Chainalysis

The 2026 Crypto Crime Report

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

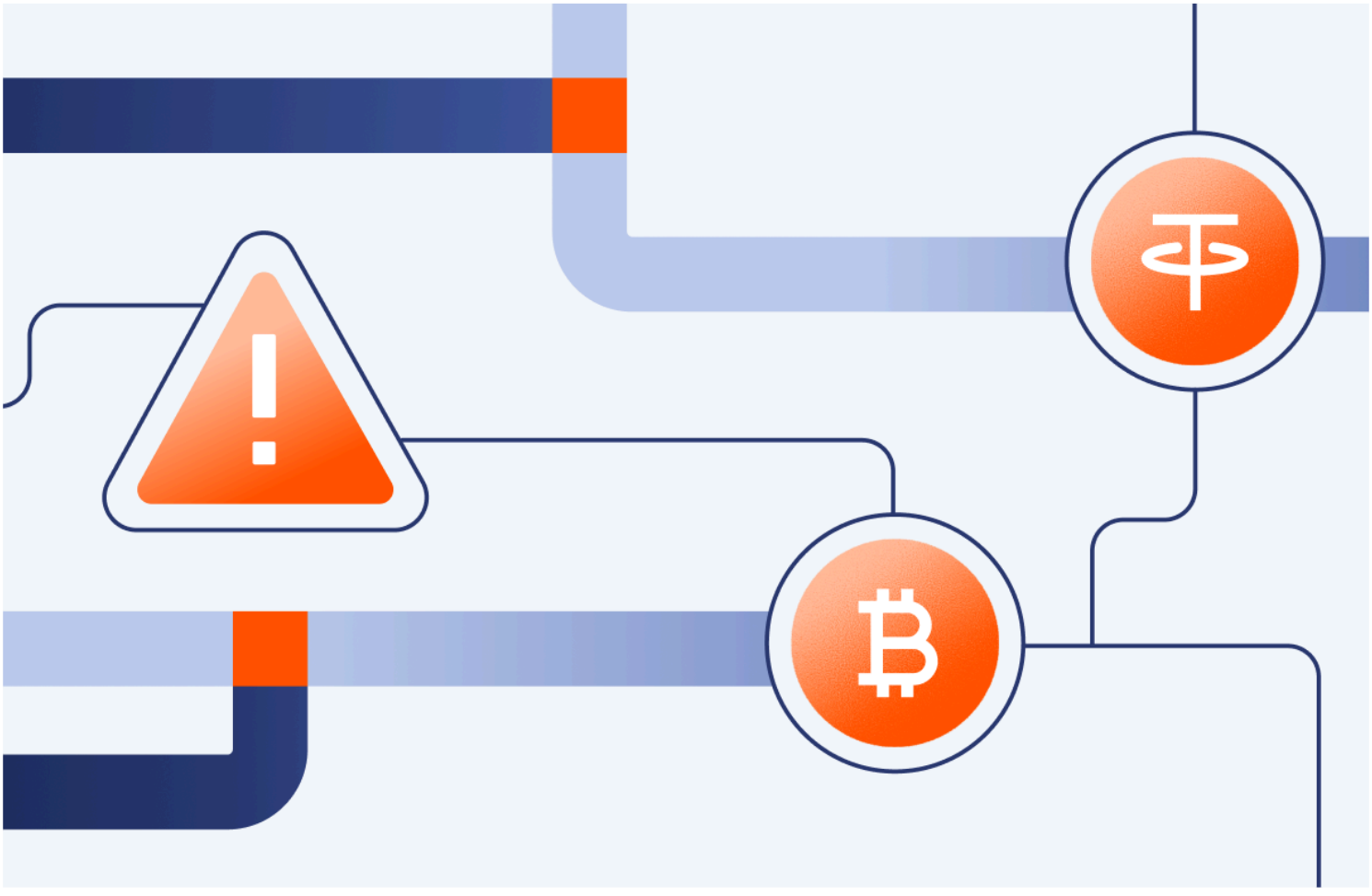


Table of Contents

Why We Publish This Research: Facts, Not Fear, About Crypto Crime

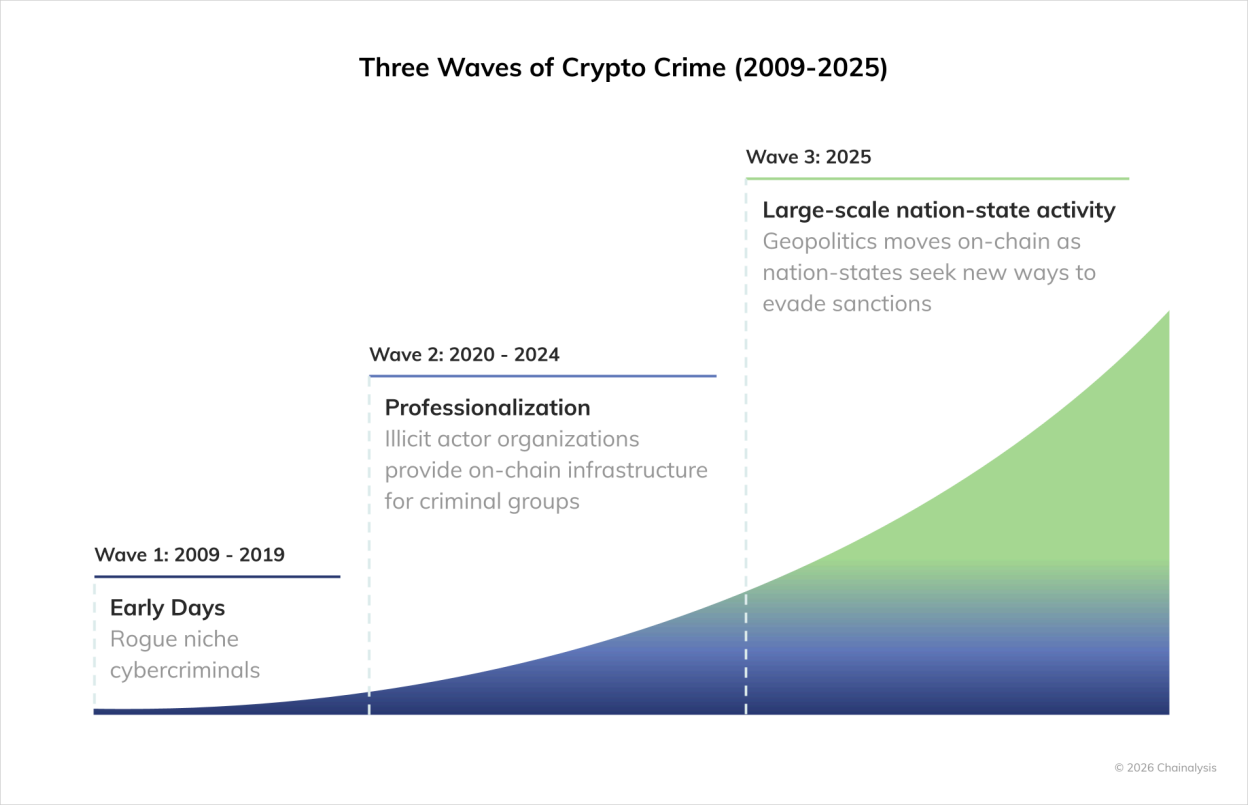
In 2026, financial institutions can no longer ignore crypto – the growth of stablecoins alone demonstrates the demand for 24/7, instantaneous, cross-border, cheap, and easy value transfer. But the defining feature of this financial era is not simply growth — it is transparency. Public blockchains represent the first global financial infrastructure where transactions are recorded on an immutable, time-stamped ledger visible to anyone willing to look. That permanence and openness fundamentally reshape how markets can be understood. For financial institutions, this is not a marginal improvement over legacy rails; it is a structural paradigm shift. The ability to trace value flows across borders in near real time, to analyze counterparties with precision, and to observe systemic patterns at scale is something that has never been possible in conventional finance, where data is fragmented across institutions, jurisdictions, and proprietary systems. Blockchain technology, by design, creates a single source of truth.

Our purpose in publishing this report is not to sensationalize illicit activity or amplify fear. Quite the opposite. The blockchain's transparency empowers us to measure risk with clarity rather than conjecture. Where traditional financial crime often remains obscured behind opaque banking relationships and siloed reporting regimes, on-chain activity leaves immutable evidence. That visibility enables rigorous analysis, informed policy discussions, and smarter compliance frameworks. It allows institutions to contextualize illicit activity within the overwhelmingly broader growth of legitimate adoption and to distinguish between perception and measurable reality. In other words, the same openness that makes digital assets innovative also makes them uniquely measurable — and measurable systems are ultimately more governable.

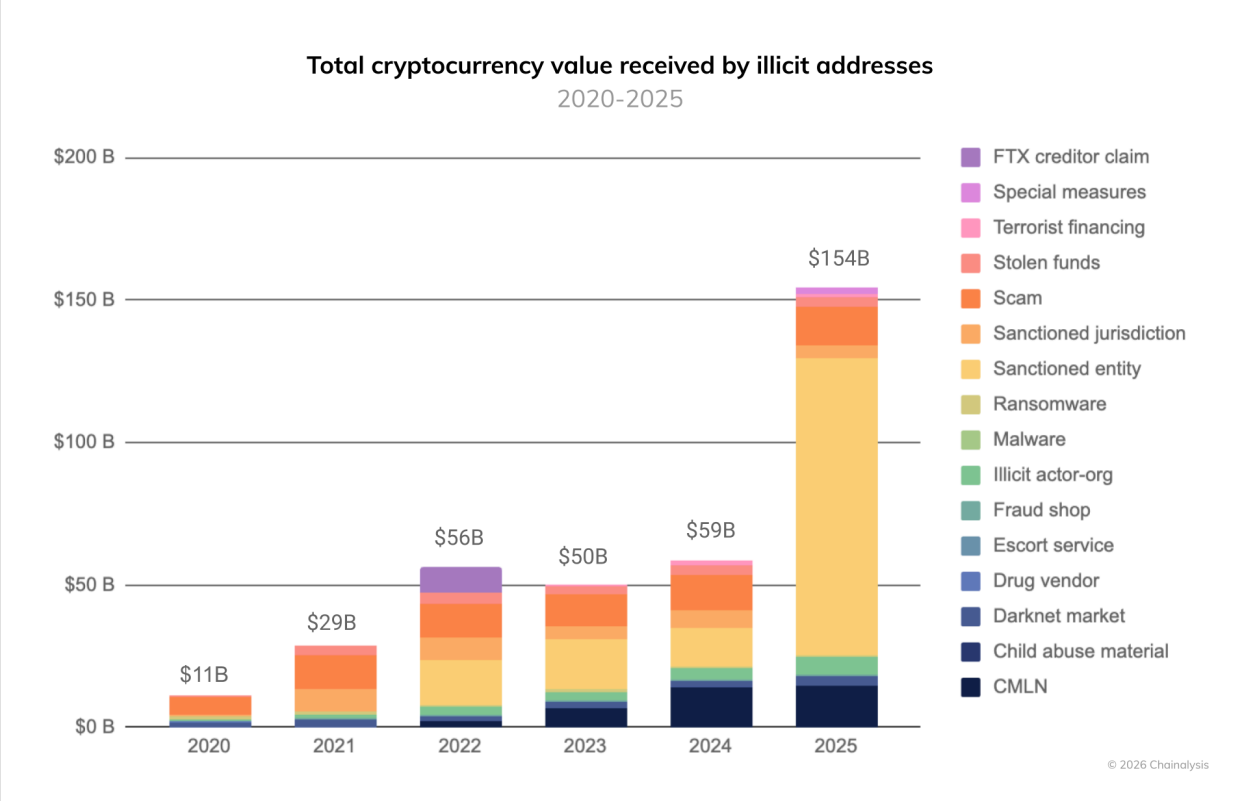
At the same time, as we make clear throughout our report, transparency does not eliminate threats. Rather, it illuminates them. Our latest findings show that on-chain illicit activity is increasingly interwoven with sophisticated, state-aligned ecosystems that exploit crypto's global reach. In particular, the Chinese cybercrime ecosystem has emerged as a central node in large-scale scam operations, human trafficking, underground banking networks, and laundering infrastructure that service threat actors across jurisdictions. The convergence of criminal enterprise and geopolitics underscores why transparent financial infrastructure matters: it allows the private and public sectors alike to see these patterns as they form in real time. As adoption accelerates across both retail and institutional markets, the ability to interpret that transparency responsibly — and collaboratively — will define the next generation of global finance.

Crypto Crime Reaches Record High in 2025 as Nation-State Sanctions Evasion Moves On-Chain at Scale

In 2025, we tracked a notable rise in nation-state activity in crypto, marking the latest phase in the maturation of the illicit on-chain ecosystem. Over the past few years, the crypto crime landscape has become increasingly professionalized; illicit organizations now operate large-scale on-chain infrastructure to help transnational criminal networks procure goods and services and launder their ill-gotten crypto. Against that backdrop, we have seen nation-states moving into this space, both by tapping into these same professionalized service providers and by standing up their own bespoke infrastructure to evade sanctions at scale. As nation-states plug into the illicit crypto supply chains originally built for cybercriminals and organized crime groups, government agencies and compliance and security teams now face significantly higher stakes on both the consumer protection and national security fronts.



How are these and other developments manifesting on-chain? Let's examine the data and high-level trends.



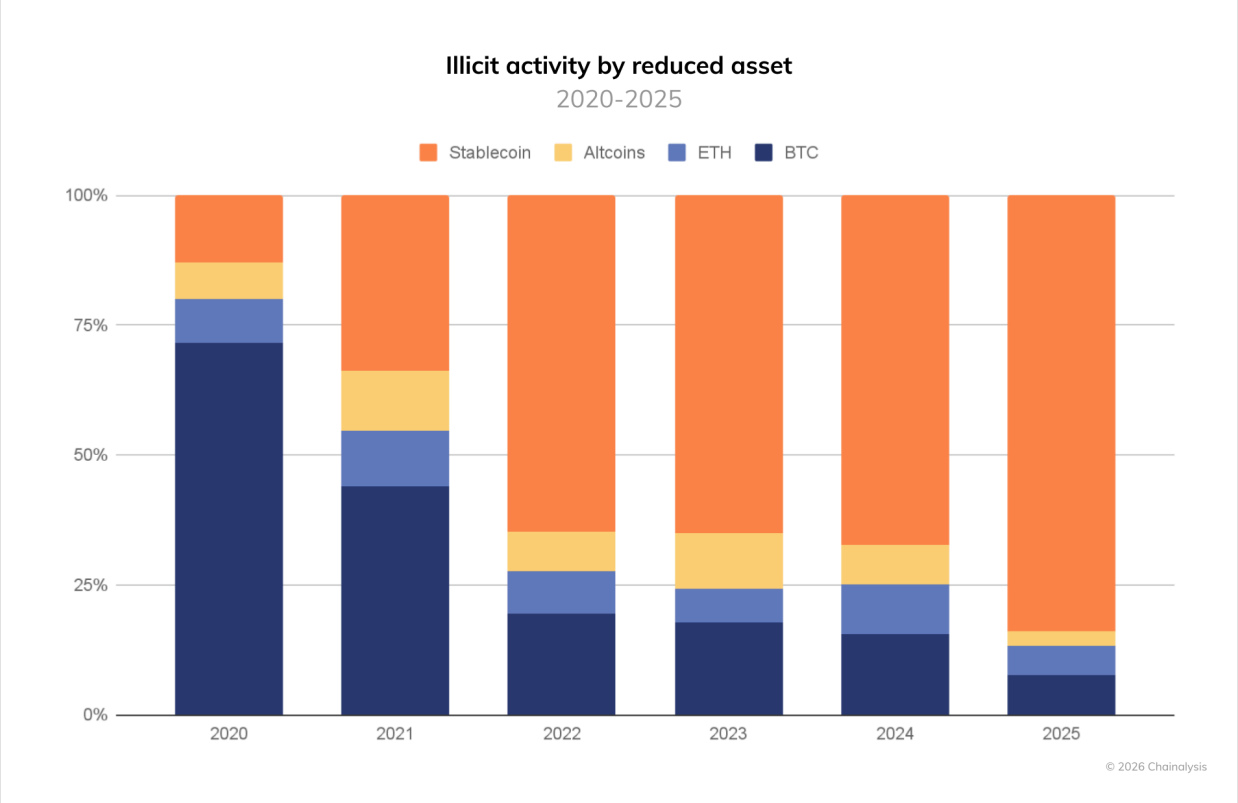
According to our data, illicit cryptocurrency addresses received at least $154 billion in 2025. This represents a 162% increase year-over-year (YoY), primarily driven by a dramatic 694% increase in the value received by sanctioned entities. But even if the value received by sanctioned entities were flat YoY, 2025 would still mark a record year for crypto crime, as activity increased across most illicit categories. As always, we must caveat that this figure represents a lower-bound estimate based on illicit addresses we've identified to date.[1]

These illicit volumes are still dwarfed by the broader crypto economy, which largely consists of legitimate transaction volumes. Our estimate for the illicit share of all attributed crypto transaction volume increased slightly from 2024 but remains below 1%.[2]

[1] A year from now, these totals will be higher as we continue to identify more illicit addresses and incorporate their historical activity into our estimates. For perspective, when we published last year's Crypto Crime Report, we reported $40.9 billion for 2024. One year later, our updated estimate for 2024 is substantially higher at $57.2 billion, with much of that growth coming from various types of illicit actor organizations providing on-chain infrastructure and laundering services for high-risk and illicit actors. 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.

[2] To calculate the illicit share of attributed transaction volumes, we determine the denominator by calculating all inflows to known services across all the assets that we track, excluding internal transfers within services. We then divide the illicit value received by the total value received by all services.

We are also observing a continued shift in the types of assets involved in crypto crime, as shown in the chart below.



For the past few years, stablecoins have come to dominate the landscape of illicit transactions, and now account for 84% of all illicit transaction volume. This mirrors broader ecosystem trends where stablecoins occupy a sizable and growing percentage of all crypto activity due to their practical benefits: easy cross-border transferability, lower volatility, and broader utility.

Below, we'll take a closer look at four key trends that defined crypto crime in 2025 and will be important to watch going forward.

Nation-state threats drive record volumes: North Korea steals more than ever, and Russia's A7A5 token facilitates large-scale sanctions evasion

Stolen funds remained a major threat to the ecosystem in 2025, with DPRK-linked hackers alone stealing $2 billion. Devastating mega-hacks drive that total, most notably the February Bybit exploit, the largest digital heist in crypto history, at nearly $1.5 billion. Although North Korean hackers have long been a fixture of the threat landscape, the past year has been their most destructive yet, both in value stolen and in the sophistication of their intrusion and laundering tactics.

Perhaps most significantly, 2025 saw unprecedented volumes associated with nation-states' on-chain behavior. While Russia introduced legislation in 2024 to facilitate sanctions evasion via crypto, these efforts came to fruition in February 2025, when the country launched its ruble-backed A7A5 token, transacting over $93.3 billion in less than one year.
Meanwhile, over the past several years Iran's proxy networks have continued to facilitate money laundering, illicit oil sales, and procurement of arms and commodities on-chain to the tune of $2+ billion through confirmed wallets identified in sanctions designations. Iran-aligned terrorist organizations, including Lebanese Hezbollah, Hamas, and the Houthis, are using cryptocurrency at scales never before observed, in spite of various military setbacks.

Chinese money laundering networks dominate the landscape

2025 has seen the emergence of Chinese money laundering networks (CMLNs) as a dominant force in the illicit on-chain ecosystem. These sophisticated operations have dramatically expanded the trend of crypto crime's diversification and professionalization, offering a wide variety of specialized services including laundering-as-a-service and other criminal infrastructure. Building on the framework established by operations like Huione Guarantee, these networks have created full-service criminal enterprises that support everything from fraud and scams to North Korean hack proceeds, sanctions evasion, and terrorist financing.

Full-stack illicit infrastructure providers facilitate malicious cyber activity

While nation-state use of crypto is rising, more "traditional" cybercrime remains very much alive: ransomware operators, CSAM platforms, malware distributors, scammers, and illicit marketplaces still depend on a dense layer of enablers to stay effective. Illicit actors and nation-states alike are increasingly reliant on infrastructure providers that offer a full stack of services and are themselves visible on-chain, including domain registrars, bulletproof hosting services, and other technical infrastructure that can be leveraged for malicious cyber activity.

These infrastructure providers have evolved from niche hosting resellers into integrated infrastructure platforms designed to withstand takedowns, abuse complaints, and sanctions enforcement. As these offerings continue to scale, they are likely to play a key role in supporting financially motivated criminals and state-aligned actors alike to amplify the reach of malicious cyber activity.

The rising intersection of crypto and violent crime

Many people still picture crypto crime as something purely virtual — faceless bad actors behind keyboards rather than threats that manifest in the physical world. In reality, we're seeing growing connections between on-chain activity and violent crime. Human trafficking operations have increasingly leveraged cryptocurrency, while there has also been a particularly disturbing rise in physical coercion attacks, in which criminals use violence to force victims to transfer assets, often timing these assaults to coincide with cryptocurrency price peaks.

As we move forward, cooperation among law enforcement, regulatory bodies, and crypto businesses will be crucial in combating these evolving and converging threats. While the overall percentage of illicit activity remains small relative to legitimate crypto usage, the stakes have never been higher for maintaining the integrity and security of the cryptocurrency ecosystem.

How big was crypto crime in 2025?

$154B

This represents a 162% increase year-over-year (YoY), primarily driven by a **dramatic 694% increase** in the value received by sanctioned entities.

✓ 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 off-chain information.
- Funds associated with crypto platforms accused of fraud (e.g. FTX), 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.

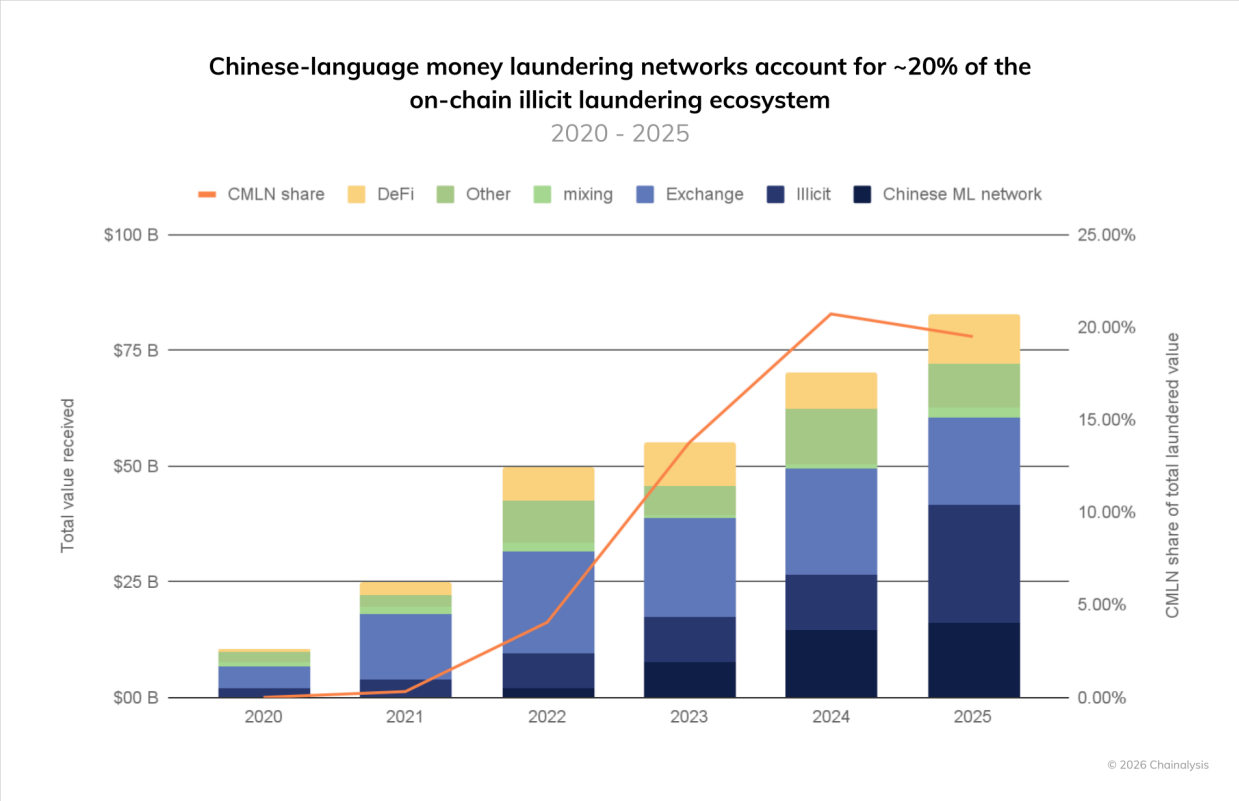
Chinese Language Money Laundering Networks Emerge as Major Facilitators of the Illicit Crypto Economy, Now Driving 20% of Laundering Activity

The on-chain money laundering ecosystem — a portion of the overall illicit crypto ecosystem that reflects the laundering of funds rather than the underlying inflows associated with illicit activity — has grown dramatically in recent years, increasing from $10 billion in 2020 to over $82 billion in 2025.[3] This substantial topline growth reflects the growing accessibility and liquidity of cryptocurrencies, as well as a fundamental shift in how this laundering activity occurs and by whom.

