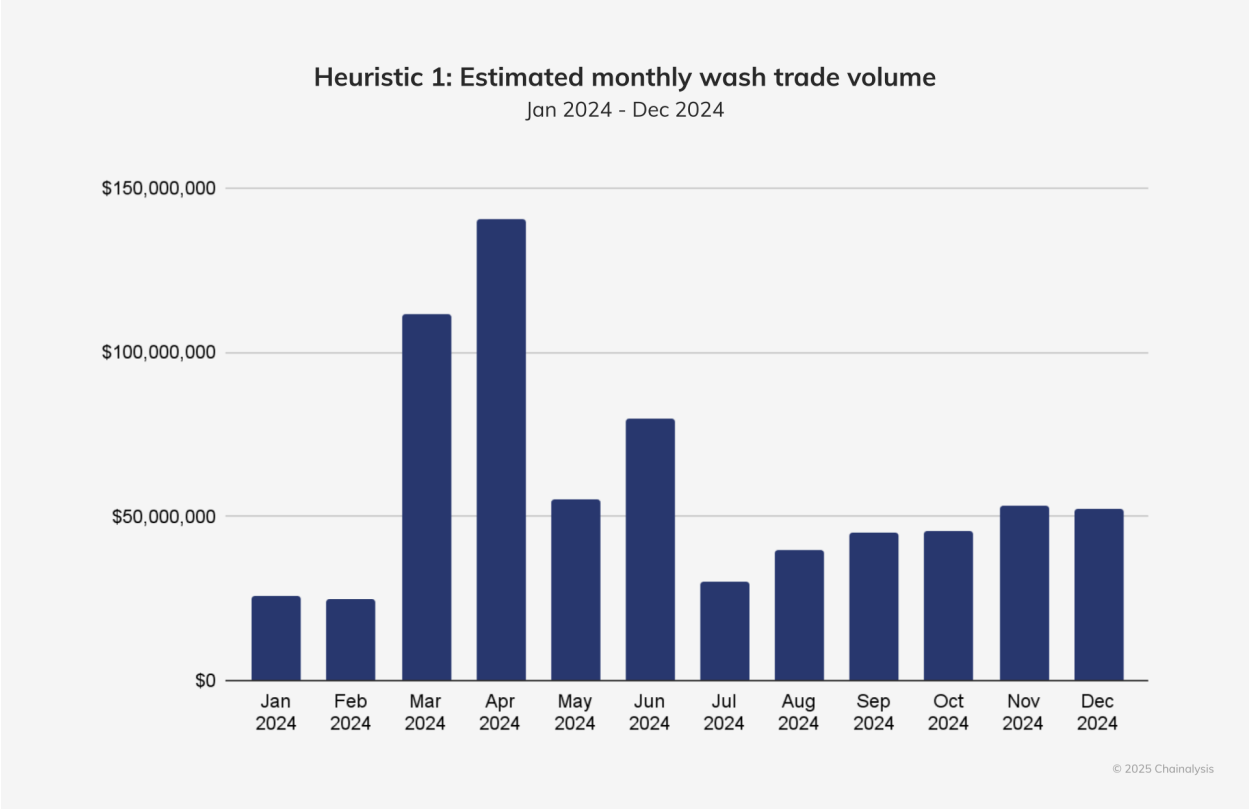
Wash trading Heuristic 1: matched buy and sell across transactions

For our first heuristic, we applied the following criteria to identify potential wash trades in a manner that avoids capturing MEV bot and arbitrager activity and excludes certain high-volume liquidity pools that are unlikely to be driven by wash trading. We looked for activity in which all three criteria were met:

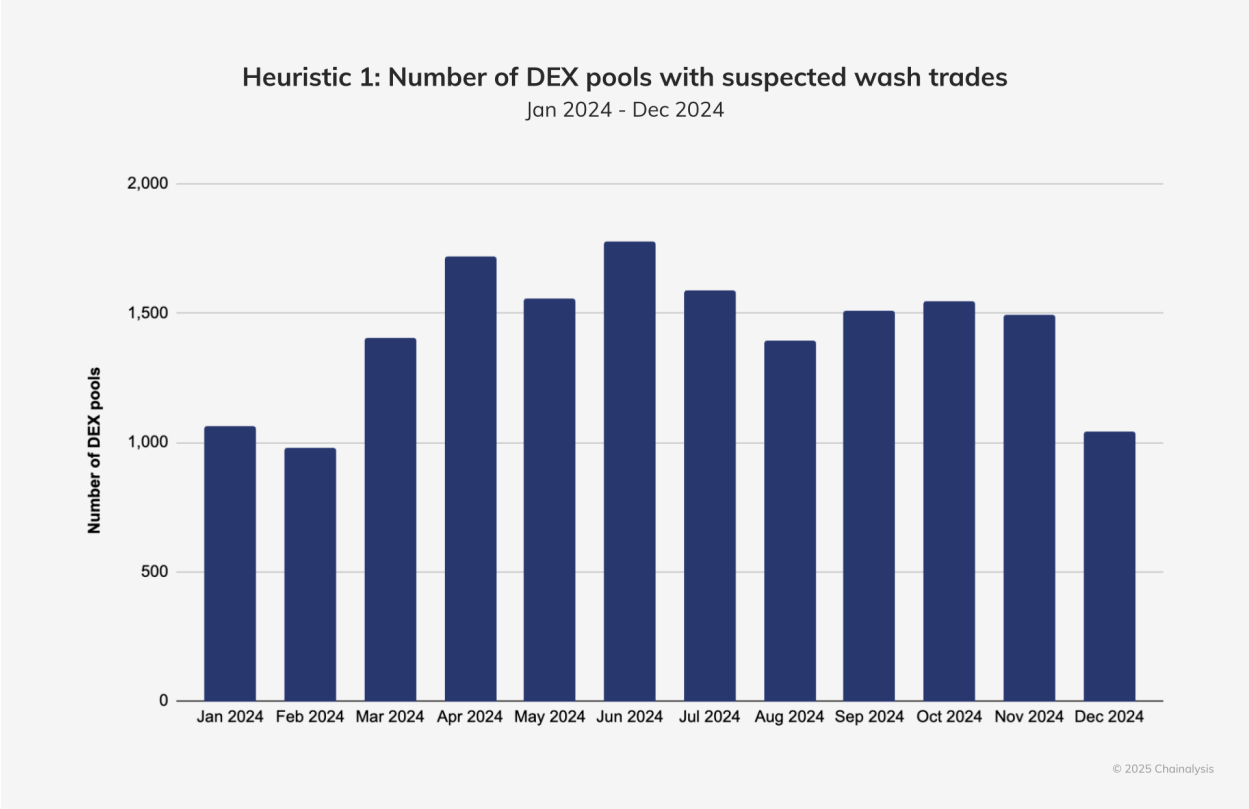
1. An address that executed one buy transaction and one sell transaction within 25 blocks (usually, 25 blocks are created within five minutes).
2. The difference in the two transaction volumes in USD is less than 1%, which suggests that the trade did not yield a meaningful profit.
3. A single address executed three or more trades that matched criteria 1 and 2 during the time period studied.

The first heuristic suggests that the combined wash trading volume on Ethereum, BNB Smart Chain (BNB), and Base was around $704 million in 2024. To put this into perspective, suspected wash trading volume identified by this heuristic accounted for 0.035% of the total DEX trade volume in November 2024.

The volume increases in March, April, and June in the below chart were most likely due to a few DEX pools with very active suspected wash trading.



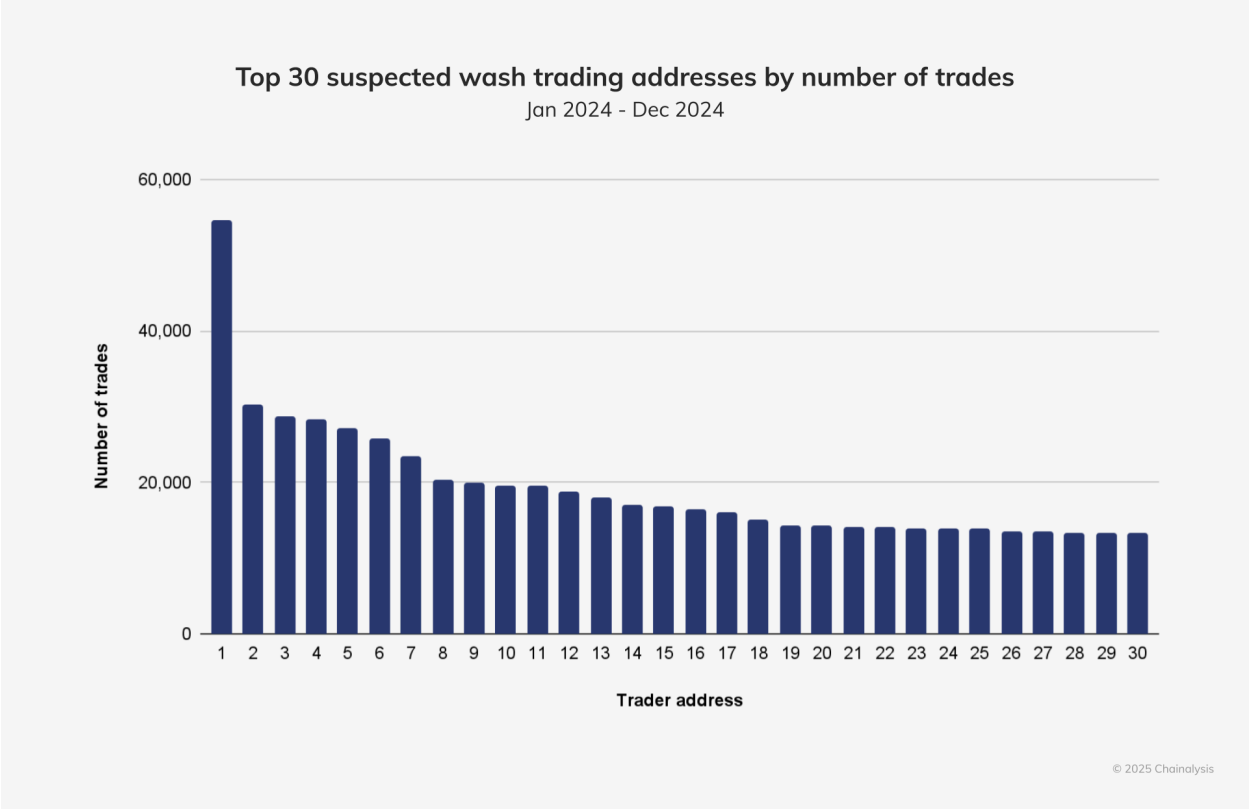
For instance, in April, five DEX pools accounted for a total of $78 million worth of suspected wash trading. Although suspected wash trading volumes fluctuated throughout the year, the number of DEX pools with associated activity remained fairly consistent, averaging around 1,000 to 1,800 pools per month, or between 0.2 and 0.3% of the approximately 500,000 pools active monthly, suggesting that wash trading may be concentrated in specific pools and/or driven by a small number of actors with targeted efforts.



We were able to identify a total of 23,436 unique addresses across Ethereum, BNB, and Base exhibiting activity consistent with the Heuristic 1 criteria. On average, each address engaged with two DEX pools and initiated 129 suspected wash trades of $30,033 in total volume during the time period studied. However, as shown in the table below, addresses that traded with four or more DEX pools accounted for 10% of total addresses identified by Heuristic 1. These addresses accounted for 43% of the total suspected wash trading volume in 2024.

	Number of DEX Pools one address engages in	Total wash trade volume one address initiates (USD)	Number of wash trades one address initiates
Average	2	$30,033	129
Median	1	$651	10
75 percentile	2	$5,940	25
90 percentile	4	$32,249	102
Max	241	$17,334,934	54,684

One address in 2024 initiated more than 54,000 buy-and-sell transactions of almost identical amounts — very suspicious in itself — illustrating the scale of this potential activity.



Wash trading Heuristic 2: disperse-based detection

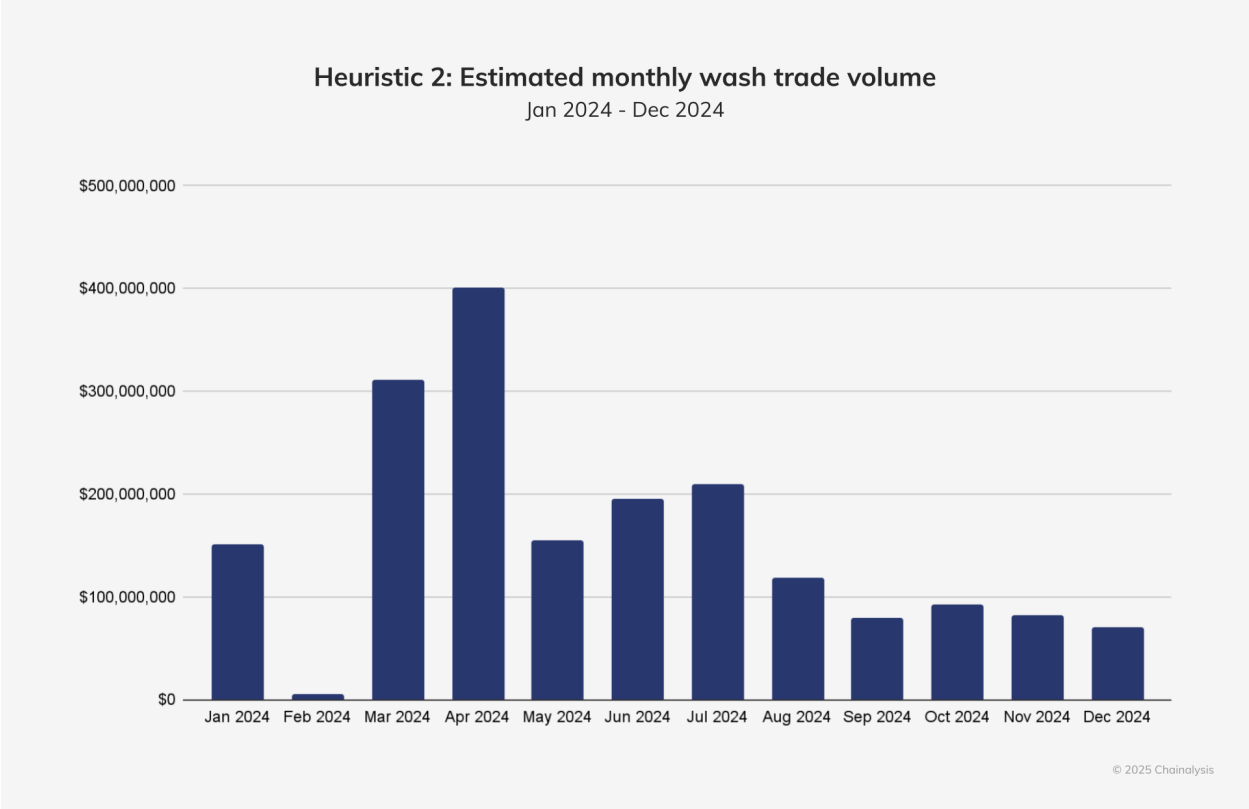
For our second heuristic, we looked at activity across token multi-senders, which were originally developed to simplify payments by facilitating simultaneous transfers of different tokens to multiple addresses. Unfortunately, many bad actors exploit these services to distribute funds across numerous addresses, managing them algorithmically in an attempt to conceal that the same actor is potentially manipulating tokens.

With this in mind, we employed the following criteria to identify suspected wash trading, accounting for ETH and BNB transfers by two multi-sender applications, and removing major pools that are unlikely to involve wash trading:

1. Controller addresses that send funds to five or more managed addresses.
2. Managed addresses that received their first ETH or BNB deposit from the corresponding controller address through a token multi-sender.
3. The difference in the total USD value between the buy and sell sides executed by managed addresses in a single liquidity pool is less than 5%.

Heuristic 2 suggests that the combined wash trade volume on Ethereum, BNB, and Base was around $1.87 billion in 2024. In November 2024, the suggested wash trade volume accounted for 0.046% of total DEX volume.

Similar to the first heuristic, the spikes observed between March 2024 and April 2024 in the below chart coincide with the activity of 2024's most prominent operators. For instance, in April, three controller addresses alone accounted for $318 million in suspected wash trading volume.



In January 2024, one controller address was responsible for approximately $142.99 million in suspected wash trade volume. Although the monthly estimated wash trade volume fluctuated significantly throughout 2024, the number of active controller addresses was more consistent, experiencing a steady upward trend between January and June.

Upon examining these addresses more closely, we learned that controller addresses managed an average of 183 addresses in 2024. As shown in the table below, a single controller address can manage tens of thousands of addresses.

	Number of addresses one operator controls
Average	183
Median	7
75 percentile	21
90 percentile	100.00
Max	22,832

	Total wash trade volume one operator executes (USD)
Average	$3,661,934
Median	$11,742
75 percentile	$223,446
90 percentile	$1,918,388
Max	$313,585,875

In 2024, the average suspected wash trade volume for one controller address was around $3.66 million in 2024. As we see in the chart below, the maximum volume of suspected wash trading controlled by one address can reach the hundreds of millions of dollars, illustrating the potential scale of this inflated activity.

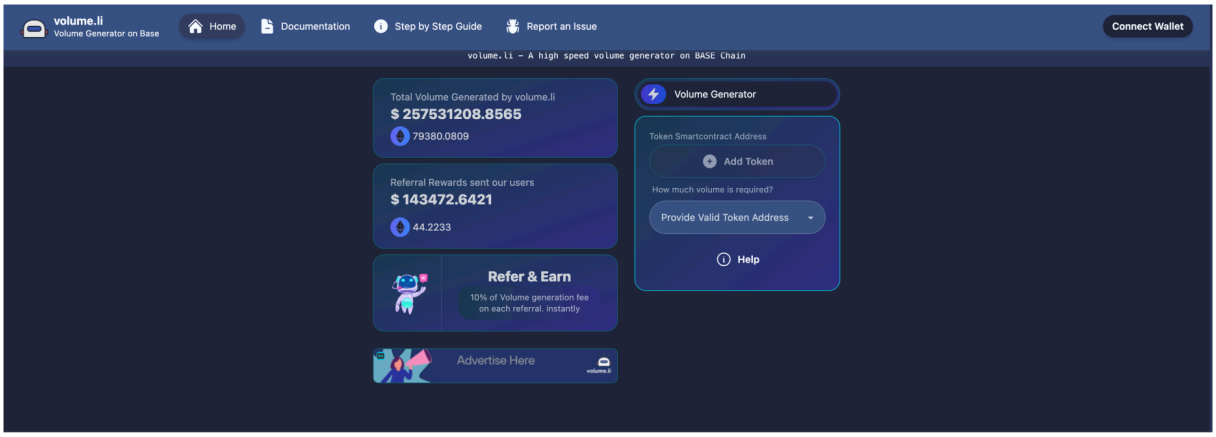
Heuristics 1 and 2 use different methodologies in order to detect different potential wash trading tactics. By adding the totals from heuristic 1 ($704 million) and heuristic 2 ($1.87 billion), we identify a total of $2.57 billion in potential wash trading activity. It is possible that there is overlap in the amounts detected by each heuristic – in other words, some suspected wash trading activity may have been detected by both heuristics – and so we consider this an upper bound estimate for this methodology.

Wash trading case study: volume boosting bot, Volume.li

Wash trading has emerged as a key concern in cryptocurrency market integrity, drawing the attention of U.S. regulators and law enforcement. For instance, on October 9, 2024, the United States Securities and Exchange Commission (SEC) charged four market makers — ZM Quant, Gorbit, CLS Global, and MyTrade — for generating artificial token trading volume. The Internal Revenue Service (IRS) later reported that this wash trading scheme involved 18 individuals and entities operating an international trading scheme with touchpoints in the U.K. and Portugal.

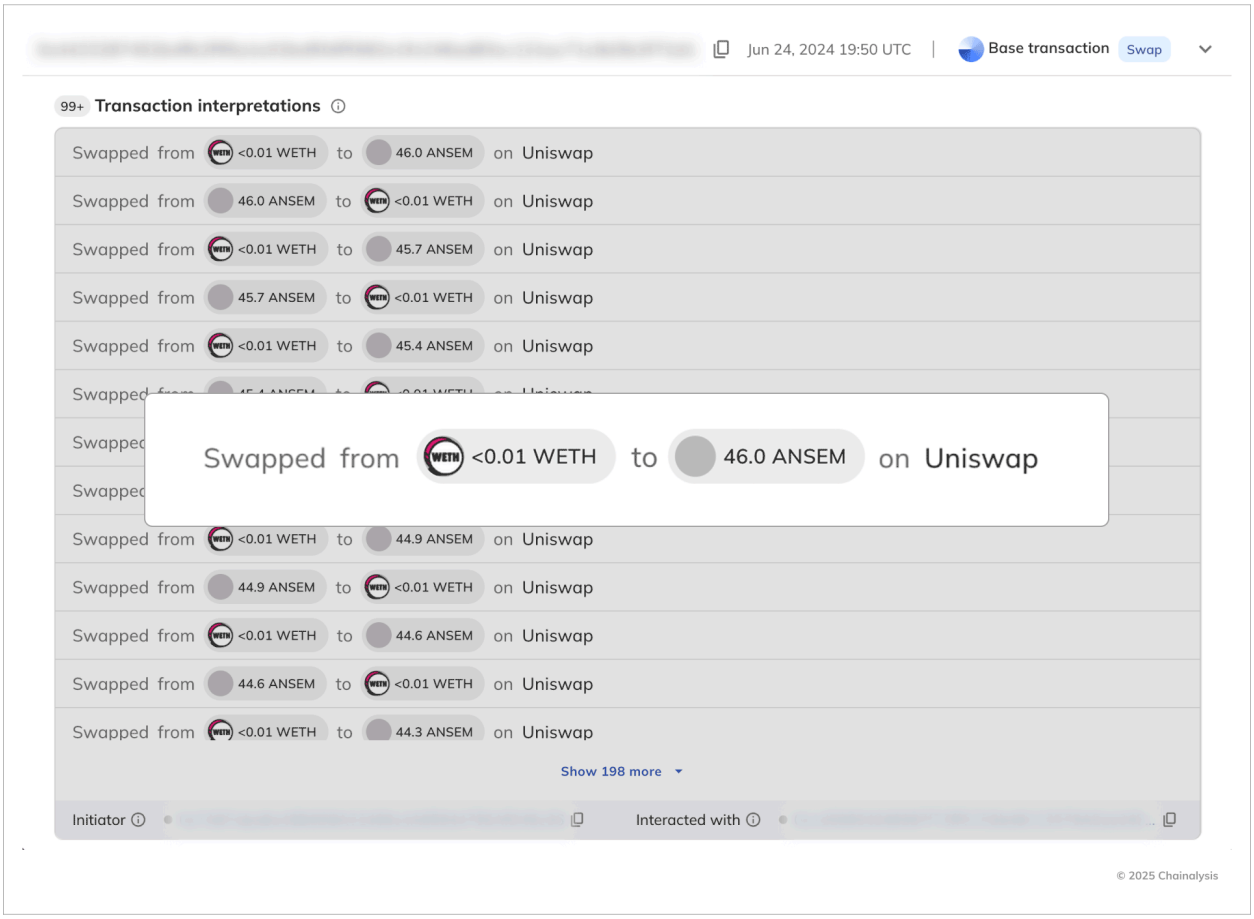
In this case, the market makers conducted the alleged illicit trading by operating trading bots that created artificial token volume. Typically, the strategy of building and operating bots for this purpose is difficult to distinguish from ordinary trading on both CEXs and DEXs.

To explore in-depth how this process typically works, we looked at a boosting bot service called Volume.li, which provides trading bots to customers who want to create fake volume on DEXs. While this service was not used by those charged by the SEC in the case above, it demonstrates how wash traders may leverage a tool to conduct similar activity. According to its website, Volume.li has generated a total of $257.5 million in trading volume to date.



Customers have the option of purchasing bots of varying degrees of volume, from $50 to $100,000, within 24 hours. The Volume.li site states that a bot generating $100,000 in volume within 24 hours costs 0.212 ETH. After the customer pays this fee, the bot will buy and sell a token 100 times in rapid succession.

In the below example, a purchased trading bot generated fake trades of the SoylanaManletCaptainZ token (ANSEM) paired with wETH on Uniswap.



We discovered that this trading bot uses a specific function (0x5f437312) to initiate its trades. Typically, swaps in Uniswap are initiated when the router contract receives a transaction, meaning that the contract is the recipient. However, in these types of trades, a few addresses — likely controlled by Volume.li — send transactions to the smart contracts they manage, invoking the 0x5f437312 function. These smart contracts act as intermediaries, subsequently triggering multiple wash trade transactions on Uniswap.

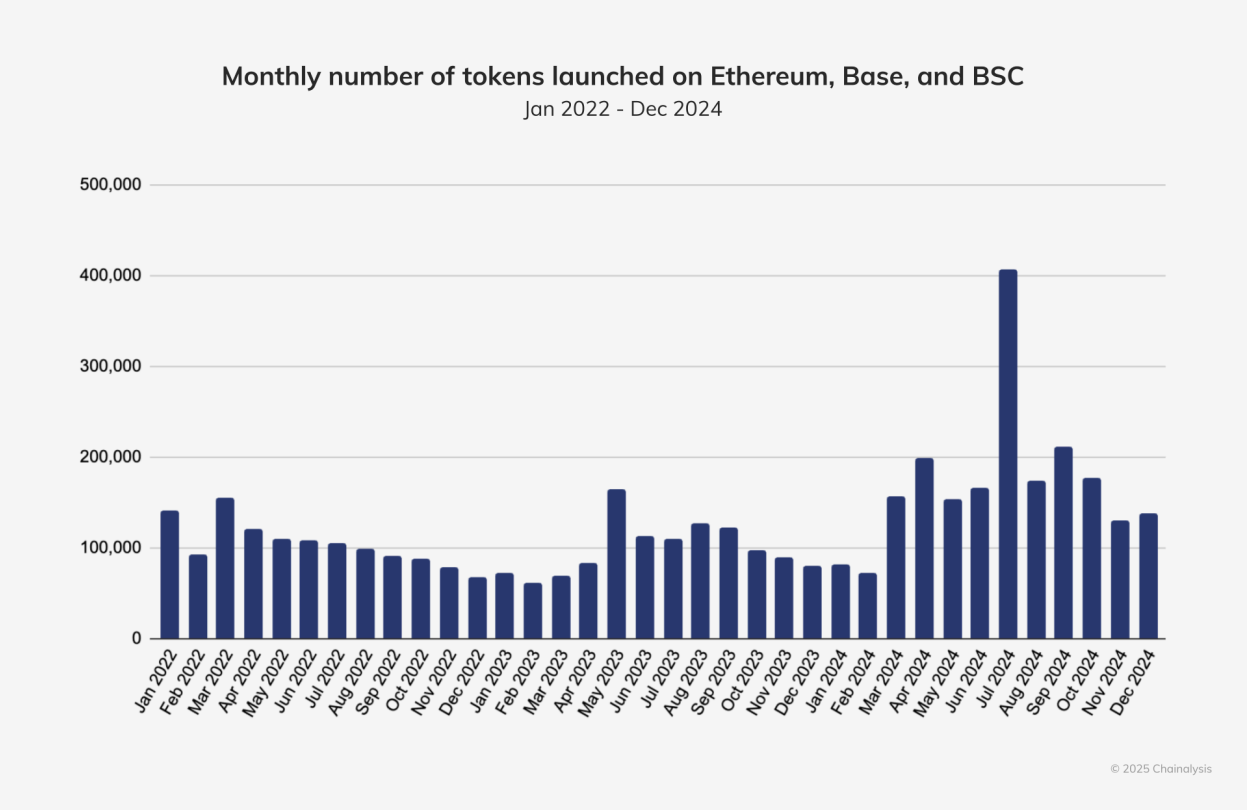
One example of an asset with trading volume boosted by Volume.li is the Donald J. Chump token, which had 6,939 holders as of January 2025. Within five days, Volume.li's bot generated 10,341 pairs of buy and sell orders using five different addresses, creating a total of $39,723 in fake trading volume. From July 27 to July 30 the token issuer relied heavily on Volume.li to generate liquidity, which accounted for approximately 43% of the token's total trading volume on Uniswap.

As Volume.li exemplifies, even when our starting point is off-chain, pairing open-source research on platforms of interest with our own heuristics can yield powerful insights about potential on-chain market manipulation.

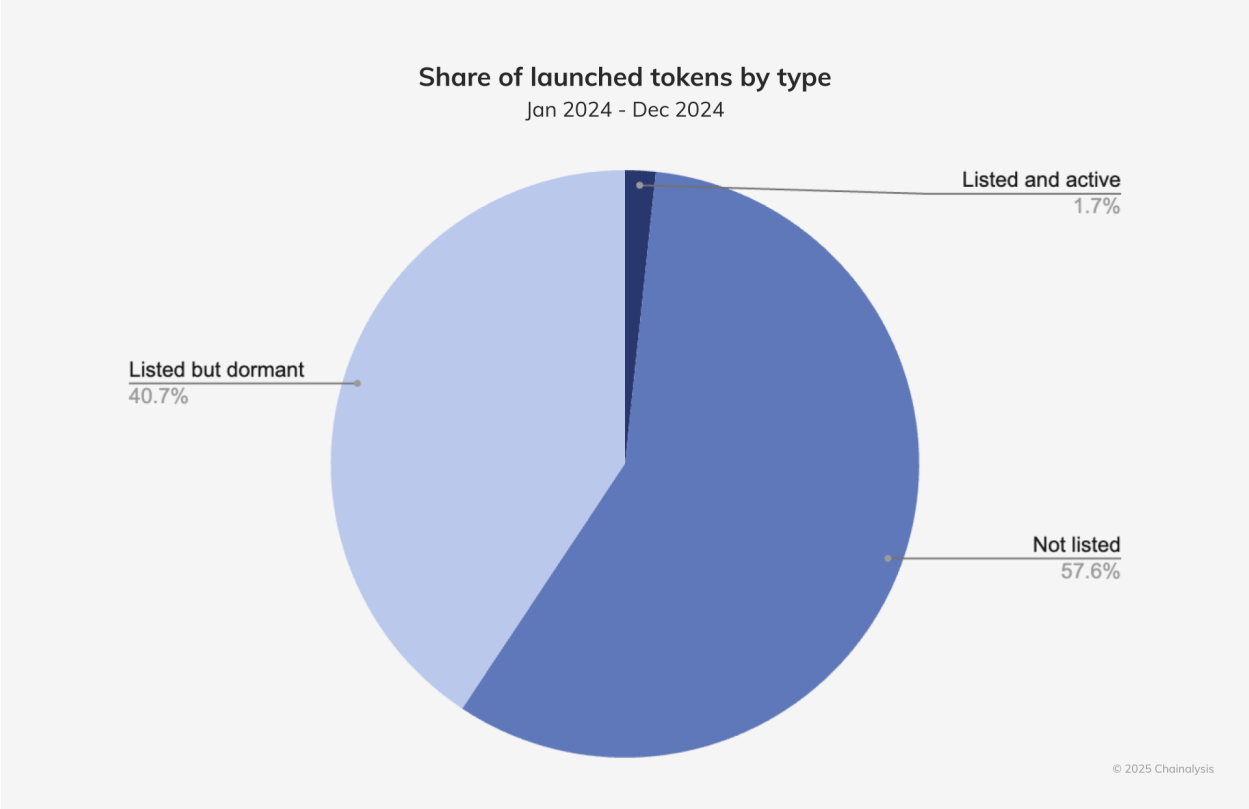
3.59% of all launched tokens in 2024 display patterns that may be linked to pump-and-dump schemes

In 2024, more than 2 million tokens were launched in the blockchain ecosystem, approximately 0.87 million of which (42.35%) were listed on a DEX.

Last year, we noted that the majority of new tokens were developed on Ethereum due to the ease of creating tokens using the ERC-20 standard. Although Ethereum is still the chain with the greatest number of tokens actively traded on DEXs, we've noticed many token creators using other chains, such as BNB and Base. In the below chart, we see that, in most months in 2024, several hundreds of thousands of tokens were launched on these chains, with July seeing more than 400,000.



Despite the staggering number of tokens launched in 2024, only a small fraction (1.7%) have been actively traded within the last 30 days. So, why do so many of these tokens appear dormant? One possibility is that many are abandoned shortly after their creation, potentially due to a lack of interest or failure to gain traction. It is also possible that some of these tokens facilitate intentional short-lived schemes designed to exploit initial hype before fading away, also known as pump-and-dumps or rug pulls.



Here's an example of how a pump-and-dump scheme might work with a token:

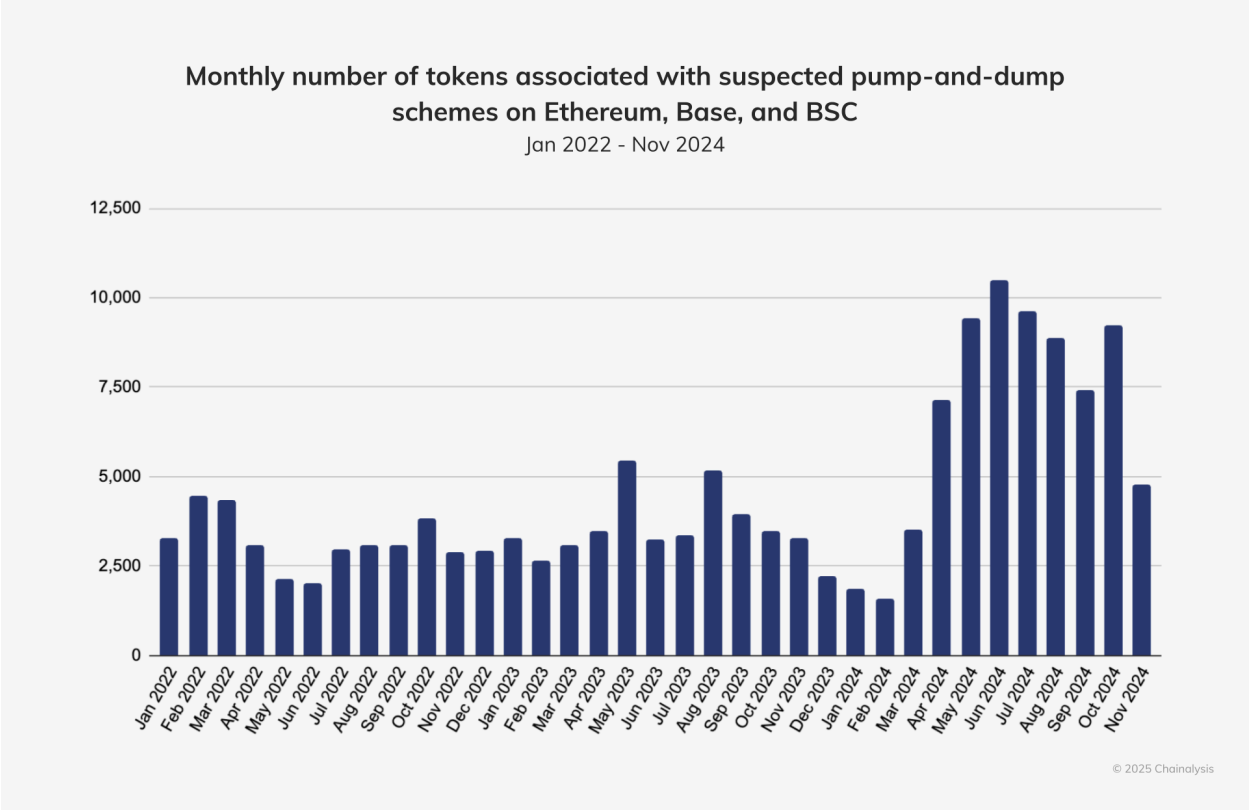
1. A crypto participant either launches a new token or buys a large share of the supply for an existing token — usually one with historically low volume.
2. This participant hypes up the token using social media and/or online chat rooms.
3. The hype attracts attention from other users, leading to an increase in buying pressure on the token.
4. The initial participant may also engage in wash trading, as described in the previous section, in order to further artificially inflate the token's trading volume.
5. If these methods are successful, the token rises in value.
6. Once the token reaches the desired price target, the original participant liquidates their position for a profit.
7. The token's price rapidly drops due to selling pressure, leaving many victims "holding the bag."
8. If the participant is also the token creator or one of the liquidity pool's primary liquidity providers, they may also completely abandon the project in a rug pull, taking more users' funds with them. In certain cases, however, governance protocols may not allow this.