As shown in the chart below, Chinese-language money laundering networks (CMLNs) have increased their share of known illicit laundering activity to approximately 20% in 2025. This regional connection is further evidenced by the off-ramping patterns we observe. To take one example, as we highlighted in the scams chapter of this report, CMLNs have grown to now consistently launder over 10% of funds stolen in pig butchering scams, coinciding with a steady decline in the use of centralized exchanges, potentially because exchanges can freeze funds.

Compared to other laundering endpoints, since 2020, inflows to identified CMLNs grew 7,325 times faster than those to centralized exchanges, 1,810 times faster than those to decentralized finance (DeFi), and 2,190 times faster than intra-illicit on-chain flows. While CMLNs are by no means the only facilitator of on-chain laundering, Chinese-language Telegram-based services now account for a disproportionate share of the attributed global on-chain money laundering landscape. In doing so, they process funds from a wide range of on- and off-chain criminal activity.

[3] This is a lower bound estimate based on CMLN activities; it only reflects services attributed by Chainalysis and does not include Guarantee Services.

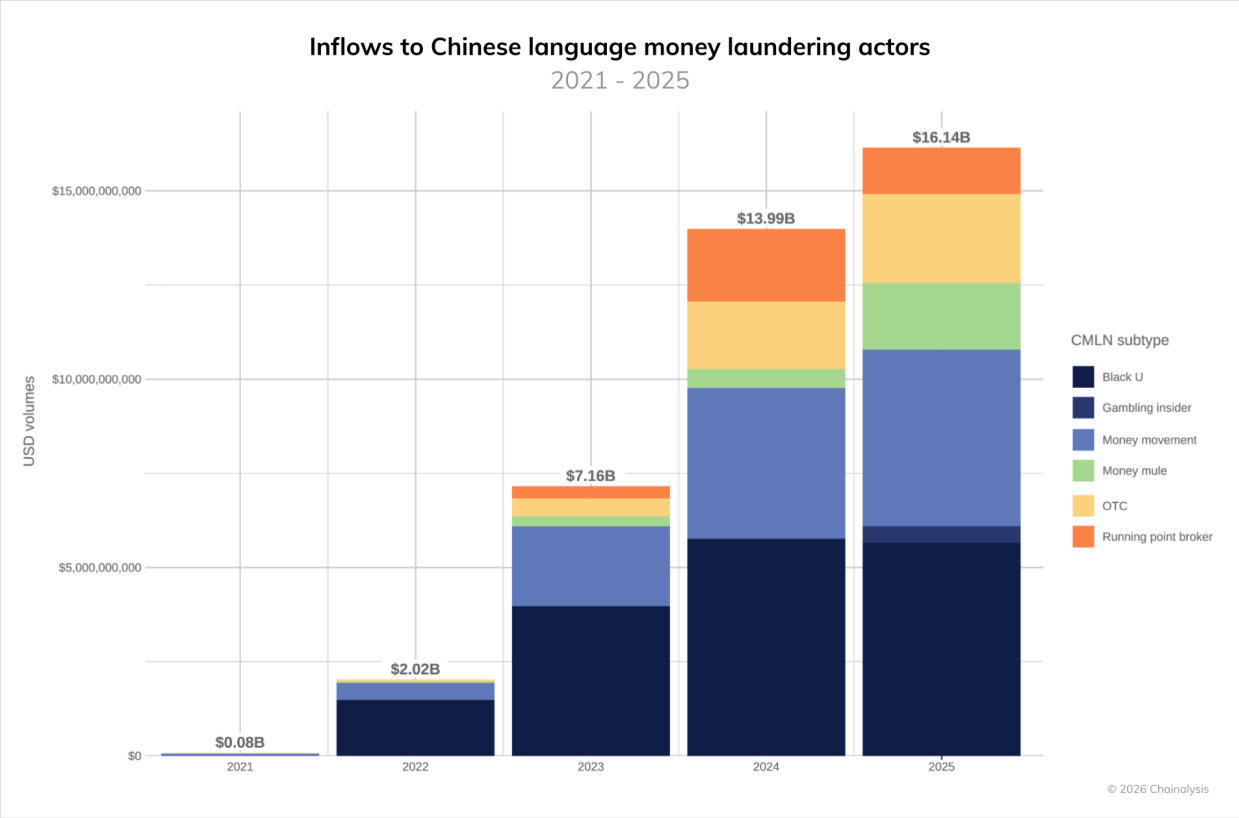


Recent enforcement actions against money laundering facilitation networks, including sanctions designations and advisories, have shined a light on the national security threat impacting victims worldwide. These actions include the designation of the Prince Group by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and the Office of Financial Sanctions Implementation (OFSI) by HM Treasury in the UK, the Financial Crimes Enforcement Network (FinCEN)'s Final Rule designating Huione Group as a primary money laundering concern, and FinCEN's advisory on Chinese money laundering networks.

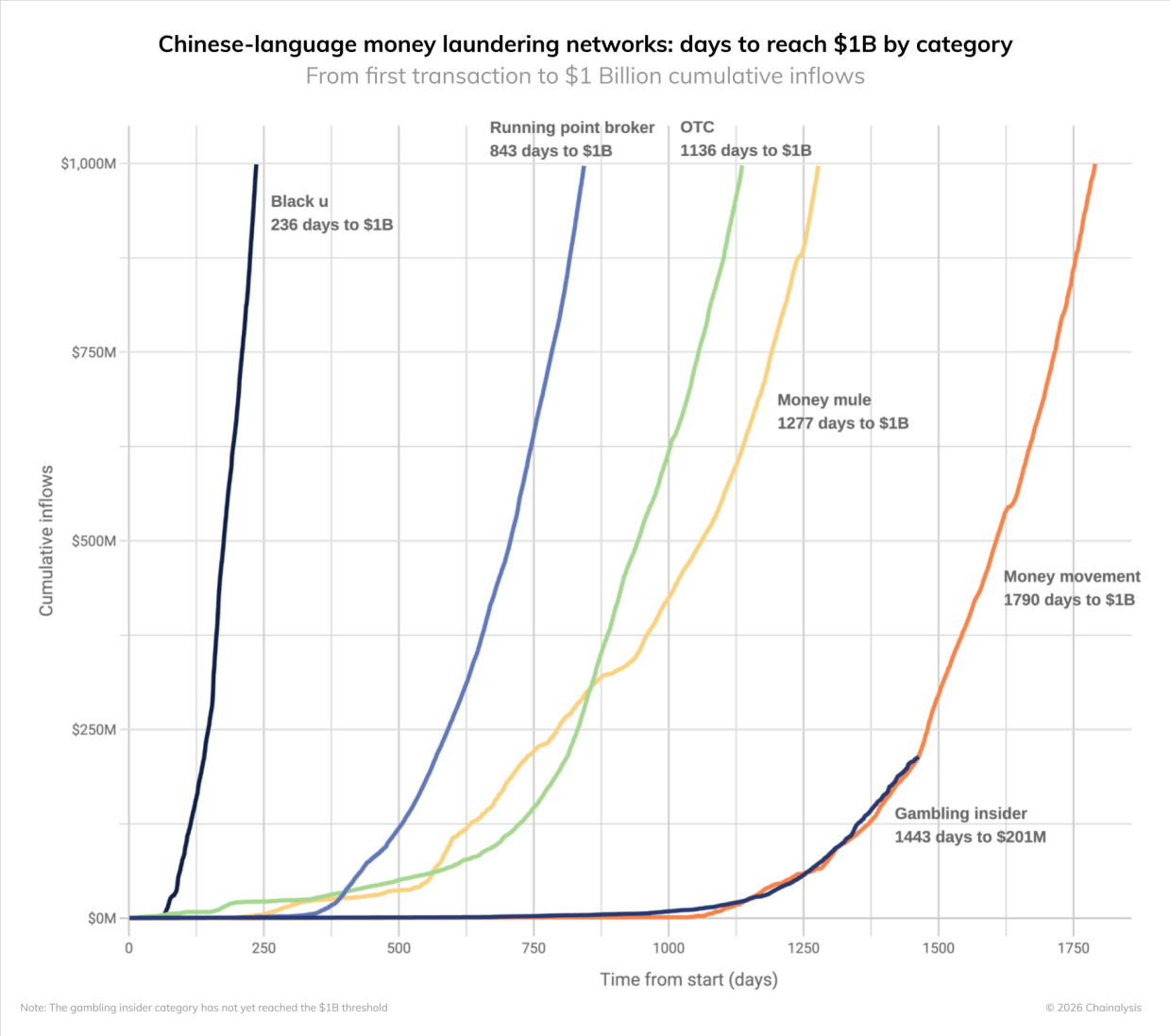
While these major facilitators have rightfully been attracting more attention in recent months, this chapter for the first time takes a deeper look at how these extensive underground laundering networks use cryptocurrency and analyzes the scale of these ecosystems. These money laundering networks operate openly across various platforms and demonstrate complex, multi-layered operations characterized by industrial-scale processing capacity, operational resilience, and technical sophistication.

The $16.1 billion scope and scale of CMLNs

We have identified six discrete service types that make up the CMLN ecosystem, which we will examine in the sections ahead. Together, these services processed $16.1 billion in inflows in 2025. The number of active entities that comprise these networks has risen from a small handful only a few years ago to over 1,799 active on-chain wallets in 2025.



The speed to scale of these operations is equally concerning. The time it takes for each service type to process $1 billion since the first known address of its category receives funds reveals both a remarkably rapid time-to-scale and striking differences between service types. Black U services reached this milestone in just 236 days, while running point brokers required 843 days and OTC services 1,136 days. Money mules (1,277 days) and money movement services (1,790 days) operate more slowly, while gambling insider services have yet to reach the billion-dollar threshold. Overall, the CMLN ecosystem in 2025 is processing almost $44 million per day.



These networks' rapid time-to-scale suggests they are tightly interwoven with off-chain criminal networks, as growth of this magnitude would be hard to achieve without significant capital pools put into play. It also reveals a sophisticated on-chain and off-chain operational infrastructure. At the center of this ecosystem sit guarantee platforms — centralized marketplaces that have become the anchor for CMLN operations.

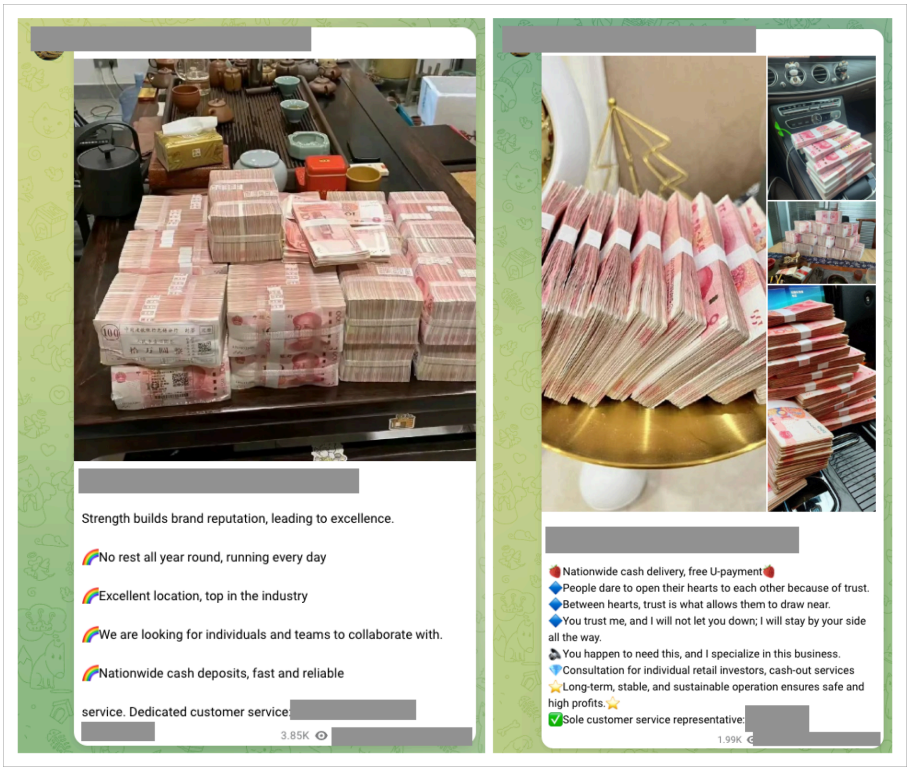
As Tom Keatinge, Director at Centre for Finance & Security (CFS) at RUSI, told us, "Very rapidly, these networks have developed into multi-billion dollar cross-border operations offering efficient, value-for-money laundering services that suit the needs of transnational organized crime groups across Europe and North America. As to why these networks have developed so fast, the short answer is that they are an unforeseen consequence of the imposition of capital controls in China. Wealthy individuals seeking to move money out of China and evade these controls provide the impetus and liquidity pool needed to service organized crime groups based in the West. The professional enablers of this capital flight provide the services necessary to match these two independent yet mutually beneficial needs."

Similarly, Chris Urben, Managing Director at Nardello & Co explained to us that "the biggest change in Chinese money laundering networks in recent years is a rapid transition to crypto from reliance on informal value transfer systems like the traditional Black Market Peso or Fei Qian approaches to underground banking. Crypto offers an efficient way to discreetly move funds across borders without having to rely on the complex manual network of informal ledgers in various countries that used to be the norm."

Guarantee platforms: the anchor of the CMLN ecosystem

Guarantee services function primarily as marketing venues and escrow infrastructure for CMLNs. While they provide trust mechanisms for vendors, they don't control the underlying laundering activity and aren't included in our total metric. Huione and Xinbi have dominated the market for the past few years, and many other guarantee services continue to operate freely.

While Huione's guarantee operations were disrupted after Telegram removed some of their accounts, vendors using Huione have continued to use or advertise on alternative platforms, their operations uninterrupted. While these hubs continue to connect vendors and buyers, most vendors promote advertisements across platforms and are not reliant on any specific service. As with legitimate e-commerce platforms, service ratings and reviews create accountability within the illicit ecosystem, and vendors often cultivate their market reputation through public attestations of their reliability and service quality, as shown in the screenshot below.



Screenshot showing vendor's service quality claims, with conspicuous display of cash likely as proof of liquidity and reserves (machine translated from original Mandarin text).

CMLNs advertising on these guarantee services offer a range of money laundering techniques with the primary goal of integrating illicit funds into the legitimate financial system. Some leverage vast networks of money mules for access to mainstream crypto exchange laundering, while others operate their own on-chain laundering infrastructure. These laundering methodologies represent distinct approaches to achieving the same goal: cleaning dirty money.

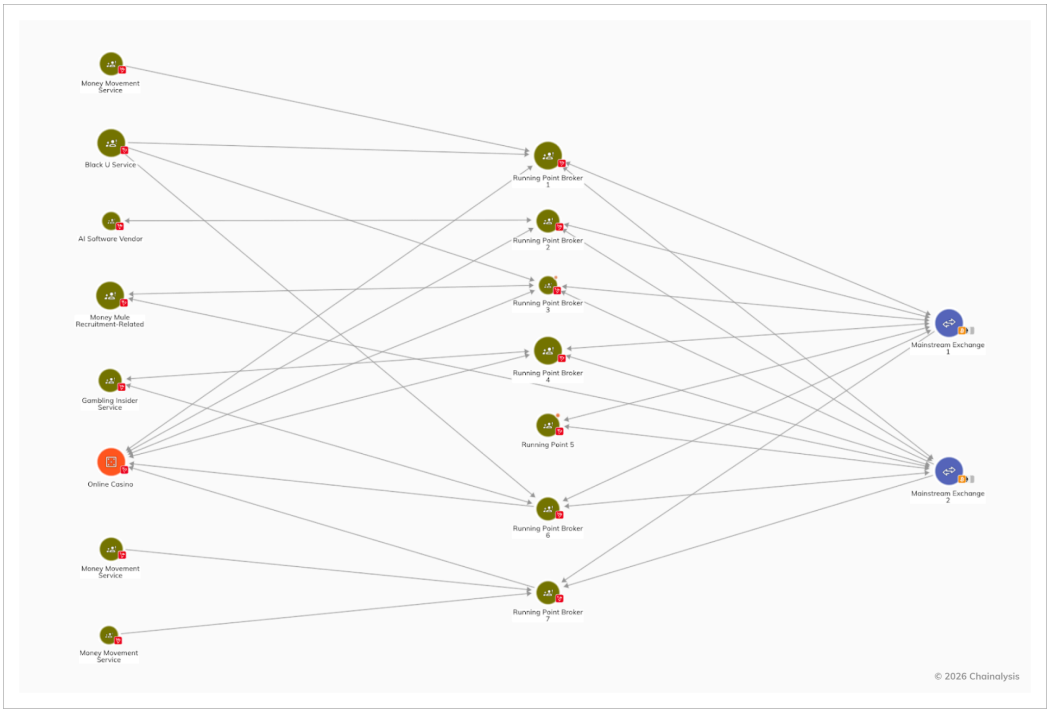
The six CMLN typologies

CMLNs offer a wide variety of laundering-as-a-service businesses. Our analysis of Chinese-language vendor posts reveals that these services deploy six primary money movement techniques: running point brokers, money mules, OTCs, Black U services, gambling platforms, and money movement services that offer mixing and swapping of crypto assets. These operations involve thousands of vendors processing tens of billions of dollars. Understanding how these entities operate and form a comprehensive laundering network provides crucial insights into potential disruption opportunities. Below, we examine these service categories in detail.

1. Running point brokers: the initial entry channel

In the money laundering process, "running points" (跑分) serve as the critical entry channel for illicit fund transfers. Individuals are recruited, typically through vendor advertisements, to rent out their financial identities, providing bank accounts, digital wallets, or deposit addresses at mainstream exchanges to receive and forward fraudulent proceeds.

Advertisements explicitly warn participants that they bear all legal consequences and economic losses when authorities intervene, leaving no doubt that the activity is illicit.



Originally concentrated in online gambling operations, running points' services have expanded to facilitate the full spectrum of illicit activities that leverage crypto for laundering, including romance scams, exchange heists, and Telegram-based human trafficking operations. This broad adoption reflects their fundamental utility: they provide the crucial bridge between legitimate financial systems and the criminal underground.

As illustrated in the Chainalysis Reactor graph below, running point brokers function as routing mechanisms for various illicit sources, ultimately sending funds to accounts — likely under a mule's name — at mainstream exchanges. Notable destinations include other laundering services, mainstream exchanges to convert to fiat, and platforms associated with the Huione Group ecosystem.

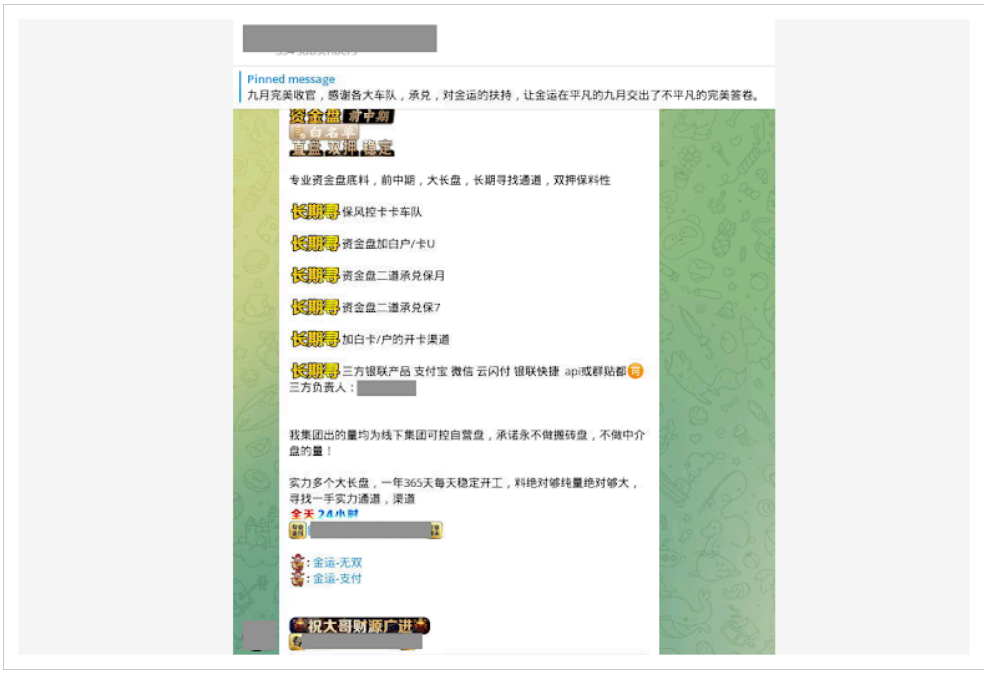
2. Money mule motorcades: the laundering intermediaries

While "running points" serve as access points to exchanges, money mules, or "motorcades," (车队) orchestrate the complex layering phase of money laundering. These specialized operators form networks of accounts and wallets to obscure fund origins through multiple transactions.

Money mule operations use a number of methods to convert between fiat and crypto, and vice-versa. This includes offline services where dealers meet customers in person; ATM cash withdrawals converted to crypto; digital wallet transfers through third-party payment platforms, and card-based schemes using credit cards and gift cards in exchange for crypto. Vendors openly advertise accepted financial institutions, crypto exchanges, and payment methods, although the actual arrangements with card merchants and intermediaries occur privately outside public Telegram channels.

Although we are unable to ascertain the nationality of the money mule motorcades based on Telegram posts alone, these posts are almost exclusively in Mandarin and often allude to bank accounts and locations in Mainland China, suggesting these money laundering vendors are likely primarily serving Chinese-speaking clientele. Recent research from the Royal United Service Institute (RUSI) has pointed to the growing involvement of Chinese organized crime. These networks, as well as legitimate crypto use, have continued to thrive in spite of China's sweeping crypto ban. Chinese authorities have focused on selective crackdowns and AML enforcement – tacitly allowing or ignoring some forms of crypto activity while aggressively targeting anything that threatens the country's capital controls or financial stability.