It is possible to identify many of these activities using on-chain analysis, and we used the following criteria to identify potential pump-and-dump schemes. We looked for activity in which all three criteria were met:

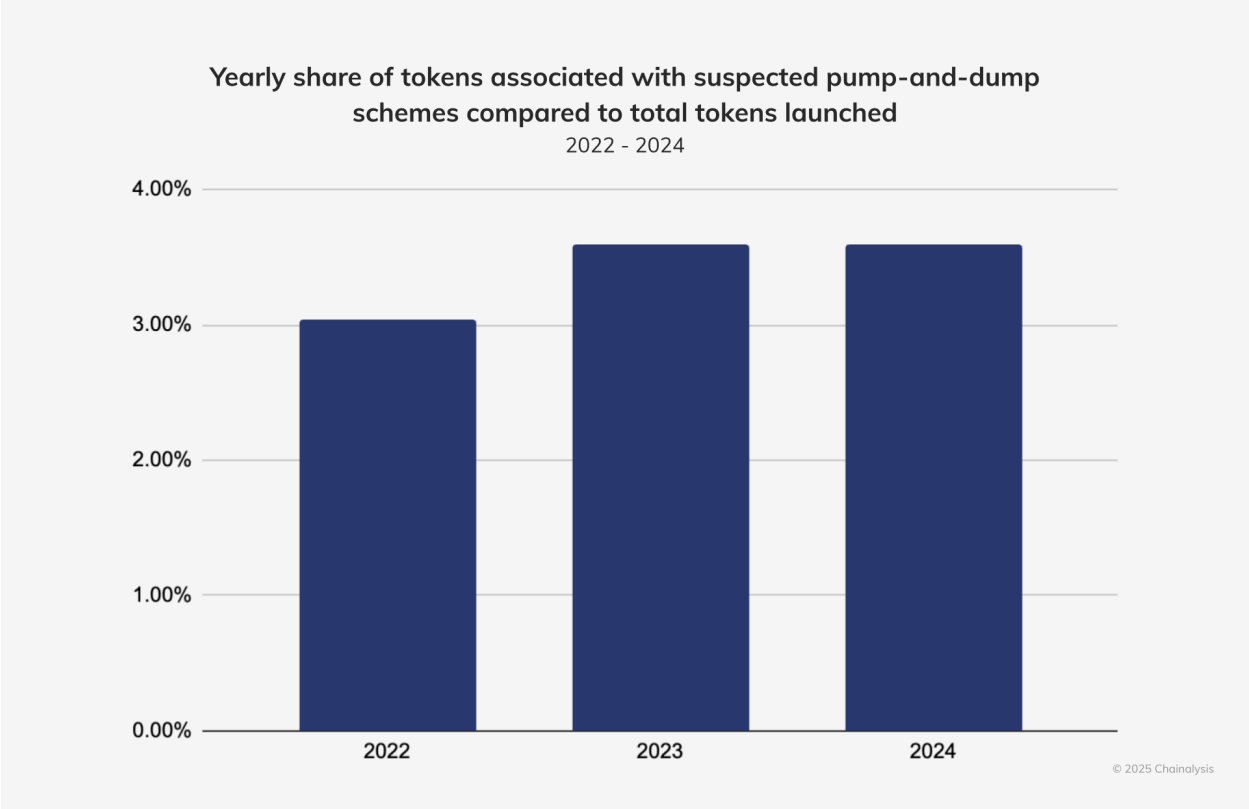
1. An address that added value to a token's liquidity pool and subsequently removed at least 65% of the pool's liquidity, valued at $1,000 or more.

2. The token's liquidity pool is no longer active.
3. The liquidity pool had previously gained traction, with more than 100 transactions occurring in it.

We made several changes to our methodology this year, employing stricter criteria to improve accuracy. First, we loosened the liquidity removal threshold from last year's 70% to 65% to capture tokens with larger liquidity volumes. We also replaced the criterion of a token having liquidity worth $300 or less with a completely inactive liquidity pool (we consider a liquidity pool inactive if no transactions occurred in the last 30 days). And finally, we replaced the original criterion of a token being purchased at least five times by DEX participants with no on-chain connection to the token's biggest holders, with the criterion of the liquidity pool having more than 100 transactions.



	Number of tokens	Percent of all tokens launched
Number of tokens launched in 2024	2,063,519	100%
Number of tokens listed on DEX	873,957	42.54%
Number of suspected pump-and-dump tokens	74,037	3.59%



Approximately 94% of DEX pools involved in suspected pump-and-dump schemes appear to be rugged by the address that created the DEX pool. The other 6% appear to be rugged by the addresses that were funded by the pool or token deployer. In some cases, the pool deployer address and the address that rugged the pool were funded by the same address source, suggesting there may have been a coordinated effort to exploit users.

	Total
Number of pools dumped by the same actor who deployed the DEX pool	69,897
Total number of DEX pools engaged in suspected pump-and-dump schemes	74,312
Share of pools dumped by the same actor who deployed the DEX pool	94.00%

	Total
Average in days	6.23
Median in days	0
75 percentile in days	0
90 percentile in days	8
99 percentile in days	123

After a DEX pool is launched, it typically takes a few days to a few months before the associated token is abandoned. As we see in the table below, it took an average of six to seven days, and 1% of suspected pump-and-dump schemes lasted longer than four to five months.

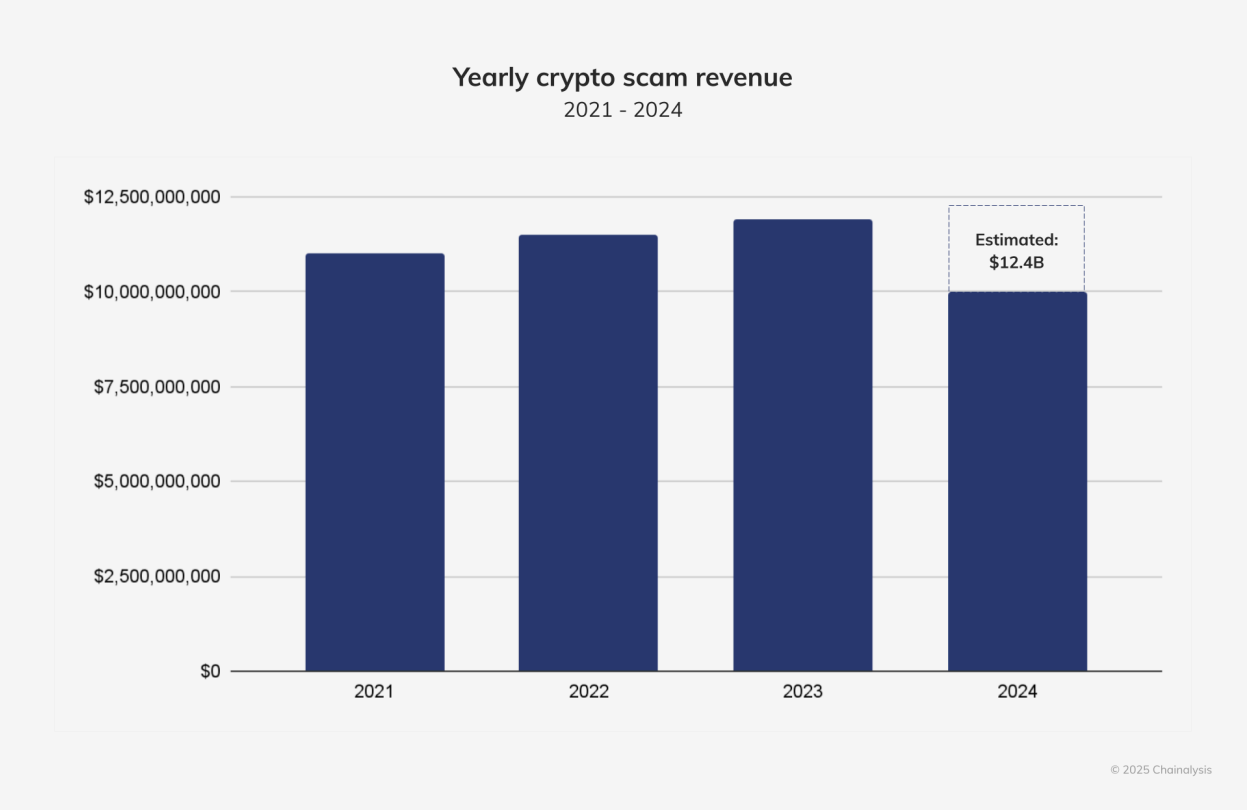
Navigating the challenges of crypto market manipulation

Market manipulation remains a critical concern for both crypto industry participants and authorities as they strive to keep pace with the rapidly-evolving sector. The complex and dynamic nature of market manipulation, compounded by crypto's unique characteristics — such as its pseudonymity and decentralization — heightens the challenge. A robust and coordinated approach is therefore essential — one that fully harnesses the power of on-chain data and analytics to enable proactive detection and prevention of manipulative activities.

Scams

Pig Butchering Grows Nearly 40% YoY as Fraud Industry Leverages AI and Increases in Sophistication

In 2024, cryptocurrency scams received at least $9.9 billion on-chain, an estimate that will increase as we identify more illicit addresses associated with fraud and scams in the coming months.



According to our metrics today, it looks like 2024 saw a drop in scam revenue; however, 2024 was likely a record year as these figures are lower-bound estimates based on inflows to the scam addresses we've identified up to today. A year from now, these totals will be higher, as we identify more illicit addresses and incorporate their historic activity into our estimates.

Since 2020, our annual estimates of scam activity have grown by an average of 24% between annual reporting periods. Assuming a similar growth rate between now and next year's Crypto Crime Report, our annual totals for 2024 could surpass the $12 billion threshold.

Further, with our recent acquisition of Alterya, we will leverage AI-powered fraud and scam detection to augment our data, and expect our totals to become even more robust than our estimates based on

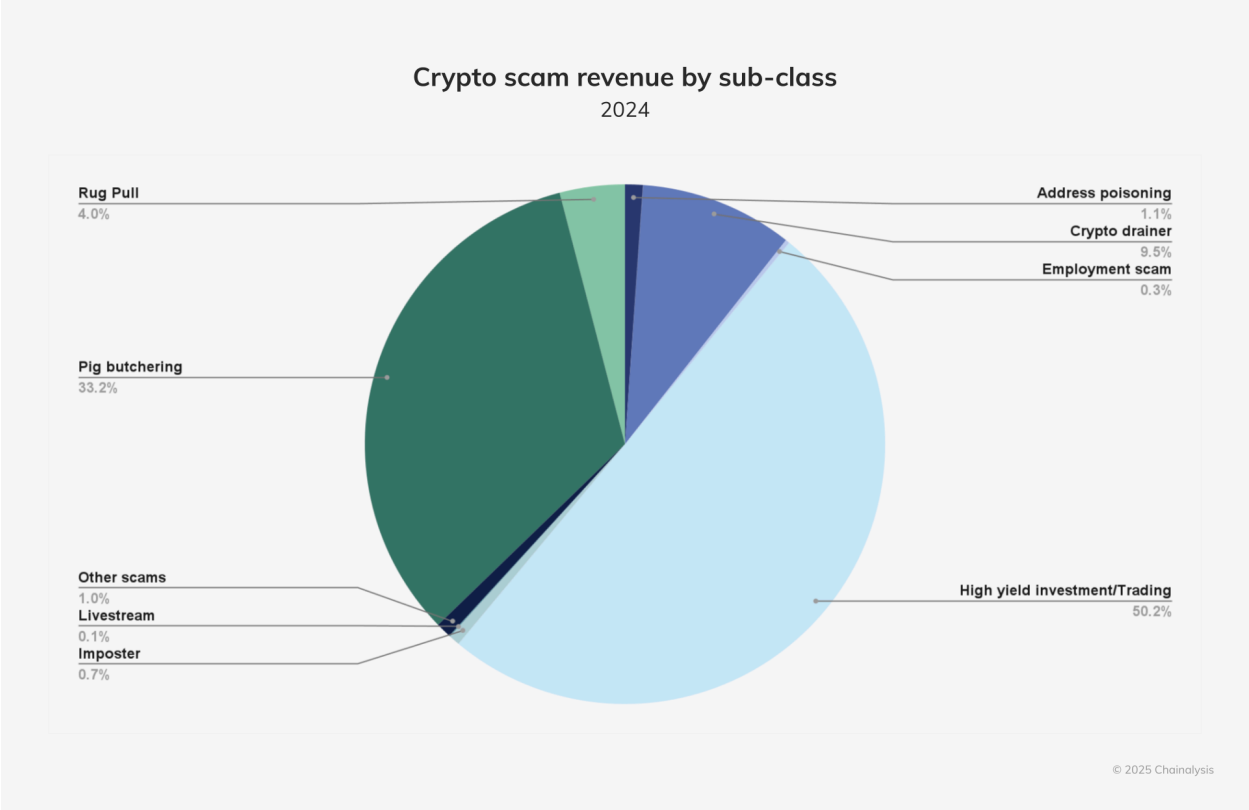
historical increases. Alterya has worked with top cryptocurrency exchanges, fintech companies, and financial institutions to proactively prevent fraud and minimize losses. In 2024, the organization detected $10 billion sent to scams.

In the last few years, crypto fraud and scams have continued to increase in sophistication, as the fraud ecosystem becomes more professionalized. Operations like Huione Guarantee, a peer-to-peer (P2P) marketplace, offer a host of illicit services that support pig butchering scamming operations and serve as a one-stop-shop for scammers' needs. These services range from the technology infrastructure required to initiate scams to money laundering services for obfuscating illicit activity and cashing out.

In this section, we'll (1) discuss fraud and scam trends in 2024; (2) profile Huione Guarantee and its role in professionalizing the scam ecosystem, and; (3) explore a crypto ATM scam story, its implications for the elderly population, and emerging regulatory priorities.

High-yield investment and pig butchering scams see highest crypto revenues

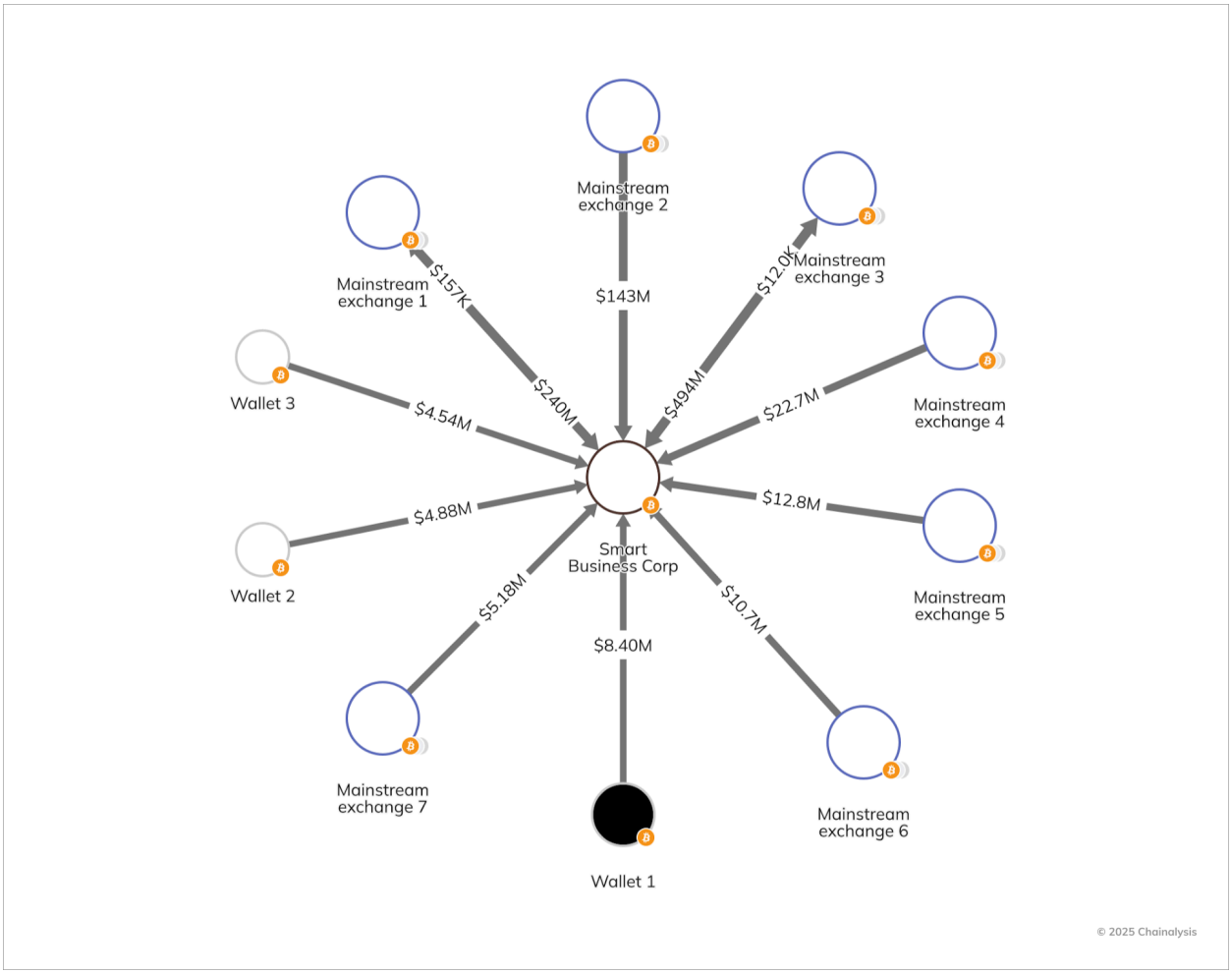
In the past year, high-yield investment scams (HYIS) and pig butchering scams received the most crypto among scam sub-classes, at 50.2% and 33.2% respectively.



Despite pulling in half of all scam revenue in 2024, HYIS inflows declined by 36.6% YoY, while pig butchering revenue increased by almost 40% YoY. These categories aside, the fraud and scam landscape is expanding into a variety of other subclasses that we'll discuss.

One lucrative HYIS active in 2024, Smart Business Corp, is a decade-old ponzi scheme targeting Spanish-speaking countries, particularly Mexico. In 2022, Smart Business Corp added bitcoin to its investment portfolio and promised affiliates outsized returns based on a tiered investment scheme. That same year, Mexican government consumer protection agency CONDUSEF warned that Smart Business Corp was not registered to offer securities in Mexico.

To date, Smart Business Corp has received $1.5 billion on-chain. The graph below shows its top 10 counterparties by crypto received, a combination of seven mainstream exchanges and three self-hosted wallets.



Pig butchering scams (also known as investment or romance scams) target and build relationships with individuals, convincing them to invest in fraudulent opportunities, and predominantly originate via large scam compounds in Southeast Asia. International Justice Mission (IJM), a global organization that protects

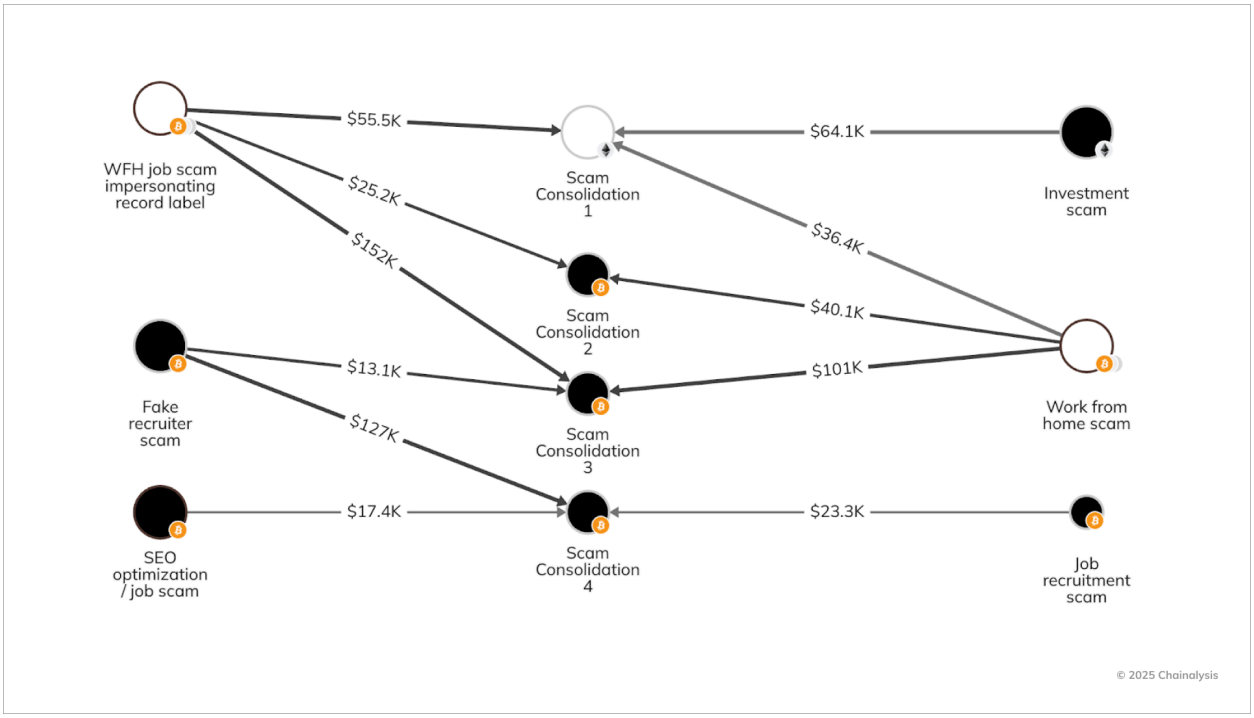
people in poverty from violence, began observing forced labor cases tied to these operations in 2021, and has since observed immense growth of these crimes. IJM's work in this region focuses on preventing human trafficking associated with these operations by strengthening justice systems.

Despite their prominent footprint in Southeast Asia, pig butchering scams have become more geographically dispersed. While none of these operations yet approach the scale of those in Southeast Asia, IJM has observed shifts to other countries over the past two years. Some recent examples:

- December 2024: Nigeria's anti-graft agency announced the arrest of 48 Chinese and 40 Filipino nationals for running an investment scam operation that targeted people mostly from Europe and the Americas. Scam operators recruited Nigerians to prospect for victims online, whom the scammers then tricked into investing in fake crypto schemes.
- June 2024: Interpol coordinated a global operation to disrupt scam operations worldwide, including one in Namibia that forced 88 youths into conducting scams as part of an international scam network.
- October 2023: Malaysian authorities announced that Peruvian police had rescued 43 Malaysian citizens trafficked to Peru who were forced to work in a scam operation.

Pig butchering scammers have also evolved to diversify their business model beyond the "long con" of pig butchering scams — which can take months and even years of developing a relationship before receiving victim payments — to quicker turnaround employment or work-from-home scams that typically yield smaller victim deposits.

One such example, a fraudulent job site impersonating a record label offering work-from-home jobs, sent crypto to consolidation wallets where a pig butchering scam also sent funds, as seen in the top left of the graph below. Researchers at cybersecurity company Proofpoint assess with a high degree of confidence that the same actors conducted these seemingly disparate pig butchering and employment scams. Chainalysis was separately able to connect these scam domains on-chain by shared consolidation addresses that Proofpoint had connected.



Though employment scam inflows represented less than 1% of total on-chain value that scams received last year, thousands of people unwittingly paid into fake job platforms and the FBI warned U.S. citizens about these schemes in 2024. Proofpoint attests that many of these platforms are getting savvier, including registering multiple backup domains for every site in case they are taken down. Scam operators are also likely wisening up to the traceability of cryptocurrency, and are now having victims reach out to "customer service" representatives to obtain a crypto address. Some scammers are foregoing cryptocurrency as a payment option altogether and are instead directing scam victims to other payment services.

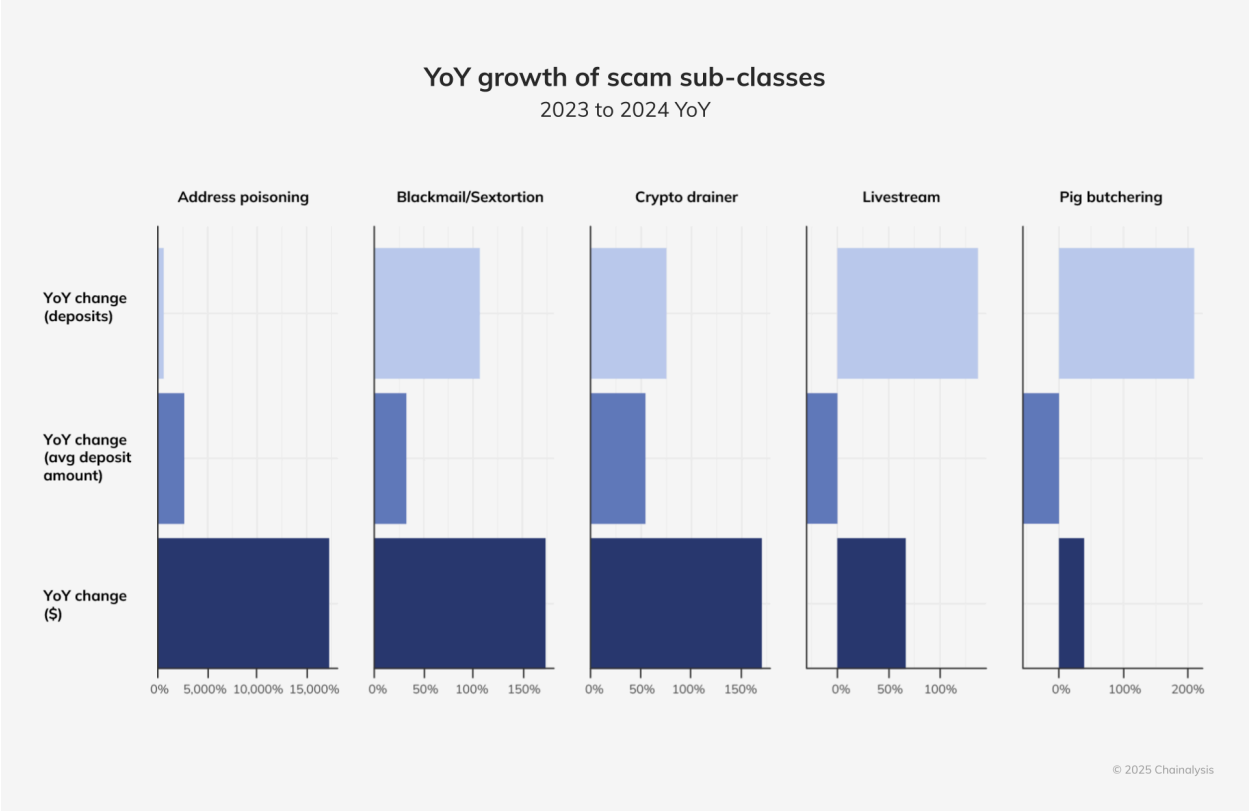
IJM began seeing instances of work-from-home scams in mid-2023, with paid social media ads using the names of real companies. Since then, it appears tactics have changed to sending targets text messages with vague job details, sometimes pretending to be from legitimate job boards. "These scams are particularly devious because anyone who has put their resume out there and is looking for a job could easily be hooked by these, especially those desperate for work," says Eric Heintz, global analyst at IJM.

Heintz said that while the scam has a few variations, generally speaking, after the target accepts the "job," the scammer has them join a platform where they complete tasks and accrue "payments". In order to withdraw money, the victim must pay a percentage in "tax", with a lower percentage required if they wait to withdraw large amounts, which causes the victim to lose even more money. The scam seems to have originally targeted people in Asia and, in 2024, shifted focus to North America and Europe.

"While pig butchering scams garner the most attention, large scam compounds are essentially havens for any type of scam that can be carried out via the internet, and it's not uncommon to have multiple criminal groups operating within the same compound focusing on different scams," says Heintz.

Growth across the fraud and scam ecosystem

In 2024, on-chain activity indicates that five scam types grew: pig butchering, address poisoning, crypto drainers, livestream, and blackmail/sextortion scams.



In 2024, pig butchering revenue grew nearly 40% YoY and the number of deposits to pig butchering scams grew nearly 210% YoY, potentially indicating an expansion of the victim pool. Conversely, the average deposit amount to pig butchering scams declined 55% YoY. The combination of lower payment amounts and increased deposits could indicate a change in strategy for pig butchering scams. Scammers could be spending less time priming targets, and therefore, receiving smaller payments, in exchange for targeting more victims.

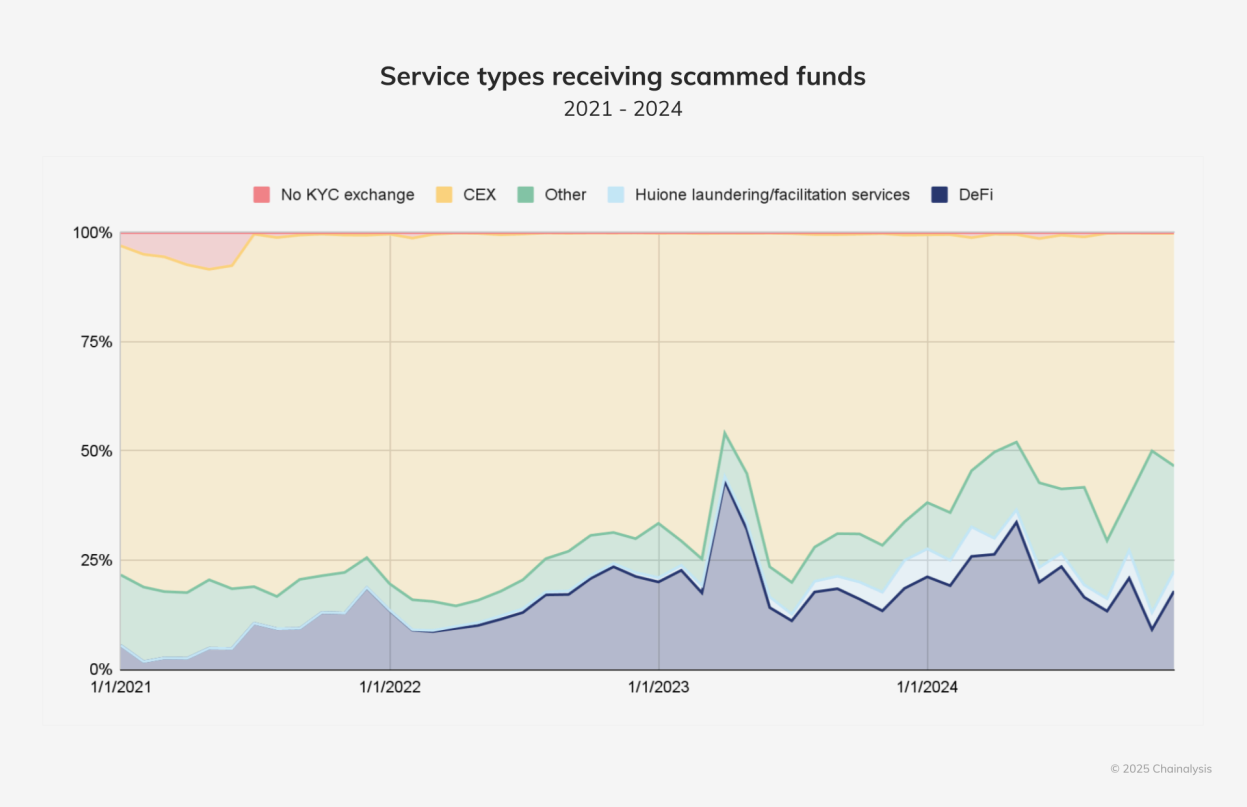
Another destination for heavy scam flows, crypto drainers continued to proliferate and grew across the board — nearly 170% YoY revenue growth, almost 55% YoY increase in deposit size, and 75% YoY growth in number of deposits. Notably, in January of 2024, a drainer posing as the U.S. Securities and Exchange Commission (SEC) prompted users to connect their wallets to claim fake tokens through an airdrop after the SEC's X account was compromised.

Like crypto drainers, address poisoning attacks use on-chain infrastructure to scam victims out of their funds. Scammers pick a target and study their transaction patterns and most frequent counterparties. Using an algorithm, scammers then will generate a new crypto address similar to one the target interacts with regularly, and send a small transaction from this newly created address to "poison" the target's

address book. In 2024, crypto sent to address poisoning scams grew over 15,000%, largely driven by a single massive attack in May. On-chain data shows that address poisoning scammers target users with higher than average wallet balances.

Where scammers send illicit crypto

In the last few years, destinations for scammed funds have remained relatively the same, with most funds going to centralized exchanges (CEXs). But as scams on more blockchains including Ethereum, Tron, and Solana have grown, so too has the use of DeFi protocols.



Since mid-2023, crypto sent from scams to Huione money laundering services has also grown. Money laundering is just one type of illicit activity the Huione Guarantee platform supports, among a host of services that facilitate scams.

How Huione Guarantee is professionalizing the scam ecosystem

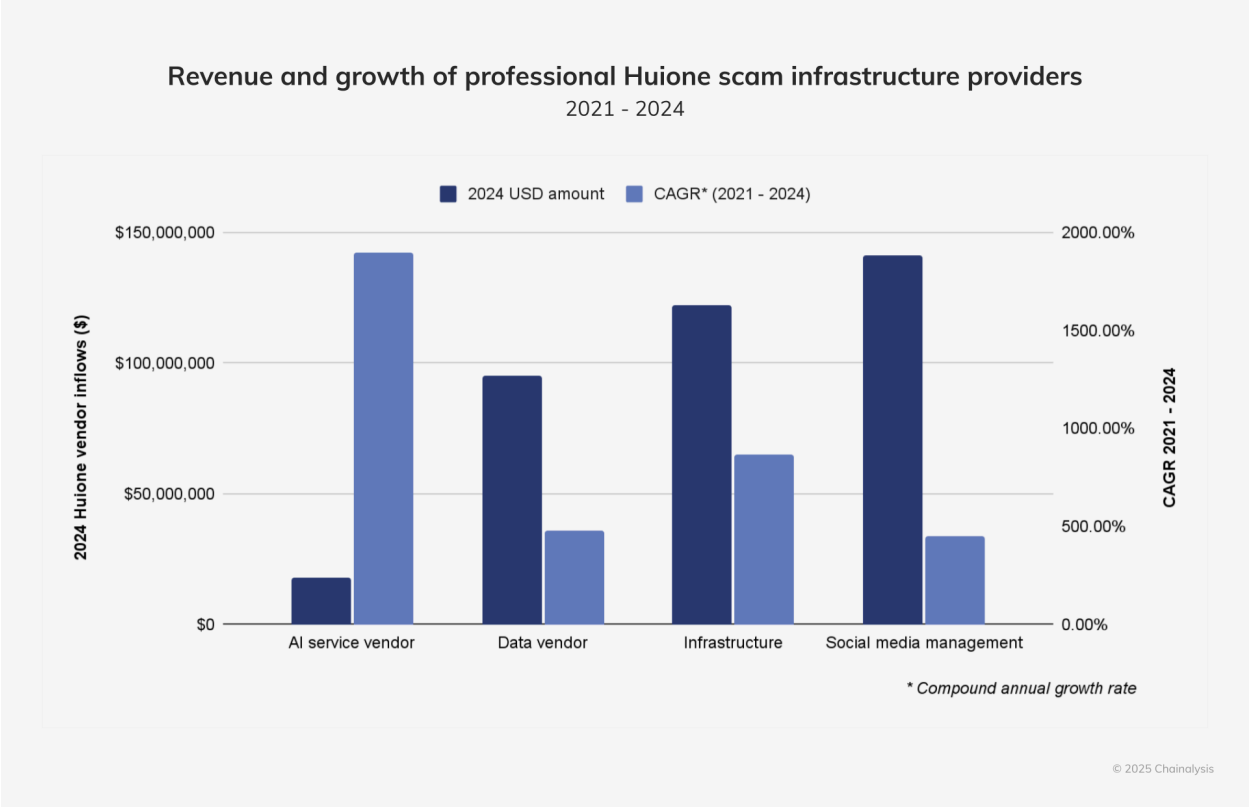
Huione Group, a Cambodian conglomerate known to offer legitimate services like remittances, insurance products, and, for a time, luxury tourism offerings, is also known to facilitate cybercrime. Since 2021, Huione Guarantee — an online forum and P2P marketplace affiliated with Huione Group — has processed

$70 billion in crypto transactions.[2] On-chain activity indicates Huione Guarantee is heavily used for illicit crypto-based activities supporting the growing pig butchering industry in Southeast Asia, including the sale of scam technology products, money laundering services, and much more.

Specifically, Huoine Guarantee has become a one-stop-shop for illicit actors needing the technology, infrastructure, and resources to conduct scams — assets like targeted data lists, web hosting services, social media accounts and content creation, and AI software. In addition to these offerings, Huione has also bolstered scores of money laundering operations that scammers use to obfuscate their illicit activity. In short, Huione Guarantee has driven and enabled a scam ecosystem that is massive, growing, and interconnected.

A large and growing fraud ecosystem

In 2024, Huione scam technology vendors collectively received at least $375.9 million in cryptocurrency. The chart below examines the types of vendors capitalizing on products and services used to facilitate scams, including, but not limited to AI services, data, infrastructure, and social media management.



When comparing crypto flows from 2021 through 2024 based on a compound annual growth rate, Huione scam infrastructure providers' revenue has increased exponentially, with AI service vendors' revenue growing by 1900%, indicating an explosion in the use of AI technology to facilitate scams. AI vendors offer

[2] These numbers include the platforms Huione Guarantee, Huione Pay, and all vendors advertising through Huione platforms.

technology that helps scammers impersonate others or generate realistic content that tricks victims into making fraudulent investments.

Huione data vendors sell stolen data such as personally identifiable information (PII) that bad actors can exploit for illicit purposes, often with information on "quick kill" targets (i.e., potential victims who are most susceptible to being scammed). Web infrastructure providers offer technology services like website hosting and mechanisms to bypass authentication on app stores, which lend credence to fake websites and apps used to scam victims. Additionally, services that facilitate mass text message marketing help scammers extend their reach across the globe to a wider set of potential victims. As for social media services, scammers can boost the legitimacy of their campaigns by leveraging services that enhance the clout of their social media accounts. The growth in data vendors, while lower than that of AI service vendors, has still seen exponential increases in inbound funds YoY.

Generative AI software: Creating fake personas for scammers

While generative AI can accelerate legitimate innovation, it can also make scams more scalable and affordable for bad actors to conduct.

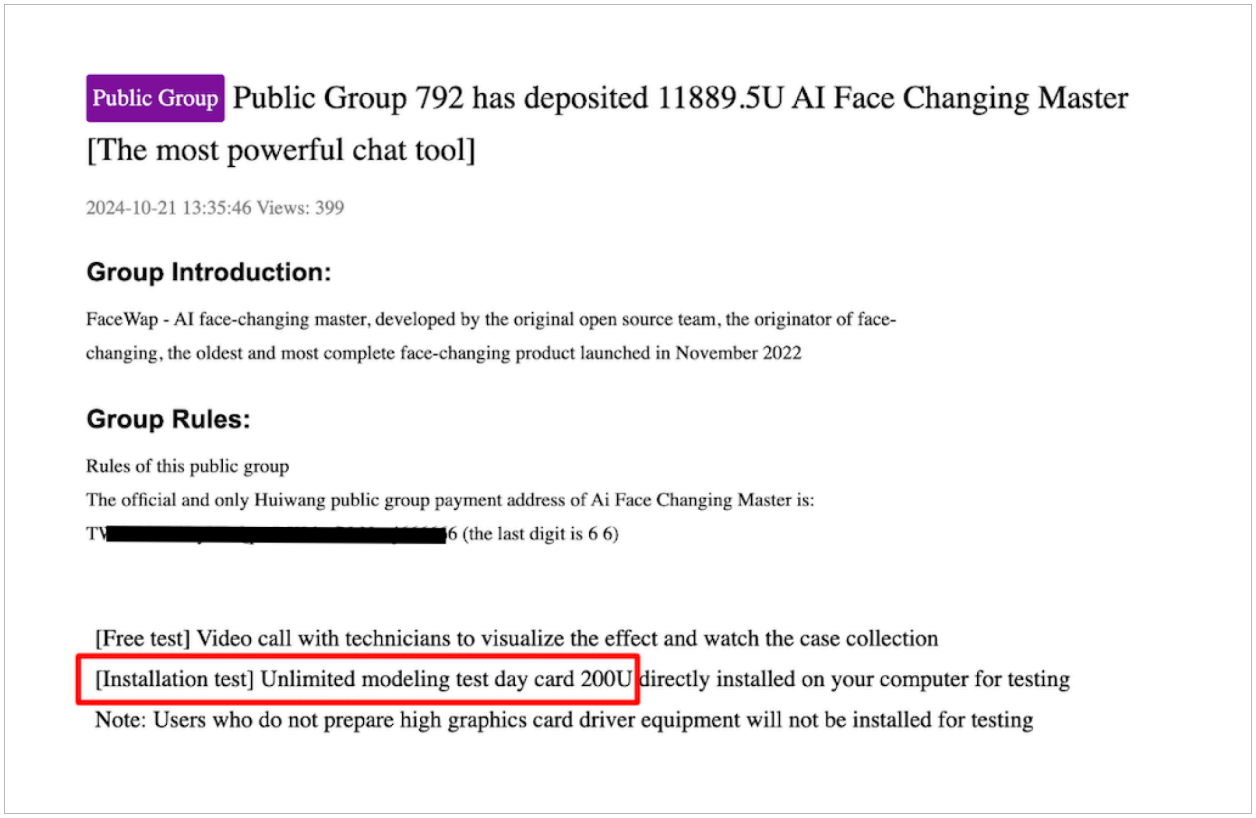
"GenAI is amplifying scams, the leading threat to financial institutions, by enabling high-fidelity, low-cost, and highly scalable fraud that exploits human vulnerabilities," says Elad Fouks, head of fraud products at Chainalysis and co-founder of Alterya. "It facilitates the creation of synthetic and fake identities, allowing fraudsters to impersonate real users and bypass identity verification controls."

In fact, Alterya found that 85% of scams involve fully verified accounts that bypass traditional identity-based solutions.

"Additionally, GenAI enables the generation of realistic fake content, including websites and listings, to power investment scams, purchase scams, and more, making these attacks more convincing and harder to detect," said Fouks.

With this technology, scammers can deceive targets into authorizing payments under false pretenses, often known as authorized push payment (APP) fraud.

The Huione Guarantee platform hosts dozens of software vendors that provide generative AI technology to facilitate scams. As we see below, one AI vendor on Huione Guarantee advertises AI "face-changing services" for $200 worth of crypto.



Public Group Public Group 792 has deposited 11889.5U AI Face Changing Master [The most powerful chat tool]

2024-10-21 13:35:46 Views: 399

Group Introduction:

FaceWap - AI face-changing master, developed by the original open source team, the originator of face-changing, the oldest and most complete face-changing product launched in November 2022

Group Rules:

Rules of this public group

The official and only Huiwang public group payment address of Ai Face Changing Master is:

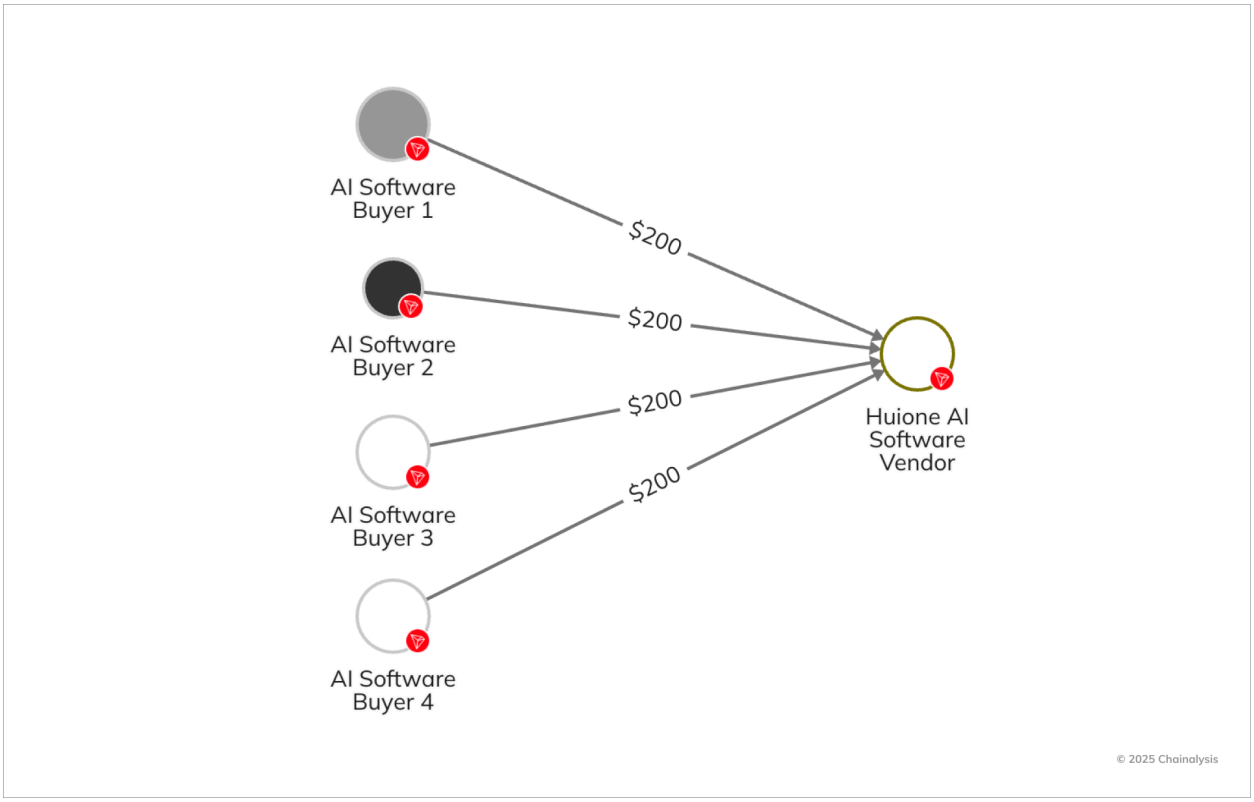
T[redacted]6 (the last digit is 6 6)

[Free test] Video call with technicians to visualize the effect and watch the case collection

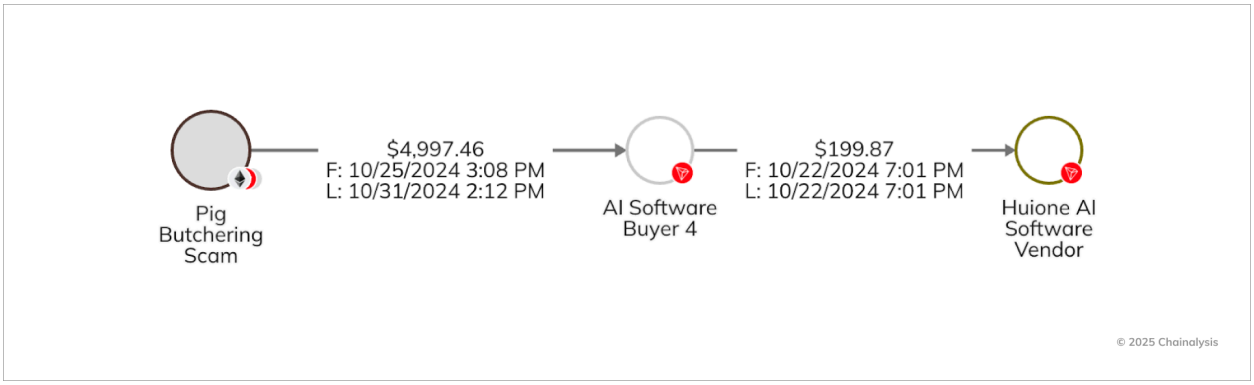
[Installation test] Unlimited modeling test day card 200U directly installed on your computer for testing

Note: Users who do not prepare high graphics card driver equipment will not be installed for testing

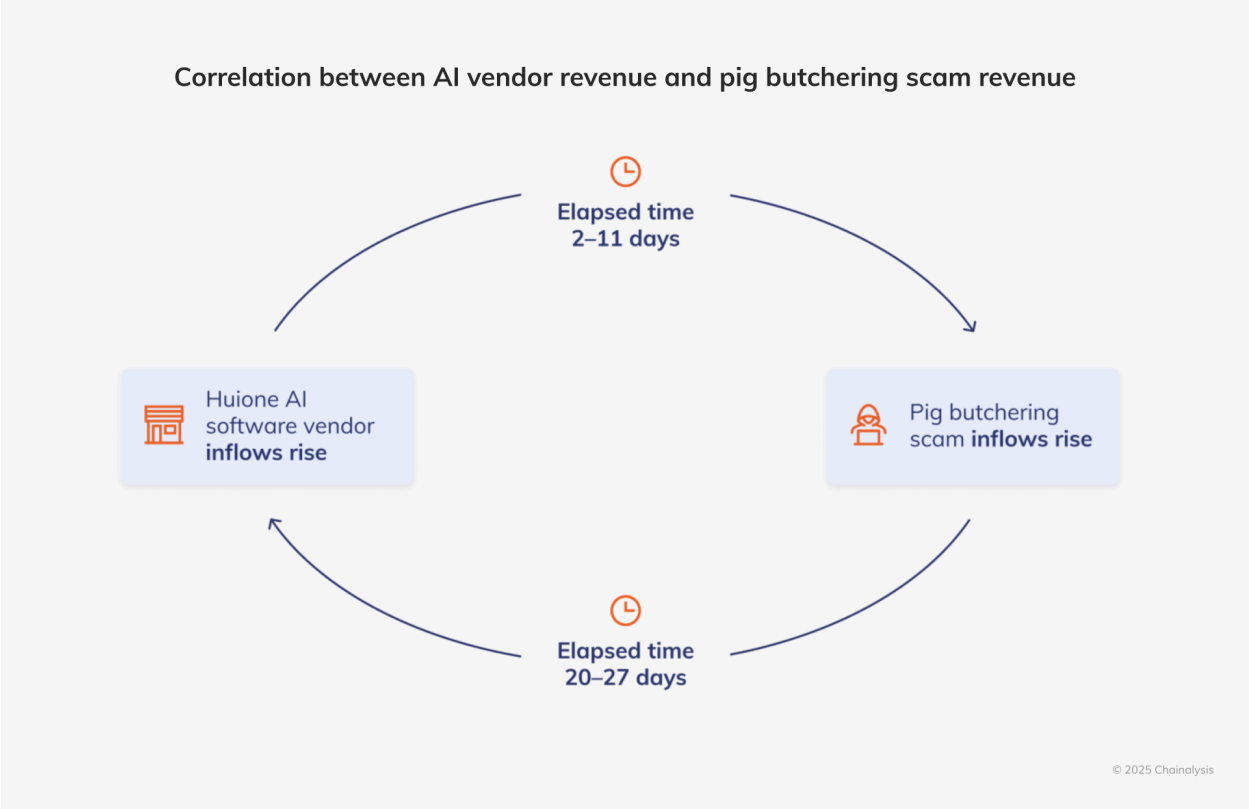
On-chain analysis reveals multiple payments sent to the above AI software vendor were consistent with the purchase price, indicating the counterparties are likely AI software buyers and potential scammers. These buyers likely made these purchases after seeing the vendor's advertisements on Huione Guarantee.



On-chain analysis, visualized below in Chainalysis Reactor, shows AI Software Buyer 4 first received pig butchering scam proceeds on October 25, three days after its AI software purchase on October 22, and another scam proceeds payment nine days later, on October 31. This narrow timeframe highlights how quickly scammers are likely leveraging Huione Guarantee's technology vendors to execute their scams against their victims.



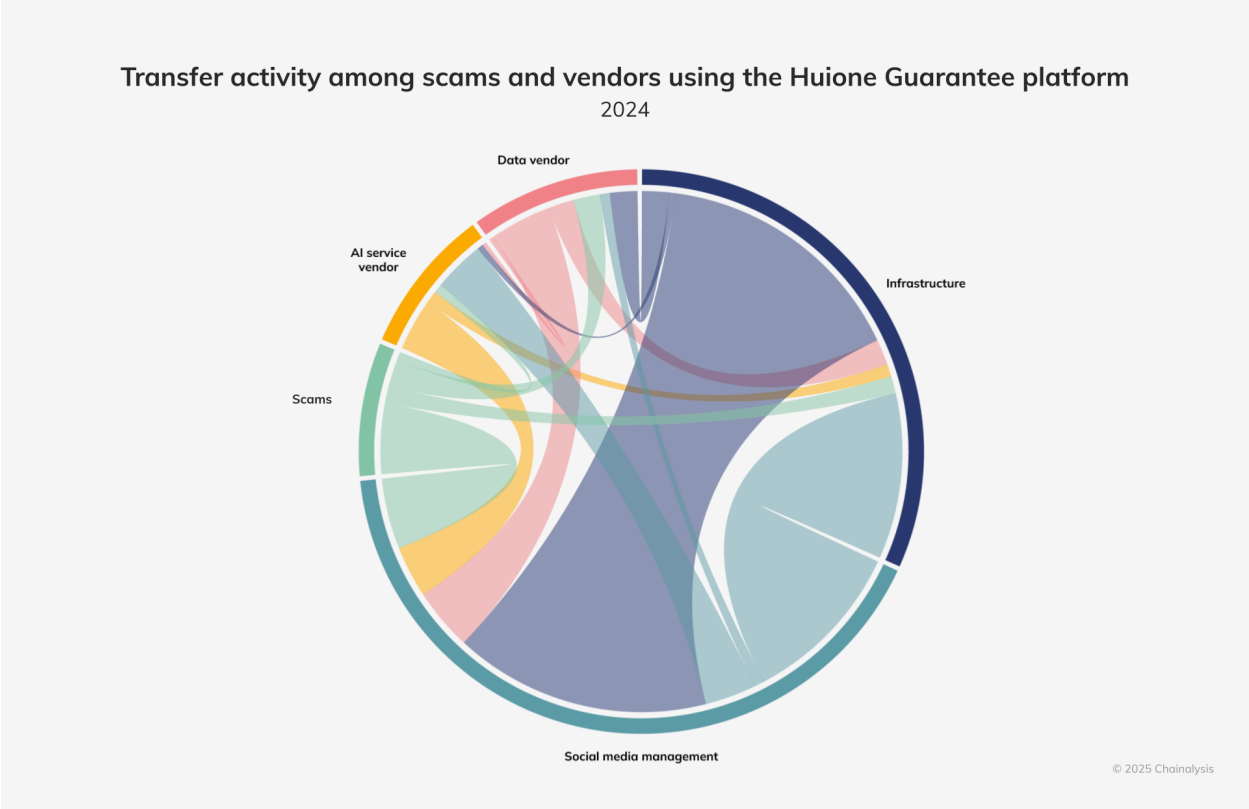
This example aligns with a cyclical pattern observed among Huione AI software vendors and five major pig butchering scams with on-chain exposure to Huoine Guarantee. When Huione AI software vendors see higher inflows, 2-11 days later, inflows rise for the pig butchering scams observed. Subsequently, 20-27 days after that increase, inflows to Huione AI software vendors rise; again, indicating that scammers are likely reinvesting scam proceeds into AI technology to execute new scams.



Last year, Huione launched a blockchain project called Xone, as well as its own USD-pegged stablecoin called “USDH”. Both entities are touted as unblockable and unrestricted by traditional regulatory agencies, likely to overcome asset seizure and freeze. Whether XOC or USDH will become Huione’s preferred means of trading remains to be seen. USDH is currently only available via Huione-affiliated websites, and according to an announcement in October 2024, the Huione Chain team is working with mainstream exchanges to allow the listing of USDH on trading platforms.

The interconnected nature of Huione vendors

A review of on-chain activity in the past year reveals the extent to which Huione vendors used each others’ services. The chart below shows the scale of this great degree of interconnectedness based on transfers within the Huione Guarantee platform.



When examining on-chain interactions in 2024 among vendors and scams on the Huione platform, the chord diagram above shows 2,345 transfers among scams, infrastructure providers, social media management services, AI service vendors, and data vendors. Given the larger width of the colored bands between infrastructure providers and social media management services, those two vendor types had the highest transaction activity in the group, sending funds mostly to each other, indicating frequent use of one another's services. Scams had moderate transaction activity, paying primarily for social media management services, as did data vendors and AI service vendors, which had the lowest amount of transfers and interaction with the other entities.

Crypto ATMs: A risk vector for fraud payments

Crypto automatic teller machines (ATMs) (also known as Bitcoin ATMs or crypto kiosks) allow users to buy and sell cryptocurrency using an ATM, and have been around for over a decade. While crypto ATMs are used for legitimate purposes, they are also popular among scammers, and in the last few years, the FBI has received thousands of reports about cybercriminals using crypto ATMs to receive payouts for scams. To receive funds from their victims, scammers often impersonate tech and customer support personnel as well as government officials. In the tech scam scenario, the common tactic is urgency: the victim must act quickly to solve an imminent personal crisis by withdrawing cash from their bank and depositing it into a crypto ATM.

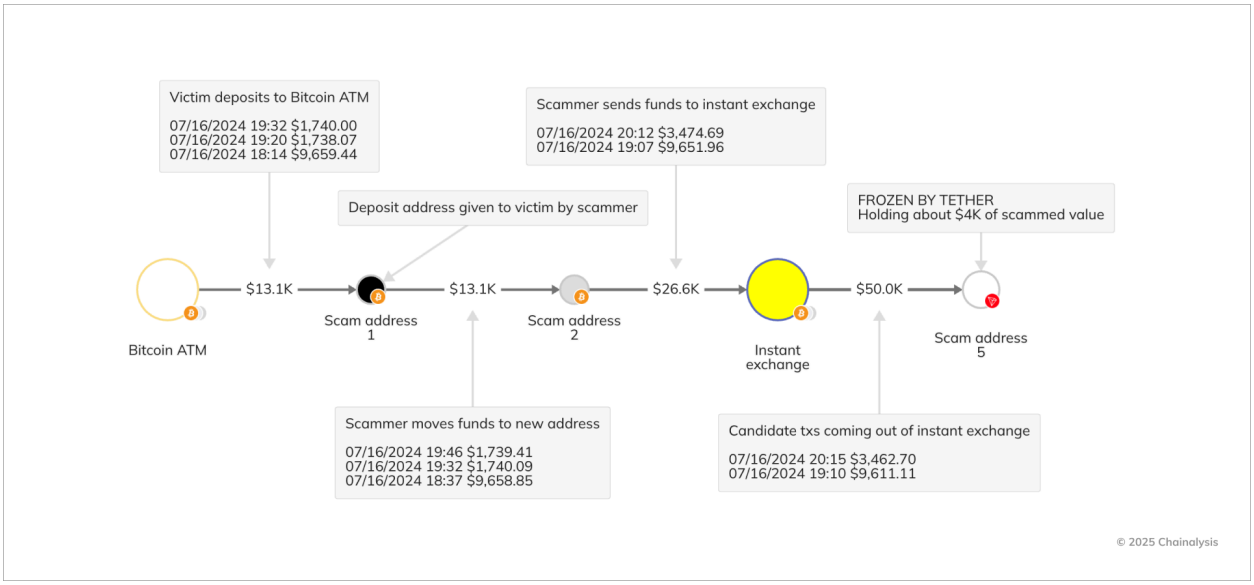
Since 2020, the Federal Trade Commission (FTC) has seen a tenfold increase in funds lost in the United States to scammers using crypto ATMs, according to reports from consumers. The FTC found that in just

the first six months of 2024, these losses exceeded $65 million with a median reported loss of $10,000 per individual.

Crypto ATM scam case study

Last year, a target living in the Midwest fell prey to a tech support scam in which scammers extracted payment via Bitcoin ATM. The victim had purchased a new laptop compromised by malware. When the victim began using the computer, a malware-initiated popup explained that a virus had infected it, and included a number to call for assistance, which led to a scammer impersonating Microsoft tech support. Ultimately, the scammer convinced the victim that $15,000 was required to resolve the issue.

The Reactor graph below shows three deposits the victim made at three Bitcoin ATMs, as instructed by the scammer. After ATM fees, the $15,000 totaled roughly $13,000 on-chain. Upon reflection, before the transactions were even confirmed, the victim returned home and reported the situation to local authorities. Using Chainalysis, investigators found that the scammer sent $13,100 from the original deposit address (Scam address 1) to an intermediary address (Scam address 2) and then onward to an instant exchange where they converted the funds to USDT (Scam address 5).



The county sheriff's department referred the case to state investigators and an FBI field office, and using the evidence gathered on-chain, brought the case to county court where the scammer was tried in absentia. After a guilty verdict was issued, authorities initiated the recovery process with Tether. When it comes to reporting crypto scams, time is of the essence, and the victim's quick action helped positively influence the outcome of this case. It's also key that law enforcement agencies have the knowledge and capabilities to investigate crypto crime.

Loss from crypto ATM scams

The FBI's Internet Crime Complaint Center (IC3) urges U.S. citizens to report all cyber-enabled crime. Using this data, the agency investigates these crimes, observes criminal trends, attempts to mitigate loss for victims, and works to prevent future cybercrime.

IC3's 2023 Elder Fraud Report disclosed that it had fielded over 15,000 scam complaints from people over 60, over 2,000 of which involved crypto ATMs. According to the report, "The use of cryptocurrency ATMs and kiosks has continued to increase as a payment mechanism, especially among Tech and Customer Support, Government Impersonation, and Confidence/Romance scams."

The FBI's 2023 Cryptocurrency Fraud Report also highlights the increasing prevalence of crypto ATM scams, reporting losses totaling $124.3 million that same year. And since 2020, 43% of crypto-related suspicious activity reports (SARs) have been tied to crypto ATMs, according to a 2024 report by the Financial Crimes Enforcement Network.

The push toward crypto ATM legislation

AARP, an organization dedicated to empowering people as they age, works to educate its audience about the risks of cryptocurrency scams and advocates for stronger consumer protections. Scams involving crypto ATMs are in the top 10 complaints the AARP Fraud Watch Network receives; on average, it fields three to four of these reports daily. Victim profiles transcend gender, and AARP often sees losses totaling in the tens of thousands of dollars or more. While the organization urges victims to submit their own reports via IC3 or local law enforcement, it also shares data with the FTC's Consumer Sentinel Network, and has strong law enforcement partnerships.

AARP explained that asset recovery for victims of crypto ATM scams is challenging for a few reasons:

1. Currently, no one is able to retrieve cash from a crypto ATM once a deposit is made, because transactions are irreversible.
2. Business owners with crypto ATMs in their stores can be uneducated about the purpose of these machines, and powerless to help customers who need assistance.
3. Police forces are generally not equipped to assist victims of crypto-related crimes, let alone those tied to crypto ATMs, because of a lack of training and resources.

In addition to these challenges, the biggest problem AARP sees with crypto ATMs is the lack of friction around their deployment and usage. When crypto ATM vendors approach business owners about installing crypto ATMs at their locations, vendors not only promise the machine will increase traffic to the store, they assure owners they will not have to maintain the ATM.

When it comes time for consumers to use these machines, friction is nearly non-existent in that process, too. Crypto ATMs are often placed in the back corner of convenience, liquor, or vape stores, and have few of the protections or security of fiat currency ATMs — like cameras and daily transaction limits. Guidance about what the machines are for, and the risks associated with them, is also limited.

Amy Nofziger, AARP Fraud Watch Network's director of victim support says, "There needs to be more transparency for business owners about what crypto ATM machines are used for and the risks they pose."

Francoise Cleveland, government affairs director at AARP, agrees. One victim calling the Fraud Watch Network Helpline had so much cash to deposit that it took her two hours. Cleveland said, “On noticing her discomfort, rather than raising concern about what she was doing, employees offered her a chair so she could sit down while she finished making her deposit.” In another case, a victim who had fallen prey to a scam was robbed as he approached a crypto ATM to make a deposit. Cleveland also learned of a scammer who pretended to be the owner of a store in which a crypto ATM was located and compelled one of the store’s employees to withdraw $3,000 from the register and deposit it into the machine.

Clark Flynt-Barr, government affairs director, financial security at AARP says, “While education is important, we can’t educate our way out of this problem, but change is possible by putting regulation in place to protect consumers.” She says that while some crypto ATM providers have tiered compliance programs, others are not compliant with federal regulations and aren’t doing as much as they should to prevent victim loss. Flynt-Barr pointed to the example of Money Gram and Western Union, formerly preferred channels for criminal wire transfers, and how protections the U.S. government enacted to help consumers made a difference.

As AARP advocates for consumer protections around crypto ATMs, here are some measures the organization believes could mitigate crime in the US:

- Crypto kiosk operators could flag an address for investigation that has received funds from crypto ATMs several times in a few hours.
- Lawmakers could:
    - Implement daily transaction limits, in particular for new customers, to limit the potential losses to fraud.
    - Require that crypto ATM operators refund fees associated with fraudulent transactions.
    - Require that all crypto ATMs include disclosures about how much fees cost, exchange rates, and warnings that criminals sometimes use the technology to facilitate scams.
    - Introduce some of the controls around crypto ATMs that exist around ATMs

In September of 2024, the U.S. Senate Committee on the Judiciary sent a letter endorsed by seven senators to the 10 largest crypto kiosk providers, urging those companies to “to take immediate action to address troubling reports that your Bitcoin ATMs (BTMs) are contributing to widespread financial fraud against elderly Americans.”

Meanwhile, several states have been working to enact legislation to protect consumers from scams facilitated by crypto ATMs. States like California and Vermont passed daily transaction limits of $1,000. Many states are requiring that vendors register as money transmitters in the state, enacting fee regulations, and requiring written disclosure notices both for business owners where kiosks are installed, and any consumers using them. So far, the most restrictive legislation comes from New Jersey, proposing a statewide ban on crypto ATMs. Here’s a list of crypto ATM legislation that some states have passed:

States that have passed crypto ATM legislation

State	Bill	Status
CA	Digital Financial Assets Law: Information for Kiosk Operators	Effective, 01/01/24
CT	5211: An act concerning virtual currency and money transmission	Passed, 01/06/24
MN	New Minnesota crypto law goes into effect to protect consumers against fraud	Effective, 08/01/24
VT	110: An act relating to banking, insurance, and securities	Effective, 07/01/24

As for regulatory measures in Europe, Markets in Crypto-Assets Regulation (MiCA) went into effect last year and reinforces existing EU and national anti-money laundering (AML) laws. Ahead of MiCA's rollout, last year, French regulators, including the French Financial Markets Authority (AMF) and the Paris inter-regional jurisdiction (JIRS), conducted search and seizure operations targeting unregistered crypto ATMs amid concerns they were being used for money laundering. French law dictates that these ATMs must be registered as digital asset service providers.

German authorities have also been cracking down on unregistered crypto ATMs. In August of 2024, Germany's Federal Financial Supervisory Authority (BaFin) seized roughly €25 million from unregistered crypto ATMs across the country. Similarly, in September of 2024, the UK's Financial Conduct Authority (FCA) charged an individual living in London for operating crypto ATMs without FCA registration. This operation was part of an ongoing effort by UK authorities to disrupt unregistered crypto ATMs, first announced in 2022.

In Türkiye, the Capital Markets Law was amended to include crypto assets in July 2024, which required that all crypto ATMs end operations within three months of the law coming into effect, i.e., by October 2024. It was further clarified that those that failed to comply would be shut down by the local authorities, with penalties for continued operations.

Across APAC, a number of regulators, such as in Singapore and Malaysia, have also taken steps to prohibit the operation of crypto ATMs. In Hong Kong, crypto ATMs would fall within the scope of the planned regulatory framework for OTC crypto businesses, which would include AML/CFT requirements. In Australia, the country which reportedly hosts the world's third highest number of crypto ATMs, the Australian Transaction Reports and Analysis Centre (AUSTRAC) has announced plans to tighten monitoring of crypto ATM providers.

As broader cryptocurrency regulation evolves worldwide, the question of who should be liable when victims are scammed is increasingly entering the conversation. For instance, the UK introduced legislation requiring that crypto businesses compensate victims of APP fraud facilitated by these platforms. Other countries are requiring firms to take more responsibility for frauds such as hacks. The policy landscape may be shifting towards making stakeholders more accountable across all fronts.

In the absence of regulation and compliance, crypto ATMs remain a well-known risk vector for illicit activity. The good news is their transactions are also transparent and traceable.

Global enablement, collaboration, and regulation are keys to fraud prevention

The analysis of 2024's crypto scams reveals a complex and evolving landscape. Platforms like Huione Guarantee enable the sophistication and professionalization of the scam ecosystem, and highlight the persistent and adaptive nature of these illicit activities. The potential of AI technology to exponentially scale crypto scams further adds to the challenges associated with combating these crimes.

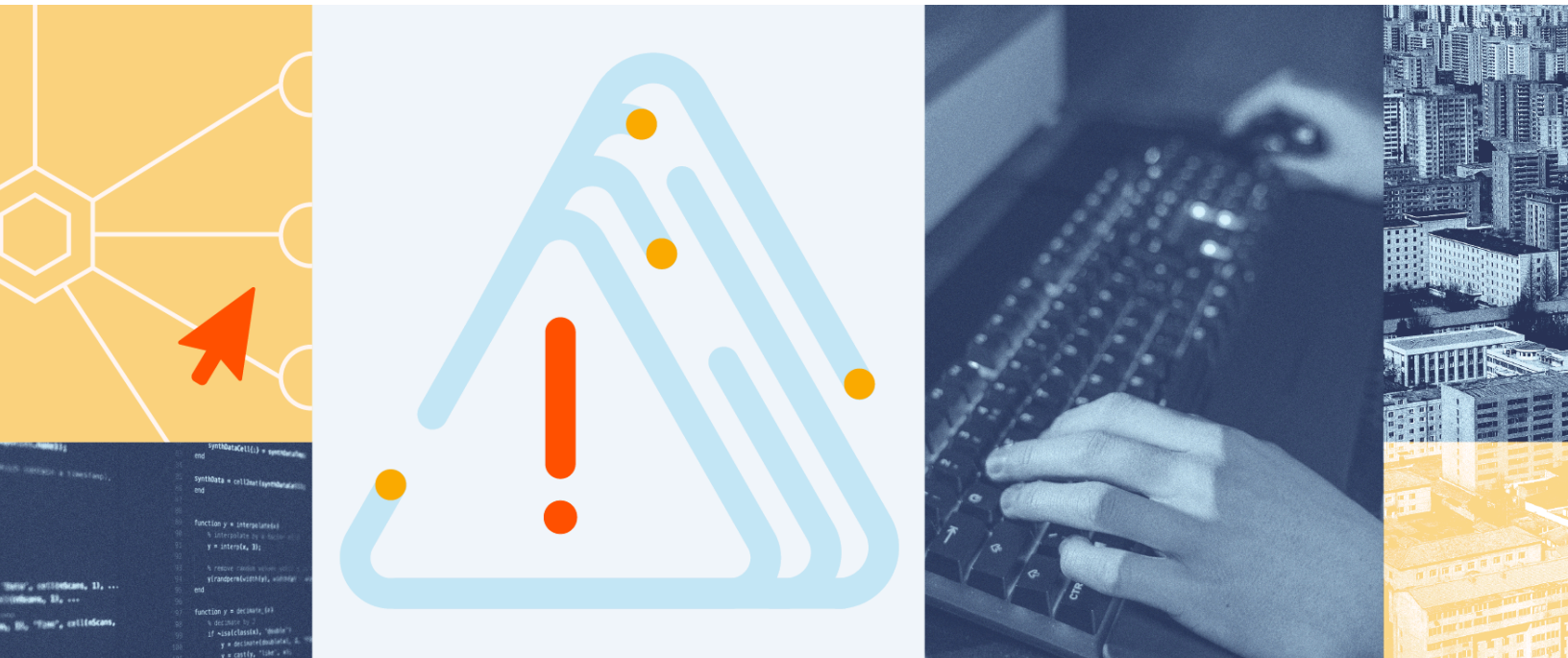
Both fraud detection and compliance rely on granular, real-time data. Combining Alterya's AI-powered fraud detection with the Chainalysis blockchain intelligence platform will enhance visibility into potential scam-related transactions, improving fraud prevention and enforcement capabilities. As scams continue to evolve, investigators need access to deeper intelligence, faster insights, and specialized expertise to detect and disrupt these emerging threats.

Efforts to combat scams must focus on both prevention and enforcement, requiring stronger investigative resources and greater enablement of government agencies and local authorities. Regulatory measures, such as those discussed for crypto ATMs, play a role in mitigating scam risk and protecting consumers. But effective disruption also requires collaboration between law enforcement, regulators, and the private sector.

A recent example is Operation Spincaster, a Chainalysis-led initiative that brings together public and private sector organizations to disrupt and prevent scams. Through our advanced blockchain tracing capabilities, data and targeted training, investigators identified and traced thousands of compromised wallets amounting to over $187 million in losses, demonstrating how a coordinated, intelligence-led ecosystem approach can disrupt scam infrastructure and support victims.

Combatting crypto scams at scale requires sustained efforts from government agencies, regulators and organizations. Chainalysis works alongside these organizations to build investigative capacity, enhance intelligence, and empower investigators with the technology needed to stay ahead of emerging threats.

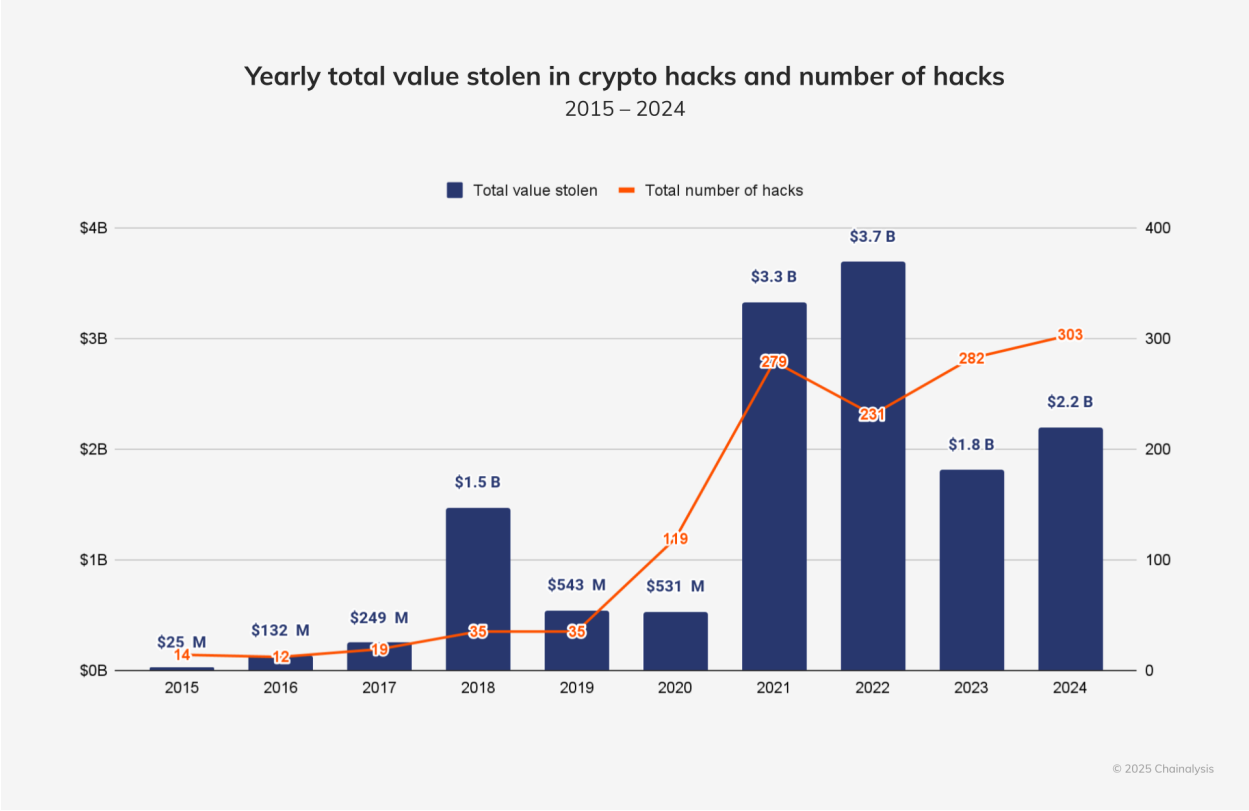
Stolen Funds



$2.2 Billion Stolen from Crypto Platforms in 2024, but Hacked Volumes Stagnate Toward Year-End as DPRK Slows Activity Post-July

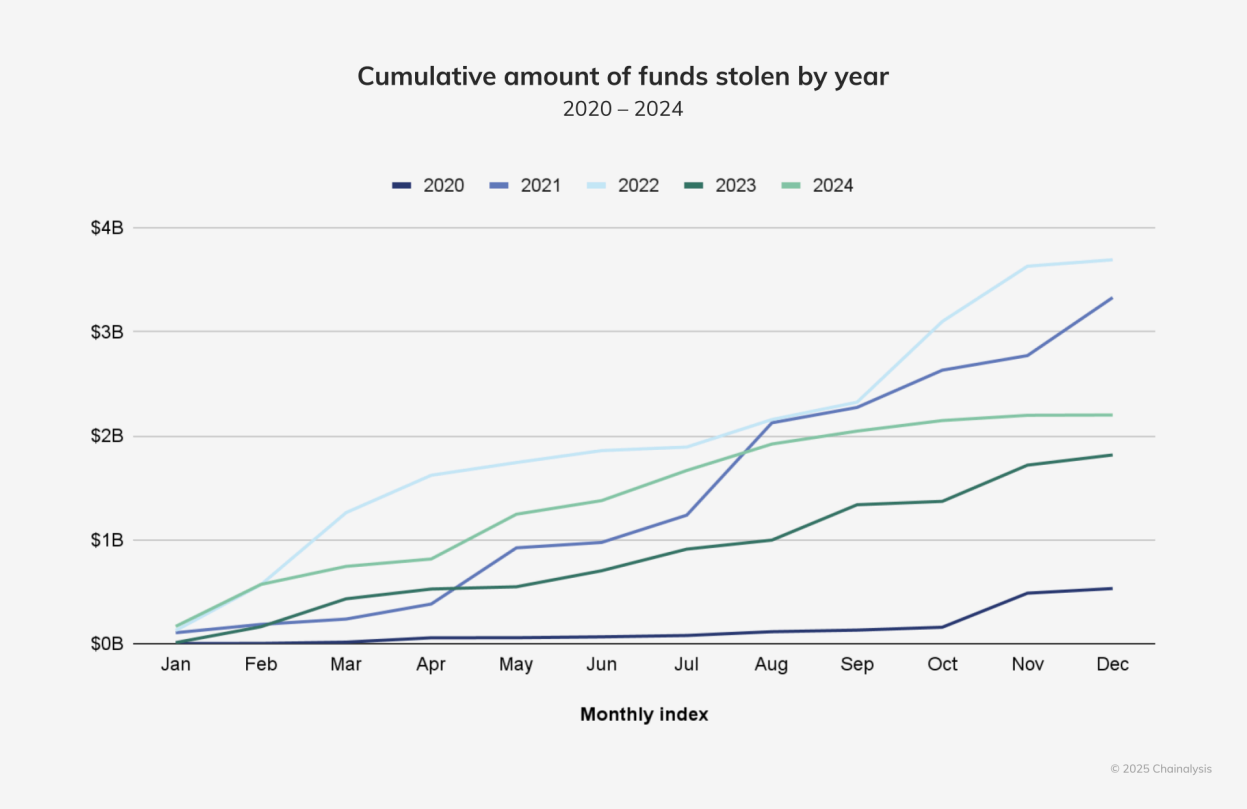
Crypto hacking remains a persistent threat, with four years in the past decade individually seeing more than a billion dollars' worth of crypto stolen (2018, 2021, 2022, and 2023). 2024 marks the fifth year to reach this troubling milestone, highlighting how, as crypto adoption and prices rise, so too does the amount that can be stolen.