Beyond domestic operations, these networks readily offer specialized services for cross-border funds transfers through global payment methods and foreign currencies. Vendor operations boast their significant geographical reach. In Telegram posts, certain vendors claim to be able to coordinate "fleets" (likely referring to collections of motorcades and money mules) across Africa, suggesting the global reach of CMLN operations is growing well beyond China and East Asia. "CMLOs rightly view crypto as having less Know Your Customer compliance than traditional banks and crypto transactions, which decrease the risk and increase the speed of the laundering process," notes Urben. "Finally, crypto makes it far easier to physically move large holdings across borders: you can carry billions of BTC in a cold wallet stored on a hard drive stuffed into your pocket."



Typical advertisement by a motorcade recruiter, which mentions a “ponzi scheme” and the types of cards and entities they work with, such as UnionPay, AliPay, WeChat, and API.

Vendor Telegram post advertising money movement in five African countries, suggesting cross-border funds movement has reached well beyond Asia (machine translation on right).

.

A recurring theme across advertisements offering money movement services is the pronounced emphasis on urgency, discretion, and speed. Vendors often stress the need to transfer funds rapidly to prevent fund freezes, while offering cursory guidance to their customers on navigating complications arising from funds and accounts that have already been restricted by financial institutions and crypto exchanges.

Within guarantee platforms, the movement of funds orchestrated by running point brokers and money mules constitute a large portion of the advertised offerings. The striking similarities in how advertisements are worded and structured suggest that these operators likely function either within larger umbrella organizations or maintain strategic collaborative relationships with one another. Collectively, these money movement services form the backbone of the money laundering infrastructure within the underground banking ecosystem.

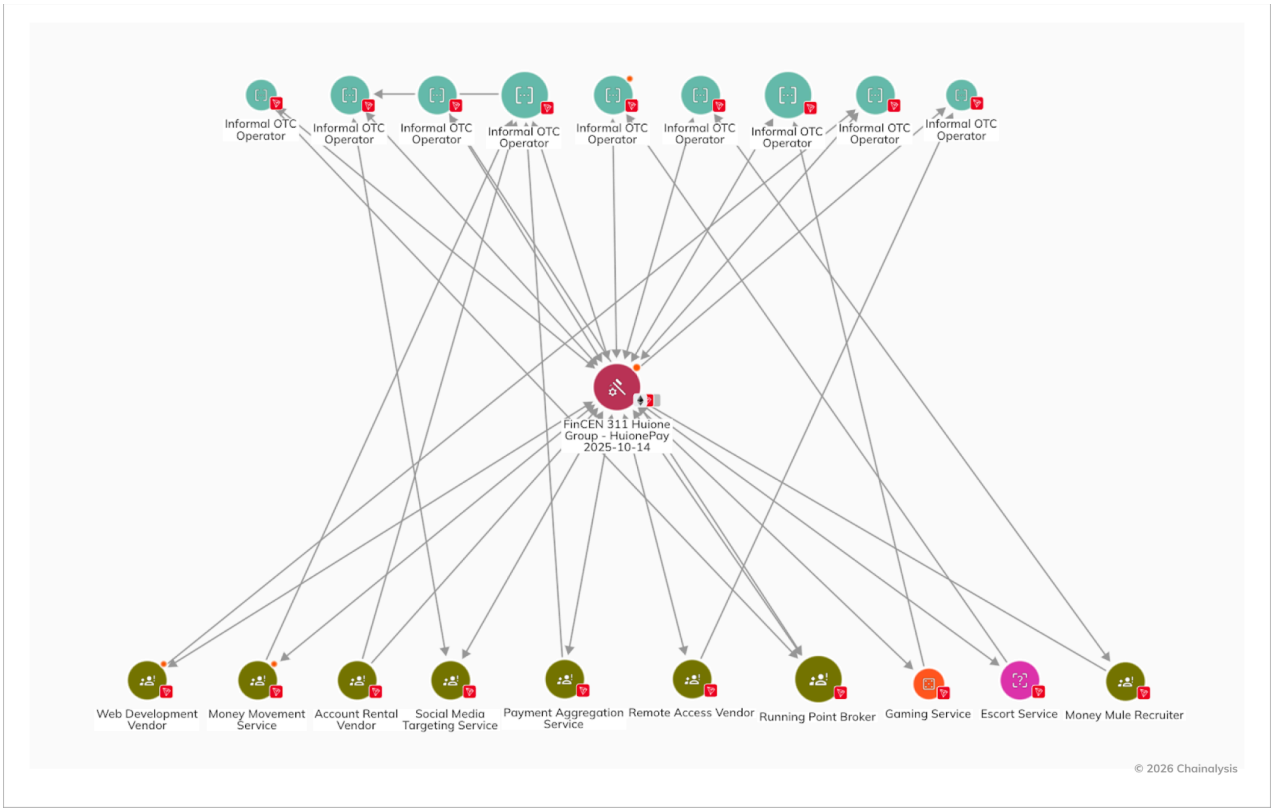
The United Nations Office on Drugs and Crime (UNODC) provides the most apt description of this relationship: motorcades function as extensions of running point syndicates, offering sophisticated layering schemes by routing illicit funds through multiple bank accounts in exchange for a cut of the total transferred funds. The UNODC's 2024 report on casinos, money laundering, and transnational organized crime in East and Southeast Asia also highlights the use of third-party and fourth-party payment providers. These networks often indicate high levels of connectivity, suggesting layers of payment services may be operating as fronts by the same groups to facilitate laundering.

3. Informal over-the-counter (OTC) and peer-to-peer (P2P) services: Circumventing controls

Informal OTC trade desks offer another critical laundering pathway. Unlike their legitimate counterparts, these services operate without regulatory oversight or jurisdictional affiliation and deliberately circumvent capital controls required in highly controlled markets, such as China. By processing fund transfers without Know Your Customer (KYC) verification, they present an attractive option for users seeking to move assets, especially those of suspicious origins.

Many OTC vendors explicitly advertise "clean funds" or "White U." Exchange rates displayed transparently in vendor posts often exceed market rates, reflecting the premium charged for regulatory evasion. These services process both domestic and cross-border transfers, expanding the geographic reach of illicit fund flows.

However, on-chain analysis contradicts "clean fund" claims. These supposedly legitimate OTC services maintain extensive connections with Huione and other guarantee platforms, revealing their deep integration within the broader CMLN ecosystem. The same vendors advertising "White U" regularly interact with confirmed money laundering services, demonstrating that informal OTC desks can function as critical bridges for illicit cryptocurrency.



4. Black U services: Discounted rates for tainted assets

Operating primarily outside guarantee platforms, "Black U" services occupy a unique niche in the CMLN ecosystem, and are the inverse of the informal “White U” OTCs. These vendors specialize in cryptocurrency derived from illicit sources, such as hacking campaigns, exploit attacks, scams, and wallet theft — and openly state this in their advertisements. Their business model involves selling illicit cryptocurrency at a discounted rate.

Buyers purchase illicitly sourced funds, sometimes 10-20% lower than standard rates in exchange for accepting assets with criminal provenance. This compensates buyers for assuming potential legal exposure and the risk of fund seizure.

The operational structure of Black U services reveals sophisticated coordination. Across different vendors, the front-end websites of Black U services often display nearly identical layouts with only superficial variations in domain names and branding. Telegram channels exhibit the same pattern. These infrastructural commonalities point to two possibilities: either these seemingly independent operations function as compartmentalized units within a single organization, or they represent a coordinated network maintaining operational consistency.

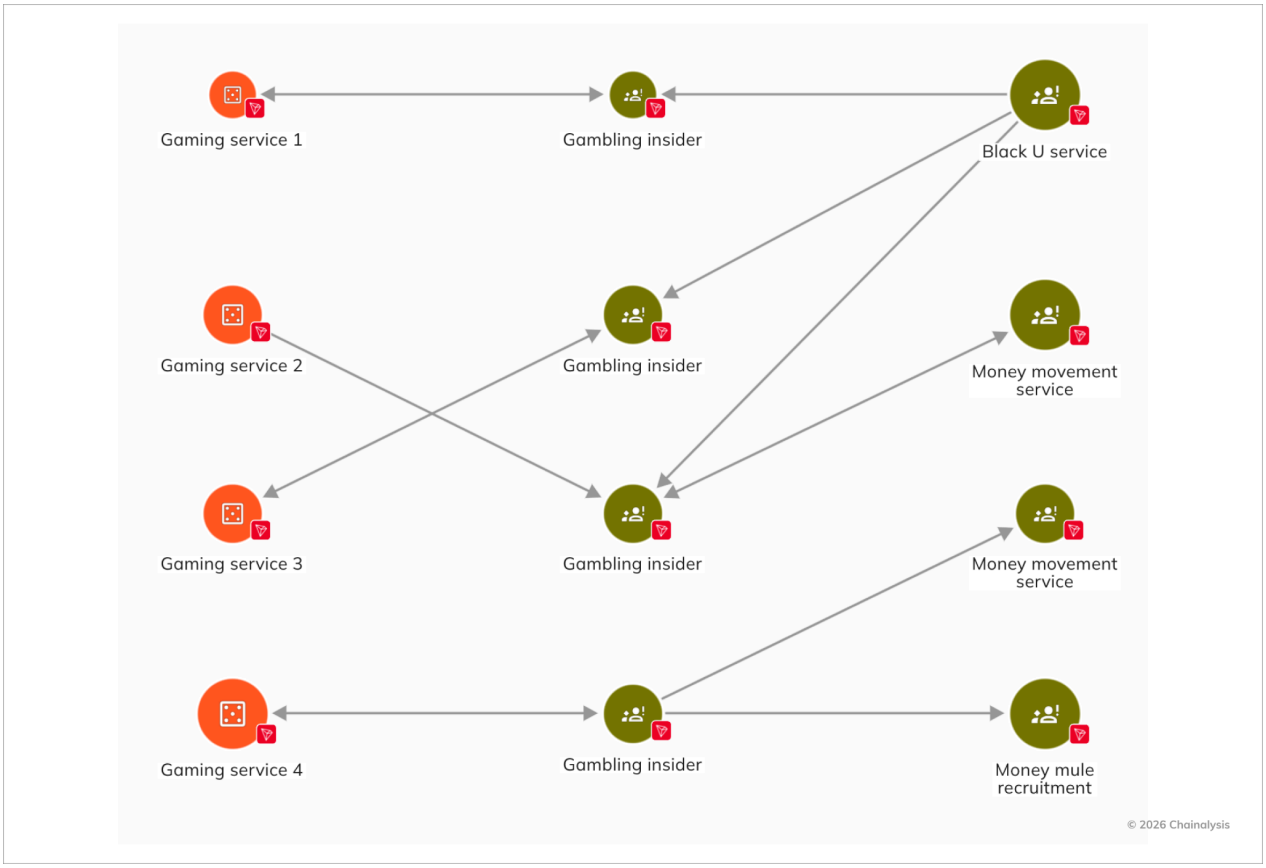
5. Gambling services: Traditional laundering goes digital

While not inherently illicit in many jurisdictions, gambling services have been used for both traditional and crypto-based laundering due to their high cash volumes, frequent transactions, and built-in mechanisms for converting funds. Both casinos and online betting platforms offer users an effective way to place, layer, and integrate proceeds into the legitimate financial system, especially because they provide plausible explanations for sudden wealth.

Many of these gambling services accept crypto and do not require KYC details. Third-party payment providers facilitate account top-ups using both fiat and crypto, with some processors handling recharges across multiple gambling sites, allowing for cross-platform fund movement. Additionally, some Telegram vendors offer insider tips suggesting predicted or rigged outcomes, with advertisements guaranteeing compensation if customers' "winning numbers" are not selected. This further suggests that some gambling services are not just a conduit for laundering, but taking an active role in facilitating fixed outcomes.

Post stipulating the service operations of a gambling service vendor offering rigged outcomes for lottery-type betting. It includes compensation details if the winning numbers are not picked.

The Reactor graph below illustrates how gambling services can be used by insiders, where the insider extracts the fixed outcome proceeds from the gambling platform, then continues the laundering process by sending onward through additional money laundering services, such as Black U services and money mules. On-chain activity indicates the gambling insider operators send funds back into the gambling platforms as well.



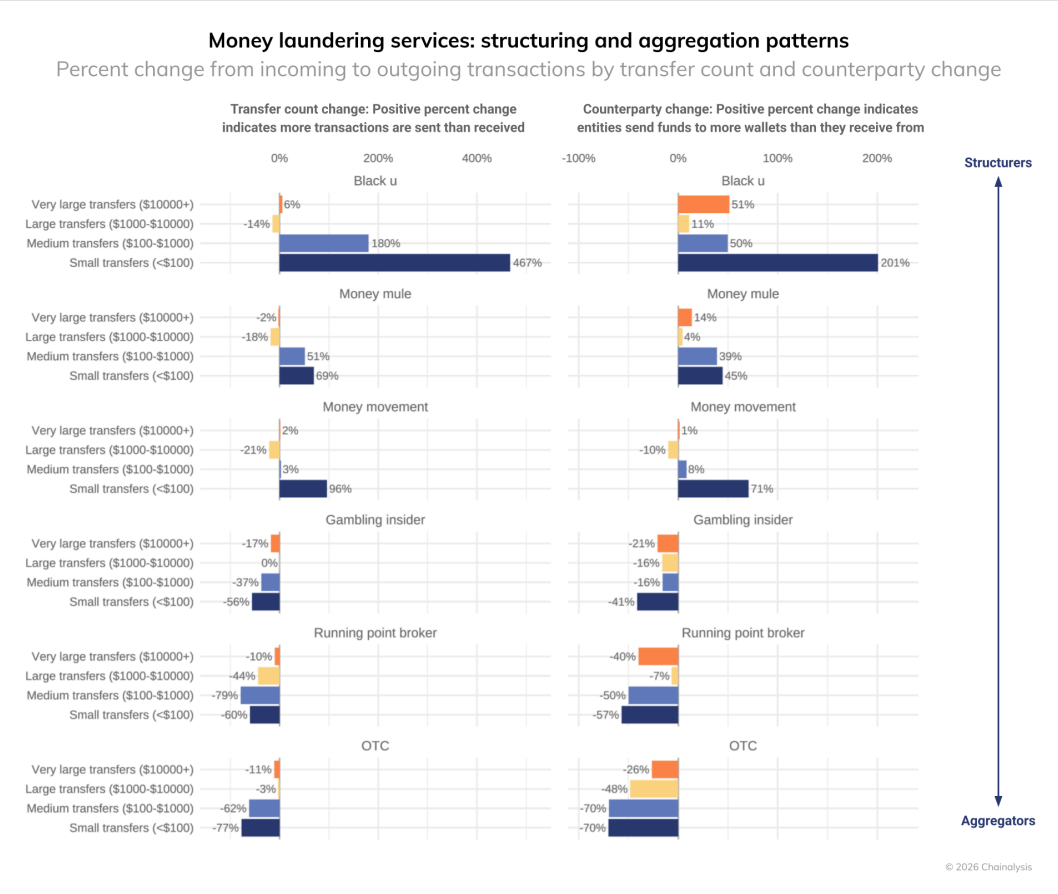
6. Money movement services: mixing and swapping-as-a-service

Fund mixing to obfuscate transaction origins is well-established in sophisticated cyber heists. Professional mixing services, including Tornado Cash and Blender.io, earned international notoriety when they were sanctioned by the US government for their role in laundering stolen funds, with Tornado Cash later being de-listed by OFAC.

Within Southeast Asia's underground banking ecosystem, specialized vendors across guarantee service platforms offer swapping-as-a-service to enable clients to convert their crypto into multiple assets. These swap services have found regional footing, especially among illicit actors active in Southeast Asia, China, and even North Korea, providing a laundering mechanism for those seeking to keep funds on-chain.

On-chain data reveals CMLN financial flows resemble traditional money laundering phases

Analysis of transaction flows through CMLN services exposes industrial-scale deployment of traditional money laundering methodologies. The following chart tracks how different services fragment and consolidate illicit funds, revealing clear patterns of "structuring" (smurfing) and "aggregation" as funds move through the laundering cycle.



This quantitative framework can help identify services and their roles within the broader money laundering ecosystem, potentially even when an entity's true operating mechanism is not yet known.

Black U services epitomize aggressive structuring behavior, with small (<$100) and medium ($100-$1000) transactions increasing by 467% and 180% respectively from inflow to outflow. These services also consistently fragment funds across more wallets, with very large transfers (>$10K) reaching 51% more destination wallets than source wallets. Money mules and money movement services, to a lesser but still significant degree, act likewise. In these cases, the shift toward smaller transactions and more counterparties represents textbook smurfing: breaking down large criminal proceeds to evade detection thresholds.

Gambling insiders, running point brokers, and OTC services operate as the ecosystem's primary aggregators. For these services, incoming transfers across almost all denominations exceed outgoing transactions, suggesting these services pool funds from multiple points and send them out in bulk batches to fewer counterparty wallets on-chain. For the OTC services in particular, this consolidation pattern reflects their role in the integration phase — collecting numerous small deposits into wholesale amounts suitable for reintroduction into legitimate financial systems.

CMLNs prioritize VIP customers; most illicit funds are moved in minutes

The speed at which funds move through the different laundering services also reveal distinct patterns. In the charts below, we see that regardless of the laundering typology, high value transfers are prioritized. However, the services that build automated laundering mechanisms tend to become more efficient across any transfer value amount with time. Those that rely on manual mechanisms still tend to prioritize higher value transfers, but are less efficient at moving smaller transfers.

Black U services show the highest efficiency when it comes to processing funds, with very large transactions cleared on average in 1.6 mins in Q4 2025. The operational imperative to move illicit funds rapidly is likely a major contributing factor shaping the technical infrastructure of Black U services. In several of these services, self-service swapping mechanisms are also available. Customers simply provide

their desired exchange amount and destination address, and the system executes the swap automatically. This automation serves a dual purpose: accelerating the laundering process while minimizing operational overhead and reducing the digital footprint that manual processing creates.

Similarly, gambling operations use integrated payment solutions to process substantial daily transaction volumes. These automated systems enable these platforms to handle large-scale financial flows efficiently, with funds deposited and cleared rapidly.

In contrast, money mules and running points exhibit far less consistency in transaction clearing patterns. These networks remain predominantly manual, requiring recruited individuals to actively process transactions in real-time using their personal bank accounts or digital wallets. This human element introduces variability into the laundering process, creating timing variations that differ from the consistent processing signatures of automated services.

Screenshot showing a post from a money movement vendor. Note the fleet operator's conditions: same-day or last minute requests are subject to availability of money mules or personnel. For long-distance trips, the operator also stipulates a surcharge of RMB 30,000 (roughly equivalent to USD 4,220).

Combating crypto-integrated laundering networks through public-private collaboration

Chinese-language guarantee platforms, money movement services, and associated financial crime networks reveal a complex and resilient ecosystem that continues to adapt despite enforcement efforts. As with other genres of illicit on-chain activity, actions against guarantee services can be disruptive, but the core networks persist and migrate to alternative channels when challenged.

The scale and integration of these operations present significant challenges for financial crime compliance, intelligence, and law enforcement efforts. Effective disruption requires targeting the illicit operators and vendors themselves, in addition to their advertising venues. These networks form the critical infrastructure enabling the conversion of illicit proceeds from fraud, scams, and other criminal activities into seemingly legitimate assets at scale.

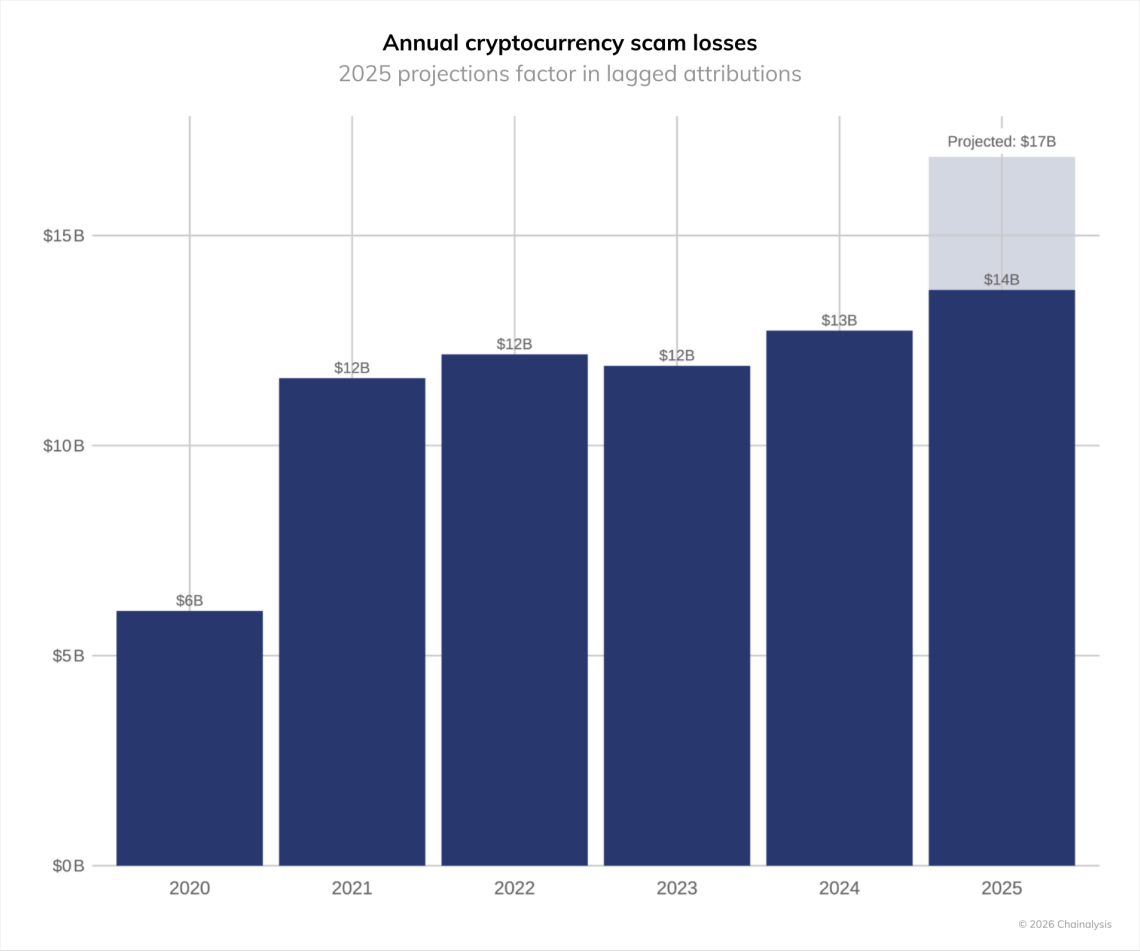
More importantly, while CMLNs play an outsized role in crypto-enabled money laundering, they are not the only laundering networks to have adapted technologically. In December 2024, the United Kingdom's National Crime Agency (NCA) disrupted a multi-billion dollar Russian-language money laundering network which provided services to a wide range of illicit actors, including Russian and international elites, cybercriminals, and drug gangs. As Keatinge noted, "There is a chasm in most countries between the capabilities of criminals and law enforcement when it comes to crypto use. A combination of nationally-based laws, barriers created by borders, poor information sharing, and limited crypto tracing and asset recovery capabilities mean that crypto offers criminals a low risk/high reward method of benefiting from their criminality. Whilst blockchain tracing companies have provided welcome assistance in some cases, this capacity building is just the tip of the iceberg. A systemic global effort to upskill the crypto capabilities of law enforcement around the world and create better information sharing mechanisms is urgently needed."