In 2024, funds stolen increased by approximately 21.07% year-over-year (YoY) to $2.2 billion, and the number of individual hacking incidents increased from 282 in 2023 to 303 in 2024.



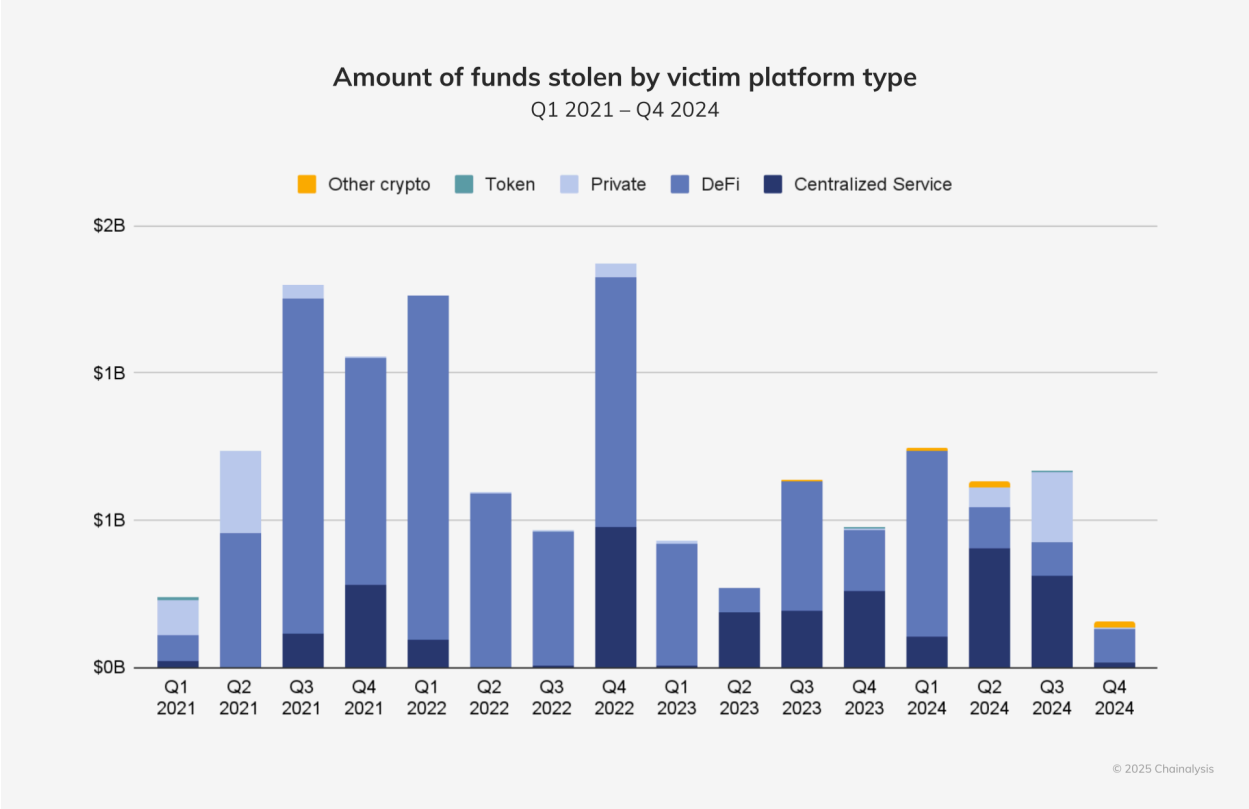
Interestingly, the intensity of crypto hacking shifted about halfway through the year. In our mid-year crime update, we noted that cumulative value stolen between January 2024 and July 2024 had already reached $1.58 billion, approximately 84.4% higher than the value stolen over the same period in 2023. As we see in the chart below, through the end of July, the ecosystem was easily on track for a year that could rival the

$3 billion+ years of 2021 and 2022. However, 2024's upward trend slowed considerably after July, after which it remained relatively steady. Later, we'll explore a potential geopolitical reason for this change.

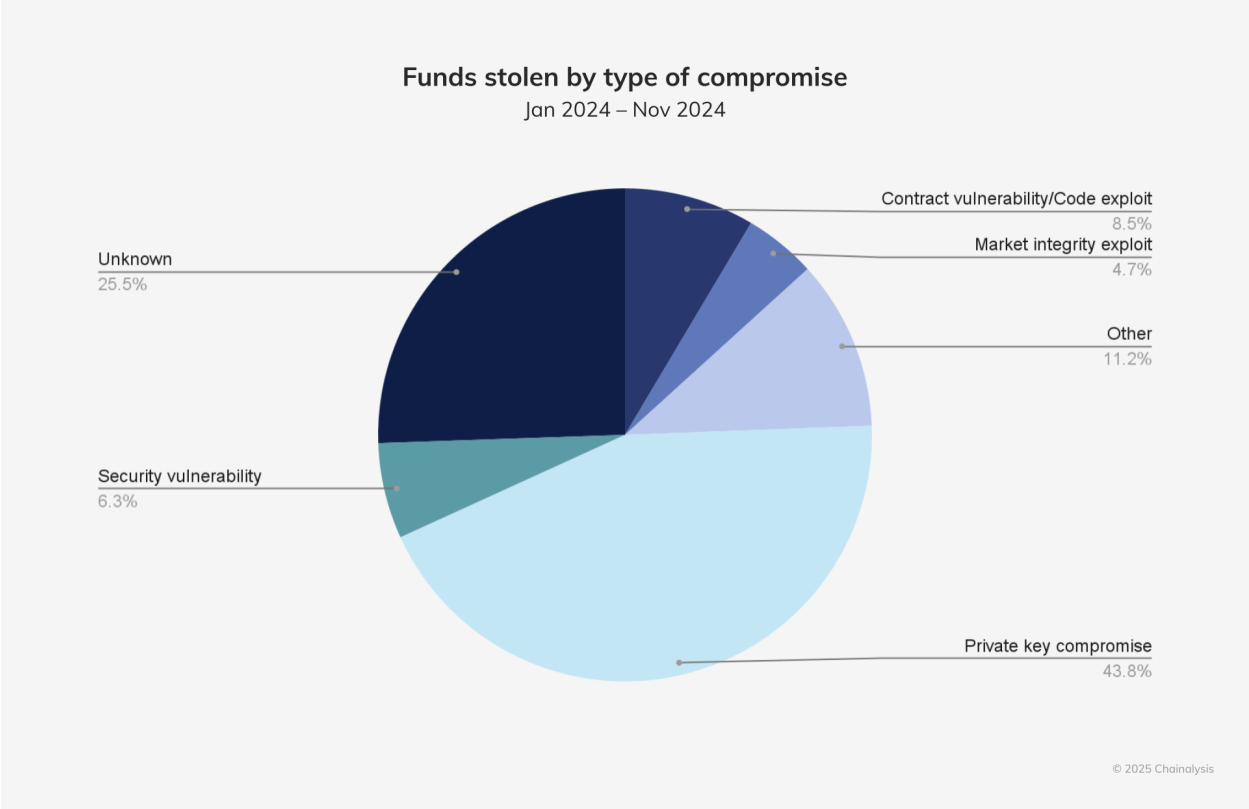


In terms of amount stolen by victim platform type, 2024 also saw interesting patterns. In most quarters between 2021 and 2023, decentralized finance (DeFi) platforms were the primary targets of crypto hacks. It's possible that DeFi platforms were more vulnerable because their developers tend to prioritize rapid growth and bringing their products to market over implementing security measures, making them prime targets for hackers.

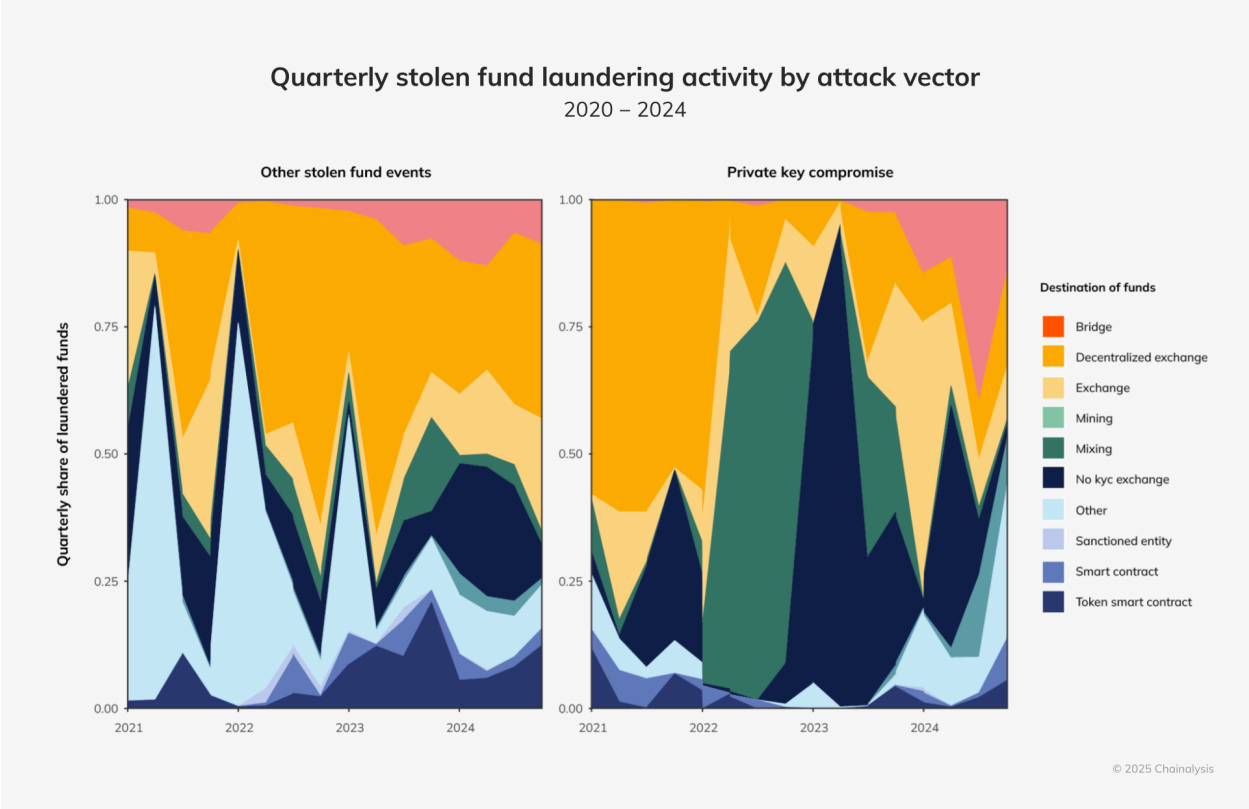
Although DeFi still accounted for the largest share of stolen assets in the first quarter of 2024, centralized services were the most targeted in Q2 and Q3. Some of the most notable centralized service hacks include DMM Bitcoin (May 2024; $305 million) and WazirX (July 2024; $234.9 million).



This shift in focus from DeFi to centralized services highlights the increasing importance of securing mechanisms commonly exploited in hacks, such as private keys. Private key compromises accounted for the largest share of stolen crypto in 2024, at 43.8%. For centralized services, ensuring the security of private keys is critical, as they control access to users' assets. Given that centralized exchanges manage substantial amounts of user funds, the impact of a private key compromise can be devastating; we only have to look at the $305 million DMM Bitcoin hack, which is one of the largest crypto exploits to date, and may have occurred due to private key mismanagement or lack of adequate security.



After compromising private keys, malicious actors often launder stolen funds by funneling them through decentralized exchanges (DEXs), mining services, or mixing services to obfuscate the transaction trail and complicate tracing. In 2024, we can see that the laundering activity of private key hackers differs meaningfully from that of hackers exploiting other attack vectors. For instance, after stealing private keys, these hackers often turned to bridges and mixing services. For other attack vectors, DEXs were more popular for laundering.

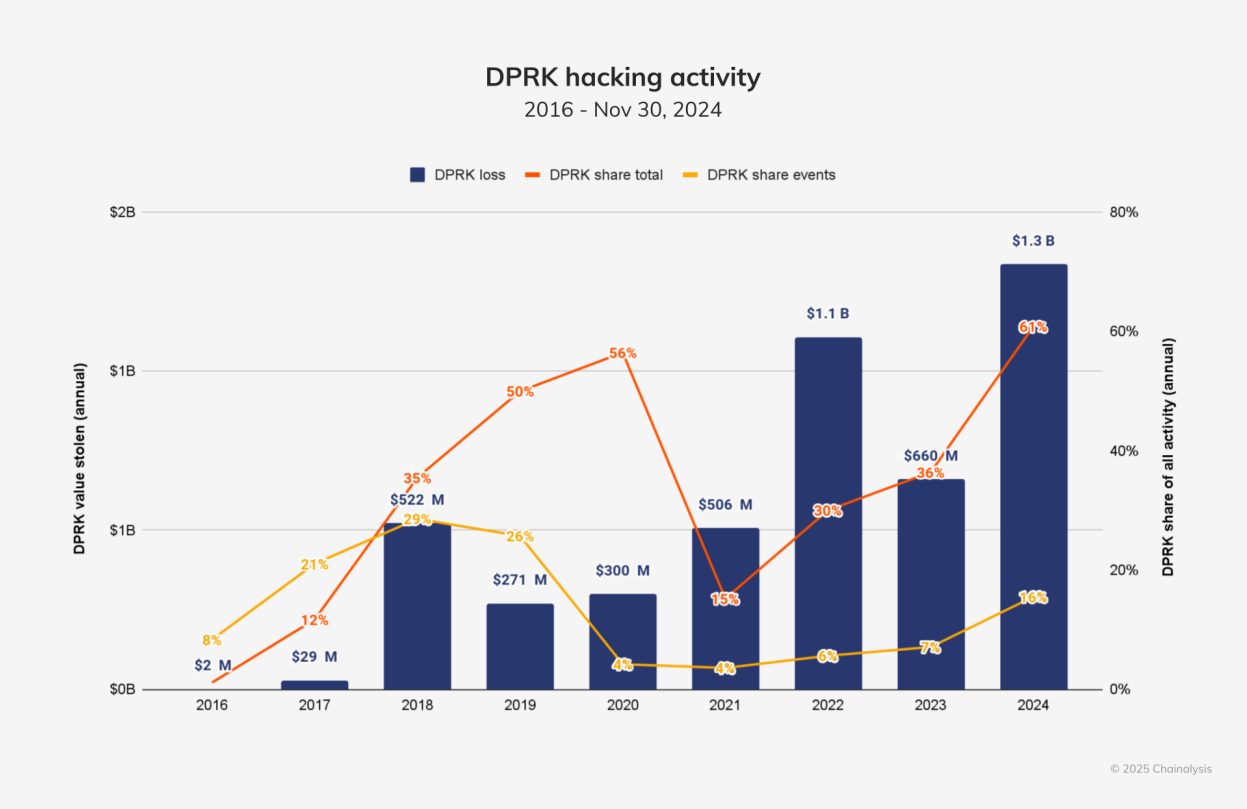


Keep reading to learn more about crypto hacking trends in 2024, the DPRK's activities, and Hexagate's use of machine learning models to proactively detect suspicious hacking behaviors, a capability recently acquired by Chainalysis.

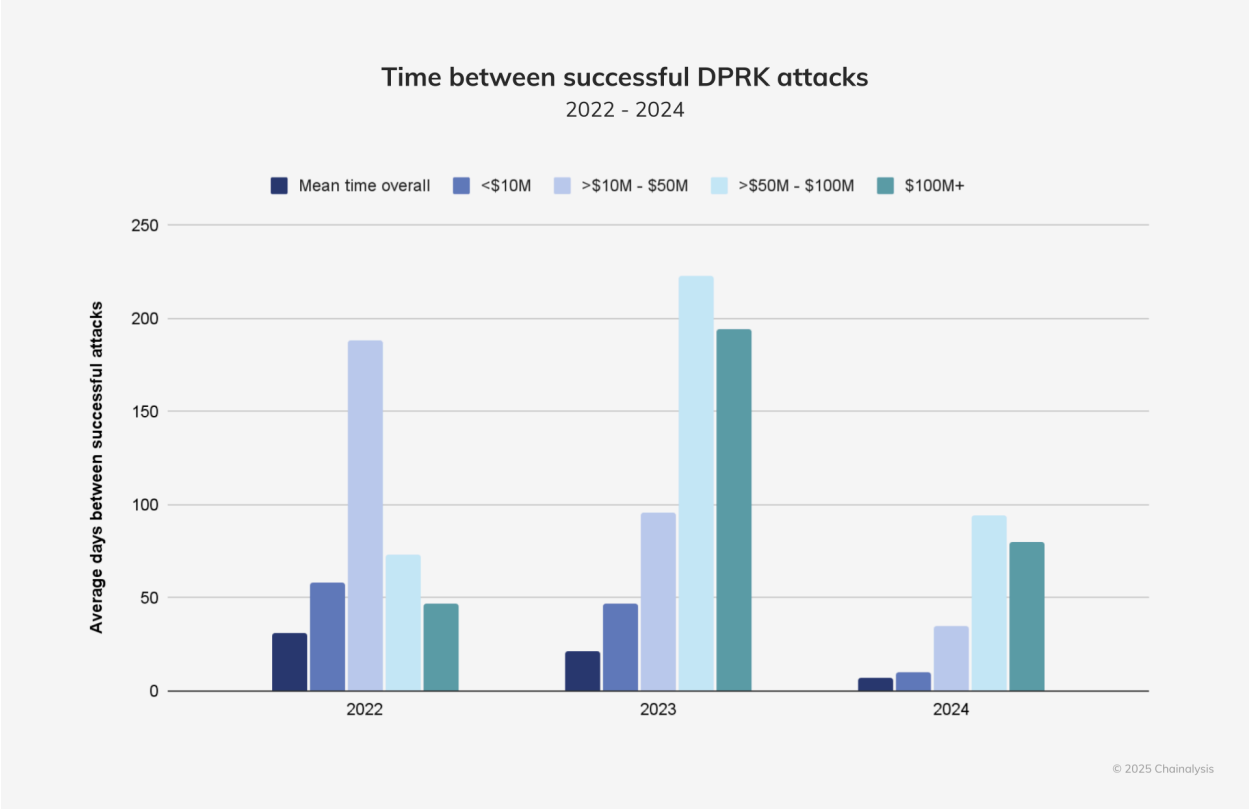
In 2024, North Korean hackers stole more from crypto platforms than ever before

Hackers linked to North Korea have become notorious for their sophisticated and relentless tradecraft, often employing advanced malware, social engineering, and cryptocurrency theft to fund state-sponsored operations and circumvent international sanctions. U.S. and international officials have assessed that Pyongyang uses the crypto it steals to finance its weapons of mass destruction and ballistic missiles programs, endangering international security. In 2023, North Korea-affiliated hackers stole approximately $660.50 million across 20 incidents; in 2024, this number increased to $1.34 billion stolen across 47 incidents — a 102.88% increase in value stolen. These figures represent 61% of the total amount stolen for the year, and 20% of total incidents.

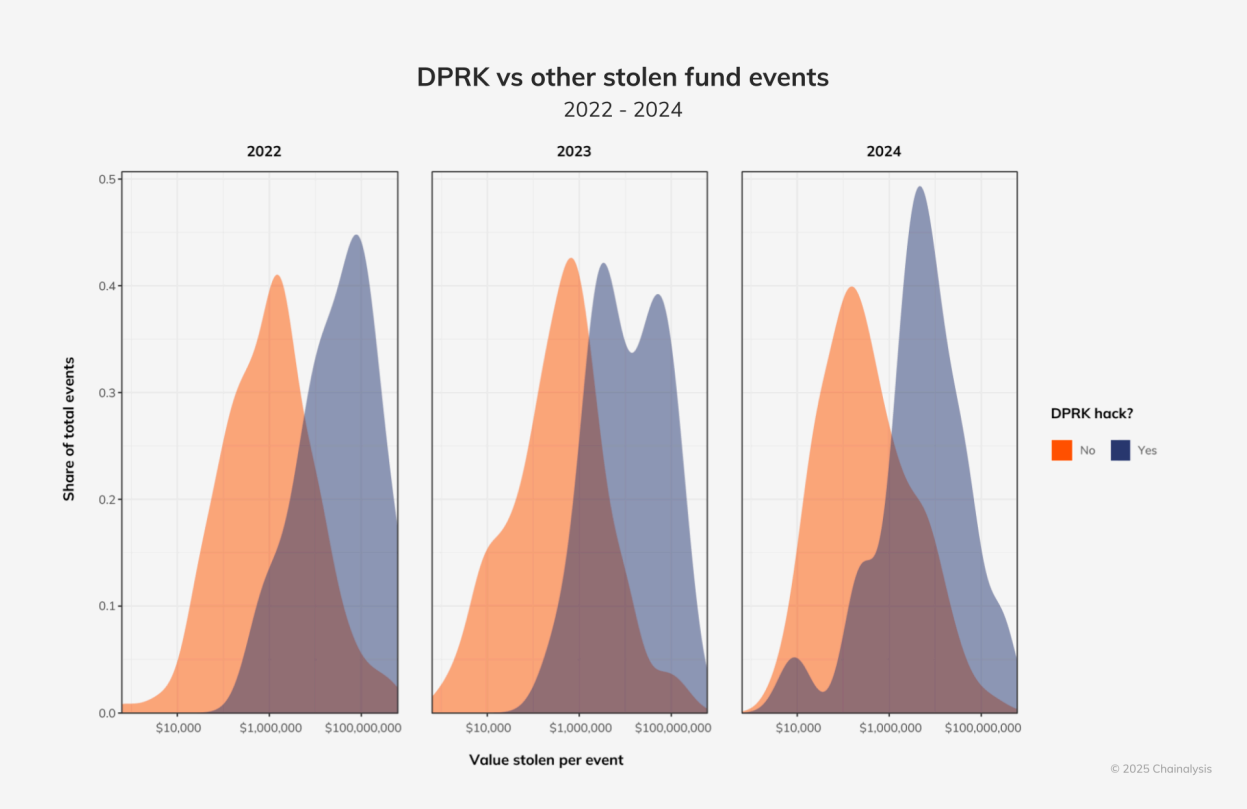
Note that, in last year's report, we published that the DPRK stole $1.0 billion across 20 hacks. Upon further investigation, we determined that certain large hacks we had previously attributed to the DPRK are likely no longer related, hence the decrease to $660.50 million. However, the number of incidents remains the same, as we identified other smaller hacks attributed to the DPRK. We aim to constantly re-evaluate our assessment of DPRK-linked hacking events as we acquire new on-chain and off-chain evidence.



Unfortunately, it appears that the DPRK's crypto attacks are becoming more frequent. In the below chart, we examined the average time between successful DPRK attacks depending on the size of the exploit and found that there was a decline YoY in attacks of all sizes. Notably, attacks between $50 and $100 million, and those above $100 million occurred far more frequently in 2024 than they did in 2023, suggesting that the DPRK is getting better and faster at massive exploits. This is in stark contrast to the previous two years, during which its exploits more often each yielded profits below $50 million.



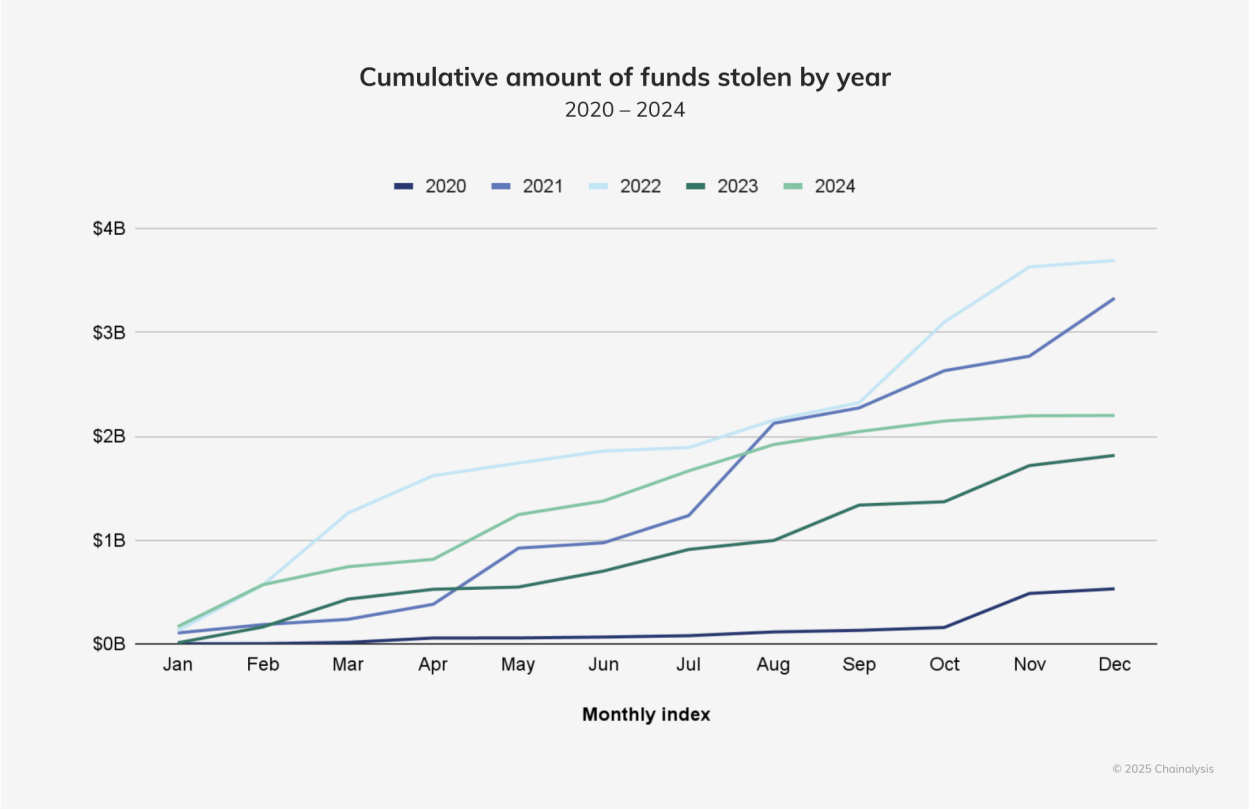
When examining the DPRK's activity in comparison to all other hacks we measured, it is clear that the DPRK has been consistently responsible over the last three years for most large-size exploits. Interestingly, the DPRK's dominance of the high end of the exploitation ladder continued in 2024, but there is also a growing density of DPRK hacks at lower amounts, most notably around $10,000 in value.



Some of these events appear to be linked to North Korean IT workers, who have been increasingly infiltrating crypto and Web3 companies, and compromising their networks, operations, and integrity. These workers often use sophisticated Tactics, Techniques, and Procedures (TTPs), such as false identities, third-party hiring intermediaries, and manipulating remote work opportunities to gain access. In a recent case, the U.S. Department of Justice (DOJ) indicted 14 DPRK nationals who obtained employment as remote IT workers at U.S. companies and generated more than $88 million by stealing proprietary information and extorting their employers.

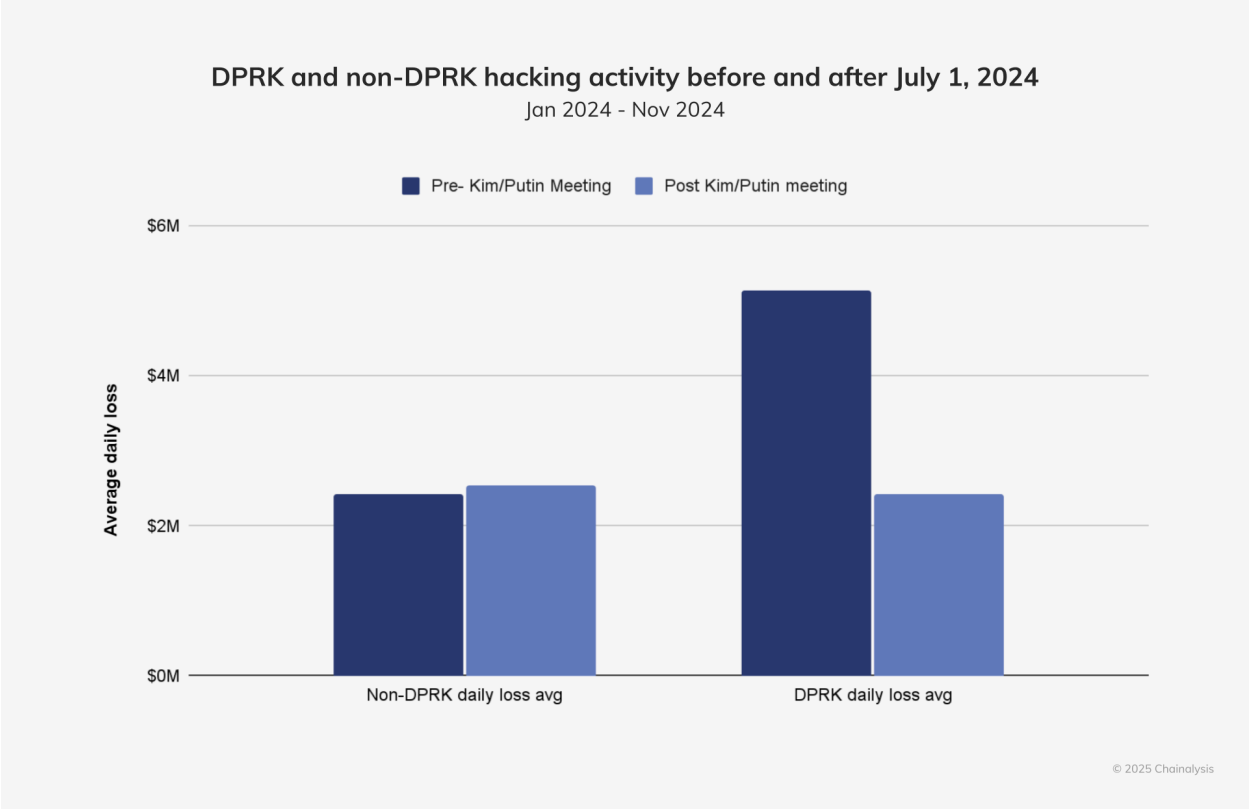
To mitigate these risks, companies should prioritize thorough employment due diligence — including background checks and identity verification — while maintaining robust private key hygiene to safeguard critical assets, if applicable.

Although all of these trends suggest a very active year for the DPRK, most of its exploits occurred at the beginning of the year, with overall hacking activity stagnating in Q3 and Q4, as shown in this chart from earlier.



In late June 2024, Russian President Vladimir Putin and North Korean leader Kim Jong Un met in Pyongyang at a summit to sign a mutual defense pact. So far this year, their growing alliance has been marked by Russia releasing millions of dollars in North Korean assets previously frozen in compliance with UNSC sanctions. Meanwhile, North Korea has deployed troops to Ukraine, supplied Russia with ballistic missiles, and reportedly sought advanced space, missile, and submarine technology from Moscow.

If we contrast the average daily value lost from DPRK exploits before and after July 1, 2024, we can see a significant decrease in the amount of value stolen. Specifically, as shown in the chart below, amounts stolen by the DPRK dropped by approximately 53.73% after the summit, whereas non-DPRK amounts stolen rose by approximately 5%. It is therefore possible that, in addition to redirecting military resources toward the conflict in Ukraine, the DPRK — which has dramatically increased its cooperation with Russia in recent years — may have altered its cybercriminal activity as well.

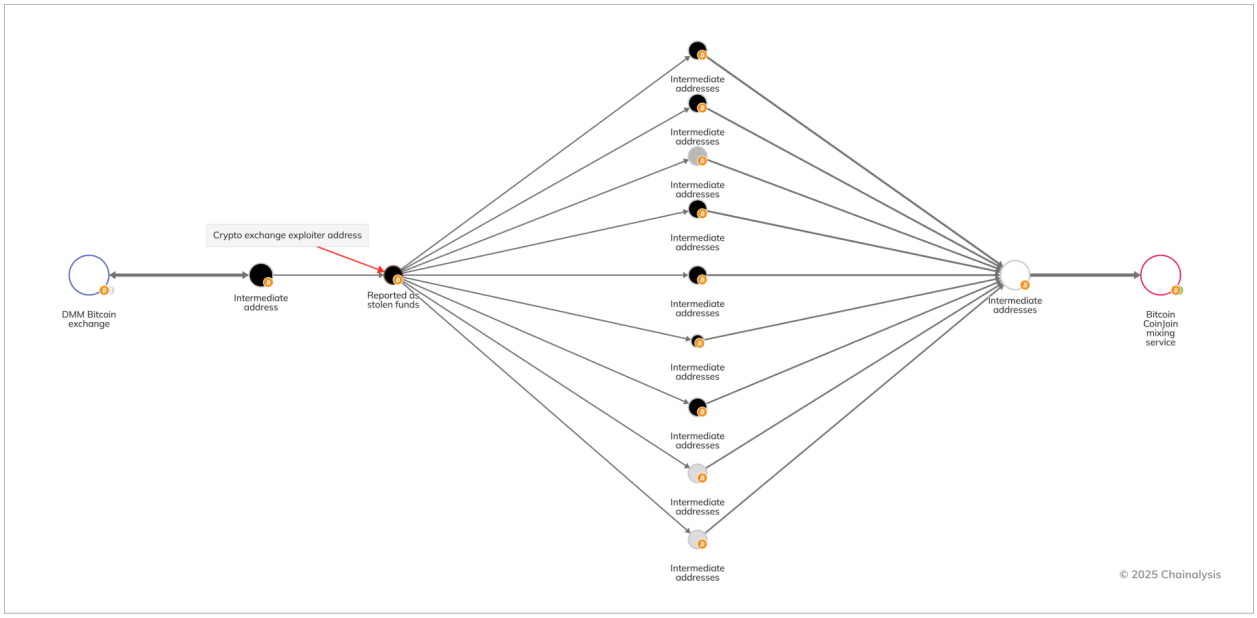


The decline in funds stolen by the DPRK after July 1, 2024 is clear and the timing is conspicuous, but it is nevertheless important to note that this decline is not necessarily associated with Putin's visit to Pyongyang. Additionally, a few events in December could alter the pattern by the end of the year, and attackers often strike over holidays.

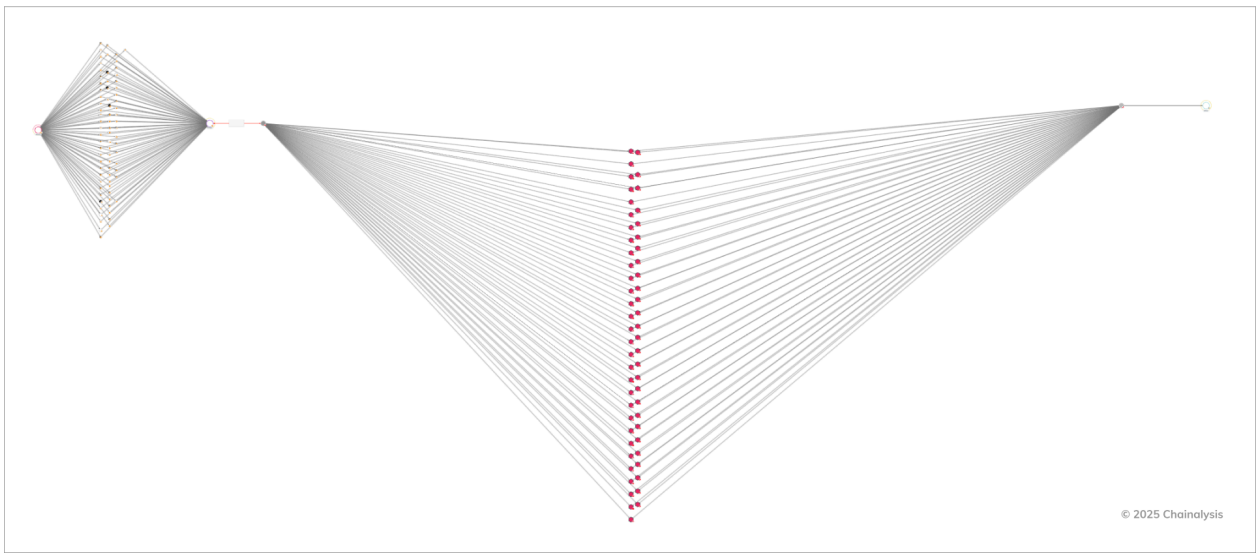
Case study: The DPRK's DMM Bitcoin exploit

One notable example of a North Korea-affiliated hack in 2024 involved Japanese cryptocurrency exchange, DMM Bitcoin, which suffered a security breach resulting in the loss of approximately 4,502.9 Bitcoin, valued at $305 million at the time. The attackers targeted vulnerabilities in DMM's infrastructure, leading to unauthorized withdrawals. In response, DMM fully covered customer deposits by sourcing equivalent funds with the support of group companies.

We were able to analyze the flow of funds on-chain after the initial attack, which we've broken down into two Chainalysis Reactor graphs below. In the first phase, we see that the attacker moved millions of dollars' worth of crypto from DMM Bitcoin to several intermediary addresses before eventually reaching a Bitcoin CoinJoin Mixing Service.



After successfully mixing the stolen funds using the Bitcoin CoinJoin Mixing Service, the attackers moved a portion of the funds through a number of bridging services, and finally to Huione Guarantee, an online marketplace tied to the Cambodian conglomerate, Huione Group, which was previously exposed as a significant player in facilitating cybercrimes.



The scale of the breach and the subsequent operational challenges led DMM to decide to shut down the exchange in December 2024. DMM Bitcoin transferred its assets and customer accounts to SBI VC Trade, a subsidiary of the Japanese financial conglomerate, SBI Group, with the transition set to be finalized by March 2025. Fortunately, emerging tools and predictive technologies, as we'll explore in the next section, are paving the way to potentially prevent such devastating hacks before they occur.

Leveraging predictive models to thwart hacks

Advanced predictive technologies are transforming cybersecurity by enabling real-time detection of potential risks and threats, offering a proactive approach to safeguarding digital ecosystems. Chainalysis recently acquired Hexagate, the leading provider of Web3 security solutions that detect and mitigate threats including cyber exploits, hacks, and governance and financial risks. Hexagate's customers have already saved more than $1 billion in customer funds by taking on-chain actions based on real-time notifications and automated responses to potential threats.

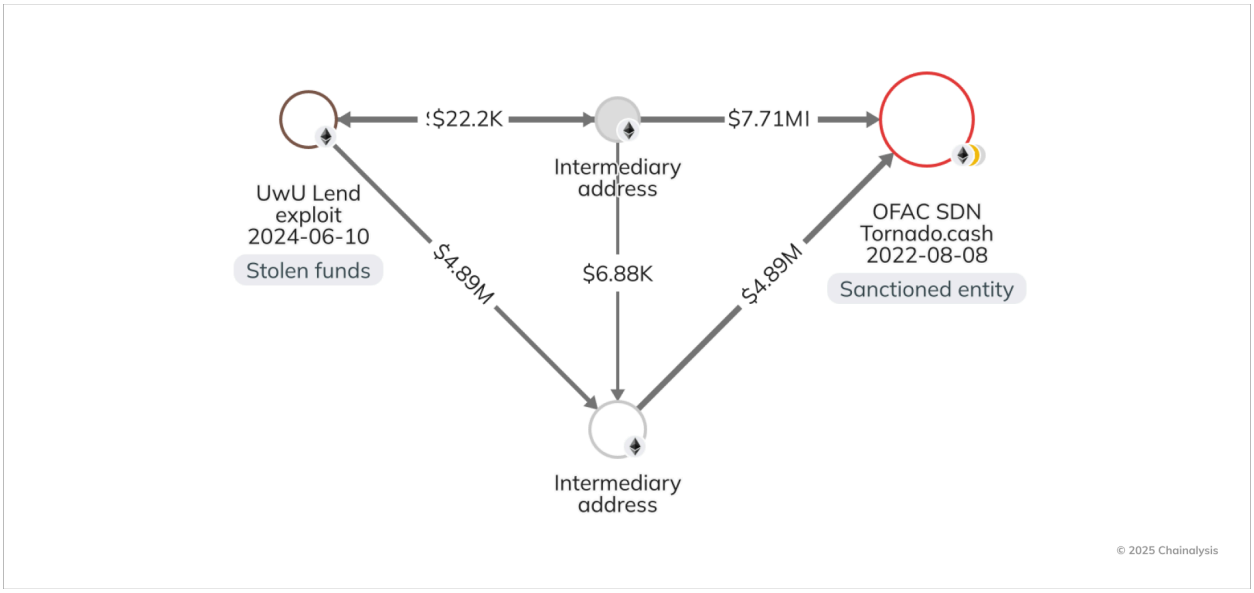
Hexagate leverages proprietary detection technology and machine learning models to proactively predict and detect unusual transactions and malicious activities across blockchain networks in real-time. By continuously scanning smart contracts and transactions, Hexagate's system identifies suspicious patterns, and potential risks and threats before they can cause financial losses. Let's look at an example below, involving decentralized liquidity provider, UwU Lend.

On June 10, 2024, an attacker exploited UwU Lend for approximately $20 million by manipulating its price oracle system. The attacker initiated a flash loan attack to alter the price of Ethena Staked USDe (sUSDe) across multiple oracles, leading to incorrect valuations. Consequently, the attacker could borrow millions of dollars within seven minutes. Hexagate's detection of the attack contract and similar deployments of it occurred approximately two days before the exploit.

Although the attack contract was accurately detected in real-time two days before the exploit, its connection to the exploited contract wasn't immediately apparent due to its design. With additional tools, such as Hexagate's security oracle, this early detection could have been further leveraged to mitigate the threat. Notably, the first attack, which resulted in $8.2 million in losses, occurred just minutes before subsequent attacks, providing another significant signal.

These types of alerts before major on-chain attacks have the potential to transform industry players' security, empowering them to prevent costly hacks altogether, rather than respond to them.

In the Chainalysis Reactor graph below, we see that the attacker transferred the stolen funds through two intermediary addresses before the funds reached OFAC-sanctioned Ethereum smart-contract mixer, Tornado Cash.



Are you a Reactor user? View this graph for yourself here.

It is important to note, however, that simply having access to these predictive models doesn't ensure hack prevention, as protocols may not always possess the proper tools to act effectively.

The need for stronger crypto security

The rise in stolen crypto in 2024 underscores the need for the industry to address an increasingly complex and evolving threat landscape. While the scale of crypto theft has not yet returned to the levels of 2021 and 2022, the resurgence described above highlights gaps in existing security measures and the importance of adapting to new exploit methods. To combat these challenges effectively, a collaborative approach between the public and private sectors is essential. Data-sharing initiatives, real-time security solutions, advanced tracing tools, and targeted training can empower stakeholders to quickly identify and neutralize malicious actors while building the resilience needed to safeguard crypto assets.

Additionally, as crypto regulatory frameworks continue to develop, the scrutiny on platform security and customer asset protection will likely intensify. Industry best practices must keep pace with these changes, ensuring both prevention and accountability. By fostering stronger partnerships with law enforcement and equipping teams with the resources and expertise to respond rapidly, the crypto industry can reinforce its defenses against theft. Such efforts are not only critical for protecting individual assets, but also for building long-term trust and stability in the digital ecosystem.

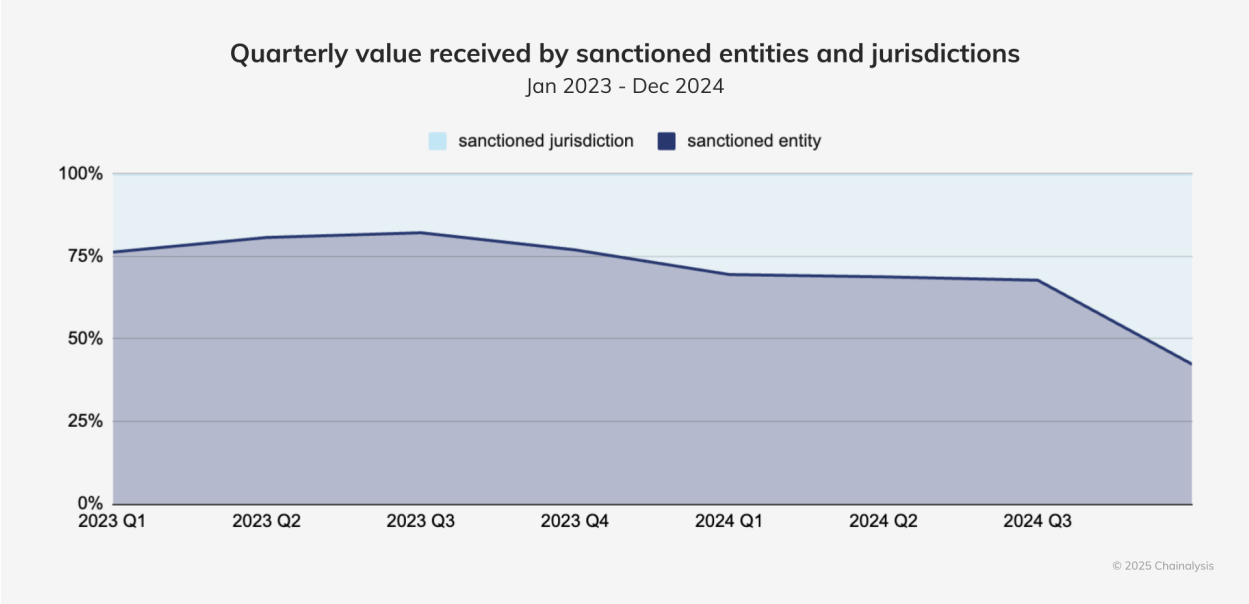
Sanctions

Iranians Flock to Crypto Amidst Geopolitical Tension; International Sanctions Actions Disrupt Russia's War Machine

In 2024, sanctions shifted in both scope and strategy, reflecting a broader evolution in illicit on-chain activity in response to increasing geopolitical tension. As sanctioned entities turn to alternative financial channels like cryptocurrency, the United States (U.S.) Treasury's Office of Foreign Assets Control (OFAC) has intensified efforts to dismantle the financial infrastructure sustaining sanctioned states, moving beyond traditional banking. The U.S. and its allies continued to take aim at Russia's wartime economy, while actions against Iran's Islamic Revolutionary Guard Corps (IRGC) escalated, affirming a deeper commitment to curbing state-backed financing.

Sanctioned jurisdictions and entities received $15.8 billion in cryptocurrency in 2024, accounting for about 39% of all illicit crypto transactions. In total, OFAC issued 13 designations that included cryptocurrency addresses — slightly fewer than in 2023 — but still the second-highest in the last seven years.

In a departure from prior years, sanctioned jurisdictions accounted for a record share of total sanctions-related activity compared to individual entities, commanding nearly 60% by the end of 2024, as we see below.



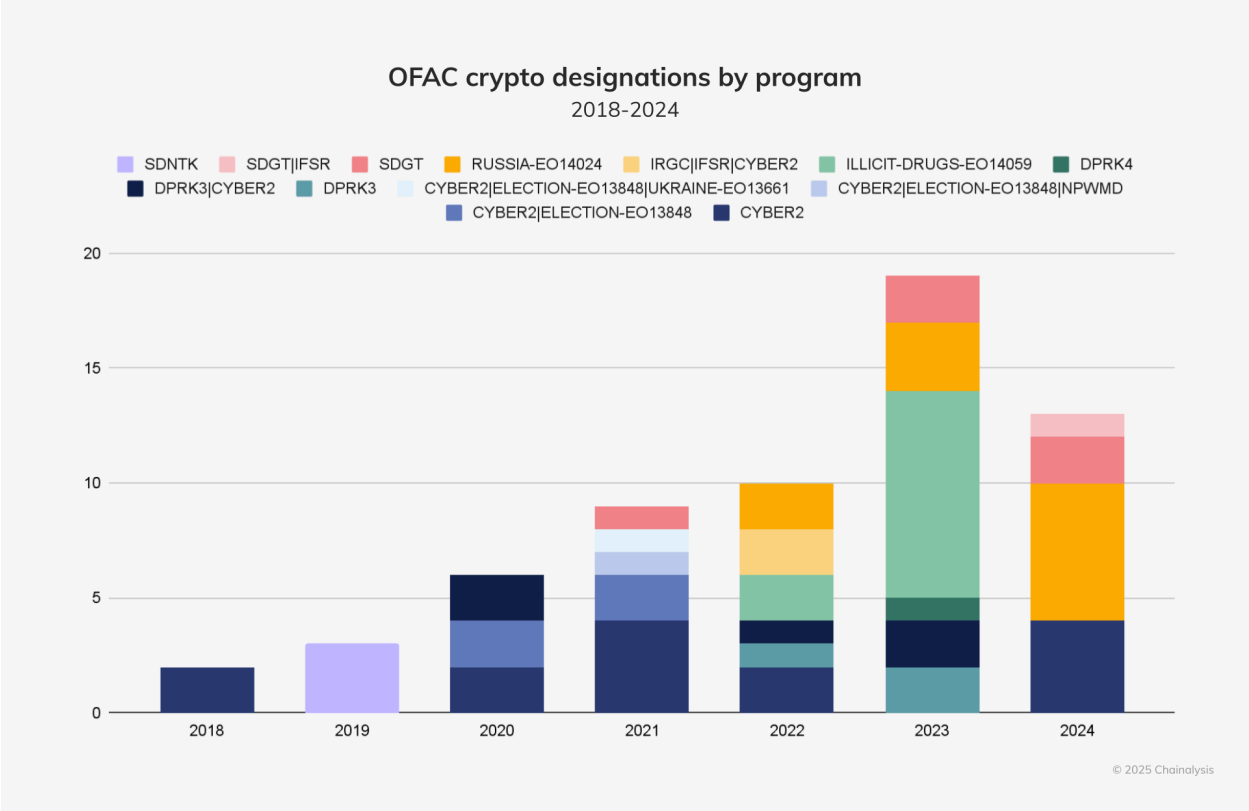
This shift was largely driven by Iran's growing use of cryptocurrency. As we'll explore further down, Iranian centralized exchanges (CEXs) saw a surge in both usage and outflows, with transaction patterns

suggesting capital flight. This reflects a broader trend among residents of sanctioned jurisdictions, who turn to cryptocurrency as an alternative system in restrictive economic environments.

Sanctions in 2024 take aim at core financial networks

In 2024, OFAC's crypto-related sanctions moved beyond mostly targeting individuals and small groups, taking direct aim at the financial infrastructure supporting illicit activity. While fewer new sanctions involving crypto were issued, the financial footprint of targeted entities remained substantial.

In the chart below, we can see how the composition of OFAC's crypto-related sanctions has evolved over time, mapped by Executive Order (EO) and sanctions program.



This focus was most evident in the increased use of EO 14024, with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation, which became the dominant program for crypto-linked sanctions as the U.S. and its allies escalated efforts to weaken Russia's financial infrastructure. Sanctions efforts primarily focused on networks facilitating sanctions evasion, cybercrime, and military procurement.

Major actions targeting Russian crypto activity

In 2024, Western agencies launched a series of major crackdowns on Russian-linked crypto entities that played key roles in supporting Russia's war economy, illicit cyber activities, and organized crime networks.

August 23, 2024

OFAC sanctioned KB Vostok OOO, a Russian UAV developer supplying drones to Russian forces in Ukraine, as part of a broader crackdown on nearly 400 entities supporting Russia's military supply chain. Like OKO Design Bureau, another UAV developer sanctioned earlier in the year with a smaller on-chain footprint, KB Vostok solicited cryptocurrency donations and likely facilitated UAV sales using crypto.

Our on-chain analysis revealed that a single counterparty of KB Vostok accounted for 16 of 24 transactions with KB Vostok's sanctioned address, with transfer amounts closely matching the price of its Scalpel UAVs. This counterparty has processed nearly $40 million in transfers and used multiple deposit addresses at the sanctioned Russian exchange Garantex, which has handled over $100 million in cryptocurrency, suggesting potential involvement of Russia's military procurement network.

September 19, 2024

The German Federal Criminal Police (BKA) seized the infrastructure of 47 Russian-language no-KYC crypto exchanges in "Operation Final Exchange." These platforms, which lacked Know Your Customer (KYC) protocols, were exploited for ransomware payments, darknet transactions, and sanctions evasion.

Our analysis of the targeted platforms revealed extensive illicit activity. Many received significant inflows from darknet markets, stolen funds, and sanctioned entities, demonstrating their deep integration into the cybercrime ecosystem. These services also enabled Russian nationals to evade sanctions, offering on- and off-ramps to and from sanctioned Russian banks. Despite using servers based in Germany, the exchanges primarily catered to Russian users, with default language settings in Russian and fiat transaction options tied to sanctioned banks like Sberbank.

September 26, 2024

OFAC sanctioned Russia-based crypto exchange Cryptex and its operator, Sergey Sergeevich Ivanov, for laundering funds linked to fraud shops, ransomware, and darknet markets. Cryptex processed over $5.88 billion in transactions since 2018, serving as a financial intermediary for illicit actors. Concurrently, FinCEN labeled the no-KYC exchange PM2BTC, which processed over $1 billion, as a primary money laundering concern under the Combating Russian Money Laundering Act. These sanctions were part of Operation Endgame, a broader, coordinated effort between U.S. and European authorities to dismantle financial enablers of cybercrime. Dutch and U.S. law enforcement seized related domains and infrastructure, while the U.S. State Department issued a $10 million reward for information leading to Ivanov's arrest. Additionally, Dutch law enforcement, with support from Chainalysis and Tether, seized €7 million worth of funds.

Cryptex, PM2BTC, and UAPS – a payment processor operated by Ivanov that catered primarily to fraud shops – handled billions in transactions for cybercriminals, including ransomware groups and fraud shops. Our on-chain analysis shows that in 2024 alone, UAPS funneled over $97 million to Cryptex, demonstrating its deep financial ties.

December 4, 2024

The UK's National Crime Agency (NCA) dismantled a multi-billion dollar Russian-speaking money laundering network in Operation Destabilise, an action that led to 84 arrests and the seizure of over €20

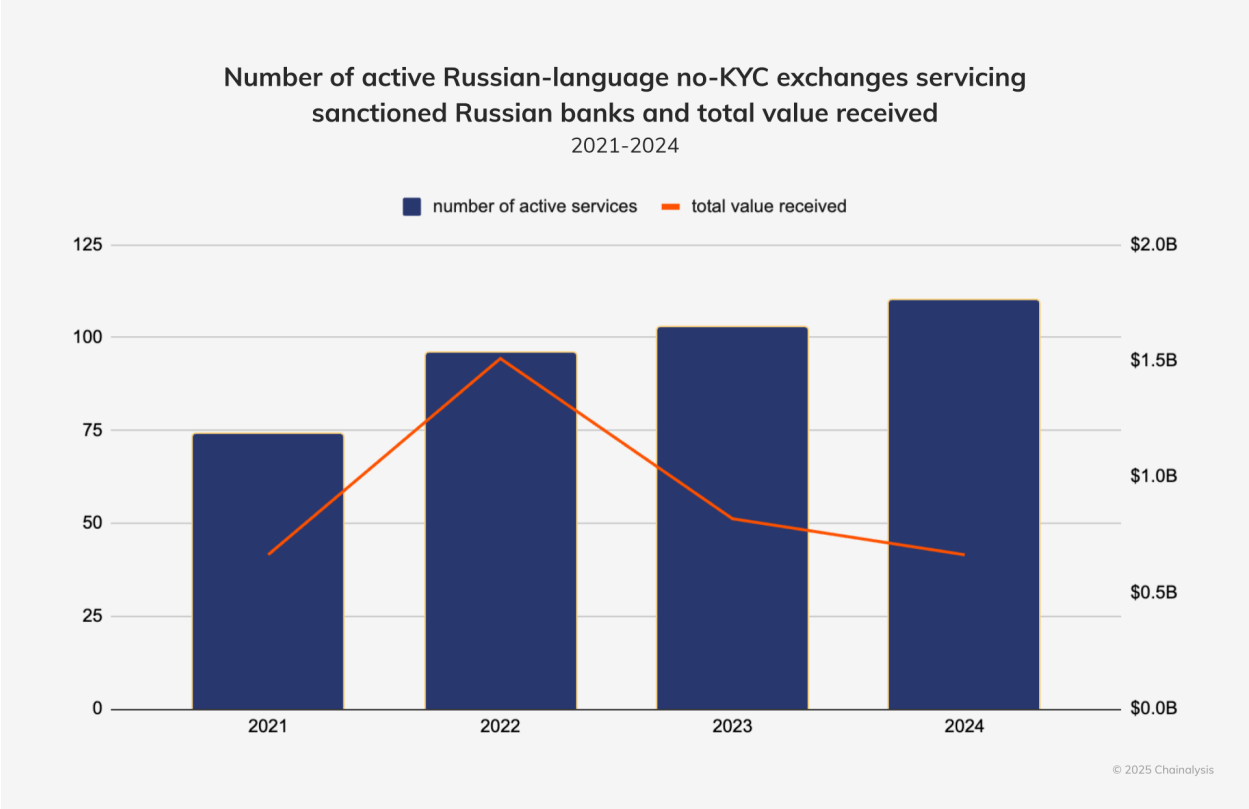
million in cash and cryptocurrency. The networks, Smart and TGR, laundered funds for Russian elites, cybercriminals, and organized crime syndicates.

The operation was an internationally coordinated effort, involving agencies from the UK, EU, and U.S., including OFAC, the DEA, and the FBI. As part of the crackdown, OFAC sanctioned four entities and five individuals tied to TGR, including TGR founder George Rossi and his associates, who facilitated illicit transactions through corporate structures in the UK, UAE, Thailand, and the U.S. OFAC also identified cryptocurrency wallets linked to TGR members, including one belonging to the sanctioned individual Khadzhi Murat Dalgatovich Magomedov that processed over $200 million in illicit funds.

Smart and TGR operated across 30 countries, moving illicit funds through cash-to-crypto swaps and facilitating ransomware payments, sanctions evasion, and drug trafficking. Notably, Smart directly funded Russian espionage operations and laundered funds for the Ryuk ransomware group, according to the NCA.

Russian-language no-KYC exchanges continue to operate

Despite enforcement actions disrupting major players, new no-KYC exchanges continue to emerge, often as rebrands of previously dismantled services.



While the number of active no-KYC exchanges has increased, as smaller start-up exchanges and rebrands fill in the gaps left by takedowns, overall inflows have declined, reflecting the disruptive impact of U.S. and international sanctions measures.

It's important to note that while these platforms operate in Russian language and service sanctioned Russian banks, they often lack incorporation or registration details, making it difficult to determine their actual jurisdiction.

As enforcement agencies gain more insight into these networks, further disruptions are likely to curb the financial flows sustaining cybercrime, drug trafficking, and sanctioned state operations. Industry-wide controls and tools like Chainalysis can enable ecosystem participants to monitor their exposure in real-time, helping to prevent illicit funds from infiltrating legitimate financial systems.

Sanctioned jurisdictions set sights on alternative payment rails, including cryptocurrency

As Western restrictions tighten, sanctioned nations are turning to cryptocurrencies and alternative financial systems to sustain trade and access capital. Russia and Iran in particular have deepened financial ties with BRICS nations — Brazil, Russia, India, China, and South Africa — to develop payment mechanisms outside the U.S. dollar (USD) and traditional banking networks. BRICS members have explored the possibility of a shared digital currency, while Russia has pushed for trade settlements with China and India using stablecoins and central bank digital currencies (CBDCs) instead of the USD.

Amid mounting financial pressure from Western sanctions, Russia enacted legislation this past fall legalizing cryptocurrency mining and allowing crypto for international payments — a stark shift from its previous stance of an outright ban on cryptocurrency. The strategic policy shift aims to ease the financial pressure of Western sanctions and enable global trade using cryptocurrencies.

Despite maintaining a ban on domestic crypto payments, Russia remains one of the top-ranking countries on our Global Crypto Adoption Index. Even before the legislation, banks like Rosbank had begun experimenting with crypto-based cross-border transactions. Now the Central Bank of Russia is driving efforts to integrate cryptocurrency into the country's financial system under regulatory oversight.

Weighing legitimate crypto activity in sanctioned jurisdictions

While cryptocurrency use in sanctioned jurisdictions may be associated with illicit state-controlled finance, it also represents an important financial lifeline for ordinary citizens facing economic hardship under restrictive regimes. Many individuals and businesses in these regions turn to cryptocurrency to preserve wealth, move funds across borders, and circumvent government-imposed financial controls — an adaptation we have identified in Iran, which we'll explore in detail below.

From a regulatory standpoint, the distinction between state-directed sanctions evasion and individual use has little impact, as broad sanctions prohibit nearly all financial interactions between U.S. persons and entities in sanctioned jurisdictions, regardless of intent. However, when considering the broader impact of cryptocurrency in these economies, it is important to recognize that individuals and businesses often turn to crypto without illicit intent, demonstrating the tension between financial enforcement and humanitarian considerations.

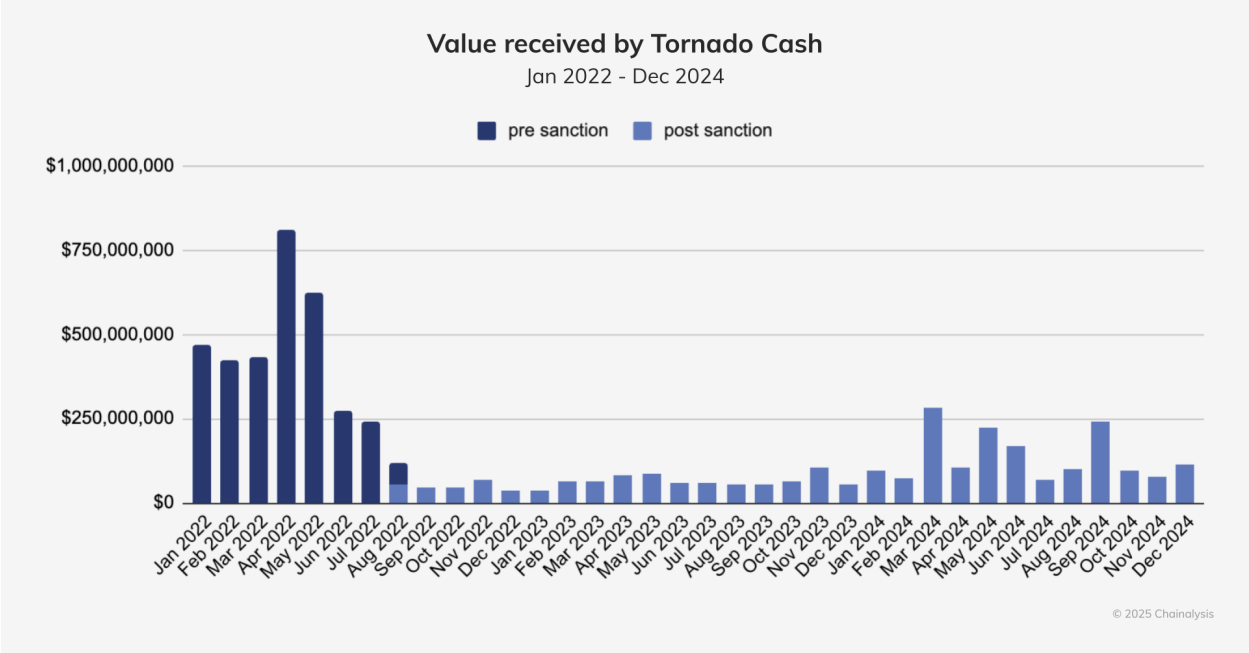
Additionally, decentralized platforms remain operational despite sanctions, complicating enforcement efforts. Unlike traditional financial institutions, these networks cannot be easily seized or shut down — requiring a wider ecosystem-level approach to compliance. As enforcement continues, addressing sanctions risks holistically — through cooperation between governments, compliance tools like Chainalysis, and Virtual Asset Service Providers — will be critical to managing illicit finance risk while preserving legitimate access to crypto.

Tornado Cash endures in the wake of sanctions and legal action

As we've called out before, crypto mixer Tornado Cash is a prime example of the challenges regulators face in enforcing sanctions against decentralized platforms. Despite OFAC sanctions, legal action, and the arrests of its developers, Tornado Cash continues to process illicit transactions.

Sanctioned by OFAC in 2022 for facilitating the laundering of over $455 million in stolen funds — primarily linked to North Korea's Lazarus Group — the core infrastructure of the platform has proven difficult to shut down. In August 2023, U.S. prosecutors indicted Tornado Cash co-founder Roman Semenov for conspiracy to commit money laundering and sanctions violations. Meanwhile, Dutch authorities convicted fellow co-founder Alexey Pertsev in 2024, sentencing him to more than five years in prison.

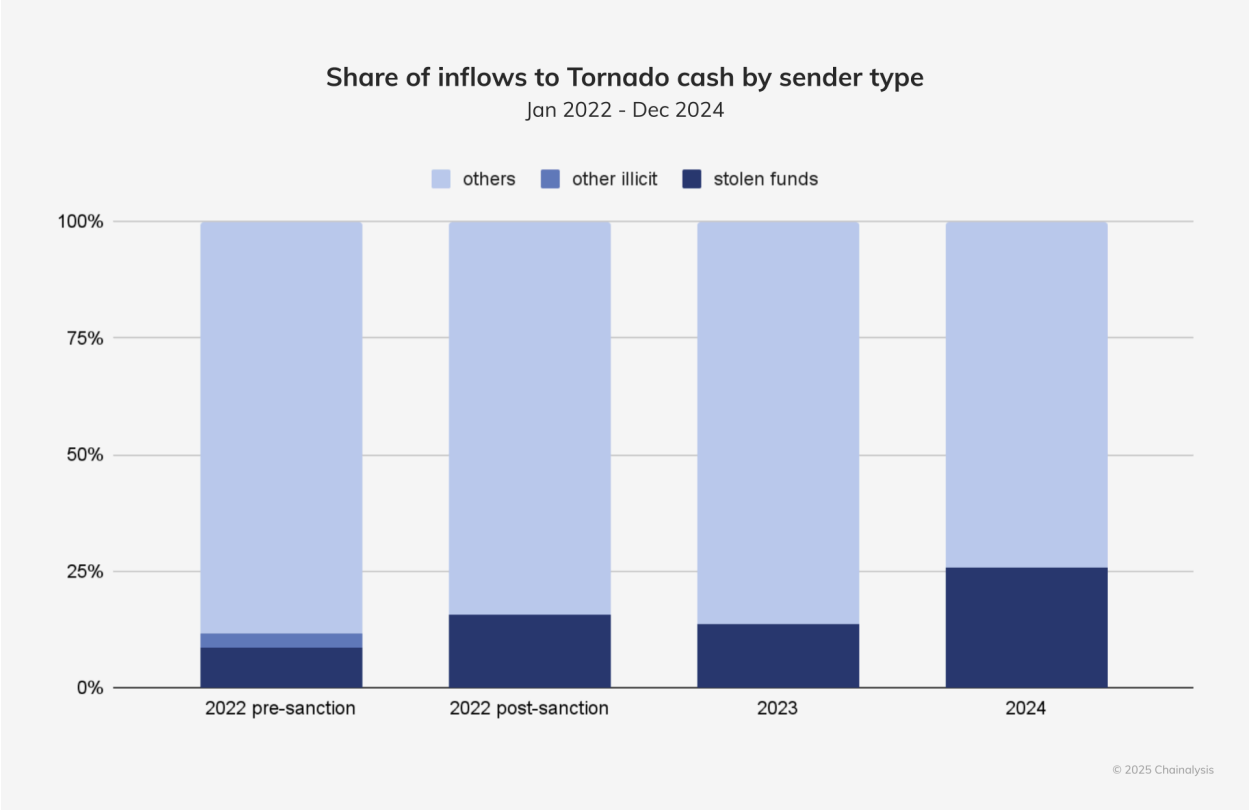
Although Tornado Cash's transaction volume initially dropped nearly 90% when its centralized web-based interface was taken offline, its decentralized smart contracts allowed it to continue operating. In 2024, inflows surged by 108% compared to the previous year, continuing the rebound trend we first identified in last year's Crypto Crime Report.



While inflows have yet to return to pre-sanction levels, Tornado Cash still facilitates hundreds of millions of dollars in transactions each month.

Stolen funds drive Tornado Cash's resurgence

The increase in Tornado Cash usage in 2024 was largely driven by stolen funds, which reached a three-year high, accounting for 24.4% of total inflows, as seen below.



One of the most significant incidents driving these inflows was the HECO Bridge exploit, in which hackers funneled $145 million in ETH through Tornado Cash in an effort to launder the proceeds.

Since 2019, we have linked over 25% of the funds processed through Tornado Cash to illicit activity, with the Lazarus Group among its highest value users. It is important to consider that although the platform has undeniably played a major role in laundering stolen funds, crypto mixers like Tornado Cash are not solely tools for criminal activity. For example, Ethereum co-founder Vitalik Buterin publicly stated that he used Tornado Cash to anonymize a donation to Ukraine following Russia's full-scale invasion in 2022, showing how these services can also be used for financial privacy in legitimate contexts.

Decentralized platforms introduce unique enforcement challenges

Unlike centralized services that can be seized or shut down, Tornado Cash operates through smart contracts on a decentralized blockchain network, making enforcement far more difficult. While the transparency of blockchain enables authorities to track illicit flows, regulators have limited power to

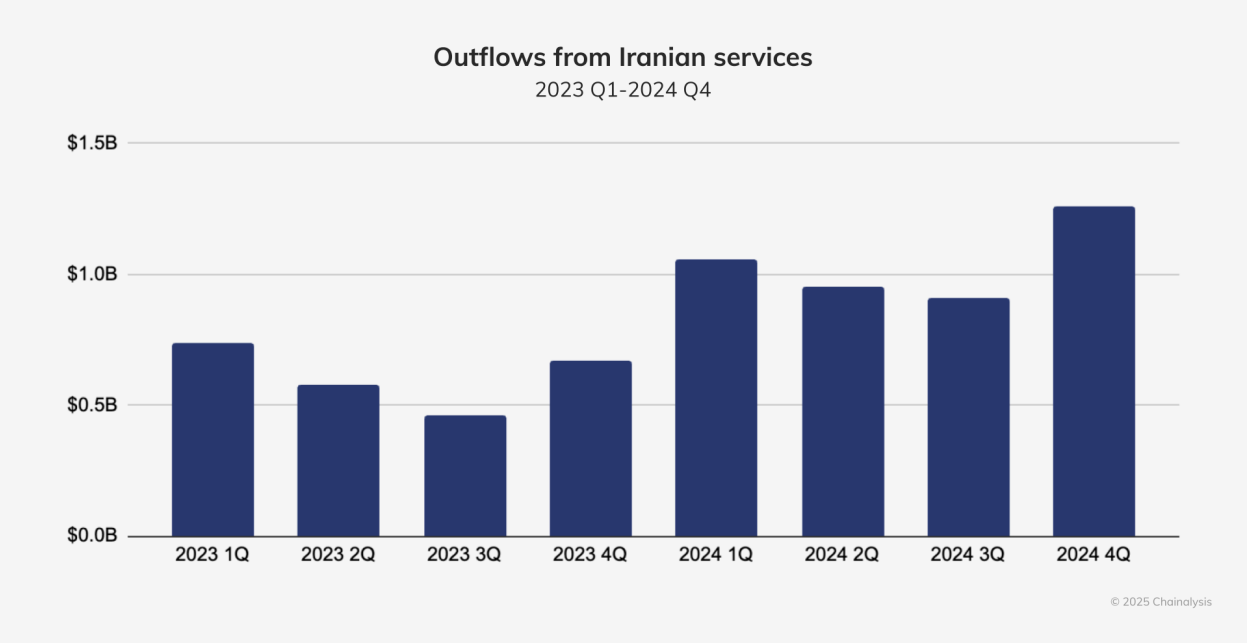
actually dismantle decentralized infrastructure. On November 26, 2024, a U.S. court ruled that OFAC had exceeded its authority in sanctioning Tornado Cash's smart contract addresses. The decision raises broader questions about the limits of enforcement against DeFi protocols and speaks to the need for international cooperation and robust compliance at the protocol and service level. The industry has decidedly made some strides in compliance over the last few years, which we'll explore in detail further down.