Addressing the challenge of crypto-integrated laundering networks demands coordinated public-private partnership and a paradigm shift from reactive enforcement against individual platforms toward proactive disruption of underlying networks. Urben emphasized that "the most effective investigative strategy is to match your investigative tools against the operational approach of the CMLOs. To detect these money laundering networks, you need to rely on open source and human source intelligence combined with blockchain analysis. Only when these tools work together, and develop leads that feed into each other, will you be able to match the players to the currency movements and map the networks."

By combining law enforcement's legal authorities with the private sector's technical capabilities and blockchain analytics expertise, the industry can more effectively identify and dismantle these services operating across multiple platforms, jurisdictions, and communication channels. On-chain transparency provides unprecedented visibility into these operations — when paired with cross-platform intelligence sharing and coordinated enforcement actions, these tools enable stakeholders to increase the cost and risk of operating large-scale money laundering services. Future intervention strategies must prioritize this collaborative approach to achieve meaningful, lasting disruption of crypto-integrated laundering networks, including CMLN operations.

Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge

In 2025, cryptocurrency scams received at least $14 billion on-chain, a significant increase from the $9.9 billion we first reported in 2024, which reached $12 billion at our recalculation as of this writing – a number that was broadly in line with our projected $12.4B for the year. Based on historical trends, in which our annual estimates grow by an average of 24% between reporting periods, we project that the 2025 figure could exceed $17 billion as we identify more illicit wallet addresses in the coming months.



This year's data show scammers continuing to adapt and innovate, with the average scam payment increasing from $782 in 2024 to $2,764 in 2025, a growth of 253% YoY. Overall scam inflows have also surged, particularly through impersonation tactics that saw a staggering 1400% year-over-year (YoY) growth. While high-yield investment programs (HYIP) and pig butchering remain dominant categories by volume, we're seeing increasing convergence across scam types as fraudsters leverage AI, sophisticated SMS phishing services, and complex money laundering networks to target victims more effectively than ever before.

Traditional scam categorizations are becoming less distinct as fraudsters incorporate multiple tactics into their operations. For example, many pig butchering and investment scams incorporate elements of impersonation, social engineering, and even technical- or wallet-focused scams.

Impersonation scams see explosive growth

Impersonation scams have emerged as a particularly concerning trend, growing more than 1400% compared to 2024, with the average severity (i.e., amount) of payments made to these clusters increasing by over 600%. These scams involve fraudsters posing as legitimate organizations or authority figures to manipulate victims into transferring funds.

Government impersonation: The E-ZPass scam network

Government impersonation has become an effective tactic, with scammers leveraging the inherent trust people place in official communications. One of the most prolific examples was the widespread "E-ZPass" phishing campaign that targeted millions of Americans using the E-ZPass electronic road toll collection system in 2025.

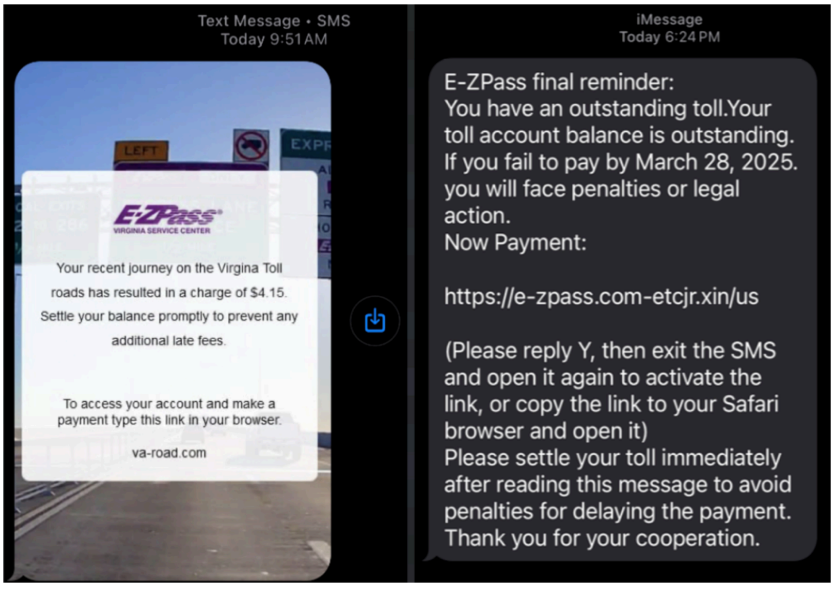
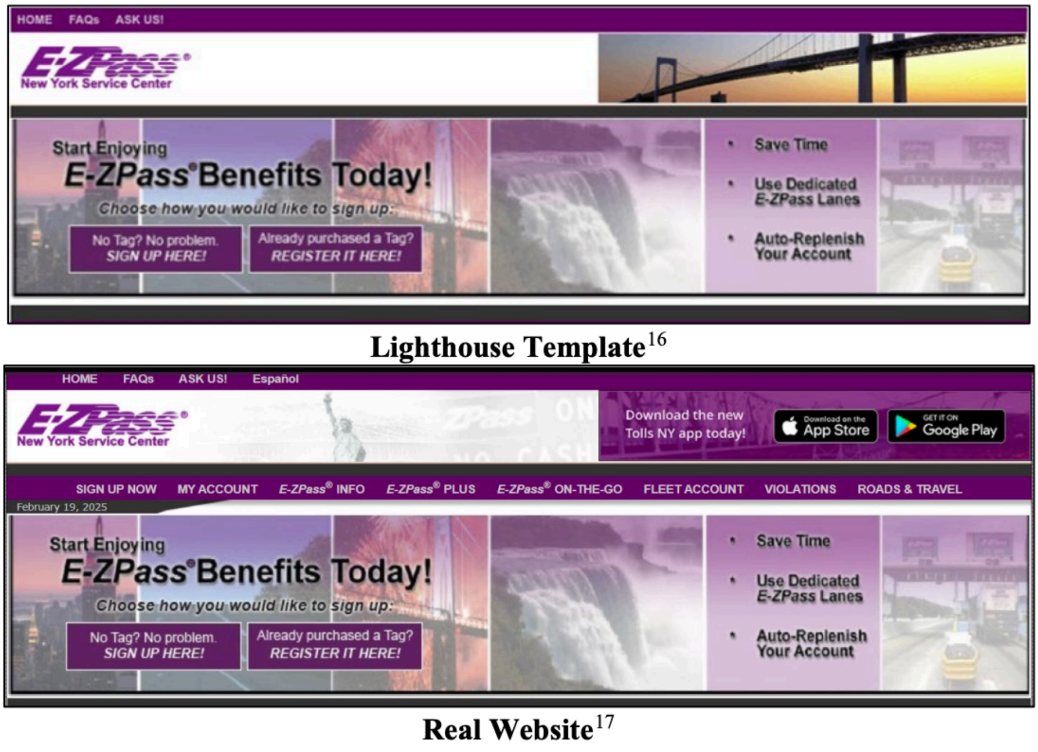


Image of Fake E-ZPass text, Source: Cisco Talos

This operation was attributed to a Chinese-speaking cybercriminal group known as "Darcula" also known as the "Smishing Triad." This China-based cybercrime network used phishing-as-a-service tools to distribute SMS messages impersonating toll collection agencies, particularly targeting E-ZPass users across at least eight states. This group specializes in these tactics and has also impersonated the U.S. Postal Service.

According to Google's lawsuit, filed in November 2025, Smishing Triad leveraged software from "Lighthouse," a Chinese-language vendor that offers cybercriminals "phishing for dummies," with hundreds of templates for fake websites, domain setup tools, and features designed to evade detection.

The group created fraudulent websites mimicking government agencies, including the New York City government official website (nyc.gov) and New York E-ZPass (e-zpassny.com), designed to be indistinguishable from the legitimate websites they impersonated.

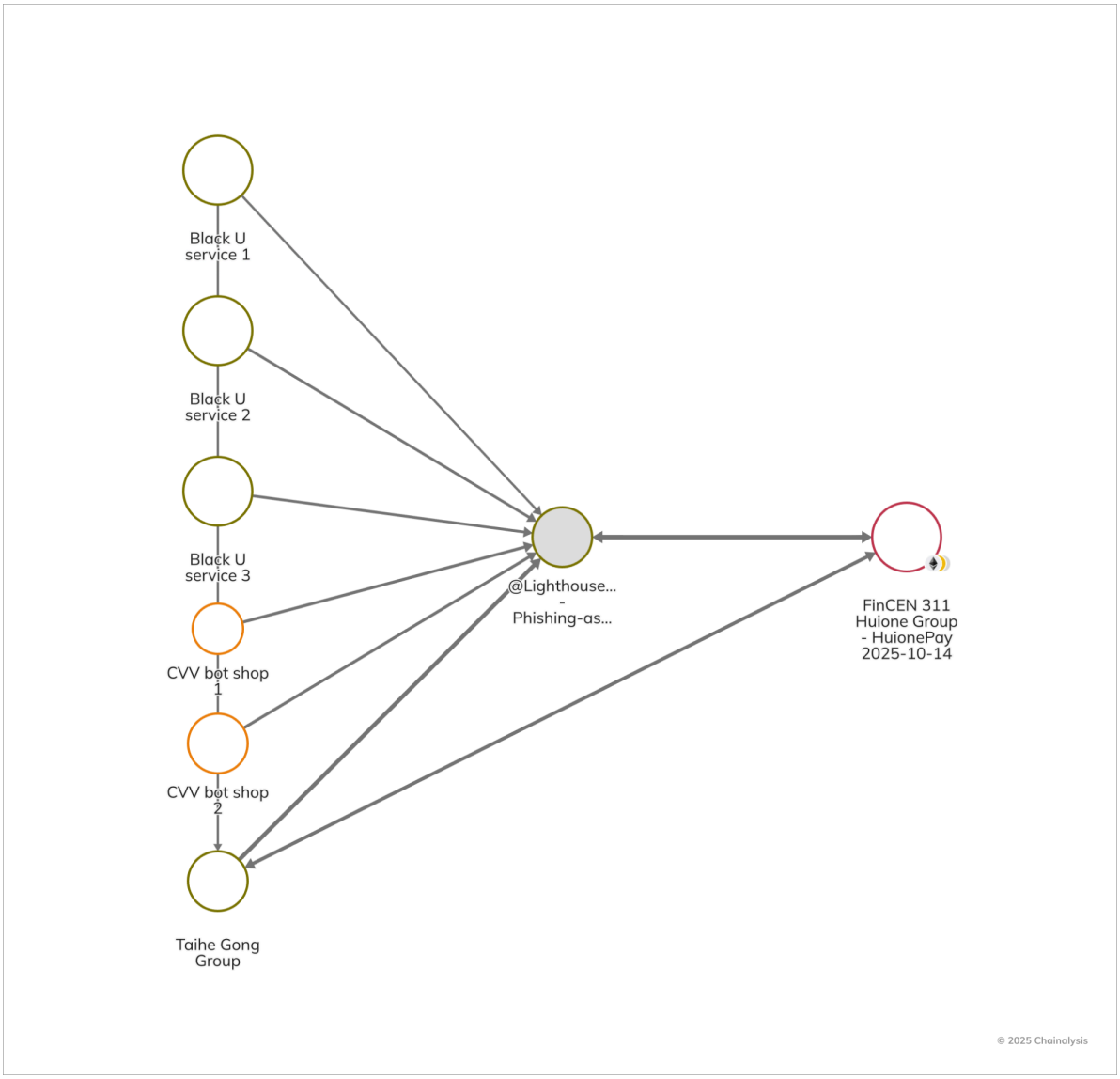


Lighthouse Template[16]

Real Website[17]

Source: Google Phishing Lawsuit Complaint

In addition to illustrating how cybercriminals leverage infrastructure purchased with cryptocurrency to carry out criminal activity, this case shows how the on-chain footprints left by cybercriminals generate actionable disruption opportunities. As depicted in the graph below, various Chinese criminal underground entities, such as the Taihe Gong scamming group, have purchased Lighthouse phishing kits and received payments from several Chinese-language money laundering networks (CMLNs) and fraud shops. Taihe Gong comprises Chinese-speaking operators suspected of engaging in fraudulent cybercriminal activities, including the sale of phishing kits. Its operational structure suggests established distribution channels for malicious tools designed to facilitate illicit activity, such as online scams and credential theft.



Taihe Gong and other Chinese criminal underground entities have purchased Lighthouse phishing kits and received payments from several Chinese-language money laundering networks (CMLNs) and fraud shops. This includes Black U services, which offer facilitation of laundering of stolen/illicitly obtained U.S. denominated stablecoins (i.e., Black U).

The E-ZPass case demonstrates how cheap the scamming infrastructure is, with some phishing kits likely purchased for under $500. But a relatively inexpensive scam at scale can still have a massive impact: the E-ZPass scheme allegedly reached 330,000 texts in a single day as part of a separate toll fee scam campaign, amassing $1 billion over three years and duping over 1 million people in at least 121 countries, according to Google's lawsuit. According to Cisco Talos, the phishing kits had different pricing tiers, including $50 in cryptocurrency for a "full-feature development," $30 for proxy development, and $20 for version updates and support. Lighthouse received over 7,000 deposits and amassed over $1.5 million in cryptocurrency in three years.

Unfortunately, Lighthouse is not the only vendor. Gary Warner, Director of Intelligence at DarkTower, is tracking eight major Chinese-language "Crime-as-a-Service" groups on Telegram, each of which has multiple vendors offering iMessage and RCS phishing services. The goal of these phish, according to Warner, is to load credit cards onto mobile wallets, then deploy to a network of shoppers around the world who facilitate trade-based money laundering by purchasing luxury goods and electronics for resale, often using "remote Tap-to-Pay" services. Everything from phishing design, hosting, and spamming, to shopping, cash-pickup, and goods purchasing is available in these Chinese criminal Telegram groups, some of which have more than 300,000 members. All buying, selling, and advertising are done using stablecoins as the currency of choice. Warner adds that much of the overseas money laundering also aims to convert goods or cash into stablecoins for easy transmission back overseas.

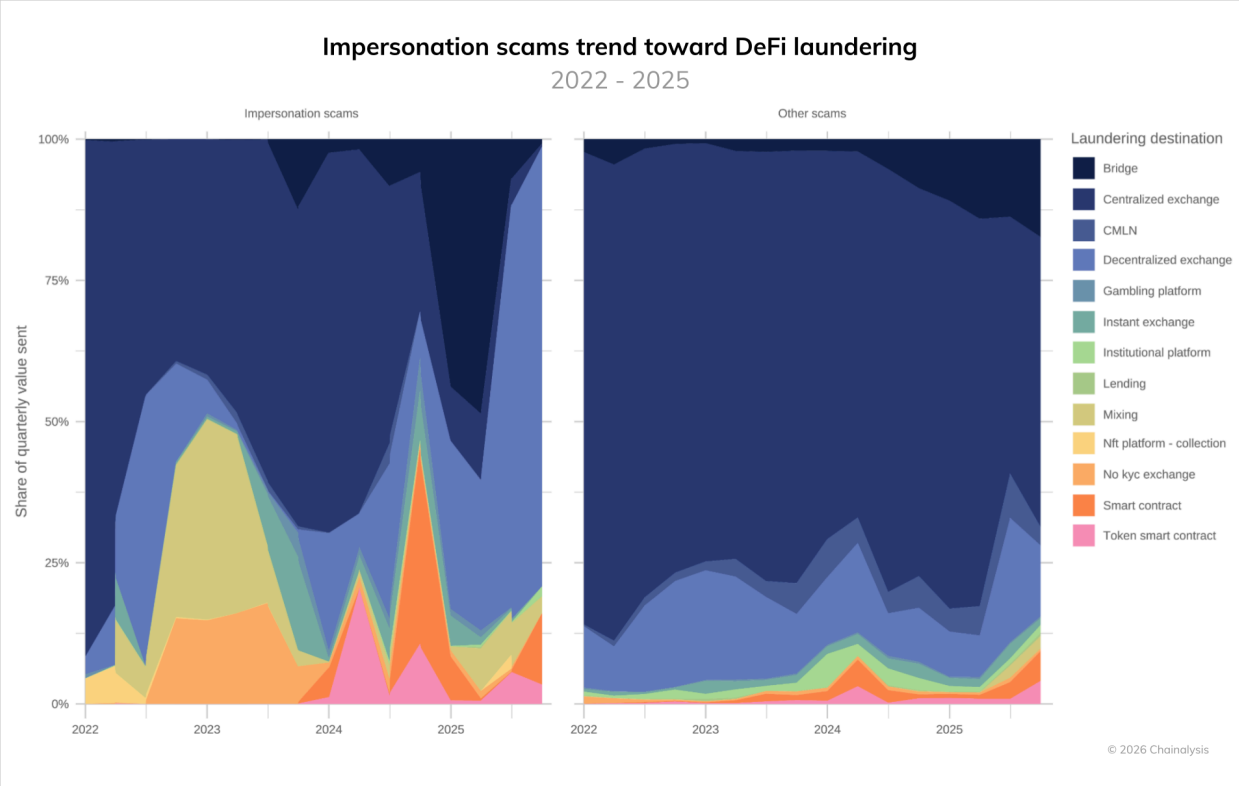
Private sector impersonation: Coinbase impersonation campaign

In December 2025, the Brooklyn District Attorney's office indicted Ronald Spektor, a 23-year-old Brooklyn resident, for orchestrating a sophisticated cryptocurrency scam that defrauded victims of nearly $16 million. Spektor and his conspirators impersonated Coinbase customer service representatives, contacting users – whose information they had stolen in a bribery scheme – with alarming claims about unauthorized access to their accounts and convincing them to transfer their cryptocurrency to "secure" wallets controlled by the scammers. The recent arrest in India of a former Coinbase customer service agent who allegedly accepted $250,000 in bribes as part of this scam underscores how human trust remains among the most exploitable vulnerabilities in security infrastructures, as this insider breach compromised nearly 70,000 customers' data and enabled credible impersonation attacks despite robust technical safeguards.

The scheme specifically targeted cryptocurrency exchange users by exploiting their trust in what appeared to be legitimate customer service communications, demonstrating how impersonation scams have evolved to leverage users' anxieties about account security. This case exemplifies the growing sophistication of exchange impersonation tactics and their devastating impact on victims who believed they were protecting their digital assets. As Brooklyn District Attorney Gonzalez said, “My office...will continue to root out every instance of cryptocurrency fraud, which is a serious problem that’s been exploding throughout the country. We will investigate offenders using the latest technology, freeze their assets whenever possible, and assist the victims.”

Following funds from impersonation scams demonstrates evolving DeFi laundering tactics

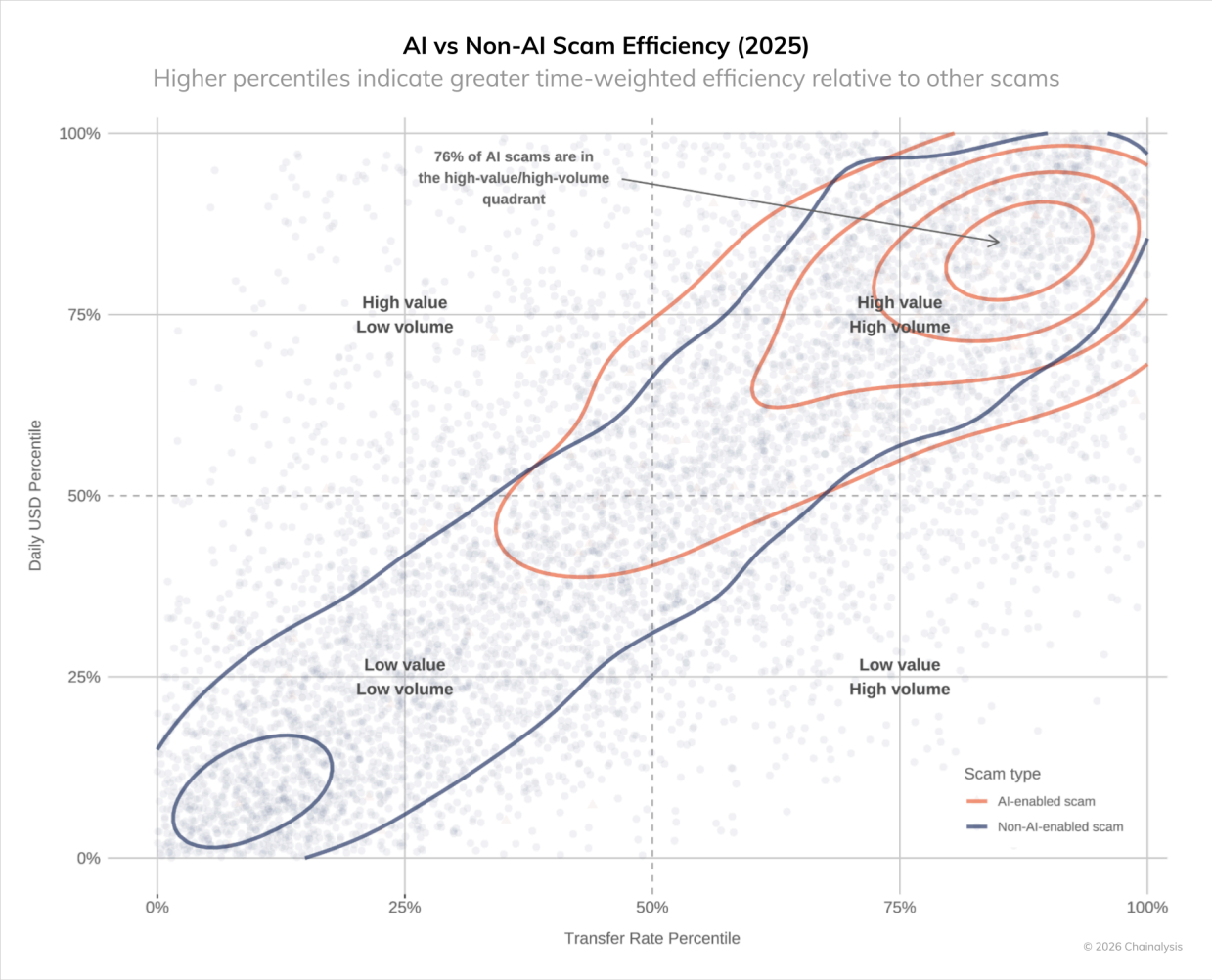
Impersonation scams also have distinctive laundering patterns that rely heavily on the DeFi ecosystem. This trend contrasts sharply with other scams, which continue to rely heavily on centralized exchanges to launder funds (a trend we will refer to later when discussing pig butchering scams). Interestingly, impersonation scams seem to have moved in distinctive waves when leveraging DeFi to layer funds. In 2024, these scams saw spikes associated with laundering via smart contracts and token smart contracts. In 2025, these pronounced volumes subsided in lieu of alternating waves associated with bridge use (early-to-mid 2025) and DEX use (second half of 2025). These patterns show the constantly adapting nature of scam operations, which vary in terms of primary laundering points and the types of services used.



AI and advanced tools are supercharging scam effectiveness

We are moving toward a future in which virtually all scams will incorporate AI into their operations to some degree. While many scammers buy AI tools through traditional payment channels, a subset buys these tools on-chain, making their transactions visible. Exploring the differences between scams with visible on-chain associations to Chinese AI vendors lets us estimate the scale and efficiency of AI.

As depicted below, 76% of AI-enabled scams are in the time-weighted high-value/high-volume quadrant. This means that a large majority of scams with demonstrable on-chain links to often Telegram-based Chinese AI vendors selling face-swap software, deepfake technologies, and LLMs tend to (1) scale more quickly (i.e., higher incoming transfer rates) and (2) be more severe (i.e., higher daily USD volumes) than scams without these clear on-chain links to AI vendors.



AI-enabled scams extract 4.5 times more money

According to a report published by J.P. Morgan in July 2025, scammers are increasingly leveraging deepfake technology and AI-generated content to create convincing impersonations in romance and investment scams. Our analysis reveals that, on average, scams with on-chain links to AI vendors extract $3.2 million per operation compared to $719,000 for those without an on-chain link — 4.5 times more revenue per scam. These AI-related operations also demonstrate significantly greater time-weighed efficiency:

- Higher daily revenue: $4,838 vs $518 median daily revenue
- Increased transaction volume: 35.1 vs 3.89 average transfers per day (9x more transaction activity)

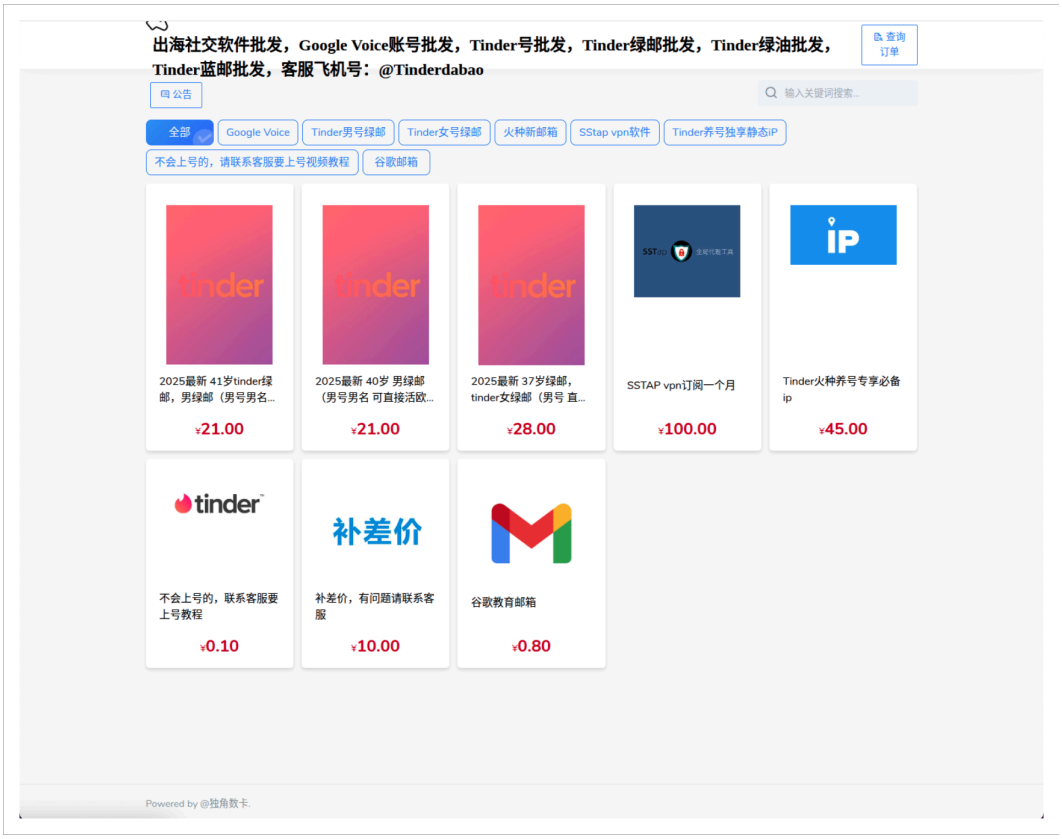
These metrics suggest both higher operational efficiency and potentially broader victim reach. The increased transaction volume indicates that AI is enabling scammers to reach and manage more victims simultaneously, a trend consistent with the industrialization of fraud we've been tracking. In contrast, the increased scam volume suggests that AI is likewise making scams more persuasive.

According to Will Lyne, Head of Economic & Cybercrime at the Metropolitan Police, “Fraud linked to cryptocurrency continues to grow in scale and sophistication, with organised crime groups increasingly using impersonation tactics, online infrastructure, and AI-enabled tools to target victims at pace and scale. However, we are also seeing a step change in law enforcement’s ability to respond. Through specialist capabilities, international cooperation, and the effective use of financial and digital intelligence, we are better equipped to identify criminal networks, seize illicit assets, and disrupt activity that causes harm in our communities.”

The industrialization of fraud

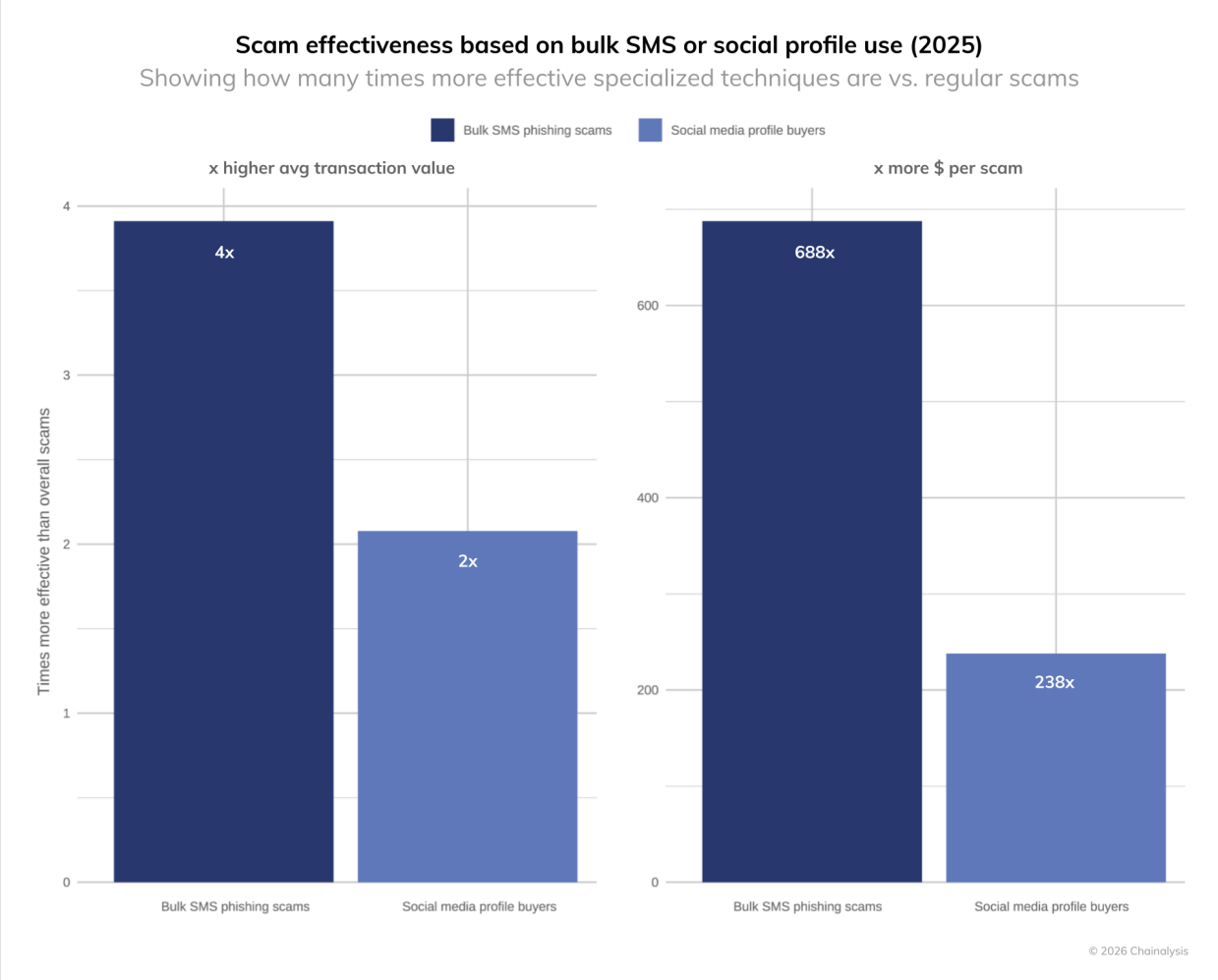
The Lighthouse case exemplifies another key trend: the professionalization and commercialization of the tools needed by scammers to execute sophisticated, industrial-scale scams. The Lighthouse Enterprise operated a complex business model where different actors specialized in distinct parts of the scams and fraud supply chain:

- Developer Group: Supplied phishing software and templates
- Data Broker Group: Provided targeted lists of potential victims
- Spammer Group: Offered tools to send fraudulent text messages at scale
- Theft Group: Specialized in monetizing stolen sensitive information
- Administrative Group: Ran online recruitment and collaboration forums

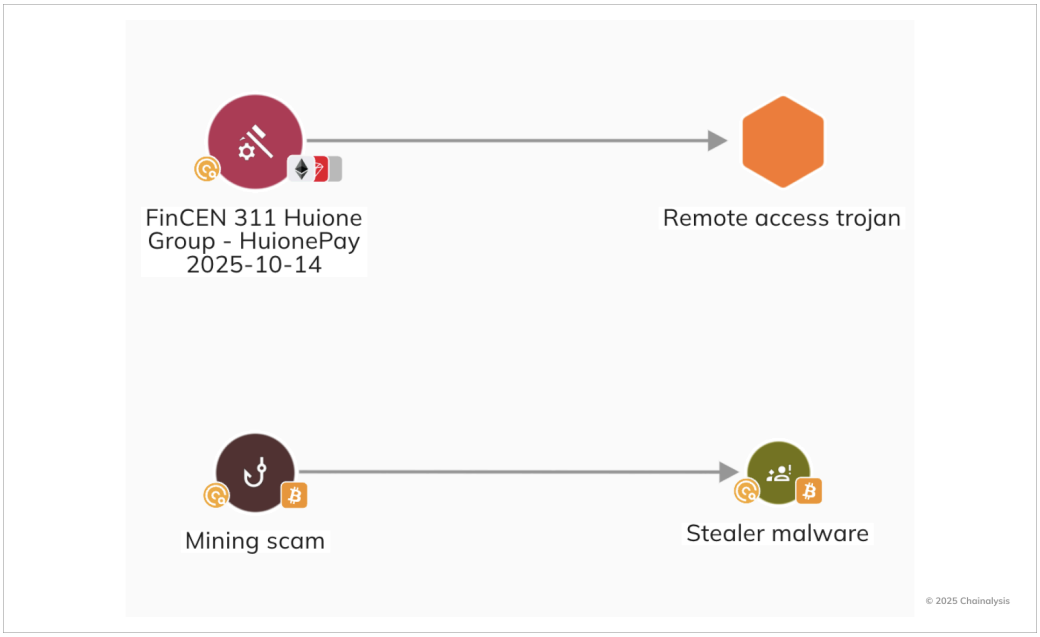


A Chinese language platform offering accounts for GMail, Tinder, and other services for scammers to target pig butchering victims. The platform also offers scammers customer service via a Telegram channel, a common practice.

This modular, service-based approach is a force multiplier and allows even technically unsophisticated criminals to execute sophisticated phishing campaigns, substantially lowering the barrier to entry for cryptocurrency fraud. Many of these campaigns have a social media angle, given that such platforms provide access to millions of users, and are thus prime targets for sending automated messages. In such cases, scammers may buy bulk social media profiles and use SMS and phishing kits to communicate. The material impact of this large-scale industrialization cannot be understated. Scams leveraging these phishing kits are 688 times more effective in dollar terms and four times more effective in average transaction size than regular scams. Scams that buy bulk social media accounts are likewise 238 times more effective in dollar terms and two times more effective in average transaction value compared to regular scams.



The UNODC has previously warned about scam campaigns' use of malware, a phenomenon we are increasingly seeing on-chain. Chinese scammers, in particular, regularly lace scams with Stealer Malware or Remote Access Trojans (RATs) that can drain accounts without interacting with victims. The bar for success is then much more achievable for scammers, who only need one click from a victim rather than developing a relationship with them.



Chainalysis Reactor graph showing transactions between known scam-related entities, stealer malware, and remote access trojan

Law enforcement on the offensive, with record seizures targeting scam operations

The growing scale and sophistication of scam activity prompted unprecedented law enforcement action in 2025, culminating in two of the largest-ever crypto-related law enforcement actions directly connected to scam operations.

Jian Wen and Yadi Zhang

In November 2025, the UK's Metropolitan Police secured convictions in a landmark crypto money laundering case that led to the world's largest confirmed cryptocurrency seizure, recovering over 61,000 Bitcoin — currently valued at around £5 billion — from Chinese national Zhimin Qian (also known as Yadi Zhang), who orchestrated a multibillion-pound investment fraud in China that victimized more than 128,000 people between 2014 and 2017. Qian was sentenced to 11 years and eight months' imprisonment for possessing and transferring criminal property, while her accomplice Seng Hok Ling received a nearly five-year term for his role in laundering the cryptocurrency. This case not only underscores the scale and sophistication of crypto-linked money laundering networks spanning jurisdictions, but also highlights the persistent threat posed by criminals attempting to convert illicit crypto proceeds into real-world assets through complex international schemes.

"This was a long, complex, and unprecedented investigation into the laundering of criminal proceeds through cryptocurrency. Over a number of years, significant efforts were made to move and disguise the

funds and convert them into assets in the UK," said Detective Sergeant Isabella Grotto, the lead investigating officer on the case. "By working closely with partners in the UK and overseas, with support from Chainalysis, we were able to trace the movement of the cryptocurrency, identify assets linked to the offending, and ultimately recover more than 61,000 bitcoin. That work was central to building the case and securing this outcome."

The investigation, built on information dating back to 2018, revealed that Qian had fled to the UK under a false identity after amassing illicit funds and had attempted to launder them via luxury property purchases and other high-value assets, a pattern seen in many large-scale fraud operations. The record-setting seizure and subsequent prison sentences demonstrate law enforcement's growing capability to trace and disrupt sophisticated fraud-to-crypto money laundering globally, reinforcing the value of blockchain transparency in dismantling even deeply entrenched criminal networks.

The Prince Group

In a major disruption of the global scam ecosystem, the U.S. Department of Justice (DOJ) unsealed charges against Prince Group chairman Chen Zhi for allegedly overseeing Cambodian forced-labor scam compounds that powered large-scale cryptocurrency fraud targeting victims worldwide. According to prosecutors, these compounds operated as vertically integrated fraud factories: trafficked individuals were coerced into running pig butchering investment scams and romance fraud schemes, laundering proceeds through cryptocurrency to obscure attribution and scale operations globally. The case underscores how modern scam networks have professionalized, integrating human trafficking, money laundering, and crypto-enabled fraud into a single, industrialized business model.

Critically, U.S. authorities paired these indictments with large-scale financial disruption, including arrests across transnational money laundering networks and actions to seize and forfeit more than $15 billion in illicit proceeds linked to scam activity. In October, working in close coordination with the UK's Foreign Commonwealth and Development Office (FCDO), the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) jointly designated 146 targets within the Prince Group Transnational Criminal Organisation. The designation cited a "laundry list of transnational crimes, including the construction, operation, and management of scam compounds reliant on human trafficking and modern-day slavery where industrial-scale cyberfraud operations target victims around the world, including U.S. citizens." In a development that demonstrates the complex geopolitical dimensions of prosecuting transnational crypto crime, Chen was arrested in Cambodia in January 2026 after his Cambodian citizenship was revoked in December, and was subsequently extradited to China for investigation rather than to the United States where he faces indictment, highlighting the jurisdictional challenges in dismantling global scam networks.

These actions mark a shift from reactive victim recovery to systematic dismantling, targeting not just front-line scammers, but also the executives, infrastructure, shell companies, and financial rails that sustain them. Together, the Prince Group case and related DOJ, OFAC, and FCDO actions illustrate a new, more integrated phase in scam enforcement: one focused on breaking the economic backbone of crypto-enabled fraud at scale and across borders, rather than treating scams as local, isolated, or purely digital crimes.

Tickmilleas

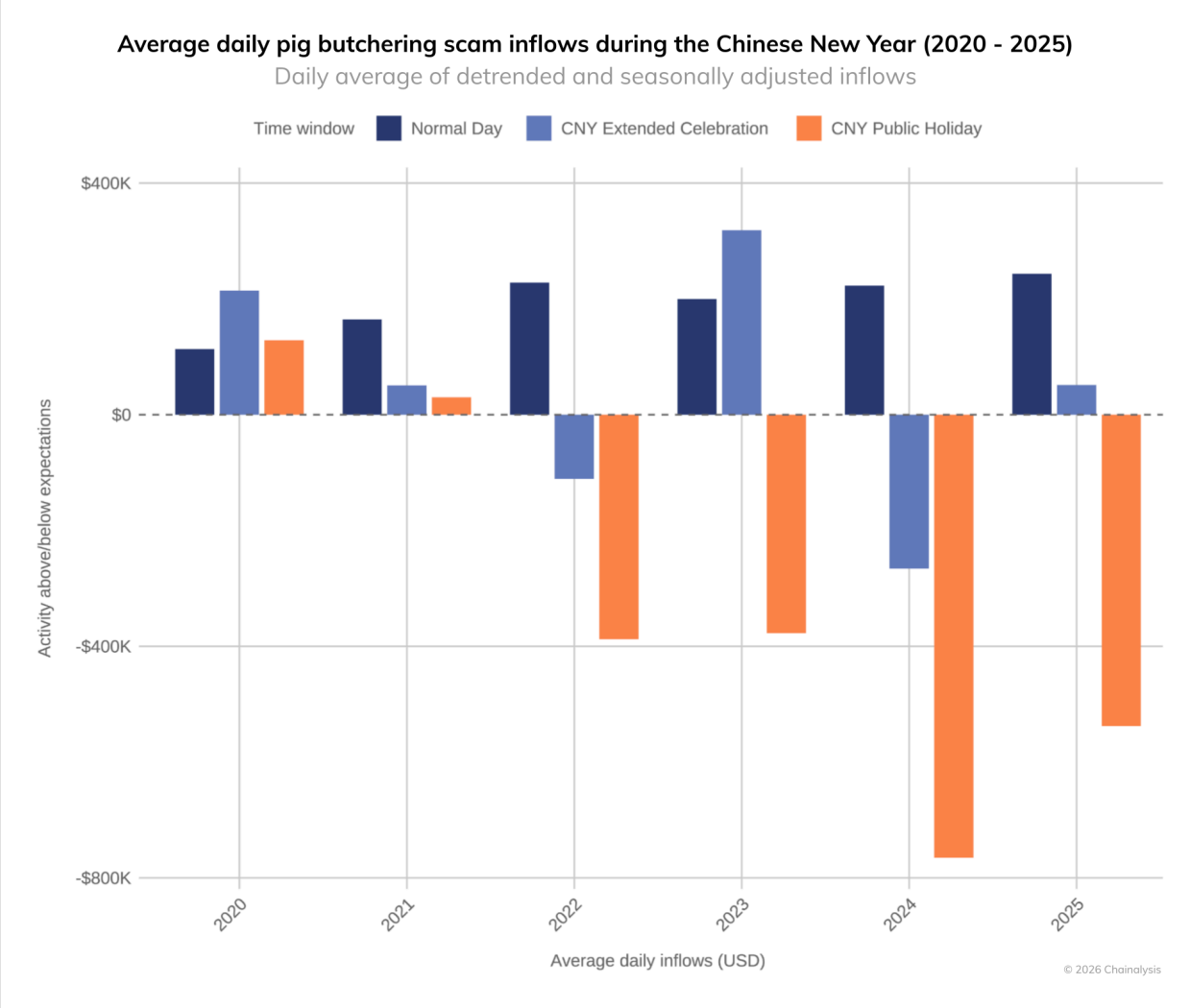
The U.S. government is pursuing a forfeiture of tickmilleas[dot]com, a scam domain that served as core infrastructure for a transnational crypto investment fraud network operating out of the Tai Chang scam compound along the Myanmar-Thailand border. Registered in November 2025 via a Singapore-based registrar, the site impersonated a legitimate financial services firm to deceive primarily U.S.-based victims into sending BTC, ETH, USDT, and USDC to crypto wallets controlled by overseas scammers. Blockchain analysis shows victims were funnelled through U.S. crypto exchanges before funds were rapidly moved through multiple wallets and consolidation addresses – hallmark tactics of professional on-chain money laundering – explicitly linking the domain to cross-border professional money laundering. Tickmilleas's operators are tied to Chinese organized crime syndicates embedded in Southeast Asia's scam compound ecosystem, with on-the-ground protection from the DKBA, an armed group sanctioned by OFAC for supporting cyber scam centers.

These cases demonstrate the scale of modern cryptocurrency scam operations and their increasing integration with traditional organized crime. They also reveal the human cost of these schemes, which exploit both financial victims and the trafficked individuals forced to operate them, itself an unspeakable crime. These prosecutions' success also underscores the growing capability of international law enforcement to trace cryptocurrency flows and dismantle complex criminal enterprises. However, the industrial scale of global scam operations suggests the challenge remains considerable.

Strong regional nexus to East and Southeast Asia persists

Our on-chain analysis continues to show persistent connections between cryptocurrency scams and operations based in East and Southeast Asia. While the Huione Guarantee platform identified in our 2025 report was effectively shut down following FinCEN's 311 designation — which severed its access to the U.S. financial system — we've observed expansion of similar operations across the region.

The centrality of the region to pig butchering is a defining characteristic of the scam ecosystem. The chart below shows the 'holiday effect' associated with the Chinese New Year public holiday (7 days at the start of the 15-day new year celebration). Starting around 2022, roughly when Huione began to play a central role in laundering funds from scam compounds such as KK Park, there was a notable reduction in pig butchering scam activity during the 7-day public holiday associated with the Chinese New Year. After the data have been detrended and seasonally adjusted, average daily pig butchering activity drops notably during these short windows. This pattern suggests that the Chinese holiday is associated with a reduction in inflows to pig butchering scams, indicating that actors in East and Southeast Asia play an important role in this scam ecosystem.