The Tornado Cash case illustrates the delicate dance between innovation, financial privacy and compliance in decentralized protocols. As DeFi expands globally, developers must navigate increasing pressure to implement safeguards that prevent illicit activity while preserving legitimate use cases for privacy. Ensuring compliance without compromising the ethos of decentralization and privacy is an overarching challenge for an industry built on decentralized technology. Proactive monitoring and risk mitigation are essential as regulatory expectations evolve. Chainalysis provides solutions to help address these challenges in real-time.

Cryptocurrency enables capital flight in Iran amidst geopolitical tensions

Since the 1979 seizure of the U.S. Embassy in Tehran, the U.S. has imposed extensive financial restrictions on Iran. Despite sanctions, access to the international financial system remains paramount for Iran due to the stability and liquidity it provides. In countries like Iran, where local currencies have been volatile and devalued, the inability to engage with global banks severely limits financial mobility — driving individuals and businesses to seek alternatives.

In 2024, Iranian services took a significantly larger share of sanctions-related crypto activity, fueled by rising distrust in the government and ongoing geopolitical instability.



In 2024, outflows surged to $4.18 billion — up about 70% year-over-year.
While cryptocurrency adoption in these regions is often viewed primarily through the lens of sanctions evasion, it is also a broader reflection of the fundamental need for reliable financial tools in economies cut off from the global banking system.

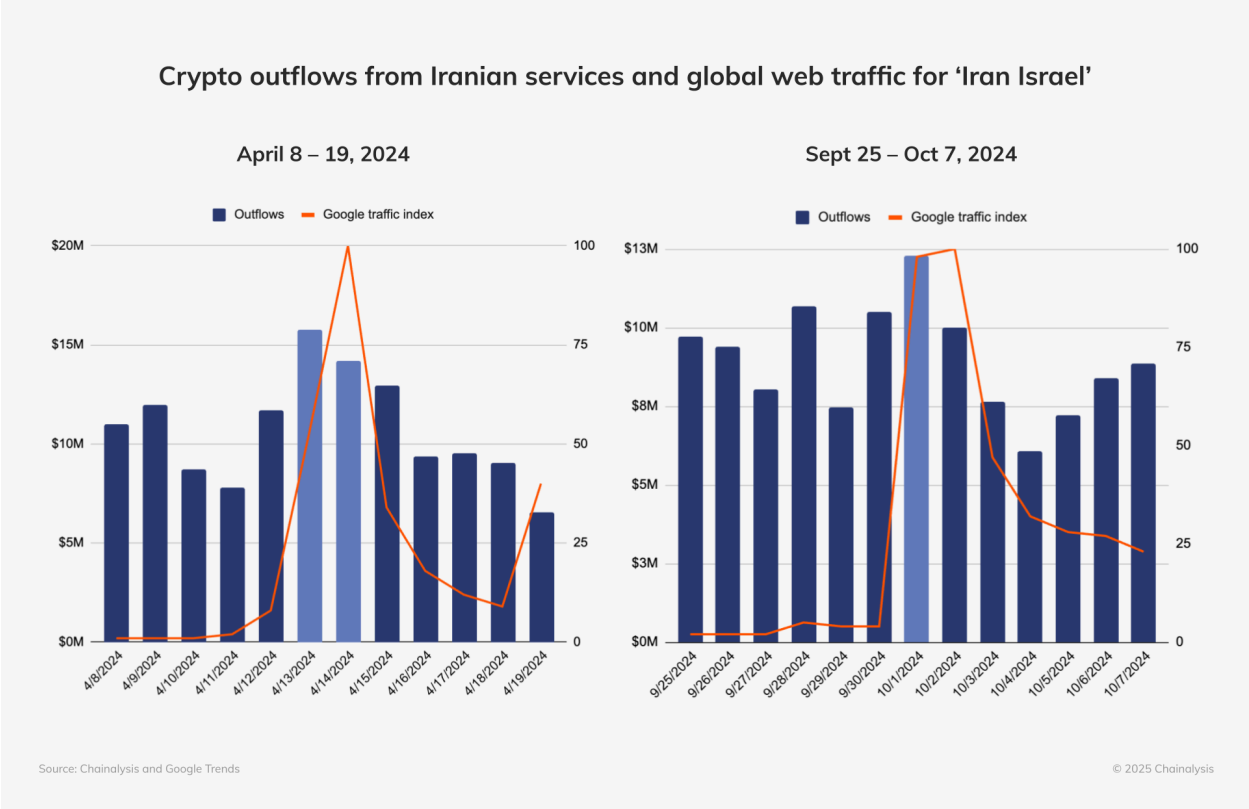
Government control and capital flight

Iran's government maintains extensive control over the country's financial system, including cryptocurrency infrastructure. This reality became especially apparent in December 2024, when authorities abruptly halted withdrawals from Iranian exchanges in response to the record decline in value for the Iranian rial (IRR). This move demonstrated the government's ability to restrict financial outflows at will to prevent capital flight — a growing concern as inflation hovers around 40-50% and the rial continues on a downward trajectory. Since the U.S. withdrew from JCPOA in 2018 and imposed sanctions on Iranian oil, the currency has shed approximately 90% of its value, with depreciation accelerating amid escalating tension in 2023 and 2024.

For many Iranians, cryptocurrency represents an alternative financial system, and the increasing use of Iranian crypto exchanges suggests that more individuals and institutions are resorting to crypto to safeguard wealth and circumvent financial restrictions. A closer examination of these outflows suggests they are not necessarily driven by illicit finance or state-sponsored activity, but rather by Iranian citizens' deepening distrust in the government and a pressing need to move funds out of the country.

Geopolitical flashpoints drive crypto outflows in Iran

During periods of heightened geopolitical instability involving Iran, we found that cryptocurrency outflows from Iranian exchanges spiked — particularly on the day of, or immediately following events of conflict.

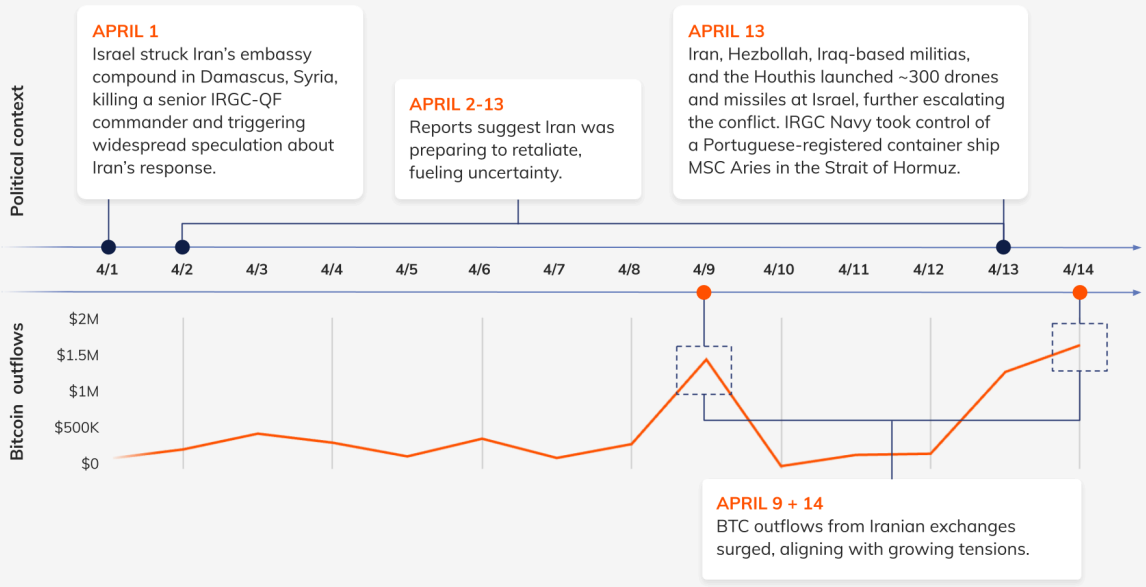


Google Trends data reinforces this connection, showing global spikes in search interest for "Iran Israel" on April 14th and October 1st — dates closely aligned with conflict escalation. This pattern aligns with broader financial developments in Iran, where the rial's parallel market rate fluctuates sharply in response to political and military developments.

Interestingly, while increased outflows were observed across all assets, including stablecoins, we noted a significantly higher volume in bitcoin. The timeline below contextualizes bitcoin outflows in relation to key geopolitical events.

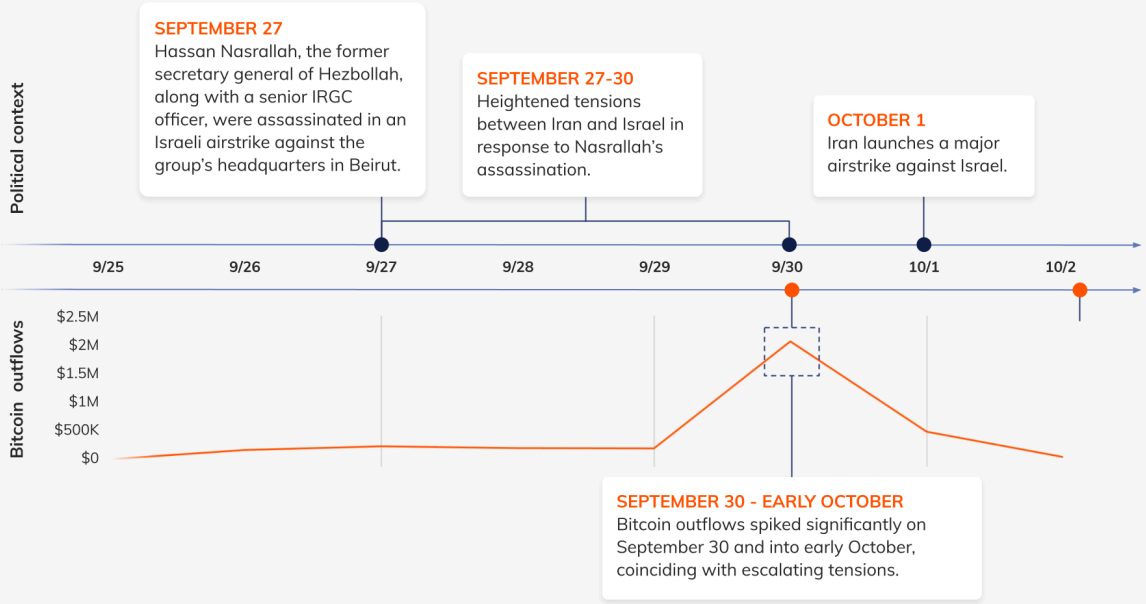
Geopolitical events and bitcoin outflows

April 1-14, 2024



Geopolitical events and bitcoin outflows

September 25 - October 2, 2024



Spikes in bitcoin outflows occurred around the time it became known that Iran was likely to launch missiles, as well as within a few days after the events.

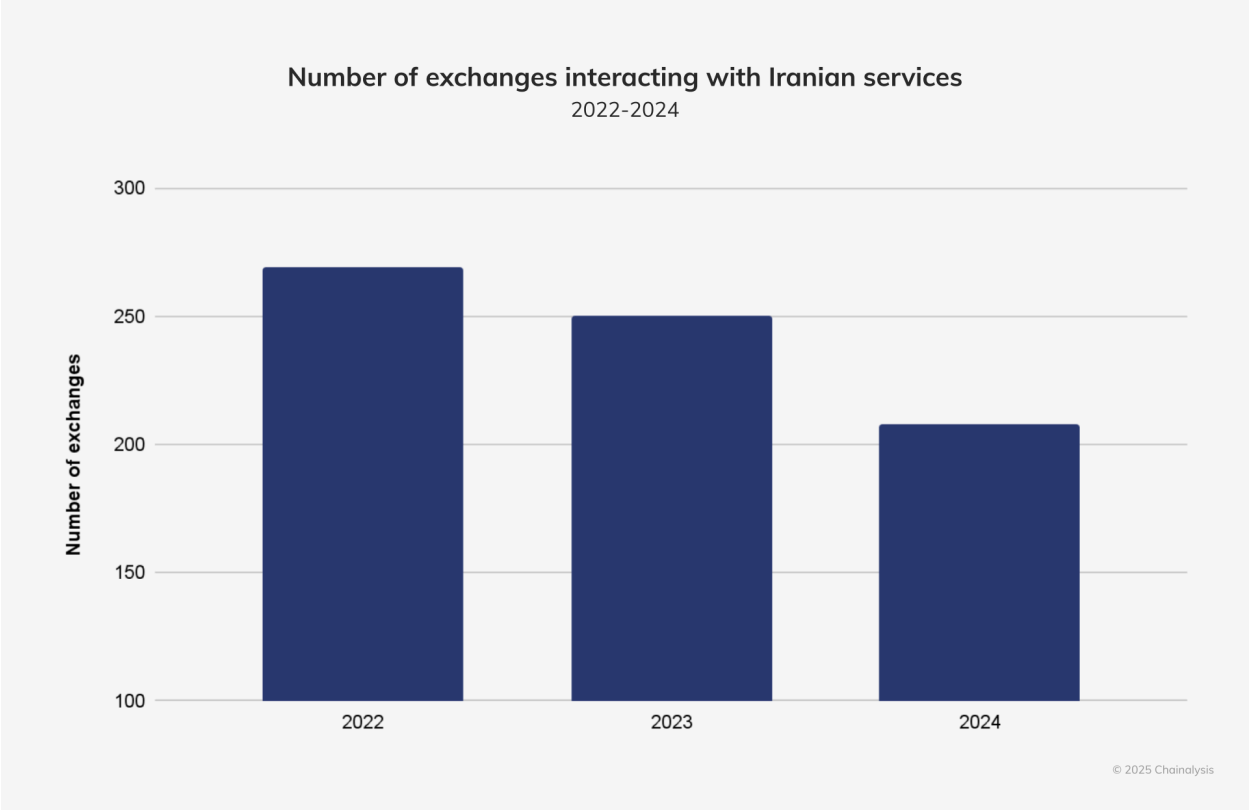
This suggests that heightened public concern over geopolitical strife was mirrored in financial behavior, with individuals turning to crypto as a hedge against geopolitical or economic uncertainty. The demand for crypto will likely remain high as sanctions pressure intensifies and Iran's economic uncertainty persists.

Bitcoin's role in uncertain times

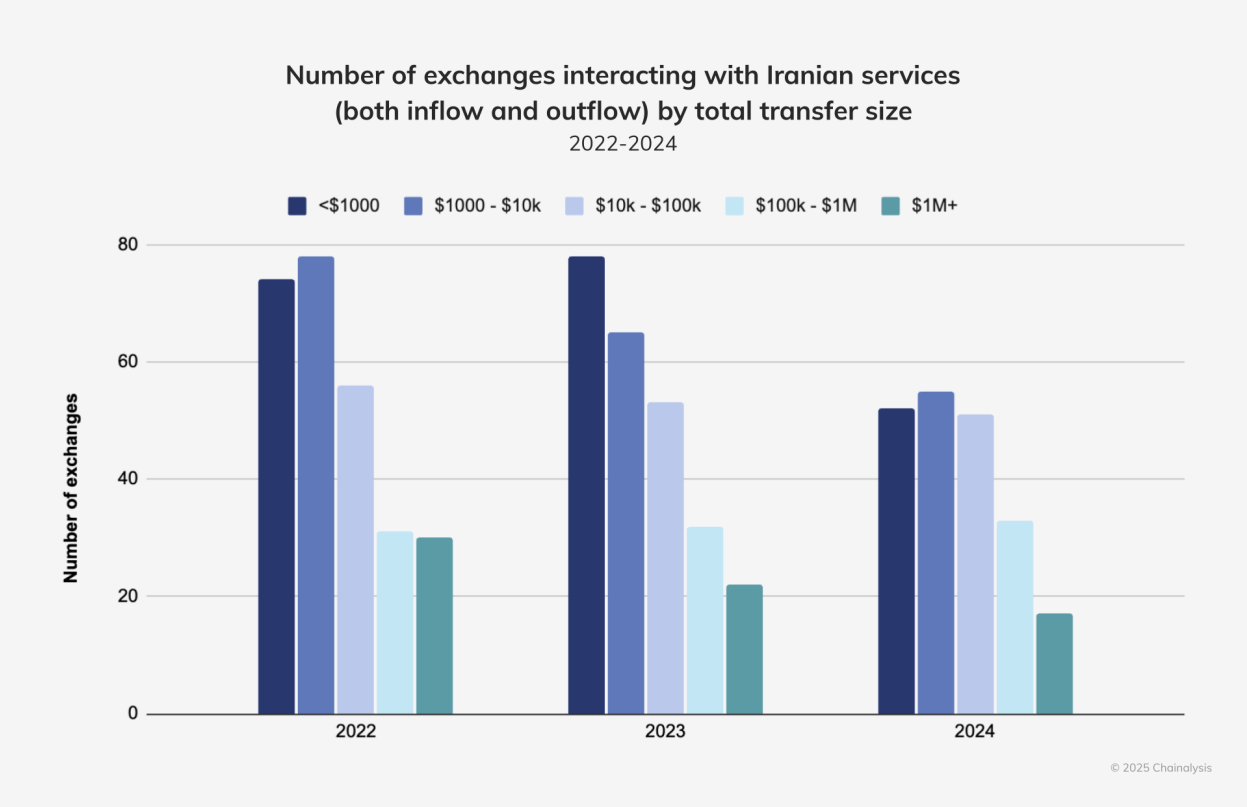
While these trends are pronounced in Iran, we have also observed similar patterns globally during times of war, economic turmoil, or government crackdowns. Bitcoin's censorship-resistant, self-custodial nature makes it an appealing option during crises. Unlike traditional assets, bitcoin can be transferred across borders, held on-chain as a hedge against instability, and require only the storage of a seed phrase — offering financial flexibility in situations where individuals may need to flee. This makes it uniquely suited for those in jurisdictions facing geopolitical volatility and financial restrictions.

Looking ahead: Holistic compliance at the ecosystem level

Although many Iranians have relied on cryptocurrency for capital flight, compliance programs across the global crypto ecosystem are closing off these avenues. As compliance takes center stage, exchange exposure to Iranian services continues to decline each year, dropping by about 23% between 2022 and 2024.



A closer look at transfer sizes between Iranian platforms and other exchanges reveals that the number of exchanges interacting with Iranian exchanges has declined across almost all transaction brackets between 2023 and 2024.



The largest drop occurred in the <$1000 bracket, which saw a 33.33% decline from 2023. The >=$1 million bracket also saw a sizable reduction by 22.73%.

The measurable decline in exchange interactions with Iranian services speaks to the tangible impact of compliance measures in limiting exposure to sanctioned jurisdictions. Exchanges have a growing responsibility to mitigate financial activity associated with sanctioned regions.

Global policy pressure on Iran raises financial risks

Iran's actions have heightened the stakes of doing business with its financial ecosystem, both on- and off-chain. Over the past 12-18 months, Iran has deepened its economic and military ties with Russia — which presently has the most targeted sanctions in the world — raising additional red flags for global regulators. As one of just three countries on the FATF blacklist (alongside North Korea and Myanmar), Iran continues to face scrutiny for its weak anti-money laundering (AML) and countering the financing of terrorism (CFT) controls. Additionally, Iran continues to provide material support to groups such as Hezbollah and Hamas, further amplifying regulatory and national security concerns.

In February 2025, the new U.S. administration introduced the National Security Presidential Memorandum (NSPM-2), reinstating the "maximum pressure" campaign on Iran. The directive mandates a more

aggressive enforcement posture, outlining specific measures for the U.S. Department of Justice (DOJ), including:

- Investigating and prosecuting Iranian-linked financial and logistical networks, as well as operatives or front groups within the United States that are sponsored by Iran or Iranian proxies.
- Impounding illicit Iranian oil cargoes.
- Identifying Iranian governmental assets for seizure in the U.S. and abroad.
- Indicting and prosecuting leaders of Iranian funded terrorist groups.
- Leveraging criminal, regulatory, cyber tools and authorities to disrupt Iran's espionage, sanctions evasion, and malign financial activities.

With the sustained intensity of targeted and sectoral sanctions, along with the crackdown on Iranian oil and shipping, the situation remains acute and is likely to further drive demand for cryptocurrency and other financial workarounds. As sanctioned actors adapt to a crypto-activated world, enforcement will increasingly rely on blockchain intelligence to track illicit financial flows, identify sanctioned entities, and mitigate exposure to restricted jurisdictions like Iran.

Blockchain analysis ensures a compliance-forward future

Decentralized technologies introduce complex enforcement challenges, making compliance at both the protocol and service level essential. Chainalysis supports exchanges, DeFi platforms, regulators, and enforcement agencies by providing real-time transaction monitoring, wallet screening, and risk-based controls to help detect and prevent exposure to sanctioned entities. As regulatory expectations increase, proactive compliance measures will be critical to maintain financial integrity while also preserving legitimate access.

By leveraging on-chain analytics, crypto service providers can assess counterparty risk and intercept illicit transactions before they access the broader financial system. Improved compliance programs supported by blockchain analysis have contributed to a measurable decline in exchange interactions with sanctioned entities, demonstrating the effectiveness of data-driven de-risking strategies.

As sanctioned nations explore alternative financial channels, close collaboration between ecosystem participants as well as private and public sector partners is essential. A risk-based approach that differentiates between state-directed sanctions evasion and individual financial lifelines will be critical in shaping fair and effective regulatory frameworks. A combination of regulatory oversight, industry-wide cooperation, and advanced blockchain analytics tools can ensure that cryptocurrency remains a viable and legitimate financial system while eliminating channels for illicit actors and states.

Crypto-linked entities sanctioned in 2024

The table below includes various sanctions events and coordinated law enforcement takedowns with a cryptocurrency nexus that occurred throughout 2024.

Name	Reason for Sanction	Date Sanctioned	Designation Type
Artur Sungatov and Ivan Kondratyev	Two Russian nationals accused of acting affiliates for LockBit RaaS	February 20	Ransomware
Ilya Andreevich Gambashidze and Nikolai Aleksandrovich Tupikin	Facilitating disinformation campaigns on behalf of the Russian government, using cryptocurrency for funding	March 20	Disinformation and financial facilitation
Netex24 and Bitpapa	Assisting in building or operating blockchain-based services to facilitate potential sanctions evasion for Russian nationals	March 25	Sanctions evasion through cryptocurrency
Tawfiq Muhammad Said Al-Law	Syria-based hawala operator who was previously identified by NBCTF as having worked with Hezbollah operatives on cryptocurrency funding infrastructure	March 26	Terrorism financing
Gaza Now and several associated individuals	Social media news outlet and associates for their role in raising money for Hamas following the October 7 attacks against Israel	March 27	Terrorism financing
OKO Design Bureau and approximately 300 individuals and entities involved in Russia's war machine	Facilitating Russian weapons production and sanctions evasion, with one entity known to have accepted cryptocurrency	May 1	Weapons procurement and sanctions evasion
Dmitry Yuryevich Khoroshev	Leader of the LockBit RaaS group, for developing and distributing ransomware	May 7	Ransomware
Yunhe Wang and multiple individuals connected to 911 S5 botnet	For alleged control of a botnet of infected computers associated with the residential proxy service	May 29	Cybercrime and botnet operations
Individuals linked to Nordic Resistance Movement	Involvement in violent extremism and terrorism, funded through cryptocurrency donations	June 14	Terorrism financing and extremism
KB Vostok OOO	A Russian unmanned aerial vehicle (UAV) developer known for designing UAVs used by Russian forces in Ukraine	August 21	Arms development
Sergey Sergeevich Ivanov and Cryptex	Laundering hundreds of millions in cryptocurrency for cybercriminals and darknet vendors	September 26	Money laundering and cybercrime

Members of Evil Corp	Developing and distributing Dridex malware, leading to significant financial losses globally	October 1	Cybercrime and fraud
Smart and TGR Networks	Operating extensive Russian money laundering networks with links to drugs, ransomware, and espionage, resulting in 84 arrests	December 4	Money laundering and organized crime
Sa'id al-Jamal	Iran-based Houthi financier involved in arms trafficking, money laundering, and illicit shipping of Iranian oil, using cryptocurrency	December 19	Terrorism financing and arms trafficking

Extremism

Cryptocurrency donations to extremist groups dip globally, but white supremacism, nationalism, and anti-Semitism grow across Europe

Extremism, in its many forms, represents an ongoing threat to global peace and security. Often fueled by ideological grievances and disinformation, these movements exploit the financial system — including through cryptocurrency — to disseminate propaganda through their own media platforms, garner support for their causes, and carry out attacks.

Regulators and law enforcement in many jurisdictions are increasingly turning their attention towards groups that fall outside the traditional definitions of terrorism, but still pose risks due to their transnational influence and reach. Unlike internationally recognized terrorist organizations like the Islamic State of Iraq and ash-Sham (ISIS) or Boko Haram, which are defined by direct acts of violence and meet explicit government-defined criteria, many groups espousing extremist ideology advance their agendas without directly engaging in violence themselves. However, such groups often incubate and promote escalation to violence, making it critical to understand and disrupt their financial lifelines.

To that end, recent international actions demonstrate a growing effort to disrupt the financial activities of groups that operate in the grey areas of traditional counterterrorism frameworks. For instance, the United States (U.S.) Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned the Nordic Resistance Movement (NRM), while the U.S. Department of State designated the white supremacist group The Terrorgram Collective and three of its leaders. These measures form a broader strategy to address the threat posed by racially or ethnically motivated violent extremism (REMVE) and the transnational threat of violent white supremacism. Similarly, the European Union (EU) sanctioned The Base, a neo-Nazi accelerationist group also designated as a terrorist organization by Australia, Canada, and other jurisdictions.

This section explores cryptocurrency flows to groups across the political and ideological spectrum, including groups that would be considered far-right and far-left in traditional parlance. We examine the ideologies driving their activities, donor patterns, and regional and cross-ideological dynamics. Although cryptocurrency contributions to these causes remain relatively small, any amount directed toward extremist ideologies can have an outsized impact and warrants deeper scrutiny. By analyzing these networks, we aim to provide insights into how these groups operate and identify emerging threats that extend beyond the conventional understanding of terrorism.

A note on methodology

The analysis in this section draws on multiple sources, including public sanctions lists and research from organizations specializing in extremism and terrorism financing. We categorize groups based on their stated ideologies, documented activities, and identifiable links to extremist behavior.

Through blockchain analysis, we investigate known wallet addresses associated with these organizations to uncover patterns of financial support, regional dynamics, ideological crossovers, and on-chain behavioral trends of donors and recipients. These insights provide a clearer picture of how these groups are leveraging cryptocurrency to sustain their operations.

We contextualize these findings within the broader landscape of increased regulatory scrutiny on extremist financing and risk-based debanking[3]. By examining the typologies of groups across the gamut of extremism, we seek to deepen the analytic and policy community's understanding of their funding mechanisms.

While this analysis sheds light on certain on-chain activities, it is impossible to capture the full scope of financing, as much likely occurs off-chain through traditional banking and informal systems, as well as content monetization and crowdfunding platforms.

A note on terminology

In this report, we use the term "extremist group" or "extremist financing" to describe organizations or financial activities involving groups across the political and ideological gamut that may still not meet the criteria for designation as Foreign Terrorist Organizations (FTOs) in the United States. While FTOs are formally recognized entities based on specific government-defined criteria, the groups referenced here may engage in a broader range of activities that do not explicitly involve terrorist acts, but still contribute to the incubation or spread of radical ideologies that often defend or legitimize political violence. This includes groups that fall under the umbrella of REMVE — promoting ideologies grounded in racial or ethnic hatred. A broader lens is essential for understanding how such groups fund themselves, as their activities may eventually lead to violent outcomes. By addressing the full scope of extremist financing, we aim to surface proactive strategies to mitigate risks.

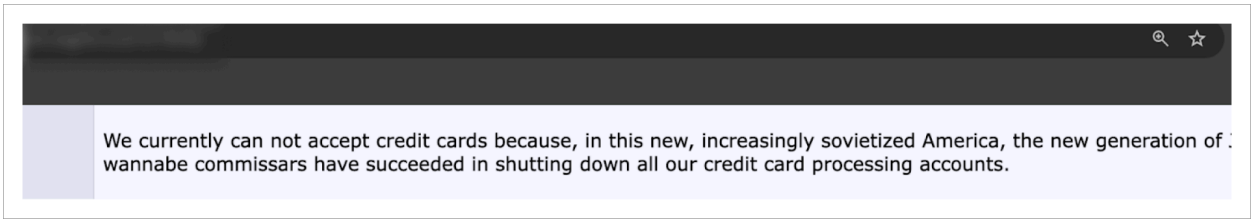
The term "extremist financing" is similarly broader in scope than the legal definitions of terrorism financing found in international frameworks, such as those of the Financial Action Task Force (FATF). Generally, terrorism financing is defined as the collection or provision of funds with the intent or knowledge that they will be used to carry out acts of terrorism. By contrast, extremist financing in this report includes financial flows that support groups engaging in ideological or political activities that promote or reinforce professed hatred of a group of people, even in the absence of direct violence.

Trends in crypto contributions to extremist groups decline overall, but show concerning traction in Europe

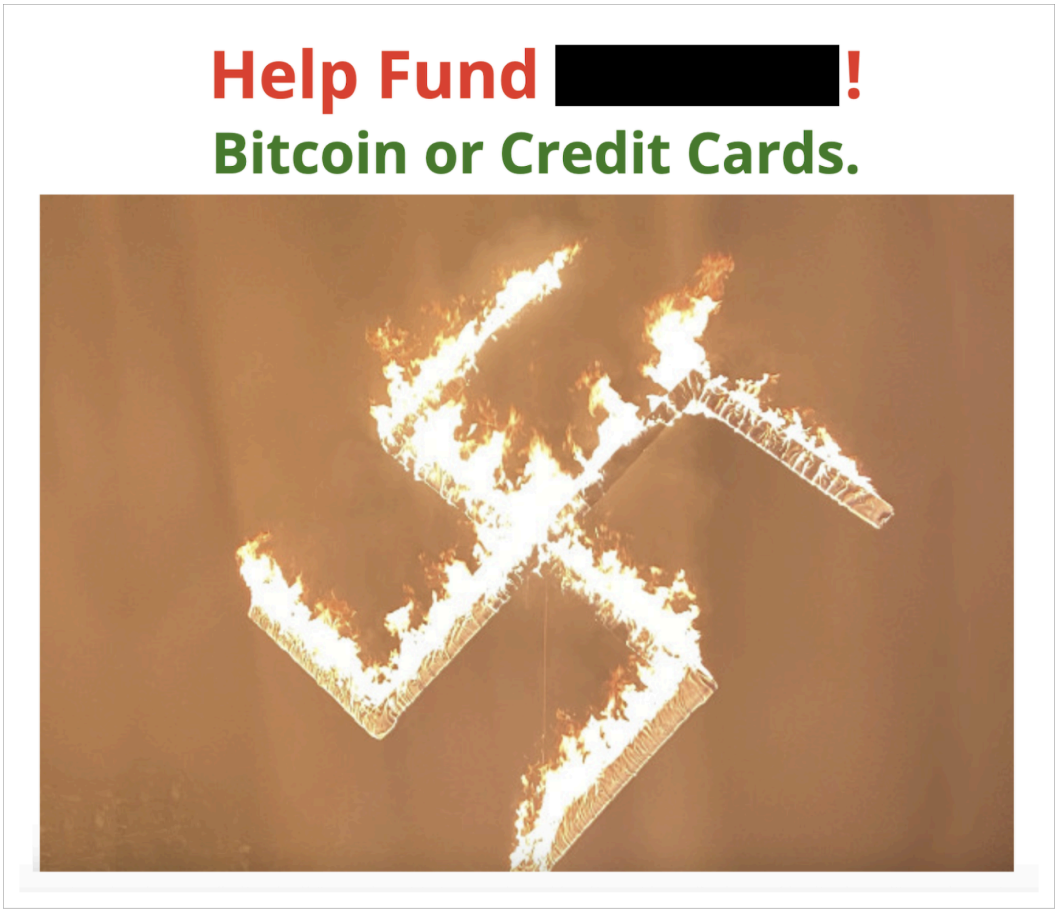
Groups espousing extremist ideology have increasingly turned to cryptocurrency as a means of securing financial support, particularly after being excluded from traditional financial institutions (FIs). Many of these groups have faced debanking, forcing them to seek alternative methods of funding. For example, one

[3] **Debanking or de-risking** refers to the practice of financial institutions (FIs) restricting accounts or denying banking services due to perceived risks associated with the account holder's activities. This has raised debates, including in the U.S., about financial inclusion and whether some groups are being unfairly excluded from banking services.

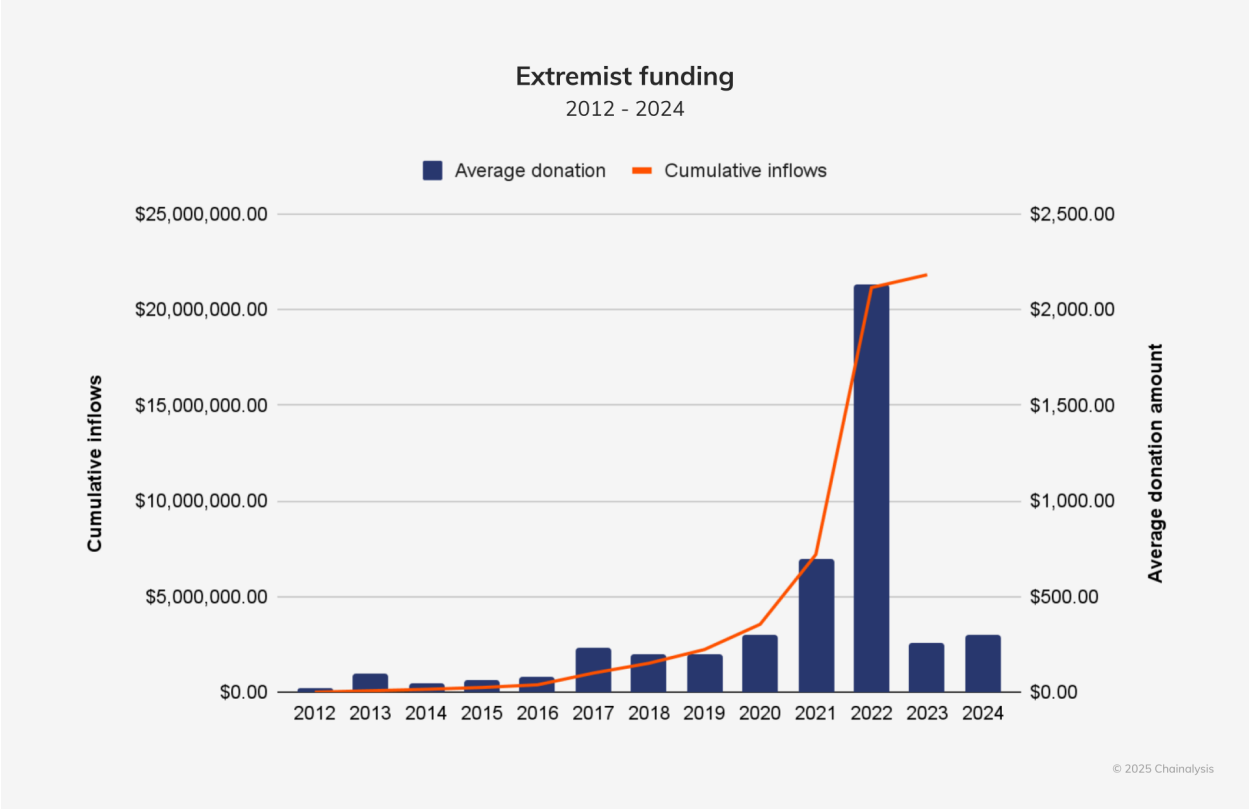
U.S.-based white supremacist group explicitly cited their loss of access to traditional payment rails, redirecting donors to cryptocurrency.



The transition to crypto proved effective for this particular group, netting them roughly $40,000 worth of cryptocurrency since publishing a donation address. The shift from traditional banking to cryptocurrency represents a broader trend among ideological groups seeking to maintain their financial lifelines. As shown below, one group solicits donations via bitcoin and credit card, while leveraging a burning swastika to promote their cause.



The chart below shows an upward trend since 2012 in cumulative flows to ideological groups worldwide.



Despite the cumulative growth in contributions, the average payment size generally has remained in the hundreds of dollars each year (with the exception of 2022). This suggests that grassroots campaigns, consisting of small contributions from individual donors, continue to drive cryptocurrency funding for ideological groups.