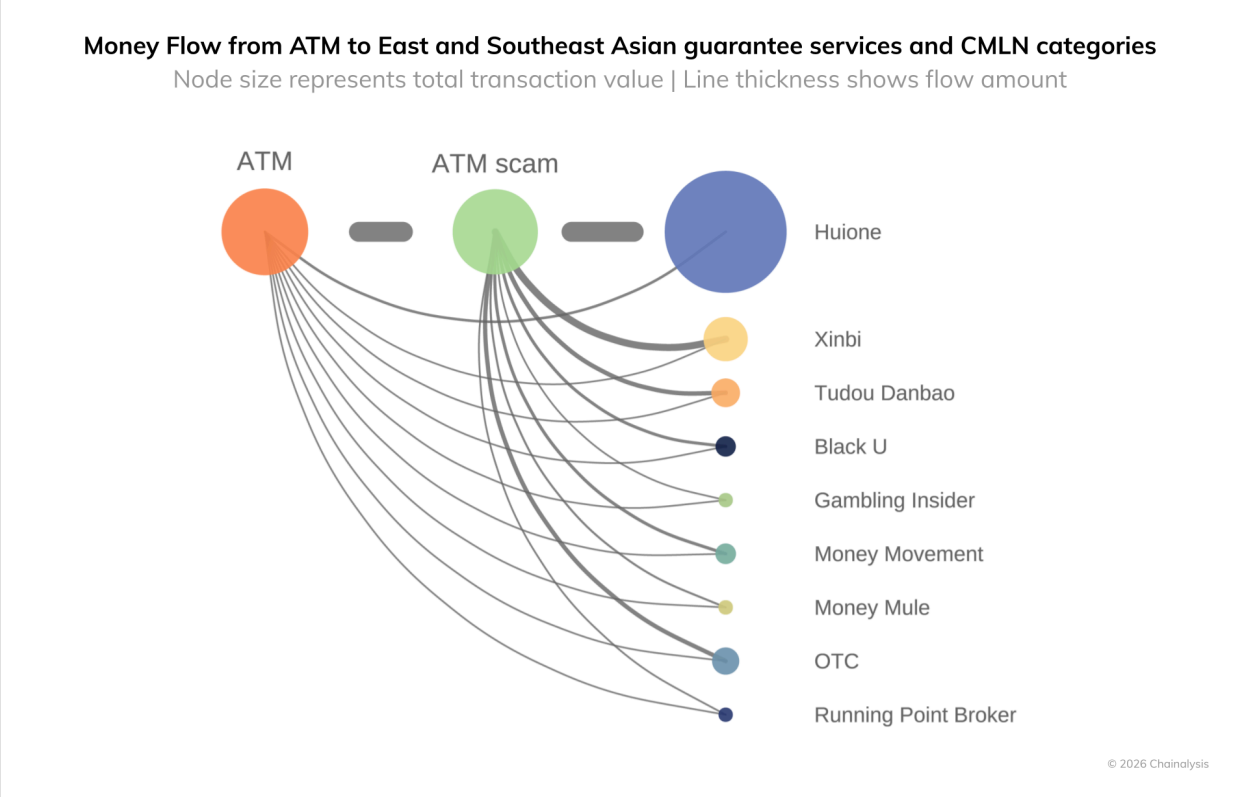
Our research shows that pig-butchering networks across Southeast Asia, drawing heavily on CMLNs, generate billions of dollars annually and rely on layered wallet structures, exchanges, shell companies, and informal banking channels to launder funds and convert crypto into real-world assets, including real estate and luxury goods. The Prince Group case study reflects this model, underscoring how scam operators and underground laundering networks form a resilient ecosystem that rapidly adapts to enforcement pressure, shifts infrastructure, and continues to scale globally.

ATM scams targeting the elderly launder funds via guarantee services and CMLNs

Scams targeting older adults represent some of the most financially devastating frauds reported in the US, with recent estimates indicating that Americans aged 60 and older lose billions of dollars annually to financial exploitation and fraud, including nearly $4.9 billion in reported losses in 2024 alone, more than any other age group, according to AARP and FBI data. The FBI's Internet Crime Complaint Center (IC3) further underscores this trend: in 2024, individuals aged 60 and older reported $2.8 billion in losses from crypto-related scams, reflecting both the scale and the growing role of digital assets in modern fraud.

While elder fraud encompasses a broad range of schemes, cryptocurrency ATMs have emerged as a notable on-ramp for scams. Reported losses from Bitcoin ATM fraud have risen sharply in recent years, and older victims are disproportionately affected by these kiosk-based conversions. The elderly, who often have significant retirement savings yet limited familiarity with irreversible digital payment methods, remain particularly vulnerable to such tactics.

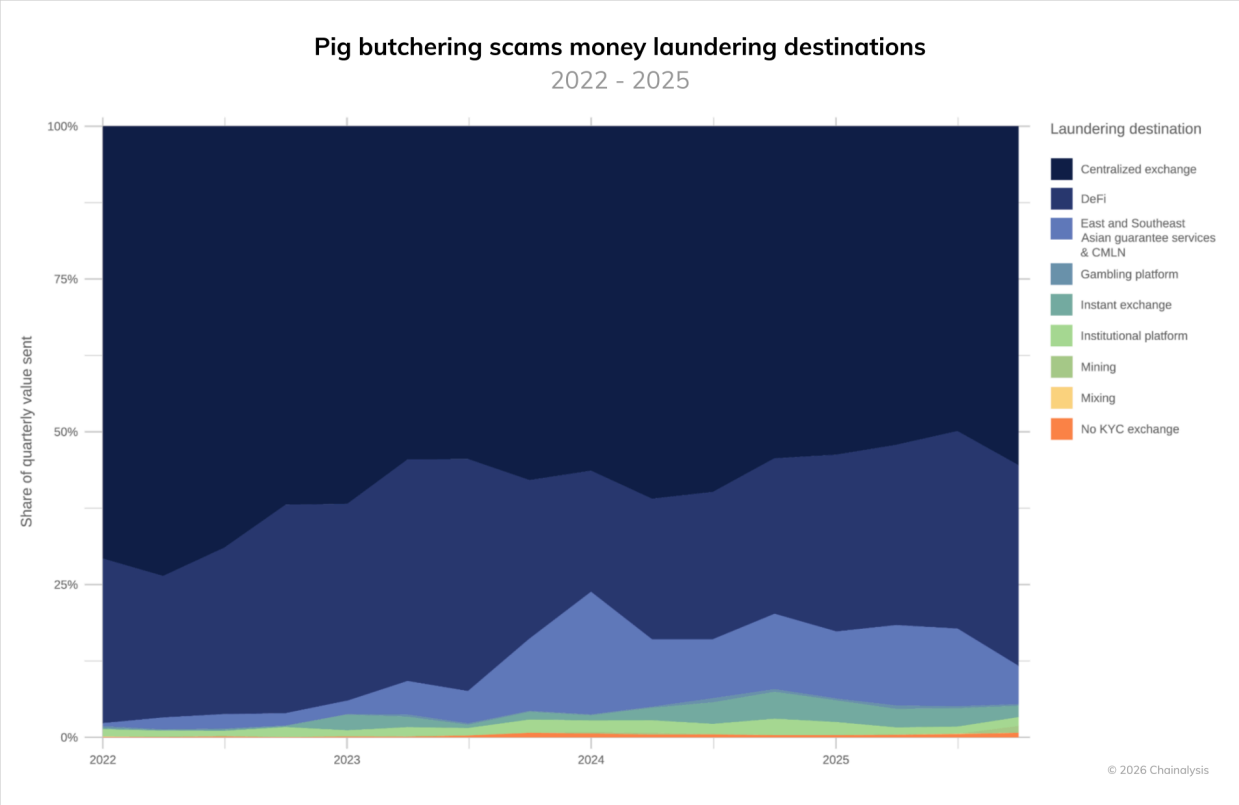
Our on-chain analysis reveals that funds originating at U.S. crypto ATMs frequently flow into wallets associated with Southeast Asia-based CMLNs and guarantee services, which serve as key intermediaries in the broader global scam infrastructure. While not all on-chain flows from scams to CMLNs can be traced directly to ATM on-ramps, crypto ATMs remain a critical input for scammers targeting older adults, who are often instructed to convert cash into cryptocurrency at these kiosks before funds are quickly transferred. In this context, actors leveraging crypto ATMs as both payment conduits and loci of fraud increasingly depend on CMLNs to launder and integrate stolen funds into the wider financial system, illustrating how traditional elder fraud has evolved into a transnational, crypto-enabled ecosystem.



Regional infrastructure beyond KK Park and Huione compounds

The regional connection is further evidenced by the off-ramping patterns we observe, with a significant portion of pig butchering scam proceeds flowing to CMLNs. In Q1 2022, less than 1% of pig butchering scam laundering flows went to CMLNs. By Q1 of 2024, these services processed slightly over 20% of pig butchering scam laundering flows for the quarter, and these networks consistently laundered over 10% of scam funds in 2025. Interestingly, the growth in CMLN activity related to pig butchering scams has

coincided with a steady decline in the use of centralized exchanges to launder or offramp funds, potentially because exchanges can freeze funds. Broadly, this rapid and sustained growth of CMLNs showcases the persistent, multi-year interconnection between pig butchering scams targeting individuals in the U.S., Canada, Europe, and elsewhere, and Chinese-language laundering services based in Southeast Asia.



The industrialization of cryptocurrency scams demands a proactive, multidisciplinary approach

The 2025 data reveal the extent to which cryptocurrency-enabled scams are becoming more sophisticated, organized, and efficient. Increasingly accessible AI tools, phishing-as-a-service platforms, and the convergence of different scam methodologies have reduced barriers to entry and enabled scamming at scale. While high-profile enforcement successes in 2025 are encouraging, the criminal networks orchestrating scams remain of persistent concern. These transnational groups have taken advantage of governance weaknesses in low-capacity jurisdictions, and have demonstrated flexibility and resilience, moving to new locations within and beyond Southeast Asia and adapting their operating models as necessary.

There are no silver bullets to tackling such entrenched, industrial-scale scamming activity and to be effective, a multi-pronged response is required, including:

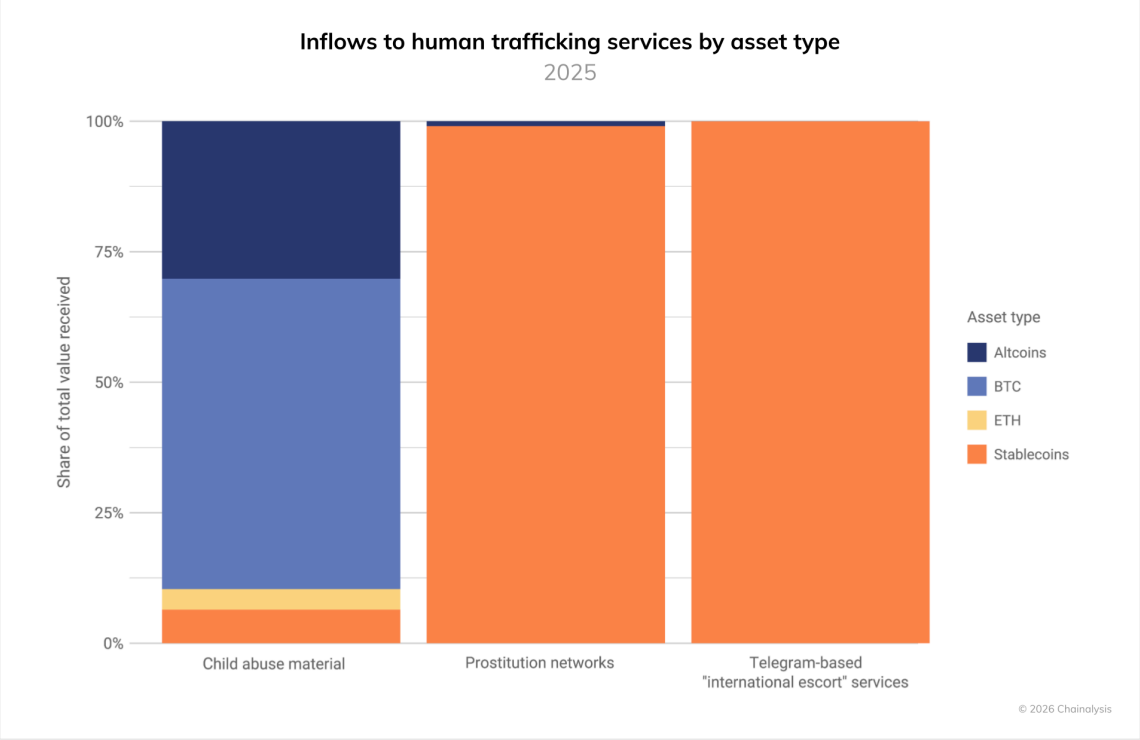
- A stronger emphasis on preventing victim harm, including greater adoption of real-time fraud and mule detection systems such as Chainalysis Alterya by financial institutions and cryptocurrency businesses, and enhanced detection tools that can help victims protect themselves;
- Enhanced cross-border law enforcement coordination to facilitate rapid fund tracing and freezing, to disrupt financial flows and make it harder to cash out illicit proceeds; and
- International support for capacity building and technical assistance, to strengthen institutions and enforcement in low-capacity jurisdictions.

As we move into 2026, we expect further convergence of scam methodologies as scammers adopt multiple tactics and technologies simultaneously.

Cryptocurrency Flows to Suspected Human Trafficking Services Surge 85% Year-over-Year

The intersection of cryptocurrency and suspected human trafficking intensified in 2025, with total transaction volume reaching hundreds of millions of dollars across identified services, an 85% year-over-year (YoY) increase. The dollar amounts significantly understate the human toll of these crimes, where the true cost is measured in lives impacted rather than money transferred.

This surge in cryptocurrency flows to suspected human trafficking services is not happening in isolation, but is closely aligned with the growth of Southeast Asia–based scam compounds, online casinos and gambling sites, and Chinese-language money laundering (CMLN) and guarantee networks operating largely via Telegram, all of which form a rapidly expanding local illicit ecosystem with global reach and impact. Unlike cash transactions that leave no trace, the transparency of blockchain technology provides unprecedented visibility into these operations, creating unique opportunities for detection and disruption that would be impossible with traditional payment methods.



Our analysis tracks four primary categories of suspected cryptocurrency-facilitated human trafficking:

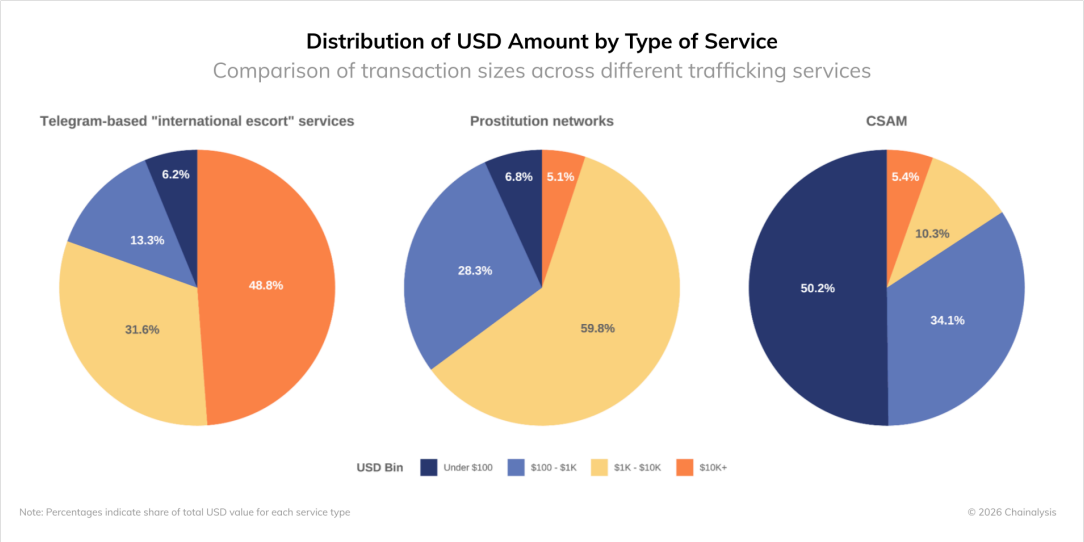
1. “International escort” services: Telegram-based services that are suspected to traffic in people
2. “Labor placement” agents: Telegram-based services that facilitate kidnapping and forced labor for scam compounds
3. Prostitution networks: suspected exploitative sexual service networks
4. Child sexual abuse material (CSAM) vendors: networks of individuals engaged in the production and dissemination of CSAM

Payment methods vary significantly across these categories. While "international escort" services and prostitution networks operate almost exclusively using stablecoins, CSAM vendors have traditionally relied more heavily on bitcoin. However, even within CSAM operations, bitcoin's dominance has decreased with the emergence of alternative Layer 1 networks. Broadly, the predominant use of stablecoins by “international escort” services and prostitution networks suggests that these entities prioritize payment stability and ease of conversion over the risks that these assets might be frozen by centralized issuers.

As we detail below, the “international escort” services are tightly integrated with Chinese-language money laundering networks. These networks rapidly facilitate the conversion of USD stablecoins into local currencies, potentially blunting concerns that assets held in stablecoins might be frozen.

Nearly half of Telegram-based “international escort” service transactions exceed $10,000, demonstrating professionalized operations

The distribution of transaction sizes reveals distinct operational models across different types of suspected trafficking services. "International escort" services show the highest concentration of large transactions, with 48.8% of transfers exceeding $10,000, suggesting organized criminal enterprises operating at scale. In contrast, prostitution networks cluster in the mid-range, with approximately 62% of transactions between $1,000-$10,000, indicating potential agency-level operations.



These “international escort” services operate with sophisticated business models, complete with customer service protocols and structured pricing. For example, one prominent operation advertises across major East Asian cities with a tiered pricing system ranging from 3,000 RMB ($420) for hourly services to 8,000 RMB ($1,120) for extended arrangements, including international transport. These standardized pricing models create identifiable transaction patterns that investigators and compliance teams can use to detect suspicious activity at scale.

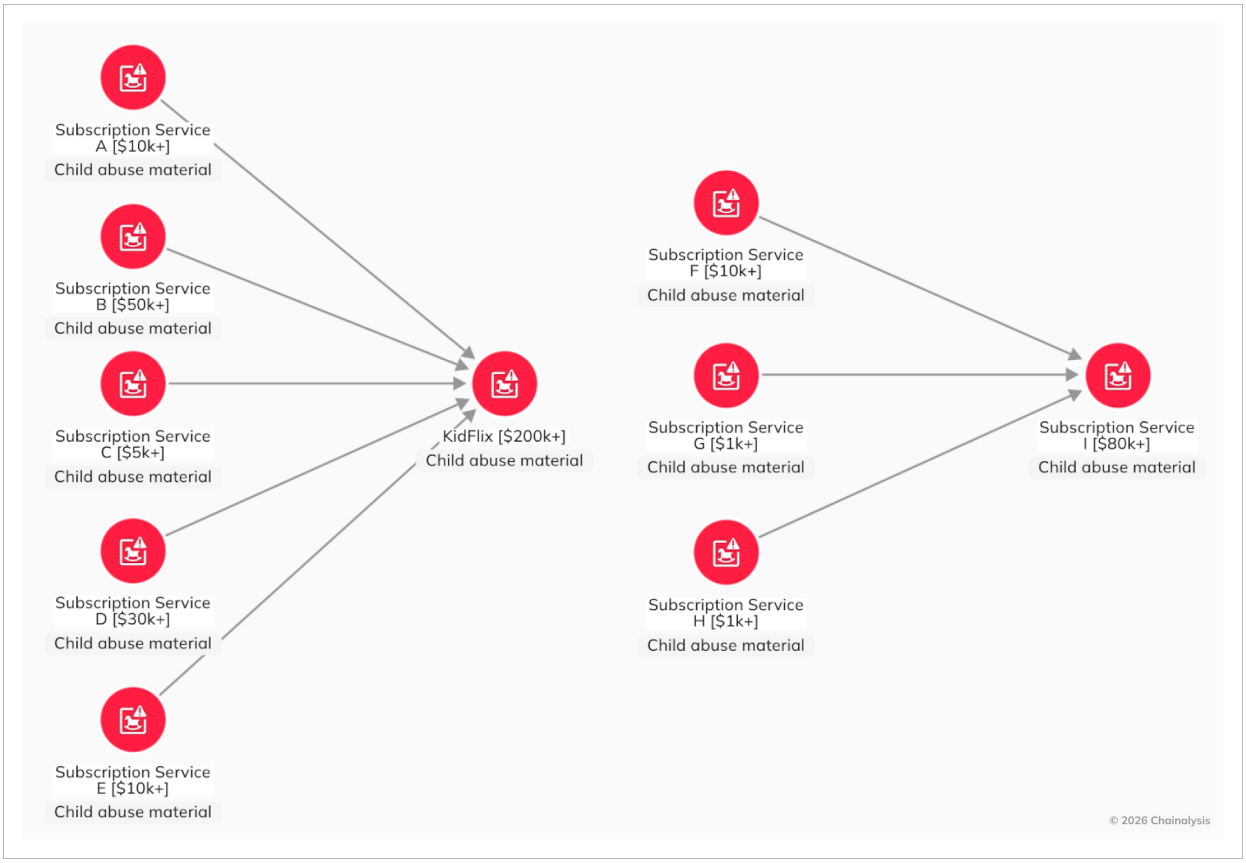
Screenshot showing an advertisement from an escort service provider, which include the locations that the provider serves and pricing for escort services

CSAM vendors and marketplaces

CSAM operations demonstrate different but equally concerning patterns. While approximately half of CSAM-related transactions are under $100 – unfortunately, there’s more CSAM on the internet than ever before, and it’s never been cheaper to produce – these operations have evolved sophisticated financial and distribution strategies. In 2025, we observed that, while these networks still collect payments in mainstream cryptocurrencies, they increasingly use Monero for laundering proceeds. Instant exchangers, which provide rapid and anonymous cryptocurrency swapping without KYC requirements, play a crucial role in this process.

The business model for CSAM operations has largely consolidated around subscription-based services rather than pay-per-content transactions, generating more predictable revenue streams while simplifying administration. These subscriptions typically cost less than $100 per month, creating a lower barrier to entry while establishing regular revenue for operators.

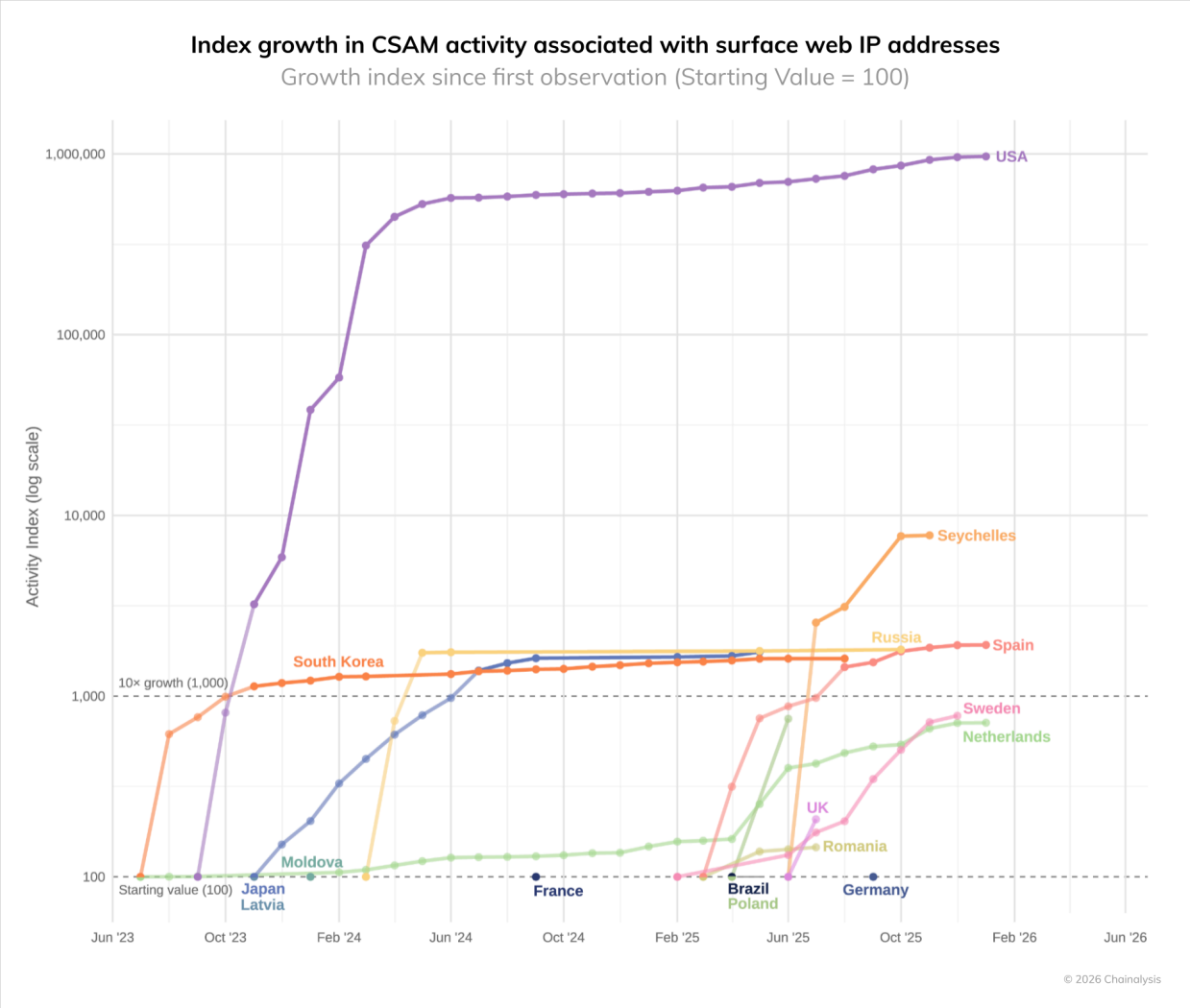
A disturbing trend emerged in 2025 with increasing overlap between CSAM networks and sadistic online extremism (SOE) communities. Following law enforcement actions against groups like "764" and "cvlt," we observed SOE content appearing within CSAM subscription services, commonly advertised as "hurtcore." These SOE groups specifically target and manipulate minors through sophisticated sextortion schemes, with the resulting content being monetized through cryptocurrency payments, perpetuating cycles of abuse.



The scale of these operations became particularly evident in July 2025, when Chainalysis identified one of the largest CSAM websites operating on the darkweb following a UK law enforcement lead. This single operation utilized over 5,800 cryptocurrency addresses and generated more than $530,000 in revenue since July 2022, surpassing the notorious "Welcome to Video" case from 2019.

Geographic analysis of clearnet CSAM operations reveals strategic use of U.S. infrastructure[4]. While U.S.-based IP addresses account for a large portion of CSAM activity associated with surface websites, IPs from other countries like South Korea, Spain, and Russia show smaller flows. This suggests that these operations leverage U.S.-based infrastructure for scale, reliability, and an initial appearance of legitimacy that helps the activity blend into normal traffic and delays detection. Further, if the operators are outside the U.S., it reduces their personal exposure.

[4] This analysis is limited to the clearweb portion of the CSAM industry. A significant portion of CSAM transactions are conducted peer-to-peer through encrypted messaging apps or the darkweb, where reliable IP addresses can not be obtained for this analysis.



Chris Hughes, Internet Watch Foundation Hotline Director, told us, “In 2025, the Internet Watch Foundation identified 312,030 reports containing child sexual abuse images and videos. This is more than ever before, with an increase of 7% from the previous year. Early analysis of IWF data indicates that most clearweb sites offering virtual currency as a payment for child sexual abuse are hosted in the US, while darkweb sites were the second highest. Any payment information that we identify on commercial websites is captured and shared with global law enforcement and organisations like Chainalysis to disrupt further distribution of criminal imagery and to help in the investigation of those who create, share and profit from the sale of child sexual abuse material.”

Despite these concerning trends, 2025 saw significant law enforcement successes, including the takedown of "KidFlix" by German authorities and increased arrests of CSAM consumers across the United States. These cases demonstrate how blockchain analysis can provide critical evidence for identifying, investigating, and prosecuting both operators and consumers of CSAM networks.

Telegram-based services show deep integration with Chinese-language money laundering networks (CMLNs) and guarantee platforms

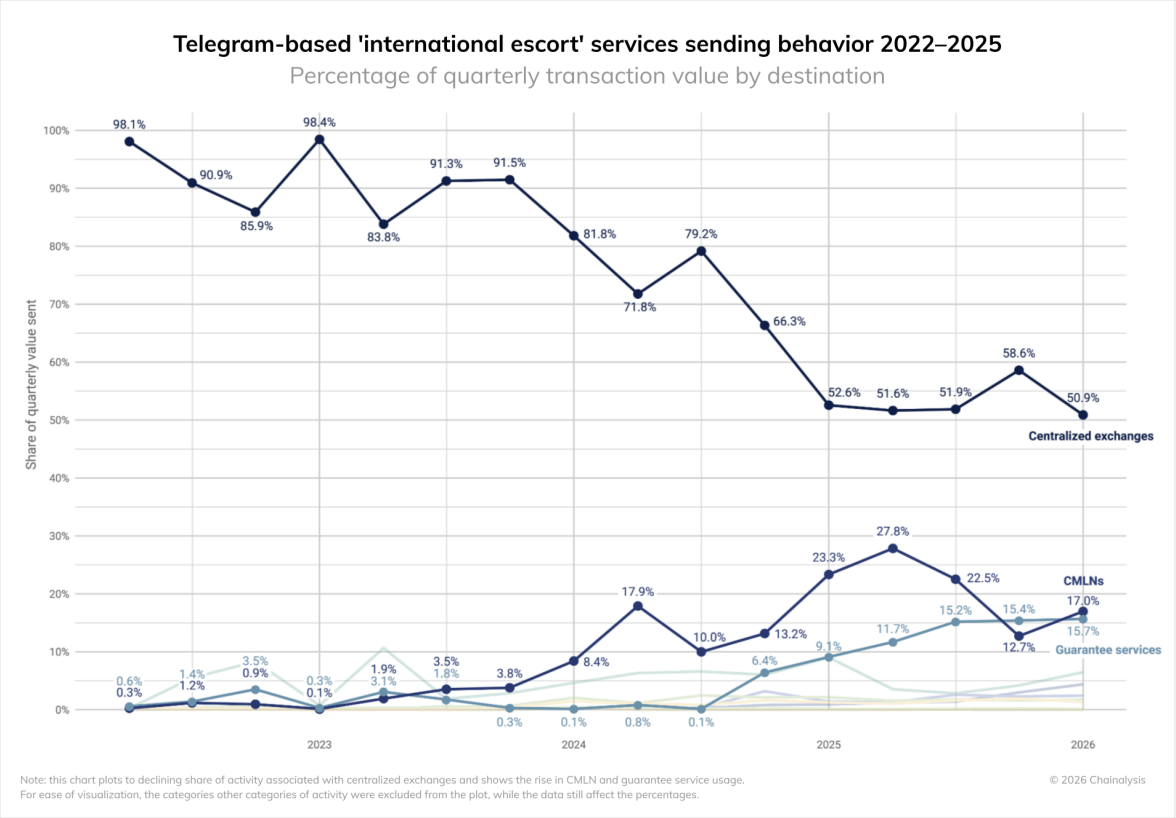
“International escort” services

The cryptocurrency footprint of escort services reveals sophisticated integration with established financial infrastructure, particularly CMLNs and guarantee platforms. While some escort services operate legally, cryptocurrency transaction patterns help identify potential trafficking operations through their distinct financial behaviors.

The majority of cryptocurrency movements flow through a combination of mainstream exchanges, institutional platforms, and guarantee services like Tudou and Xinbi. This creates both vulnerabilities and opportunities: while these platforms provide easier access to the financial system, they also serve as critical chokepoints where compliance teams can detect and investigate suspicious patterns.

“Labor placement” agents

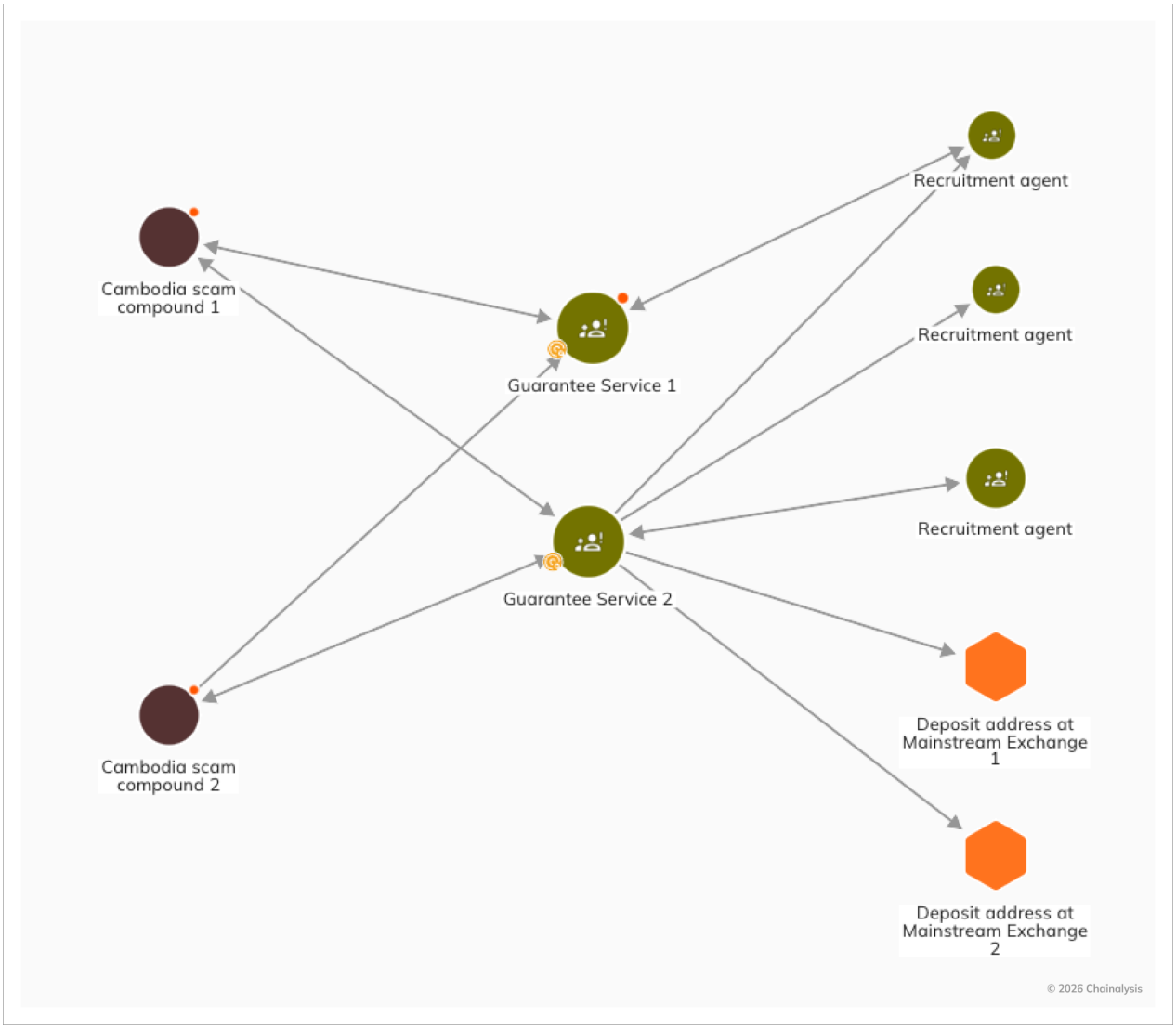
It’s been widely reported that scam operations — pig butchering schemes in particular — are deeply intertwined with human trafficking. Victims are often lured by fake job offers before being forced to work in Southeast Asian scam compounds, where they face brutal conditions and are coerced into operating romance/investment scams under threat of violence.



These operations utilize guarantee services' "human resource" vendors to facilitate recruitment. Channel participants inquire about methods to transport workers who have been detained at immigration checkpoints, while compound administrators provide updates concerning regional developments that might affect their operations, such as the ongoing border tensions between Thailand and Cambodia.

Screenshot of advertisement on Telegram, detailing compensation terms and personnel requirements, including differentiated pricing for workers.

Blockchain analysis shows that recruitment payments typically range from $1,000 to $10,000, aligning with advertised pricing tiers. This provides another opportunity to leverage identifiable transaction patterns to detect suspicious activity at scale. These agents maintain presence across multiple guarantee platforms to maximize their reach, with some operating through mainstream cryptocurrency exchanges.



The involvement of established criminal organizations became evident through our analysis of trafficking-related channels. For example, we identified an administrator account linked to the "Fully Light Group," a Kokang-based organization previously flagged by the United Nations Office on Drugs and Crime (UNODC) for illegal gambling and money laundering. Their presence in channels facilitating transactions between scam compounds and "labor placement" agents suggests how established criminal networks provide critical financial infrastructure for trafficking operations.

Screenshot of administrators in a recruitment channel, with an account linked to Fully Light designated as an "admin" account

Southeast Asian organizations facilitating potential trafficking show global reach through cryptocurrency

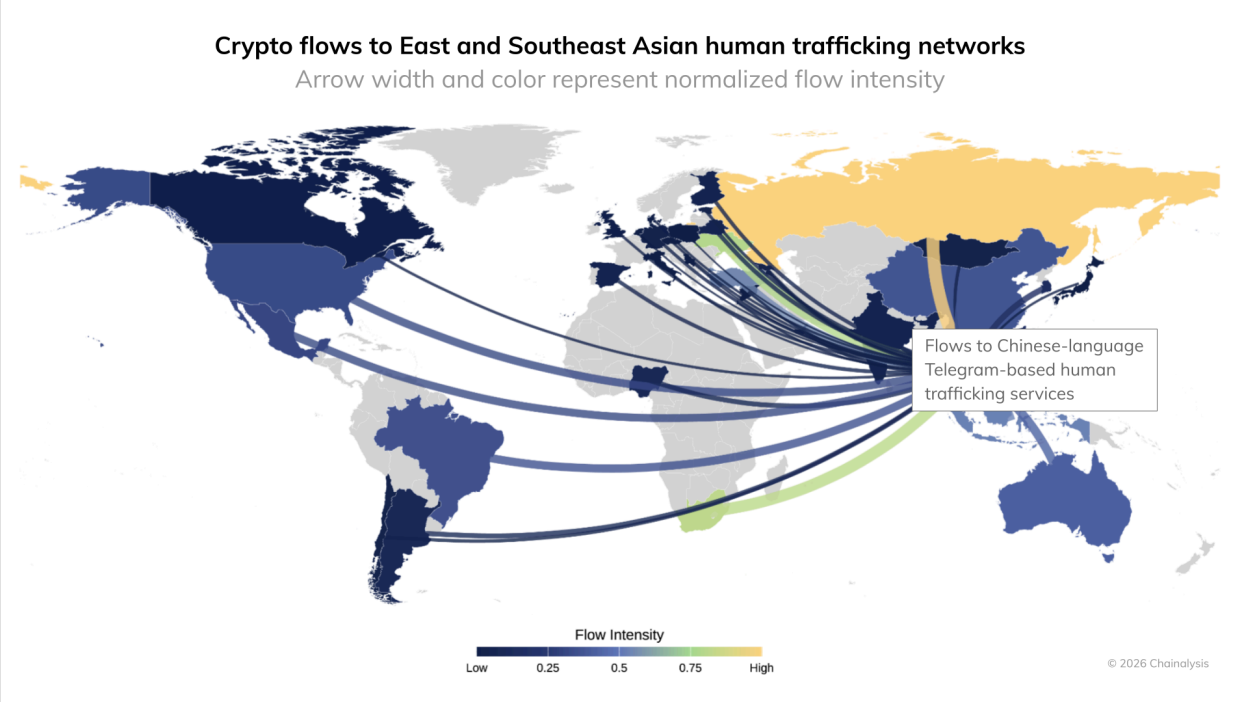
Geographic analysis of "international escort" services in 2025 reveals how Southeast Asian services, particularly Chinese-language operations, have expanded their reach globally through cryptocurrency adoption[5]. The transparency of the blockchain provides valuable insight into broader trafficking patterns and financial flows of these types of operations.

Based on our data, Chinese-language services operating through networks spanning mainland China, Hong Kong, Taiwan, and various Southeast Asian countries demonstrate sophisticated payment processing capabilities and extensive international reach. Their large-scale cryptocurrency transactions show significant flows from countries including Brazil, the United States, the United Kingdom, Spain, and Australia, indicating the truly global scope of these operations.

While traditional trafficking routes and patterns persist, these Southeast Asian services exemplify how cryptocurrency technology enables trafficking operations to facilitate payments and obscure money flows

[5] This analysis involved a combination of signals to estimate the country of origin, including web traffic data and the use of regional crypto exchanges.

across borders more efficiently than ever before. The diversity of destination countries suggests these networks have developed sophisticated infrastructure for global operations.



Key risk indicators and monitoring strategies

While the sophistication of cryptocurrency-facilitated trafficking operations continues to grow, the transparent nature of blockchain technology provides powerful tools for detection and prevention. Our analysis has identified several key indicators that compliance teams and law enforcement can monitor:

- Large, regular payments to labor placement services paired with cross-border transactions
- High-volume transactions through guarantee platforms
- Wallet clusters showing activity across multiple categories of illicit services
- Regular stablecoin conversion patterns
- Concentrated fund flows to regions known for trafficking operations
- Connections to Telegram-based recruitment channels

The increasing sophistication of these operations, particularly their growing intersection with legitimate businesses and professional money laundering networks, requires a comprehensive monitoring approach that leverages blockchain analysis alongside traditional anti-trafficking efforts and public education. As these networks continue to evolve, the transparency of blockchain technology provides unprecedented opportunities for detection, disruption, and enforcement that would be impossible with traditional payment methods.

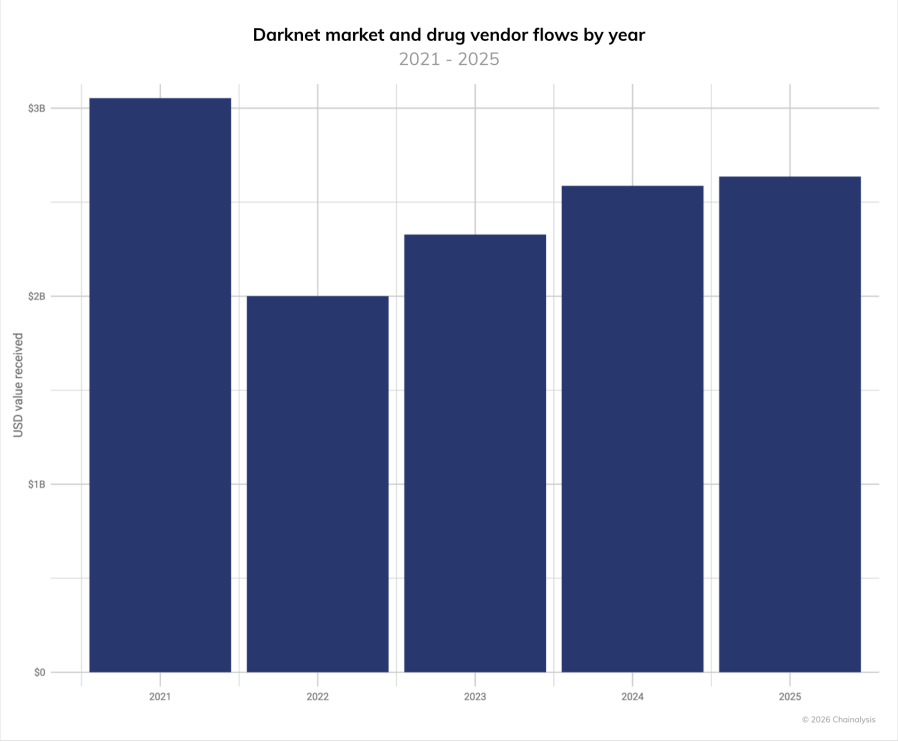
From Fentanyl to Fraud: On-Chain Activity Highlights Illicit Market Evolution

Darknet markets (DNMs) remain one of the most persistent segments of the crypto-enabled illicit economy. Despite repeated law enforcement takedowns, market exits, and infrastructure disruptions, DNMs continue to facilitate the sale of illicit drugs at scale, while also serving as key hubs for fraud-related services. In 2025, on-chain activity associated with DNMs rose YoY, but fraud shops contracted, showing important structural shifts within the ecosystem — particularly in how illicit drug markets resupply, how fraud services are organized, and how crypto-based drug purchasing can shed light on public health crises.

Over the years, one of our most consistent findings has been the resilience of darknet drug markets and the growing analytical value of blockchain data. Crucially, this on-chain data can be operationalized, not only by law enforcement and the private sector, but also by public health authorities — providing real-time, actionable insights.

Darknet markets continue to process billions in annual crypto flows

Total crypto inflows to drug vendors and DNMs increased slightly YoY in 2025 to slightly over $2.5 billion.



Drug vendors and darknet markets, which are grouped together in the Crypto Crime Report but are distinct entities in our product suite, facilitate retail and wholesale drug sales, with payments typically flowing from personal wallets and exchanges into escrow services or vendor-controlled addresses. While mainstream darknet marketplaces also offer fraud-related goods and hacking tools, drugs generally account for the majority of listings. Taken together, aggregate flows tell us how large an ecosystem is — but not how it affects the real world. To understand that, we turn to a specific drug category where on-chain activity intersects directly with off-chain realities and public health outcomes.

On-chain data reflect fentanyl supply chain disruption

Some good news: deaths from fentanyl overdoses in the U.S. have declined since they peaked in 2023. Given that explaining this dramatic drop is of interest to scientists and policymakers alike, academics recently made the case in Science for one major driver: a reduction in the supply of fentanyl. Specifically, they analyzed public reports and communications to make the case that improved collaboration between the U.S. and China, which led to China taking direct action on online fentanyl precursor vendors, disrupted supply at the source. These actions translated into sharp reductions in overdose mortality, a trend first observed in 2023 that continued into 2025 in both the US and Canada.

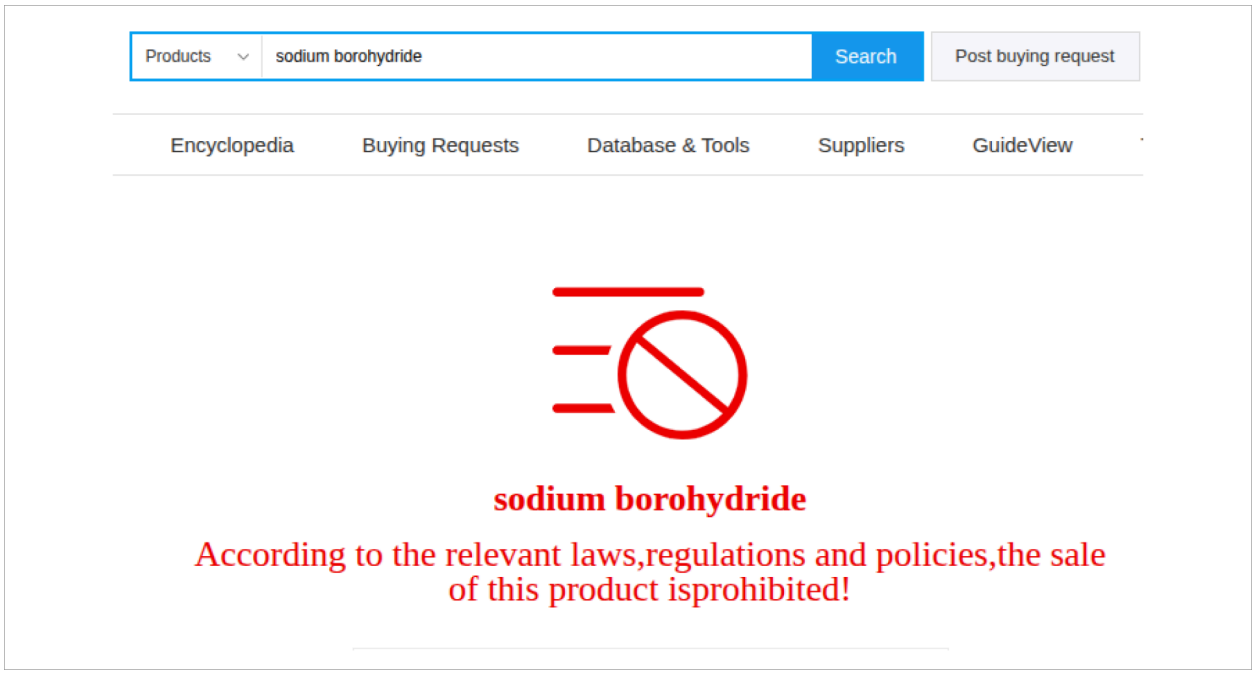
On-chain data reflect this development. Throughout 2022, crypto transaction volumes to fentanyl-related precursor brokers – operating disproportionately in China – steadily climbed. These fluctuations preceded the sustained high levels of overdose deaths in the US that persisted through 2022 and early 2023, when the 12-month rolling death toll remained around 80,000.