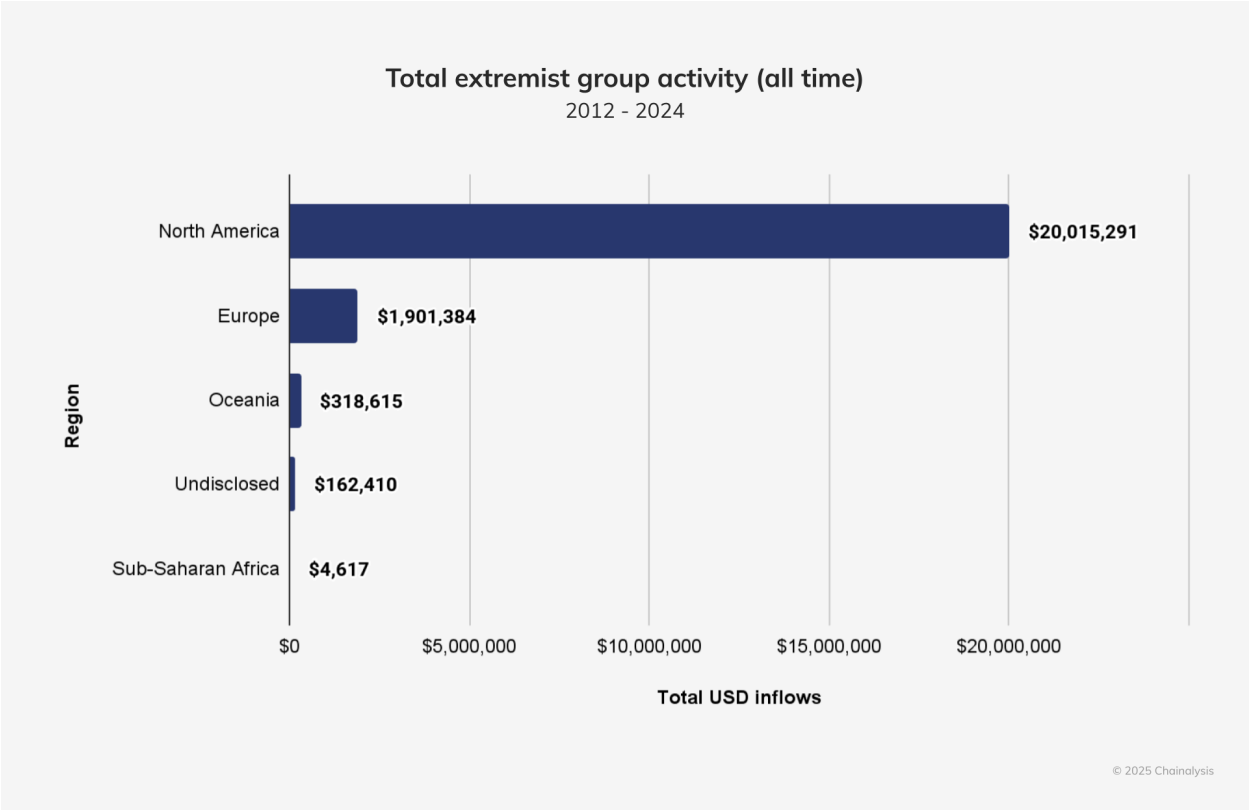
However, there was a notable increase in cumulative contributions and average payment amount during the COVID-19 pandemic era, circa 2020-2022 — a time marked by heightened ideological divisions and the rapid spread of misinformation. This growth reflects an expansion in both the number of donors and the size of individual contributions.

The spike in average annual deposit amount in 2022 is anomalous. That year, the far-right conspiracy theory and disinformation platform InfoWars received an $8 million contribution from a single donor. This coincided with a series of legal losses related to the Sandy Hook defamation case, significantly skewing the data for that year. This speaks to how specific events can act as flashpoints for increased donations — a dynamic we will explore in greater detail later on.

North America is number one for extremist financing, but Europe is the fastest growing region

The intersection between regional and ideological dynamics presents a complex picture. While overall observable crypto funding is somewhat stagnating overall year-over-year (YoY), certain ideologies in specific regions are experiencing significant YoY growth. This suggests localized surges in support for particular causes, driven by political, social, or cultural factors that resonate strongly in those regions.

North America is the global leader in extremist funding via cryptocurrency, with over $20 million in total contributions, far surpassing other regions.[4]



Undisclosed may refer to groups or organizations that either do not publicly reveal their location of operation or operate in a manner that obscures their geographic presence.

This dominance likely reflects the presence of prominent groups and platforms like The Daily Stormer and InfoWars in the U.S, which serve as hubs for both domestic and international activity. Debanking efforts in the United States targeting both far-right and left-leaning groups may have driven many to cryptocurrency as an alternative financial system.

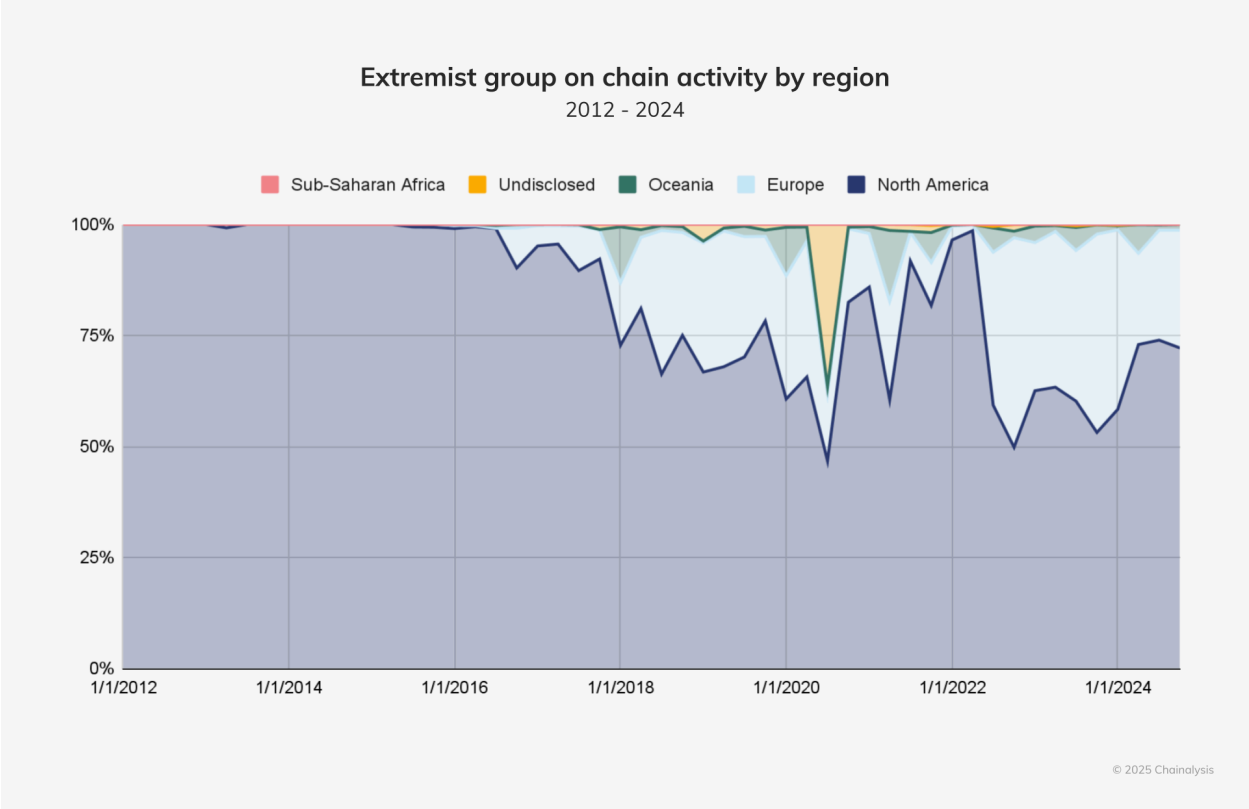
With $318,615 in inflows, Oceania, reflecting contributions in Australia and New Zealand, stands out relative to its small population and fewer extremist organizations. The Christchurch mosque attacks in

[4] It's important to note that many groups in our sample are now inactive, while others have shifted their strategies by using alternative content monetization platforms or transitioning to privacy coins for greater anonymity. This report does not include analysis of transactions in privacy coins in totals.

2019, which cost approximately NZ $60,000 (roughly $33,567 USD) to execute according to estimates by the New Zealand Police, underscore that extremist groups can achieve devastating impact without vast sums.

Europe's share of cryptocurrency inflows to extremist groups is on the rise

Until 2017, North America accounted for virtually all on-chain flows to extremist groups, reflecting earlier adoption of cryptocurrency. Beginning in 2017, Europe began to capture a noticeable share of these inflows, as we see below, and its share has grown steadily since.

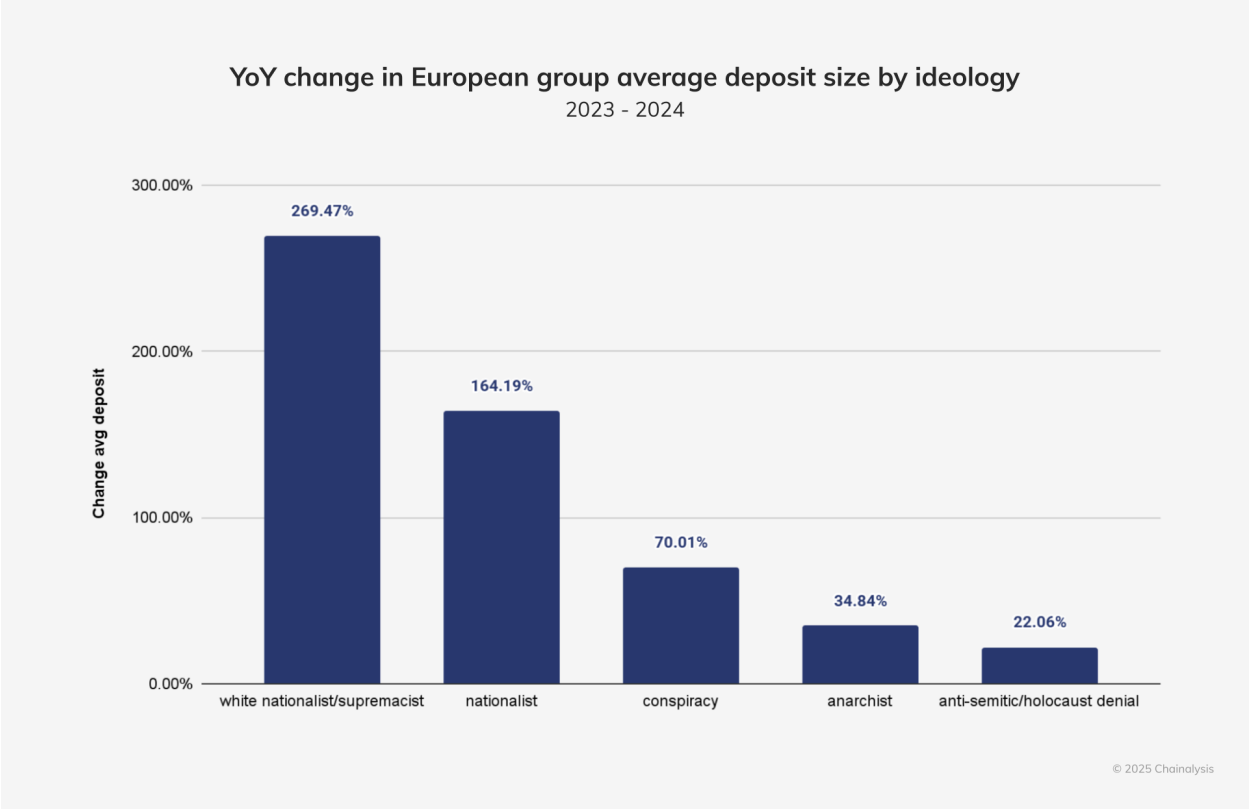


Between 2022 and 2024, Europe's share rose dramatically, commanding as much as nearly 50% of total inflows.

This growth is likely driven by rising white supremacist, nationalist, anti-Semitic and Holocaust denial narratives, as well as "remigration"-focused organizations that advocate for reversing migration trends. These groups have successfully used divisive narratives to attract funding in increasingly polarized political climates.

Europe is also seeing increased donor intensity

In addition to growth in overall inflow share, some ideologies are experiencing marked increases in average deposit size, reflecting a rise in the intensity of donor support. The chart below shows the top five ideologies in Europe by growth in average deposit size.



While marginally distinct, groups that espouse white nationalist and white supremacist views, as well as anti-Semitic and Holocaust denial views have been bucketed together respectively due to significant ideological overlap. White supremacists advocate for the inherent superiority of white people and racial hierarchies, while white nationalists seek to establish or preserve a white ethnostate, ultimately rooted in white supremacist ideals. Holocaust denial is a specific form of anti-Semitism that rejects or distorts facts about the Holocaust to delegitimize Jewish suffering and propagate anti-Jewish sentiment.

White nationalist and nationalist groups lead, with conspiracy, anarchist, and anti-Semitic/Holocaust denial groups also showing marked growth, suggesting European groups have successfully leveraged these narratives to mobilize financial support.

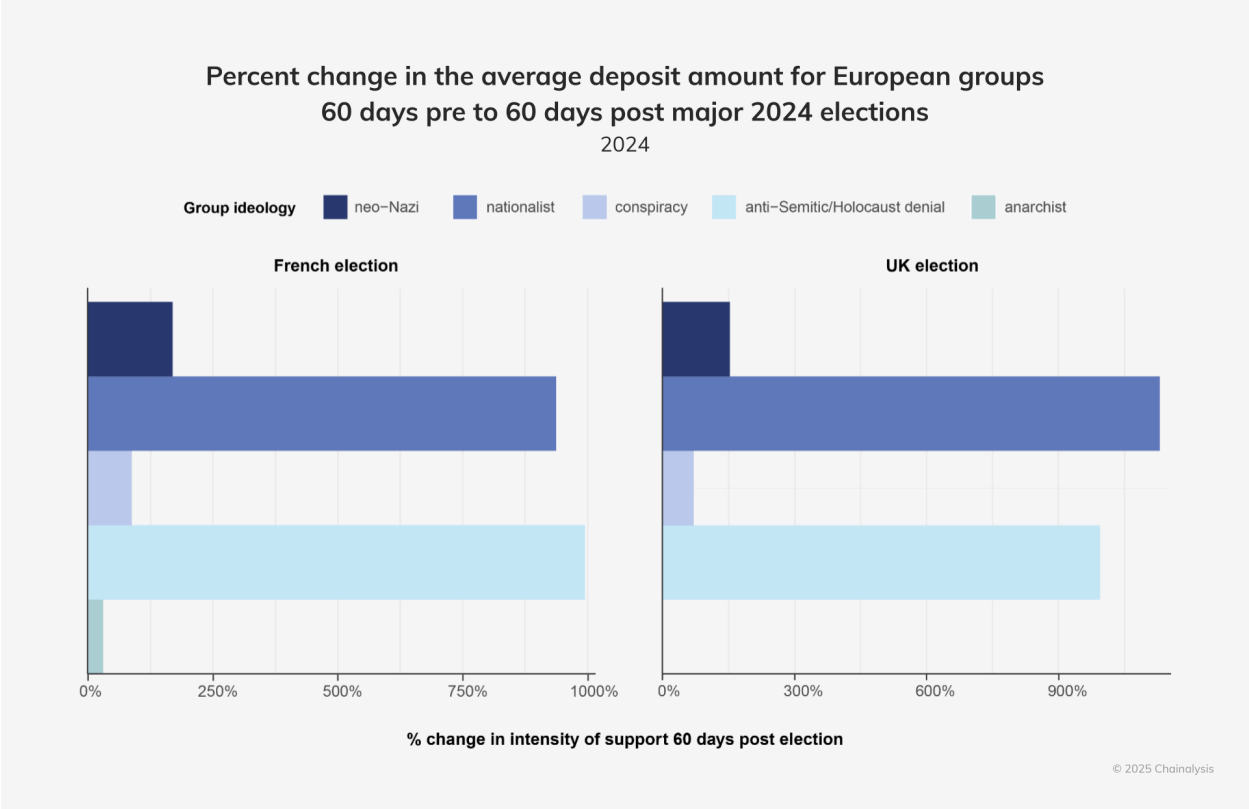
This is particularly striking in the context of stricter regulations and outright bans on hate speech, Nazi symbols, and Holocaust denial in countries like Germany, Austria, and the Baltic states. Furthermore, many European countries limit open solicitation of funds, pushing some extremist groups toward more covert fundraising methods to avoid scrutiny, such as through privacy coins — an issue we will explore later on. This makes it likely that the true scale of ideological support is even greater.

Highly polarized political events, such as national elections, often catalyze surges in donation and donation amounts. Major European election events prompted significant increases in average deposit sizes, reflecting the donor enthusiasm and strategic leveraging of political moments by ideological groups.

Donations surge in Europe around major political events

The chart below shows how average deposit sizes surged across select ideological categories in response to major 2024 European elections, illustrating the connection between on-chain financial activity and

off-chain political developments. Changes in average deposit size are an indicator of the intensity of donor support, which can provide a more nuanced view than total donation volume alone.



Significant increases in donation amounts were observed around elections in France and the United Kingdom (UK). Nationalist and anti-Semitic groups in particular, as well as neo-Nazi and conspiracy-oriented groups benefited from these moments, increasing their backing. While some of this growth may be part of longer-term cyclical trends, these spikes reflect how elections can act as flashpoints for extremist fundraising, driving greater financial contributions from ideologically aligned donors.

Many of these surges appear linked to event-specific campaigns. For example, targeted fundraising around near-wins or setbacks for ideologically aligned candidates often prompt increases in the intensity of support. Election outcomes also drive donor enthusiasm, with spikes post-election likely reflecting either celebration of favorable results or urgency following perceived losses.

How extremist groups leverage ideological overlaps to strengthen networks and amplify resources

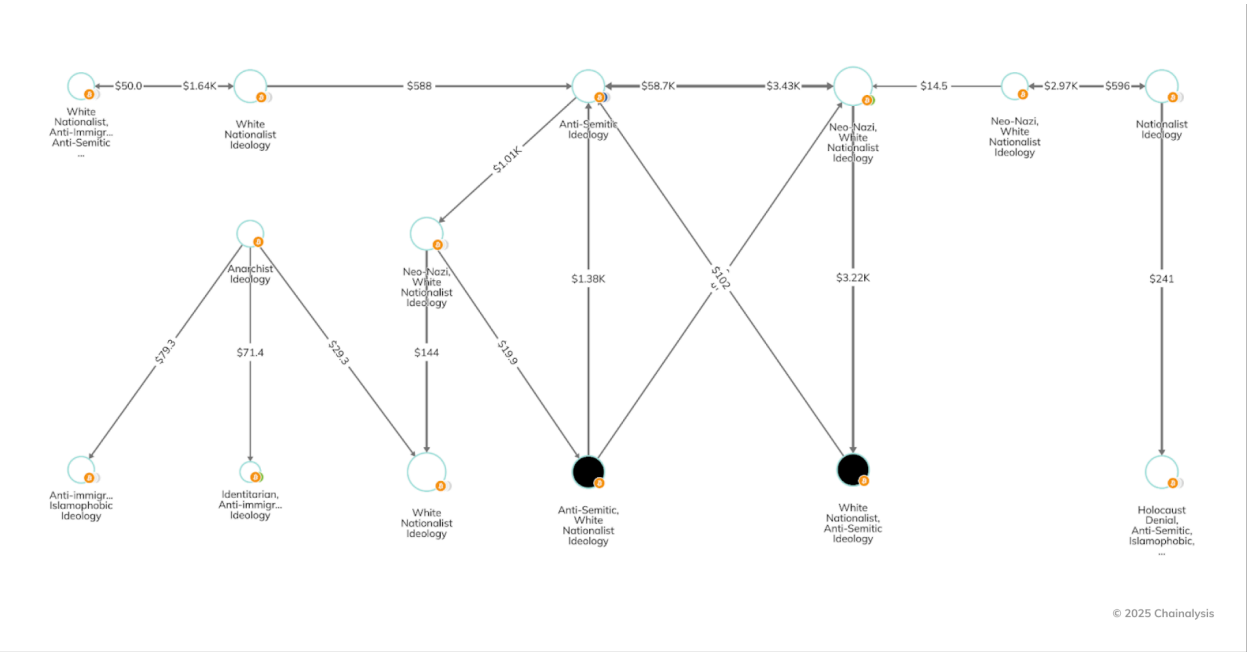
A concerning trend among ideological groups is the deliberate blending of ideologies to broaden appeal. For example, movements might combine homophobic rhetoric with white supremacist or pro-Russia themes, strategically attracting wider audiences by capitalizing on overlapping grievances and similar narratives.

The imagery below — sourced from a content platform promoting anti-Semitic, homophobic, pro-Russia content and conspiracy theories — illustrates how groups strategically overlay hateful ideologies.

Casting a wide net, these groups unite seemingly unrelated grievances by rallying around a common enemy or shared cause.

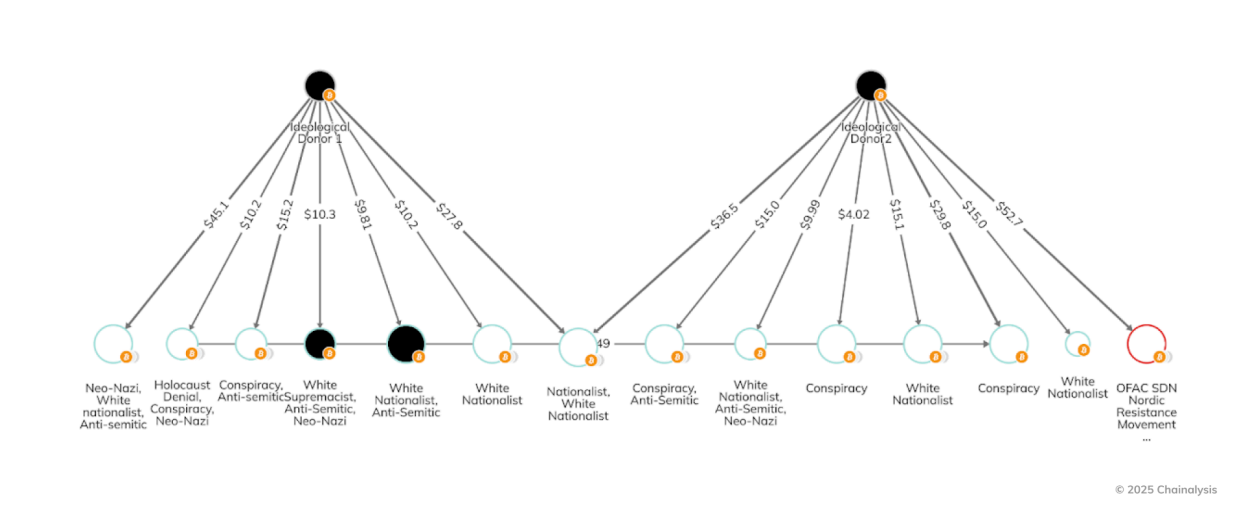
In addition to ideological crosspollination, on-chain transactions reveal further evidence of pan-ideological alignment. Understanding these connections through blockchain analysis not only reveals how these groups align ideologically, but also refines our understanding of their relationships, financial behaviors, and operational strategies. For example, white nationalist organizations have shown a propensity to donate to other extremist organizations, suggesting collaboration and shared goals that cross ideological boundaries.

The Reactor graph below reveals cryptocurrency contributions from white nationalist groups to a variety of organizations promoting ideologies such as Islamophobia, anti-Semitism, and Holocaust denial.



Financial interconnectedness further strengthens their networks and sustains their operations, amplifying collective influence. On-chain interactions also reveal how these groups identify allies both ideologically and financially.

Additionally, we have observed that individual donors — who collectively have the most impact on overall extremism funding through cryptocurrency — frequently support multiple causes. In the Reactor graph below, we see two donors contributing to a range of campaigns.



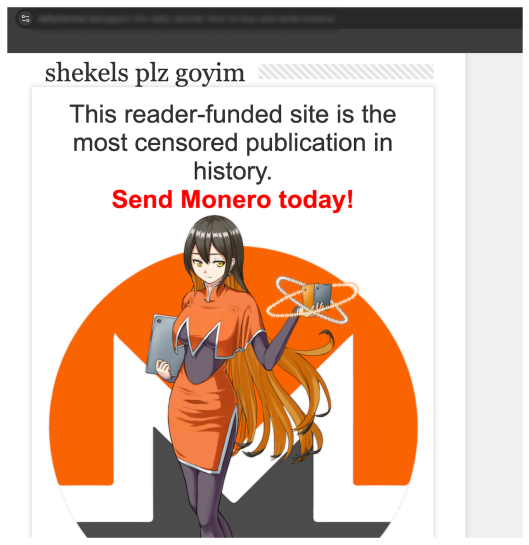
The ability to visualize the on-chain footprint of a neo-Nazi, Holocaust-denying, white nationalist donor alongside the financial behavior of their broader network, is an invaluable tool. Blockchain analysis

provides a broader understanding of the entire ecosystem, going beyond isolated incidents to reveal connections between entities and uncovering insights that are often inaccessible through traditional financial rails, especially for private sector partners. It enables proactive, continuous monitoring of evolving tactics as groups adapt to new challenges, and reveals the links between ideological groups and the behavior of donors who contribute to their activities.

How ideological groups are leveraging privacy measures to evade detection

Many groups are increasingly concerned about being targeted, particularly those that have already been debanked or have faced financial restrictions due to their activities.

For example, the neo-Nazi and white supremacist website The Daily Stormer, has faced significant backlash for its role in inciting violence and promoting hate speech. The site gained widespread notoriety after publishing content glorifying violence and racism, including during and after the 2017 white supremacist rally in Charlottesville, Virginia that turned deadly. The nature of its content led multiple hosting providers to revoke its web domain. Despite deplatforming, the website moved to the darknet to circumvent these restrictions and continues to maintain operations and fundraise via the privacy coin Monero, as seen below.



Shekel, the currency of modern Israel (and historically of the ancient Jews), and goyim, a Hebrew term for non-Jews, are used here in a highly incendiary and trolling manner. Both terms are commonly co-opted by extremists to mock or provoke, laden with anti-Semitic undertones. Extremist actors often use coded language, humor, memes, and video game culture to spread ideologies.

Some groups have stopped publicizing cryptocurrency donation addresses altogether, opting instead to share donation details privately or exclusively through direct communication. These adaptations reflect efforts to evade detection while maintaining funding streams.

Although these groups are not yet highly sophisticated in their use of advanced tools such as mixers, bridges, or decentralized exchanges (DEXs), their growing reliance on privacy-focused cryptocurrencies reflects a developing awareness of the stakes of transparency in traditional blockchain networks and a desire to preserve their operational anonymity.

Challenges and opportunities in managing extremist financing risks

Groups espousing extremist ideology, particularly those operating across multi-ideological networks, present challenges for monitoring and regulation. One of the most fundamental obstacles lies in the inconsistency or outright absence of a clear legal framework addressing extremism across jurisdictions. Unlike FTOs, many groups fall into a grey area, making it challenging to identify them under the existing anti-money laundering and countering the financing of terrorism (AML/CFT) frameworks. This lack of consensus further complicates enforcement efforts, as regulatory obligations for monitoring or blocking transactions involving these groups are not always well defined.

Extremist groups thrive in legal grey area created by jurisdictional inconsistencies

Extremist groups often occupy a legal grey area, depending on the country, complicating global efforts to track, report, and disrupt financial flows associated with them. For example, a neo-Nazi group in the U.S may be legally allowed to operate and fundraise under free speech protections, while similar groups in countries like Germany are banned outright. In some cases, removing such groups from platforms could be considered debanking, which raises political and ethical debates about free speech and financial access, as seen in ongoing discussions in the U.S. But in countries with stricter anti-extremism laws, not only are such groups denied access to bank services, they could also face criminal prosecution. This inconsistency extends to centralized exchanges (CEXs) — the primary cash-out points to convert cryptocurrency to fiat currency — which operate under varying AML/CFT standards. While many enforce strict Know-Your-Customer (KYC) measures, others operate under looser regulations, creating gaps that extremist groups may use to their advantage. The unclear legal status of many such groups further complicates whether exchanges are legally obligated to block transactions or file suspicious activity reports (SARs) related to these actors.

Complex categorization of actors

Determining whether a group fits into a banned category often requires deep analysis of specific country regulations. Ideologically extreme groups that blend legal and illegal activities can evade clear categorization, which complicates monitoring efforts. Without specific groups being blacklisted or sanctioned, the approach to identifying and taking action against such groups may vary drastically depending on jurisdiction.

Blockchain analysis enhances awareness of extremist activity on-chain

While the overall amount raised through cryptocurrency by ideologically extreme groups is relatively small, any amount is concerning given the potential activities it could support. Even modest amounts of funding can finance propaganda, recruitment, or violence — making proactive oversight essential. Blockchain analysis provides critical insights about the financial activity of such groups that would otherwise be difficult to uncover.

While global regulation on extremism remains inconsistent, the insights offered by Chainalysis can support efforts to establish monitoring practices across jurisdictions. By shedding light on how these groups leverage cryptocurrency, Chainalysis equips both the public and private sectors with the tools needed to better mitigate risks.

Organized Crime

Organized Crime Shows High Level of Professionalization, Low Level of Crypto Sophistication

Organized crime has always quickly adapted alongside progress in technology and law enforcement, exploiting innovations that improve efficiency and financial anonymity. The rise of cryptocurrency has accelerated this dynamic, enabling cross-border transactions with unprecedented speed and scale. As adoption continues to accelerate overall, crypto is now involved in a range of illicit activities, spanning drug smuggling, human trafficking, intellectual property theft, and even violent home invasions. Traditional crime groups that once relied on cash increasingly turn to crypto in an attempt to obscure proceeds, facilitate payments, and evade detection.

Despite this shift, many criminal networks exhibit high levels of professionalism but a relatively low level of crypto sophistication. While traditional organized criminal networks have turned to crypto for its speed and perceived anonymity, they often lack the technical expertise needed to effectively conceal their activities. As a result, they inadvertently expose their financial dealings, making it easier for investigators to trace their operations. Even when advanced obfuscation techniques are present, blockchain analysis can reveal relationships that traditional investigative methods struggle to detect. A money service business in West Africa processing illicit funds may be directly tied to Europe-based wildlife smugglers, or a darknet market may route payments for fentanyl through a financial facilitator by cybercriminals. Once fragmented and difficult to see, these connections are now visible in ways that fundamentally change how law enforcement can disrupt transnational organized crime.

Following the supply chain from Chinese labs to Latin America

The global fentanyl trade has long depended on financial secrecy, with Mexican drug cartels leveraging opaque banking systems and underground money networks to pay Chinese chemical vendors for precursor materials. Historically, tracing these financial relationships required infiltrating closed networks, navigating opaque banking systems, or relying on siloed intelligence. Now, blockchain transactions provide a clear record of payments between cartel-linked wallets and international suppliers, revealing not just individual transactions, but the broader financial infrastructure that sustains this fatal trade.

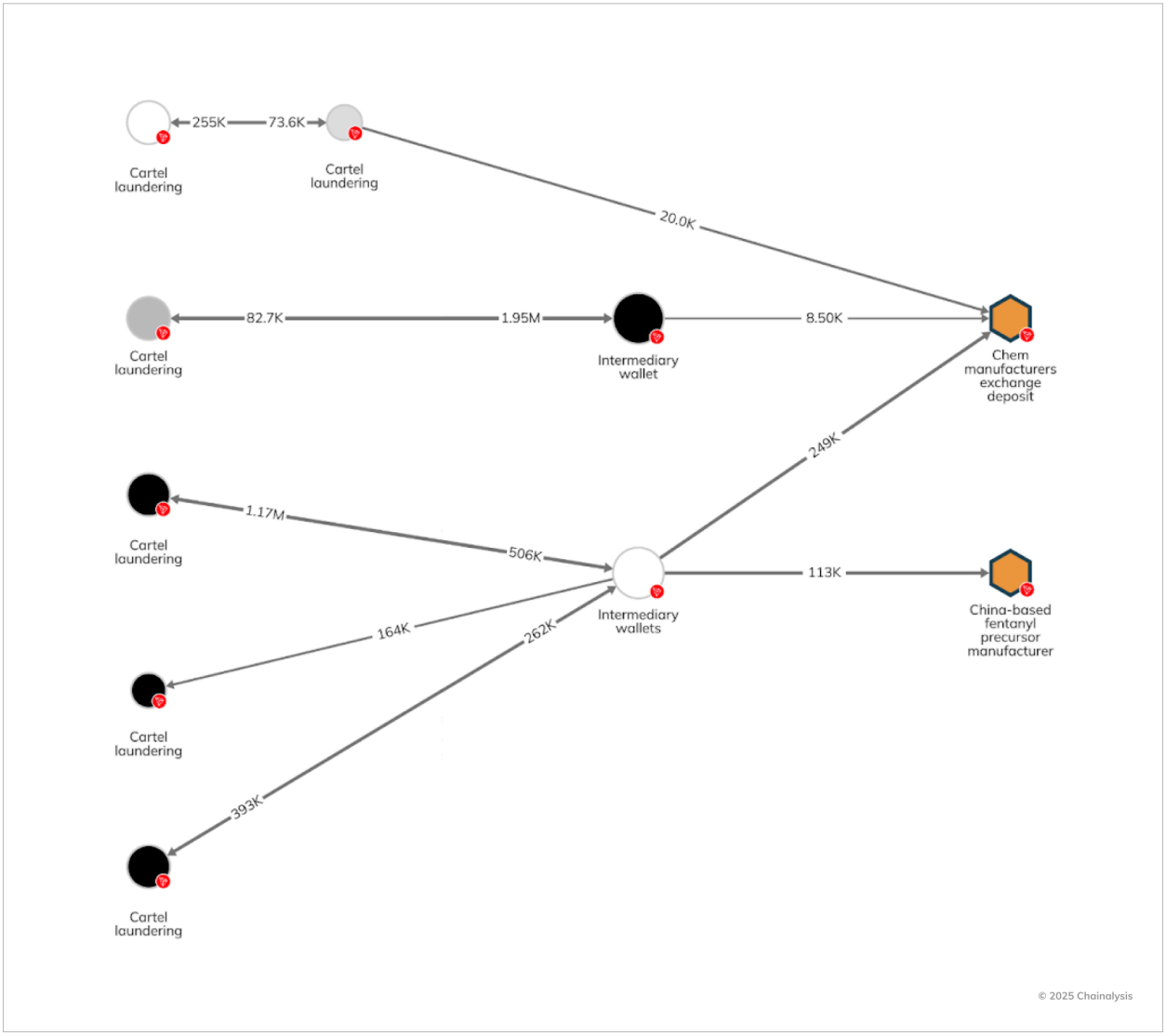
A recent civil forfeiture case in the Eastern District of Wisconsin has exposed crypto's growing role in transnational drug trafficking networks, particularly in the financial ties between Mexican cartels and Chinese chemical suppliers. The case, which resulted in the seizure of over $5.5 million in cryptocurrency, illustrates how blockchain analysis can reveal hidden financial flows within organized crime.

Unraveling the cartel's laundering network on-chain

The investigation began with a money laundering probe targeting a Mexican cartel-affiliated network operating in the U.S. Authorities identified centralized exchange (CEX) accounts and crypto addresses used to move illicit drug proceeds, primarily linked to the sale of fentanyl and methamphetamine. Chainalysis

traced significant transfers from these addresses to wallets previously identified as belonging to Chinese companies supplying fentanyl precursors.

The on-chain link confirmed a direct financial relationship between cartel-linked money launderers and overseas suppliers, as seen in the below Reactor graph.



What makes this case notable is the unsophisticated yet large-scale nature of the laundering operation — a pattern which is frequently observed in other forms of organized crime onboarding to crypto. Unlike cybercriminal groups such as North Korean state-backed actors who use advanced obfuscation techniques, cartel-affiliated launderers operated more openly, moving funds swiftly through centralized accounts and unhosted wallets. A quick turnaround between the laundering of cartel proceeds and the purchasing of more supplies shows their urgency.

While criminals often erroneously view cryptocurrency as a tool for financial anonymity, the cartels' adoption of crypto made them more vulnerable rather than protecting them. While the cartel may have benefitted from speed, low transaction fees, and cross-border efficiency, their reliance on the blockchain has allowed investigators to trace these transactions more easily than would have been possible with traditional cash-based money laundering. Furthermore, it allows even greater potential for disruption because issuers and centralized services typically have the ability to freeze assets when necessary.

Chinese language Crime-as-a-Service bazaars enable swift industrialization of crime

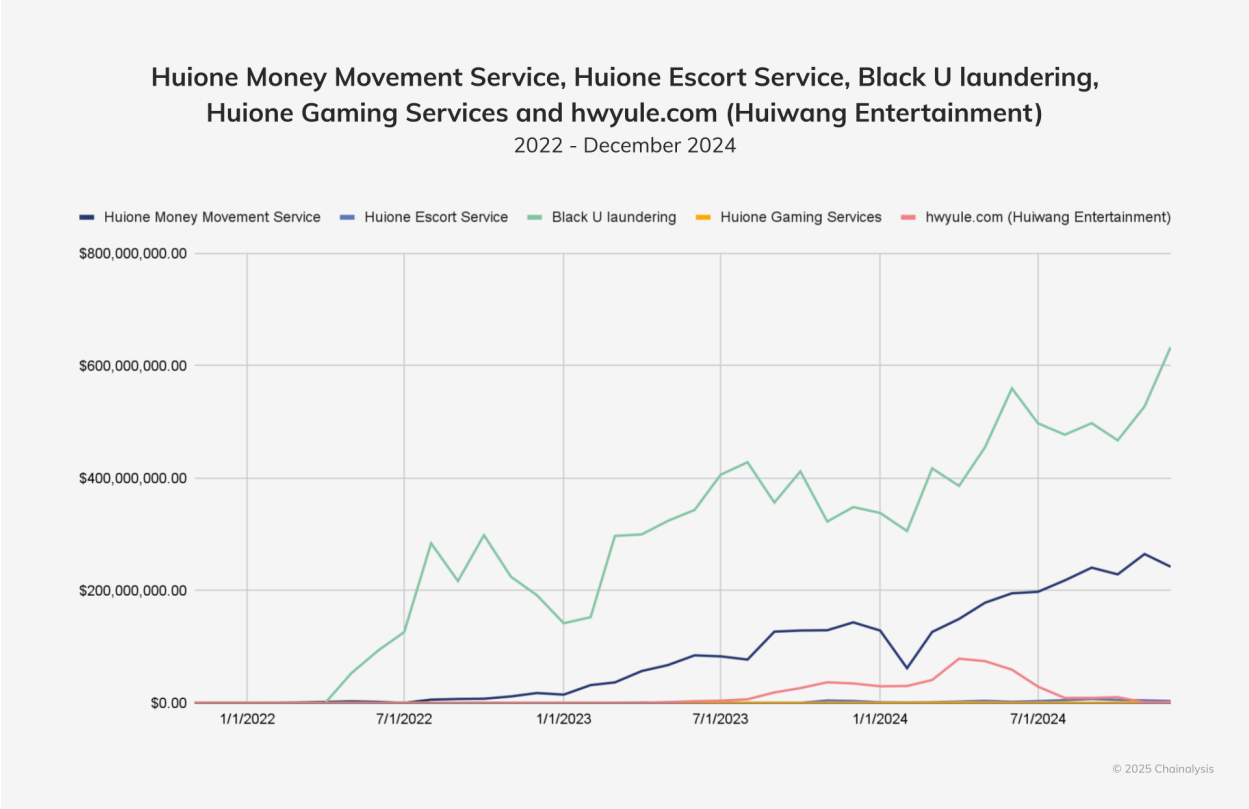
In the evolving landscape of transnational organized crime, illicit marketplaces like Huione Guarantee have emerged as a one-stop shop for nearly every form of cybercrime. Initially positioned as a financial and e-commerce platform, Huione Guarantee has evolved into an extensive hub for money laundering, human trafficking, cyber fraud, and illicit financial services. Unlike traditional darknet markets that primarily cater to cybercrime, Huione has helped industrialize crime-as-a-service (CaaS) — providing access to both the infrastructure and financial tools required to sustain global black-market economies.

At the heart of its operation is a Telegram-based peer-to-peer (P2P) ecosystem, where criminal enterprises can seamlessly move funds, purchase illicit goods and services, and leverage built-in legal and financial support to evade law enforcement. It is the dark economy's equivalent of a fully integrated Amazon-style marketplace facilitating scams, money laundering, human exploitation, and illicit financial flows.

A marketplace model for money laundering

In addition to providing the front-end services required to execute a broad range of illicit activities — data, infrastructure, social media management, and other technology support — Huione money movement services also offer the back-end support that illicit actors need to obfuscate and cash out their ill-gotten crypto. This can be done by a variety of methods, including the use of services explicitly offering money movement and running point (laundering), the use of gaming and gambling platforms, and in some cases, informal over the counter (OTC) vendors reportedly offering "clean" crypto trading proceeds via Telegram.

Hundreds of billions of dollars worth of crypto move through Huione's illicit services. The chart below shows the growth of these flows over time.



'Black U[5]' laundering services' and Huione 'Money Movement Services', have maintained an upward growth trajectory, surpassing $600,000,000 and $200,000,000 in inflows respectively since 2022, making them one of the most prolific unregulated financial services in the world.

Additionally, if a launderer's assets are seized or restricted due to suspicious activity, vendors on Huione offer legal services that claim to engage with exchanges to recover those funds for a fee, as shown below.

[5] ***Black U*** services can be defined as operations in which vendors offer facilitation of laundering of stolen/illicitly obtained U.S. denominated stablecoins (i.e. Black U) in exchange for white (clean) stablecoins. This comes at a cost of a percentage of the overall amount transferred.

[redacted] team professionally handles the freezing of exchange risk control, with high efficiency and fast processing🤝! The business is as follows:

1. Unfreeze the freezing of major exchanges,[redacted]judicial freezing/(it doesn't matter if you don't remember anything)

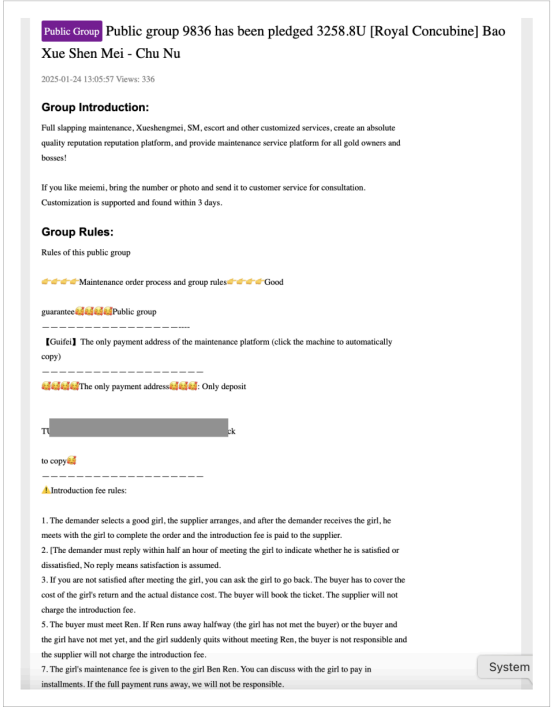
2. Retrieve the usdt that was blocked by dao (starting from 100,000 u) and the wallet forgot the password
3. Unfreeze the frozen wallet [redacted] (starting from 500,000 u)
4.

The fee for unfreezing a large frozen bank card (starting from 3 million) is 5%-50% (depending on the type of freezing, no fee will be charged if it cannot be unfrozen)

This offering claims to facilitate the unfreezing of funds as a result of compliance practices for high-volume money launderers, allowing them to continue their operations largely uninterrupted.

Huione's 'Travel Service' appears to offer a gateway for human trafficking

One of Huione's most insidious offerings is its role in human trafficking and [forced labor networks](). A deeper analysis of its escort service ecosystem reveals explicit overlaps with Huione Travel Service vendors, suggesting a highly organized pipeline where trafficked individuals are advertised, transported, and monetized across borders. Many Huione Escort Service vendors explicitly market international delivery options, shown in the below screenshots.


Public Group Public group 9836 has been pledged 3258.8U [Royal Concubine] Bao Xue Shen Mei - Chu Nu

2025-01-24 13:05:57 Views: 336

Group Introduction:

Full slapping maintenance, Xueshengmei, SM, escort and other customized services, create an absolute quality reputation reputation platform, and provide maintenance service platform for all gold owners and bosses!

If you like meiemi, bring the number or photo and send it to customer service for consultation. Customization is supported and found within 3 days.

Group Rules:

Rules of this public group

👉👉👉Maintenance order process and group rules👉👉👉Good

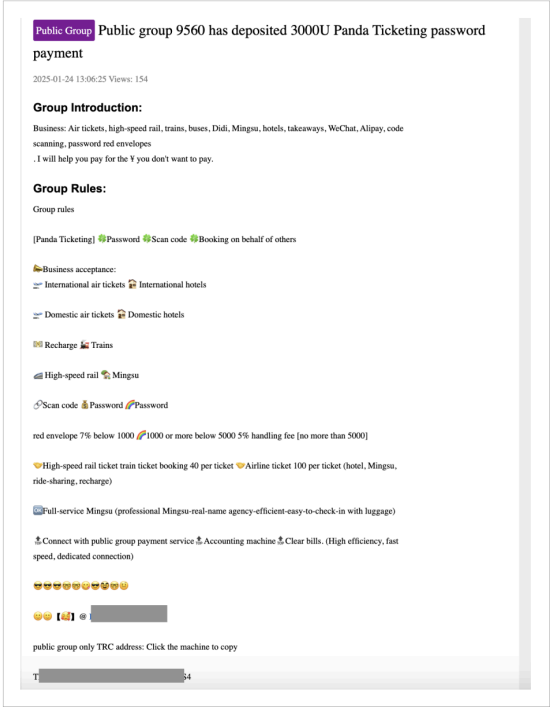
guarantee🥰🥰🥰🥰Public group
——————————————————
【Guifei】The only payment address of the maintenance platform (click the machine to automatically copy)
——————————————————
🥰🥰🥰🥰The only payment address🥰🥰🥰: Only deposit

T[redacted]ck

to copy🥰
——————————————————
⚠️Introduction fee rules:

1. The demander selects a good girl, the supplier arranges, and after the demander receives the girl, he meets with the girl to complete the order and the introduction fee is paid to the supplier.
2. [The demander must reply within half an hour of meeting the girl to indicate whether he is satisfied or dissatisfied, No reply means satisfaction is assumed.
3. If you are not satisfied after meeting the girl, you can ask the girl to go back. The buyer has to cover the cost of the girl's return and the actual distance cost. The buyer will book the ticket. The supplier will not charge the introduction fee.
5. The buyer must meet Ren. If Ren runs away halfway (the girl has not met the buyer) or the buyer and the girl have not met yet, and the girl suddenly quits without meeting Ren, the buyer is not responsible and the supplier will not charge the introduction fee.
7. The girl's maintenance fee is given to the girl Ben Ren. You can discuss with the girl to pay in installments. If the full payment runs away, we will not be responsible.

System


Public Group Public group 9560 has deposited 3000U Panda Ticketing password payment

2025-01-24 13:06:25 Views: 154

Group Introduction:

Business: Air tickets, high-speed rail, trains, buses, Didi, Mingsu, hotels, takeaways, WeChat, Alipay, code scanning, password red envelopes
. I will help you pay for the ¥ you don't want to pay.

Group Rules:

Group rules

[Panda Ticketing] 🍀Password 🍀Scan code 🍀Booking on behalf of others

🛫Business acceptance:
🛫 International air tickets 🏨 International hotels

🛫 Domestic air tickets 🏨 Domestic hotels

🎟 Recharge 🚂 Trains

🚄 High-speed rail 🛰 Mingsu

🔗Scan code 🔒Password 🌈Password

red envelope 7% below 1000 🌈1000 or more below 5000 5% handling fee [no more than 5000]

🤝High-speed rail ticket train ticket booking 40 per ticket 🤝Airline ticket 100 per ticket (hotel, Mingsu, ride-sharing, recharge)

🛄Full-service Mingsu (professional Mingsu-real-name agency-efficient-easy-to-check-in with luggage)

🕹Connect with public group payment service 🕹Accounting machine 🕹Clear bills. (High efficiency, fast speed, dedicated connection)

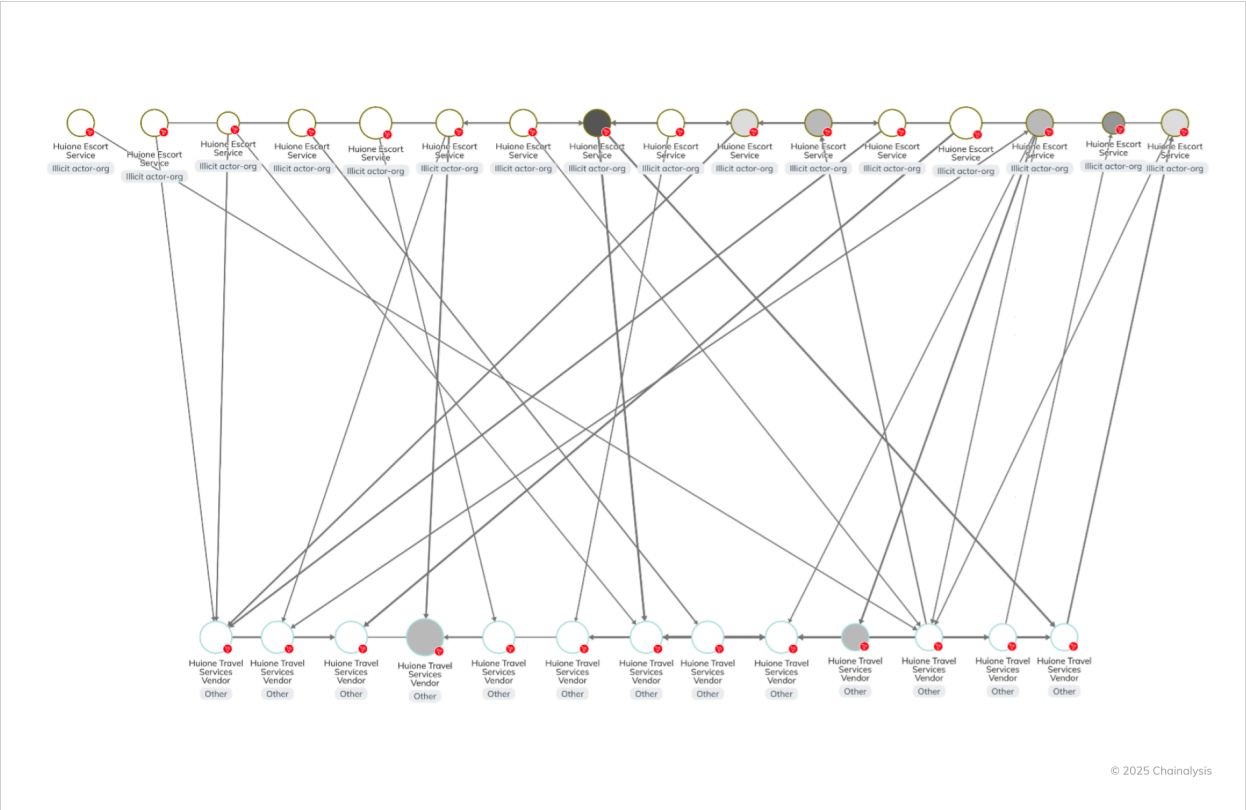
😎😎😎😎😎😎😎😎😎

🥰🥰 【🥰】@ [redacted]

public group only TRC address: Click the machine to copy

T[redacted]54

There are direct financial interactions between these escort services and Huione Travel Services vendors — strongly suggesting that travel services are being used to facilitate human trafficking logistics. In the Reactor graph below, we can see a series of overlapping on-chain connections between Huione's travel and escort services.



Given the sheer scale of Huione's ecosystem, these insights only scratch the surface of the platform's role in global human trafficking networks and other illicit activities, but provides a powerful and alarming example of how operators on Huione's platform extend well beyond the scam ecosystem.

Illicit marketplaces pose a law enforcement challenge

While Huione Guarantee is presently the largest illicit marketplace, Chainalysis is monitoring similar platforms that continue to emerge. Illicit marketplaces like Huione Guarantee operate outside of the regulated space, presenting challenges to law enforcement due to their decentralized operations, global reach, and integration with both legitimate and underground financial systems. Unlike traditional darknet markets that operate in isolated corners of the internet, Huione functions as a publicly accessible platform, blending legal and illegal transactions. Its peer-to-peer (P2P) financial services allow money laundering networks to exploit gaps in regulatory oversight, particularly in jurisdictions that have weak enforcement mechanisms or are unlikely to respond to coordinated counter-financial crimes campaigns. Efforts to dismantle these networks will require international cooperation, blockchain intelligence, and strong collaboration between financial institutions, private sector partners, and law enforcement to identify and close loopholes that allow criminal enterprises to thrive.

Combating illegal wildlife trade (IWT) with financial crime enforcement

Wildlife trafficking has long been a highly profitable form of organized crime, deeply entangled with global networks engaged in illegal activities such as drug smuggling, arms trafficking, and cyber fraud. Despite its devastating impact on conservation, biodiversity, and natural ecosystems, the trade continues to thrive due to weak enforcement and lenient penalties. Financial crime investigations, particularly those leveraging blockchain analytics and anti-money laundering (AML) strategies, are becoming powerful tools in tackling these operations.

For an inside perspective, we spoke with Robert Campbell, Programme Director of United for Wildlife, which sits within The Royal Foundation of The Prince and Princess of Wales. United for Wildlife works to tackle the illegal wildlife trade (IWT) by bringing together stakeholders from public, private and non-profit sectors to protect endangered species and disrupt the criminality behind the trade. One element of the program focuses on engaging with financial institutions, enhancing their understanding of IWT and targeting the financial infrastructures behind wildlife crime.

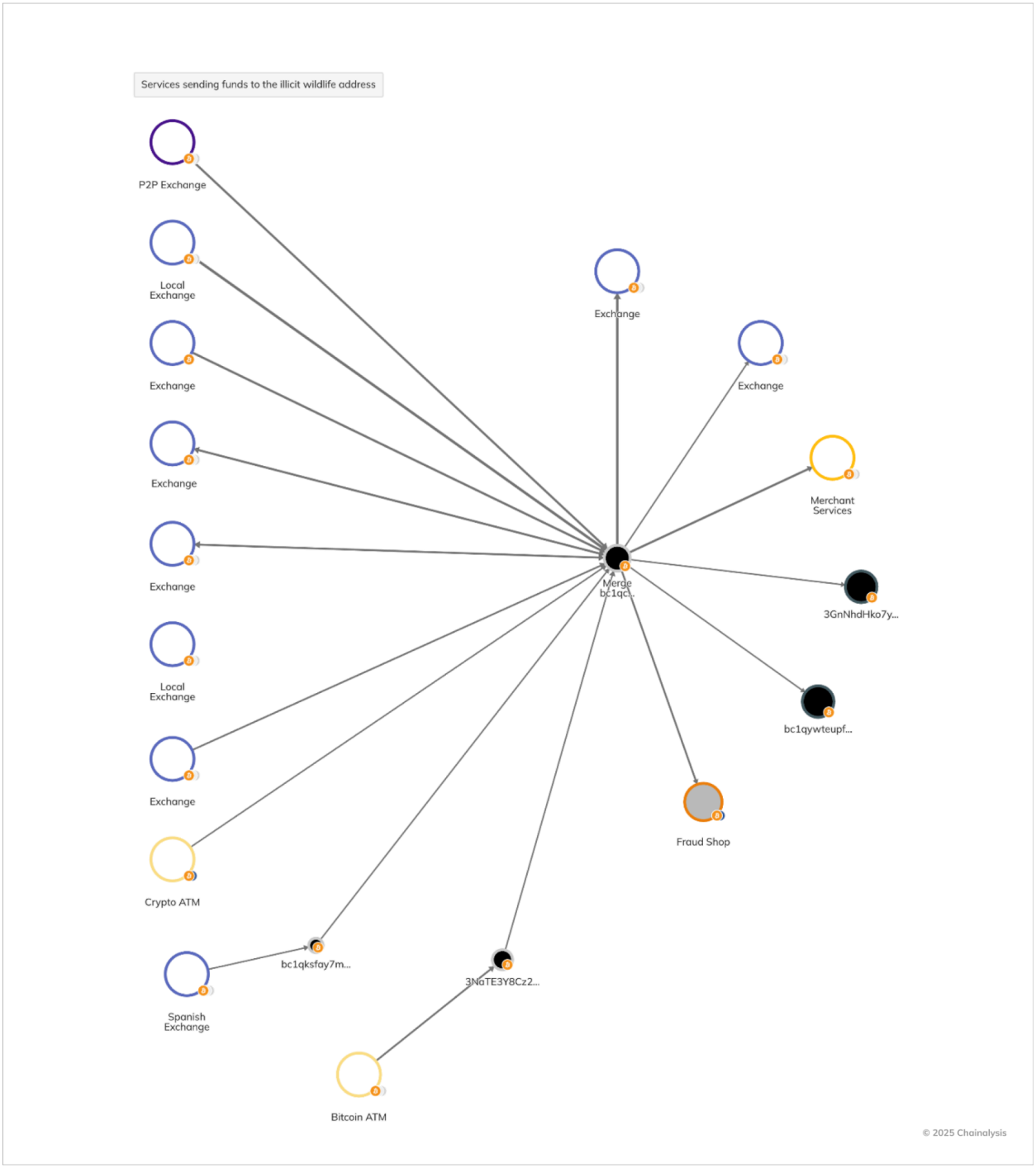
Wildlife trafficking: Low-risk, high-reward crime

One of the biggest obstacles in combating wildlife trafficking is the low level of legal risk that traffickers face in most jurisdictions. Campbell explained that in large parts of the world, the penalties for wildlife crime remain minimal, making it an attractive enterprise for criminals. "In terms of risk versus reward, the rewards far outweigh the risks for traffickers. So we see them trading openly — a lot. There's no need to trade on the dark web," Campbell said.

Unlike drug or arms traffickers, who take extensive measures to avoid detection, many wildlife traffickers operate brazenly. They sell endangered species and illegal animal products on mainstream social media and commerce platforms. "Most of this trade is happening in the open because few jurisdictions are looking for it," he added.

How wildlife traffickers use cryptocurrency

While traditional financial systems still dominate wildlife trafficking transactions, cryptocurrency is becoming an increasingly useful tool for criminals, particularly through African exchanges and peer-to-peer transactions. Blockchain analysis of a suspected cluster of wildlife trafficking addresses reveals the on-chain mechanisms of illicit wildlife trafficking, shown in the Reactor graph below.



Payments flowed from wallets to local CEXs without major efforts to conceal activity. Traffickers seem to hide in plain sight rather than deploy sophisticated laundering techniques. Crypto ATMs also play a role, allowing traffickers to convert cash from wildlife sales into crypto for easier cross-border movement. Additionally, intersections with other criminal enterprises are visible in the graph. Several wallets linked to wildlife trafficking funds also show connections to fraud shops and other illicit entities, reinforcing how wildlife trafficking and environmental crime are often embedded within larger organized crime networks.

Wildlife traffickers' reliance on centralized, KYC-compliant exchanges offers a critical enforcement opportunity. Unlike criminals who prioritize obfuscation, many traffickers move illicit funds through regulated platforms, creating a straightforward avenue for law enforcement to intervene. By strengthening relationships with exchanges, investigators can gain off-chain intelligence that helps to map financial networks and trace key players in the supply chain. However, effective enforcement requires more than just transactional data. Corruption and complicity in certain jurisdictions can make direct action difficult, reinforcing the need for collaboration with NGOs, trusted local law enforcement, and private sector organizations. With on- and off-chain financial intelligence and cross-sector partnerships, authorities can disrupt trafficking networks at multiple levels: from small-scale sellers to higher-tier operators overseeing the trade.

How financial crime laws are shutting down wildlife trafficking networks

Given the weak legal penalties for wildlife crime, financial investigations offer one of the most effective means of disrupting these networks. Law enforcement agencies are shifting their focus to financial crime laws, using money laundering statutes to impose harsher sentences on violators. "Wildlife crime does not carry a high sentence in most countries — if it's even a year, it's often a slap on the wrist," Campbell said. "But financial crimes like money laundering carry much higher penalties." Authorities in several countries are already adopting this approach:

- Mainland China has updated its anti-money laundering laws to include wildlife crime. Under the Chinese presidency in 2019-2020, FATF made tackling financial flows from IWT a priority.
- In Singapore, a transit jurisdiction for environmental crimes and associated financial flows, domestic laws have been amended to designate serious foreign environmental crimes as money laundering predicate offences. This empowers law enforcement to investigate money laundering for environmental crimes that occur outside the country's borders.
- Hong Kong has classified wildlife trafficking under its serious organized crime laws, enabling authorities to conduct in-depth investigations into money laundering and seize assets linked to trafficking networks.

Additionally, the United for Wildlife Statement of Principles has pushed financial intelligence units worldwide to prioritize wildlife trafficking investigations. Over 35 countries, particularly in notable wildlife trafficking hotspots like Sub-Saharan African and Latin America, have signed on to this initiative, including the U.S., UK, Singapore, South Africa, Brazil, and Mexico.

Crypto literacy is a major challenge for law enforcement

One of the biggest challenges in tackling wildlife trafficking through financial investigations is the lack of crypto tracing expertise. "You have this really powerful tool for law enforcement and financial units to use — if they know how to use it," said Campbell. Many law enforcement agencies still lack the necessary training to follow on-chain financial flows related to IWT. "There's such a lack of understanding of how crypto functions and how wildlife trafficking can be used for crypto," Campbell said. "Having Chainalysis provide simple, clear training has already been incredibly effective."

At a recent United for Wildlife summit, officers who received blockchain analytics training from Chainalysis were able to identify direct overlaps with their existing cases. "We've seen investigators who initially didn't understand blockchain suddenly recognize connections to cases they were already working on. That's when the lightbulb goes off," he said.

Global efforts and the role of blockchain intelligence

Campbell emphasized that cross-sector collaboration is key to making real progress. Governments, financial institutions, tech platforms, law enforcement, and Chainalysis can all work together to disrupt the financial incentives that drive the IWT. "The more we share insights on crypto trends and wildlife trafficking typologies, the better equipped we'll be to shut these networks down," Campbell said. "No longer is the investigation focused on just the person caught with wildlife. Now, financial investigations follow the money to dismantle entire networks," he added. Blockchain intelligence is uncovering surprising connections between wildlife trafficking and other forms of organized crime. "You have professional launderers, you have people on the ground — it's really insightful to see the whole network," Campbell explained.

"Crypto's transparency is an opportunity, not a threat," Campbell emphasized. "With the right knowledge and tools, we can make the financial system more secure for everyone."

Intellectual property theft on-chain: The corporate structure of digital piracy

A less obvious but growing threat, intellectual property (IP) theft has also evolved into a highly structured form of organized crime. Illicit Internet Protocol Television (IPTV) piracy networks — services that illegally stream copyrighted media — and gaming cheat distributors are leveraging crypto to facilitate transactions, obscure financial trails, and evade law enforcement. Although their use of cryptocurrency is largely unsophisticated, the shift from traditional off-chain methods to crypto-enabled crime has allowed these groups to scale and operate globally, making enforcement increasingly complex.

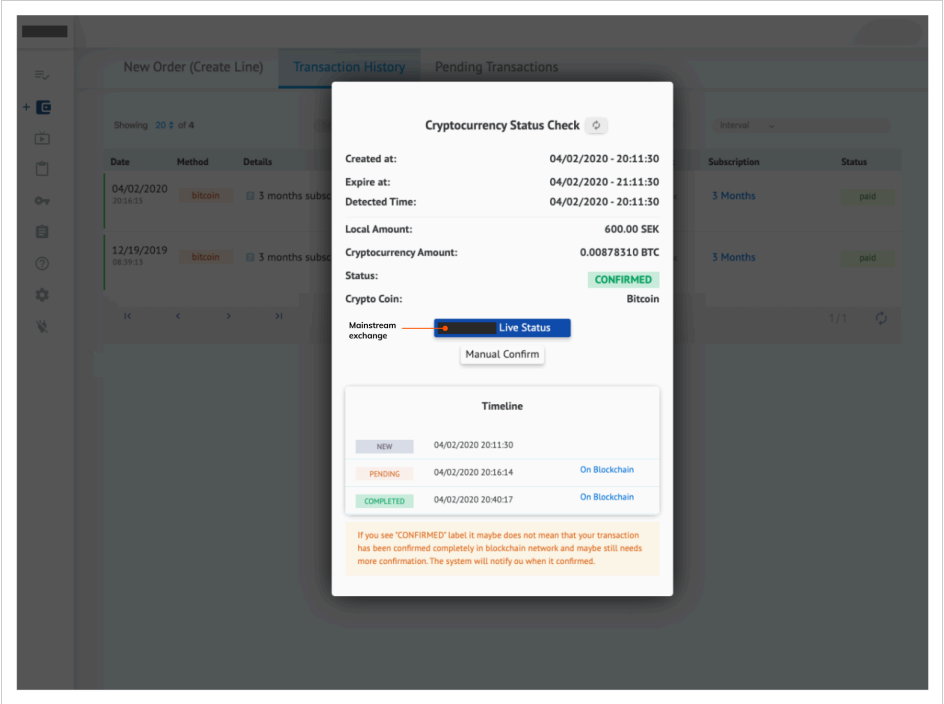
Illegal IPTV: Another high-profit, low-risk crime

Illegal IPTV services operate like shadow versions of Netflix, offering premium television, movies, and live sports at a fraction of legitimate prices. These operations run sophisticated content delivery networks while funneling payments through unregulated financial channels.

Michael Lund of Nordic Content Protection — the leading anti-piracy organization working for the television industry in the Nordics — explained that IPTV piracy has remained the most significant IP threat since 2017. "Criminals can duplicate legal products without production, licensing, or distribution costs," he said. "They sell subscriptions at a fraction of the legal price, which appeals to consumers who either don't know or don't care about copyright laws." Despite enforcement efforts, IPTV piracy remains a lucrative, yet low-risk crime. When one operation is dismantled, another quickly replaces it, ensuring uninterrupted service for customers. A reseller can invest as little as €200 to buy access credits, set up a website, and start selling illegal subscriptions, creating a recurring revenue stream.

Crypto has been one of illegal IPTV's biggest enablers. Low-cost, borderless payments make crypto an ideal financial tool for these operations. Lund emphasized that operators are not motivated by ideology, but purely by profit. "These are financial criminals — they're in it for the money," he said. "Within six months of crypto gaining mainstream attention, every single illegal IPTV operation had integrated crypto payments."

Although privacy coins like Monero can offer additional secrecy, most operators still prefer bitcoin, Litecoin, and stablecoins due to their widespread availability and liquidity, said Lund. Some even mimic integrations with mainstream crypto exchange payment modules to falsely give customers a sense of legitimacy, as seen in the screenshot of one such platform below.



Hierarchy and financial flows of IPTV piracy

Despite their high transaction volume, most IPTV resellers lack sophisticated laundering knowledge. Entry-level resellers buy access credits from larger syndicates, resell subscriptions, and cash out through exchanges. Lund explained that while smaller resellers rarely bother to hide their tracks, top-tier syndicates are much more careful. "Some engage in advanced mixing because the amounts they receive are massive," he noted.

Lund noted that globally, 20–30 major organized crime groups dominate IPTV piracy. These syndicates operate large-scale streaming infrastructures, process large payments, and employ financial specialists to launder funds. Lund described a recent IPTV operation where three criminals earned millions within months before being caught. "One guy was the technical mastermind, setting up the servers and handling crypto," he said. "The other two were his business managers, handling sales and customer relations."

Authorities seized millions in cash, cars, and real estate, but the case has dragged on for years, highlighting the enforcement and prosecution challenges of cross-border crime.

The underground gaming cheat economy

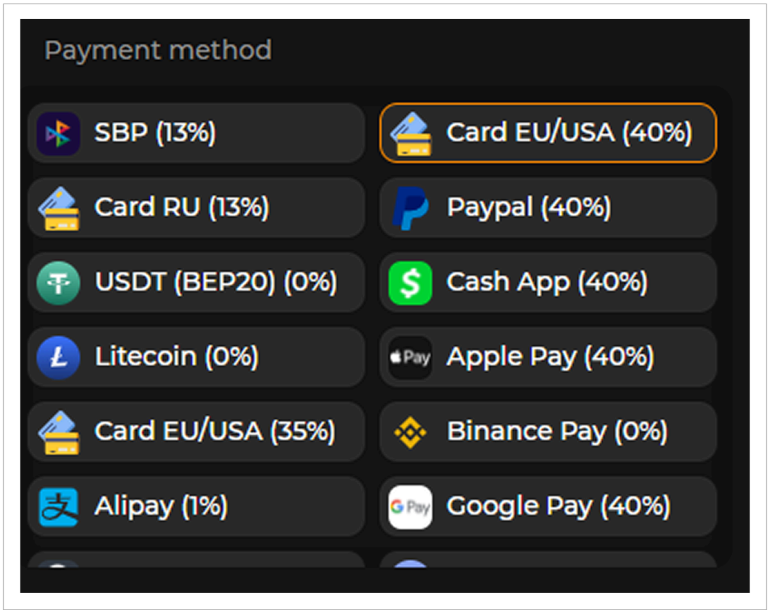
Beyond IPTV piracy, crypto payments also power the black market for gaming cheats. These cheats, designed to give unfair advantages in multiplayer games, undermine in-game economies and decrease publisher revenues.

Irdeto, a leader in digital security, tracks and combats cheat developers and sellers. They describe the cheat ecosystem as a structured, multi-tiered enterprise. Developers create cheats, sometimes keeping their communities small to avoid detection. Larger sellers expand operations, offering cheats for multiple games, while resellers distribute them at scale, handling logistics and customer service.

Irdeto noted that "resellers are the easiest to spot. These sellers often offer cheats for more than 50 titles." While some developers avoid advertising, others use forums like ElitePVPers and OwnedCore to reach buyers. Many cheat sales are fully automated with purchases processed through Shopify or Sellix, delivering subscription keys instantly.

Cryptocurrency and the cheat economy

Crypto is the cheat industry's primary financial enabler. Unlike PayPal or credit cards, which pose risks of chargebacks and account bans, crypto transactions are irreversible and borderless, allowing sellers to operate freely. "Cheat sellers often offer cryptocurrency as a payment option," Irdeto explained. "Digital currencies provide a level of anonymity not offered by more traditional payments such as a debit or credit card, which require adherence with strict anti-fraud measures."



Hax.market checkout page showing accepted payment methods and corresponding upcharges

Some cheat marketplaces, such as Hax.market, charge extra for PayPal or credit card payments but waive fees for crypto transactions. Bitcoin, Litecoin, and stablecoins dominate the market, while privacy coins like Monero are rarely used, as most buyers prefer widely recognized cryptocurrencies.

Fighting back against crypto-powered cheating

Gaming companies and cybersecurity firms are ramping up their efforts against cheat sellers. Irdeto's kernel-mode (referring to the core part of an operating system) anti-cheat solutions offer deep system monitoring, while AI-driven fraud detection identifies suspicious player behavior.

Legal frameworks like the Digital Millennium Copyright Act (DMCA) and the Digital Services Act (DSA) help take down cheat-selling websites and remove them from social media. Irdeto highlighted that Microsoft's upcoming restrictions on kernel space access could be a game changer, preventing cheat developers from embedding deep system exploits.

Defeating crypto-enabled IP crime

Despite its low risk nature, IP theft is drawing increased law enforcement and regulatory attention. As more investigators are trained on blockchain tracing , the financial backbone of these operations is becoming more exposed. Shutting down individual IPTV or cheat networks won't eliminate the industry, but financial pressure on crypto laundering channels could significantly disrupt these markets.

The rise of violent crime linked to cryptocurrency

Historically, financial crimes involving crypto theft were largely confined to internet-based fraud, malware, phishing attacks, and scams. However, criminals are now brazenly shifting to physical methods of extraction. Law enforcement agencies and cybersecurity experts have observed a sharp rise in cases where individuals are subjected to violence to force crypto transfers, often from organized gangs.

The typologies of physical crypto attacks: Targeted and opportunistic

Julia G of zeroShadow, a full-stack Web3 security company specializing in exploit prevention and incident response, describes two primary types of physical crypto theft:

1. **Targeted attacks on high-net-worth individuals:** Victims are specifically chosen because their wealth is public knowledge. "In one case we had, the victim was taken hostage at his place of work, and the attackers knew how much crypto he owned and where his children were. These details were used to coerce him into transferring the funds."

2. **Opportunistic street crimes:** Theft of a mobile phone or personal device escalates when attackers discover it contains a crypto wallet.

"Interestingly, in both cases we have seen that the attackers do very little to obfuscate the flow of funds on-chain." Julia G explained. "In the cases we have worked, we've seen funds go to a cooperative exchange and instant exchangers within the first 48 hours of the theft."

Notable incidents of crypto-related violent crime

The escalation from cyber fraud to physical attacks highlights how crypto crime, well beyond traditional categories, is blurring the line between digital threats and real world violence.

Kidnapping of Ledger co-founder and wife

David Balland, the co-founder of a popular crypto hardware wallet, and his wife were kidnapped from their home in Central France and held for ransom for cryptocurrency. Balland's hand was mutilated during the ordeal. A police operation involving over 90 officers from GIGN — one of France's elite tactical police units — rescued the couple, leading to the arrest of two individuals and the questioning of 10 others. Nearly all the ransom funds have been traced, frozen, and seized.

Home invasion network targeting crypto owners

A 24-year old Florida man led a robbery ring executing violent home invasions across multiple states, including North Carolina, Florida, Texas, and New York. Victims were restrained and forced to give up access to their crypto wallets and accounts.

Six men accused of holding Chicago family captive for $15 million crypto transfer

Six men were accused of kidnapping a family of three and their nanny at gunpoint after forcing their way inside the family's home, holding them captive for five days. The kidnappers demanded a $15 million ransom in cryptocurrency. One suspect was arrested upon re-entering the U.S. from Mexico, while others are believed to have fled to China.

UK gang members sentenced for cryptocurrency kidnapping

Seven members of a UK gang were sentenced up to 20 years in prison for kidnapping and torturing a crypto investor, extorting approximately $124,000 worth of crypto over several months. The victim was repeatedly assaulted and locked in a cupboard overnight.

Blockchain is the 'killer app' in the fight against organized crime

Traditional organized crime groups are increasingly adopting crypto, using a structured division of labor, intelligence gathering, and laundering operations. Cartels, wildlife traffickers, IPTV pirates, and even violent criminals are leveraging crypto not because they have mastered its complexities, but because it offers speed, efficiency, and a perception of anonymity.

However, their reliance on centralized exchanges, high-visibility transactions, and basic laundering techniques presents an invaluable enforcement opportunity — one that will likely not endure forever. Unlike sophisticated state-backed cybercriminals who employ advanced obfuscation tactics, many traditional crime groups are still operating in plain sight. Direct exchange cash-outs and simple P2P transfers dominate these illicit financial flows. Many traffickers and launderers are not yet using sophisticated privacy tools, meaning their transactions remain easily traceable on-chain. This transparency provides law enforcement, regulators, and financial institutions with an incentive to act now.

With the right strategies — enhanced compliance at the exchange and protocol level, advanced blockchain intelligence, and global law enforcement cooperation — authorities can dismantle these illicit networks before they adapt. While criminals see crypto as a tool for anonymity, its inherent transparency flips the advantage toward those who know how to use it. Unlike traditional financial investigations, where evidence is often siloed across different institutions, the blockchain offers a single, authoritative, and immutable ledger. Beyond just following criminals post-factum, Chainalysis enables proactive disruption — allowing investigators to follow movements real time, mapping out networks and generating leads that span across continents. As more crime moves on-chain, the ability to expose and dismantle these networks will only improve, shifting the balance in favor of those working to fight illicit finance.

Chainalysis

Building trust in blockchains

About Chainalysis

Chainalysis is the blockchain data platform, making it easy to connect the movement of digital assets to real-world services. Organizations can investigate illicit activity, manage risk exposure, and develop innovative market solutions with deep blockchain data insights. Our mission is to build trust in blockchains, blending safety and security with an unwavering commitment to growth and innovation. For more information, visit www.chainalysis.com.

FOR MORE INSIGHTS
chainalysis.com/blog

FOLLOW US ON X
@chainalysis

GET IN TOUCH
info@chainalysis.com

FOLLOW US ON LINKEDIN
linkedin.com/company/chainalysis