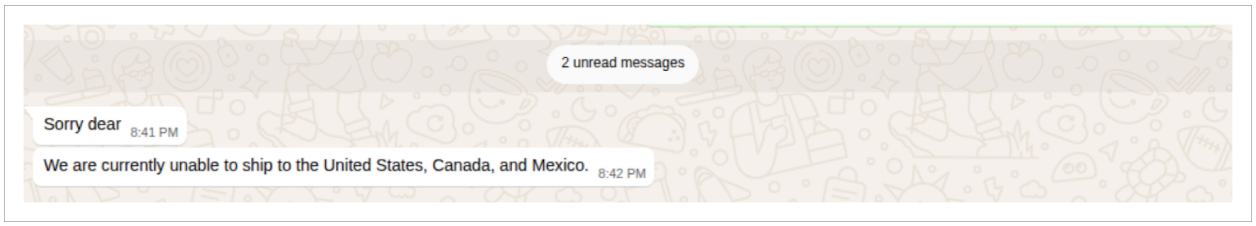
The U.S. Government then took several actions with China, including:

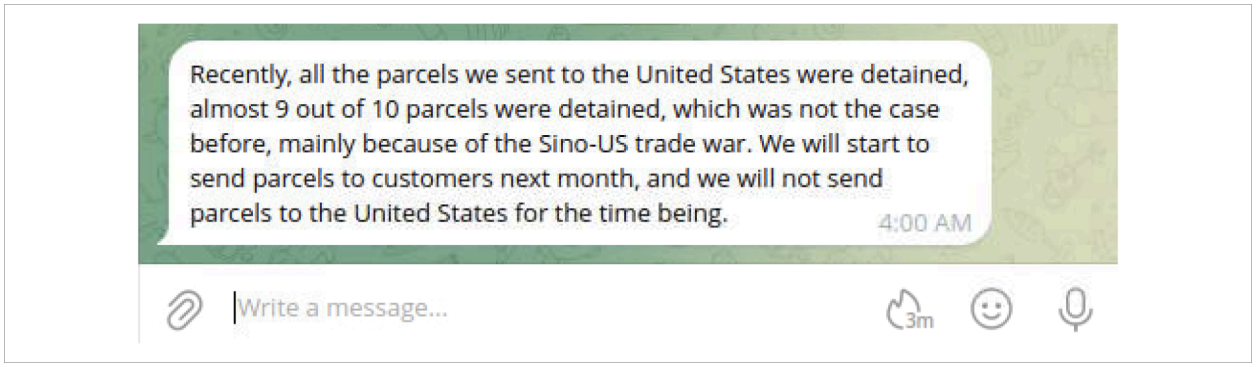
- October 2023: Sanctions and indictments against China-centric drug trafficking networks that used cryptocurrency to sell fentanyl precursors.
- November 2023: Former President Biden and President Xi Jinping announced the resumption of bilateral cooperation on counternarcotics and China's Office of the National Narcotics Control Commission published a notice urging caution in the selling of substances that could be used to produce drugs.
- January 2024: The two countries launched a bilateral working group.

In March 2025, China issued a White Paper stating that by June 2024, more than 140,000 advertisements and 14 online platforms had been taken down.

As seen on the following page, business-to-business websites that were once watering holes for brokers have strayed away from hosting listings of fentanyl-related chemicals (like sodium borohydride, which is on the DEA's Special Surveillance List due to its use as a reagent in fentanyl synthesis), and brokers have begun turning away customers in the US, Mexico, and Canada. For the chemicals that are finding their way in through US borders, brokers claim that those packages are now more likely to be seized, which adds to their hesitancy to engage with the US market.

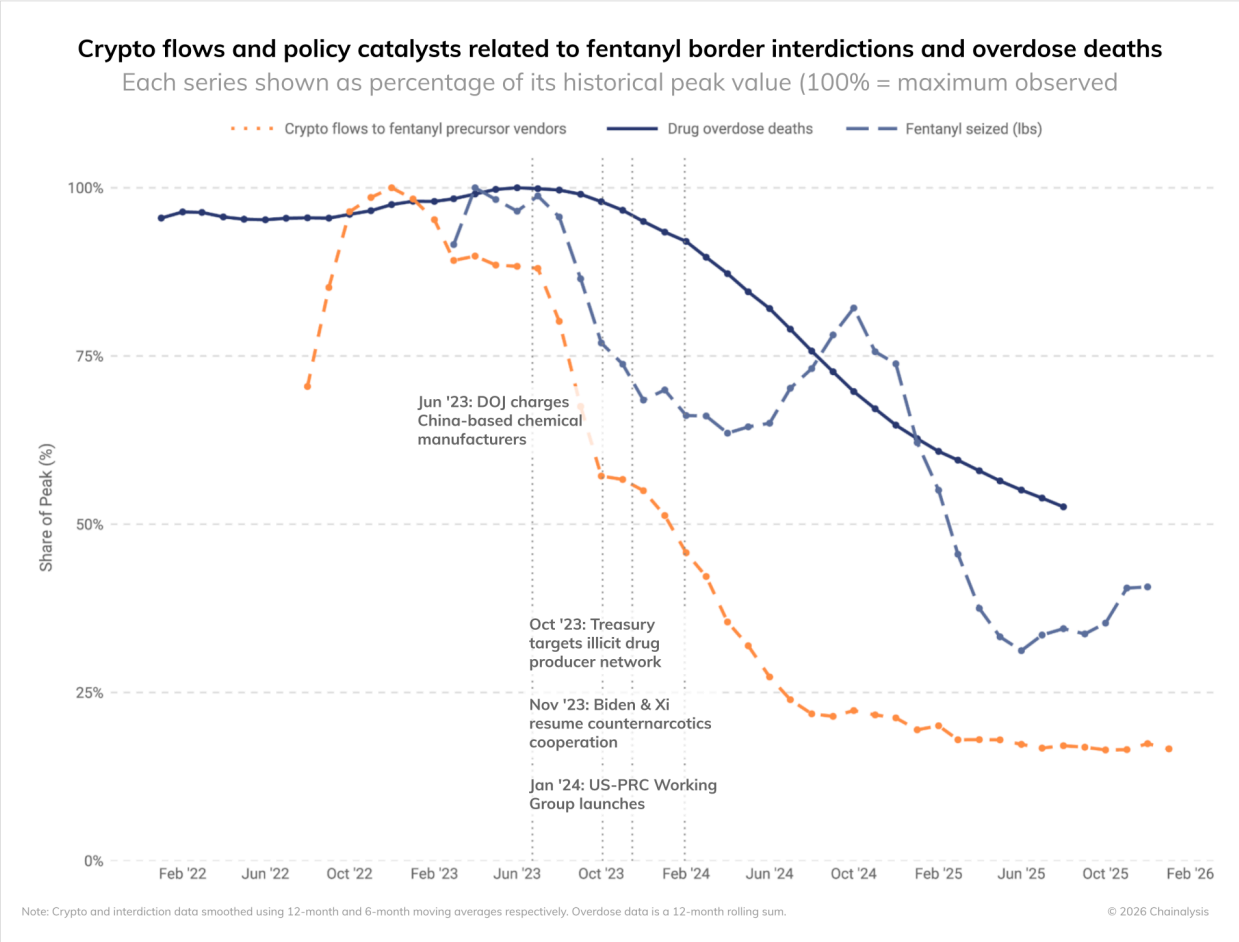






The key question, however, is whether these policy and enforcement actions translated into measurable changes in illicit supply. On-chain data can provide a compelling method to test that hypothesis in near real-time.

According to the Science article authors, it is challenging to determine whether a supply shock could account for a substantial part of the decline in deaths, because drug trafficking organizations operate clandestinely. They suggest that “developing and deploying more systematic methods for monitoring illicit drug supply chains... could improve the ability of law enforcement and public health authorities to detect and effectively address future supply shocks.”



More good news: because fentanyl supply chains operate to a large extent on crypto rails, we can gain actionable insights in real-time that are not always available through other sources. We can see that the sharp decline in crypto flows to fentanyl precursor vendors began in mid-2023, preceding the substantial drop in overdose deaths that became apparent in official statistics by late 2023 and continued throughout 2024. Disruptions to fentanyl precursor sales – which reflect the fact that many fentanyl precusor vendors either went dark, delisted fentanyl-related chemicals, or ceased shipment of such chemicals to the US – as well as a decrease in border interdictions, point to a meaningful disruption of the fentanyl supply chain at the precursor procurement stage.

We reached out to the authors of the Science article with our analysis and they shared: "The Chainalysis study adds an important additional indicator that a decrease in Chinese fentanyl precursors contributed substantially to the decline in fatal opioid overdoses. That the decline in crypto flows to fentanyl precursor vendors starts just before the downturn in deaths is also consistent with this hypothesis, since the flow of fentanyl into the US lags precursor payments."

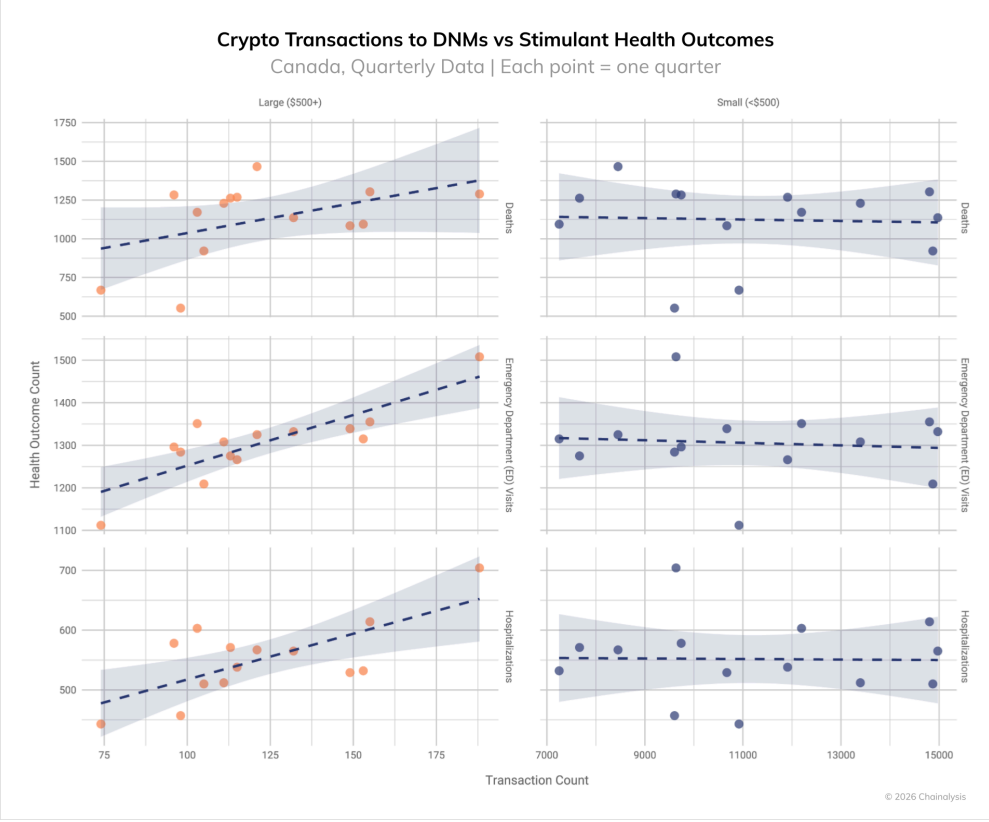
Indeed, this dramatic correlation suggests that monitoring crypto flows could potentially provide 3-6 months of advance warning for changes in overdose trends long before patient data are collected, indexed, and processed by public health authorities.

This good news, though, may not last. Supply disruptions are often fleeting, and as long as demand persists, and synthetic drug manufacturing remains a profitable alternative to agriculturally cultivated substances like heroin, trafficking organizations can adapt to supply shocks and find workarounds. In terms of non-fentanyl related synthetic drugs, precursors for methamphetamine, MDMA, and cannabinoids are still being advertised by brokers and shipped worldwide. Interdictions of methamphetamine at the southern border doubled in 2025, which further illustrates that trafficking organizations are prompt in their pivoting to the next-best profitable alternative.

China could change its posture on counter-fentanyl enforcement, against the backdrop of a range of other hotly contested geopolitical issues. Vendors in other countries, like India, could step in to fill the supply gap. Pre-precursors, and other basic pharmaceutical building blocks, could remain uncontrolled due to their many legitimate uses, which means that cartels could construct more sophisticated labs that can support the advanced synthesis required to manufacture fentanyl from these basic chemicals. And as such, government agencies and public health experts may seek data for monitoring drug markets and supply, not just drug use and deaths. And as more economic activity moves on chain – both illicit and legitimate – use cases for real-time transaction data will grow.

Transaction size separates personal use from stimulant distribution

For another example of the potential predictive power of crypto data, we turn to Canadian health data.



We analyzed the relationship between crypto flows to darknet markets and public health outcomes (ER visits, hospitalizations, and deaths). The data tells two very different stories depending on the size of the transaction:

- Small Transfers (<$500): There is no relationship between small payments and health outcomes. The trend line is flat.
- Large Transfers (>$500): There is a strong, positive link between these flows and negative health outcomes. As money flows increase, stimulant-related hospitalizations and ER visits rise.

So, what's going on here and why does it matter?

Mechanically, it is likely that transfers in excess of $500 represent larger purchases intended for either heavy personal use or redistribution. Whether this volume is consumed by the buyer or dispersed to others, the presence of this quantity in the community increases the probability of harm. This leads to more ER visits, more hospitalizations, and, tragically, more deaths within the quarter.

Just like the fentanyl example, money moves before the crisis hits. People buy drugs before they redistribute them, and users consume them before they overdose and require medical care.

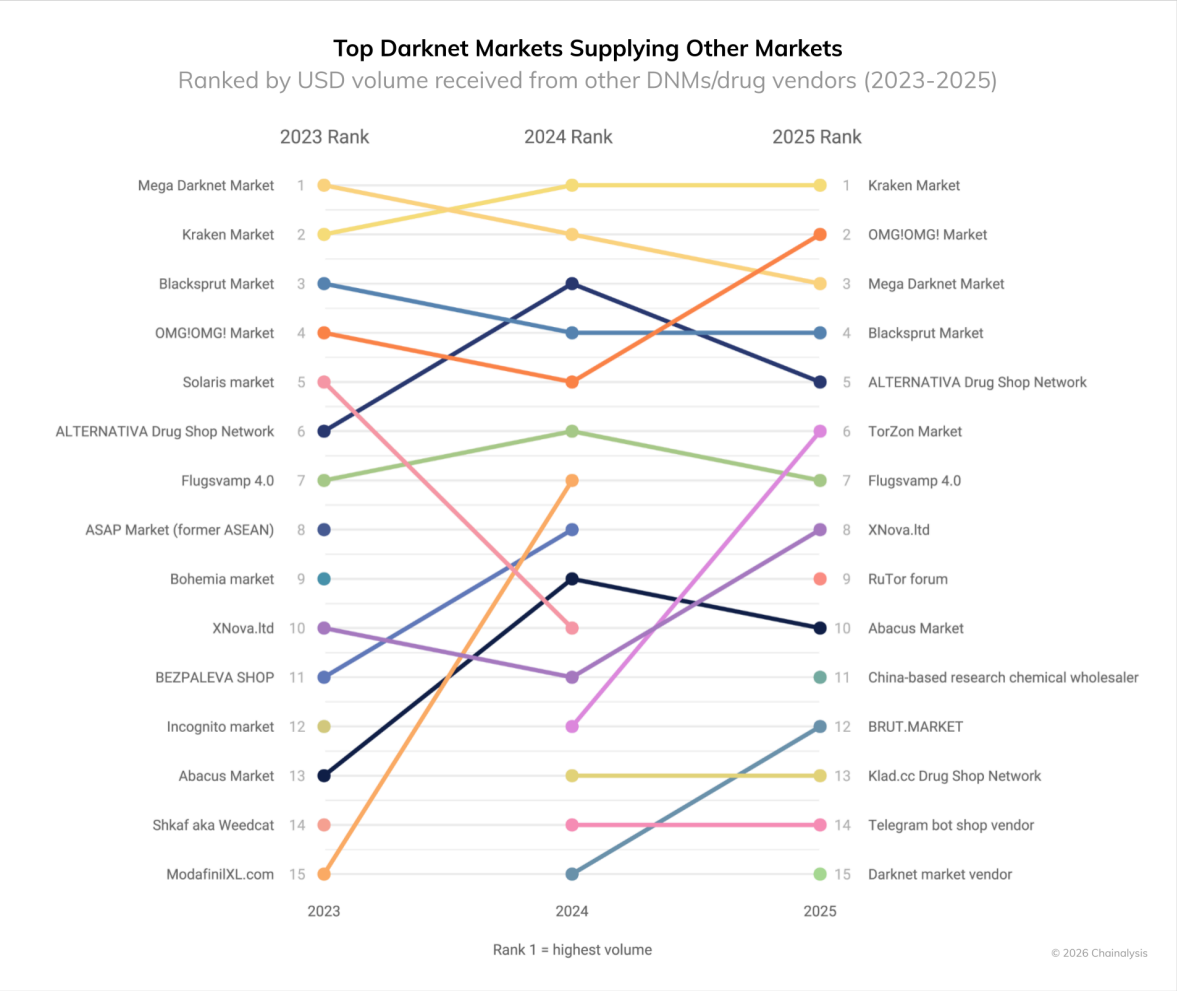
Because on-chain data is transparent and real-time, it can serve as a high-fidelity "early warning system." Public health agencies can use this data to predict spikes in hospitalizations months before they occur, allowing them to prepare rather than react. While these findings help explain downstream harm, they do not shed light on how drugs move through the darknet ecosystem itself. To understand that, we examine how markets source from one another.

Darknet markets function as interconnected global supply network

One of the clearest signals of maturation within the darknet drug economy is the degree to which DNMs increasingly function as suppliers to other DNMs, rather than solely as retail endpoints.

By ranking markets based on inbound flows from other DNMs, we can identify “anchors” that serve as upstream suppliers within the ecosystem. In 2025, a small number of markets accounted for a disproportionate share of these inter-market transfers.

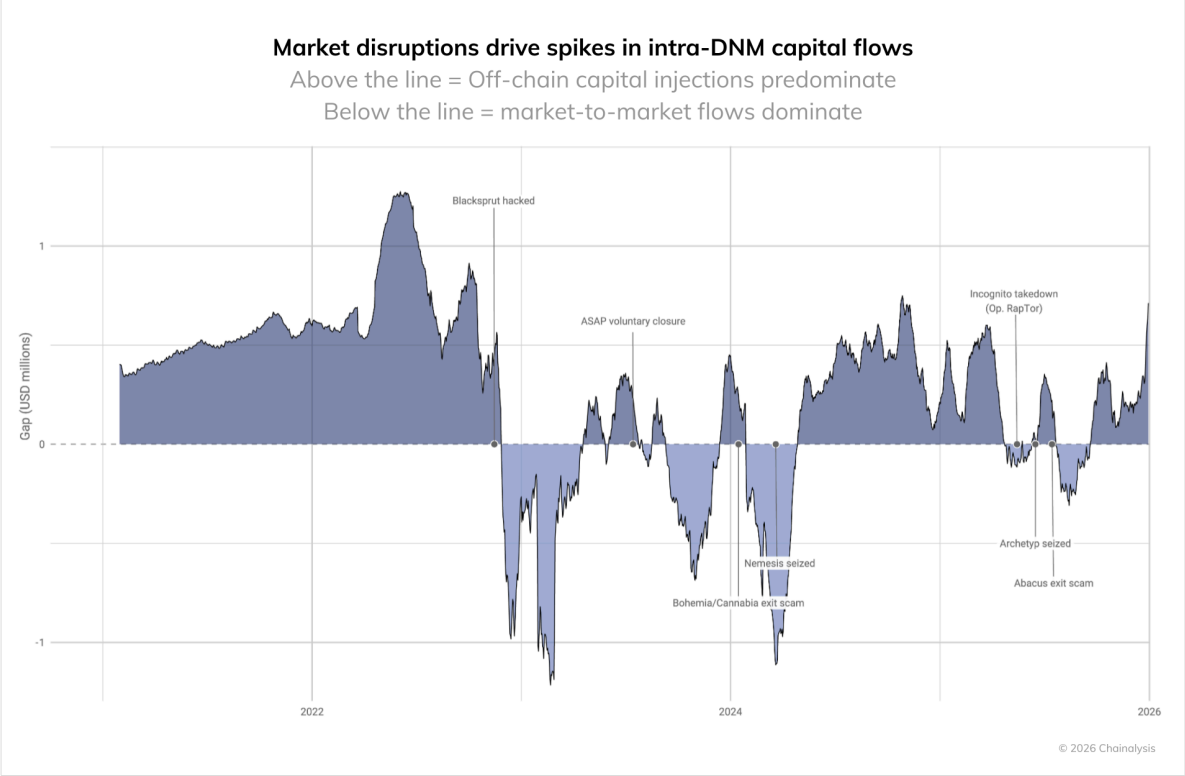
Rather than operating in parallel silos, markets are increasingly interconnected through wholesale relationships. Following the closure in July 2025 of Abacus Market, the largest bitcoin DNM for customers in the West, TorZon emerged as the dominant Western-facing DNM, effectively serving as its primary successor. In terms of supplying other markets, TorZon also ascended past western darknet markets of years past, which marks a notable shift. Russia-focused DNMs remain highly active, particularly in synthetic drug distribution, and while TorZon is not operating in the billion-dollar range like Russian markets such as Kraken, OMG!OMG!, Mega, or Blacksprut, it now occupies a central position in the inter-DNM supply network, thus putting it in the same strata.



This evolution coincides with broader changes in drug production and distribution. Western European drug services are increasingly adopting vertically integrated models, engaging more directly in production and upstream supply chains — patterns we are now observing in crypto transaction data. In Operation Fabryka, the largest-ever operation against synthetic drugs, law enforcement and judicial authorities in Belgium, Czechia, Germany, the Netherlands, Poland, and Spain shut down 24 industrial-scale "superlabs," as demand for synthetic amphetamines has continued to rise in Western Europe and Russia. Drug traffickers see the opportunity to maximize profits by investing in localized synthetic drug production (as opposed to relying exclusively on foreign suppliers), and law enforcement is cracking down.

Disruptions are triggering capital flight and resupply

One consistent trend over time has been that market disruptions consistently produce short-term moves toward capital flows between DNMs, reflecting both resupply activity and user migration. When a major market is shut down, voluntarily closes, or is otherwise compromised, vendors often turn to other DNMs to replenish inventory or re-establish distribution channels. This behavior is visible in sharp increases in DNM-to-DNM transfers following major events.



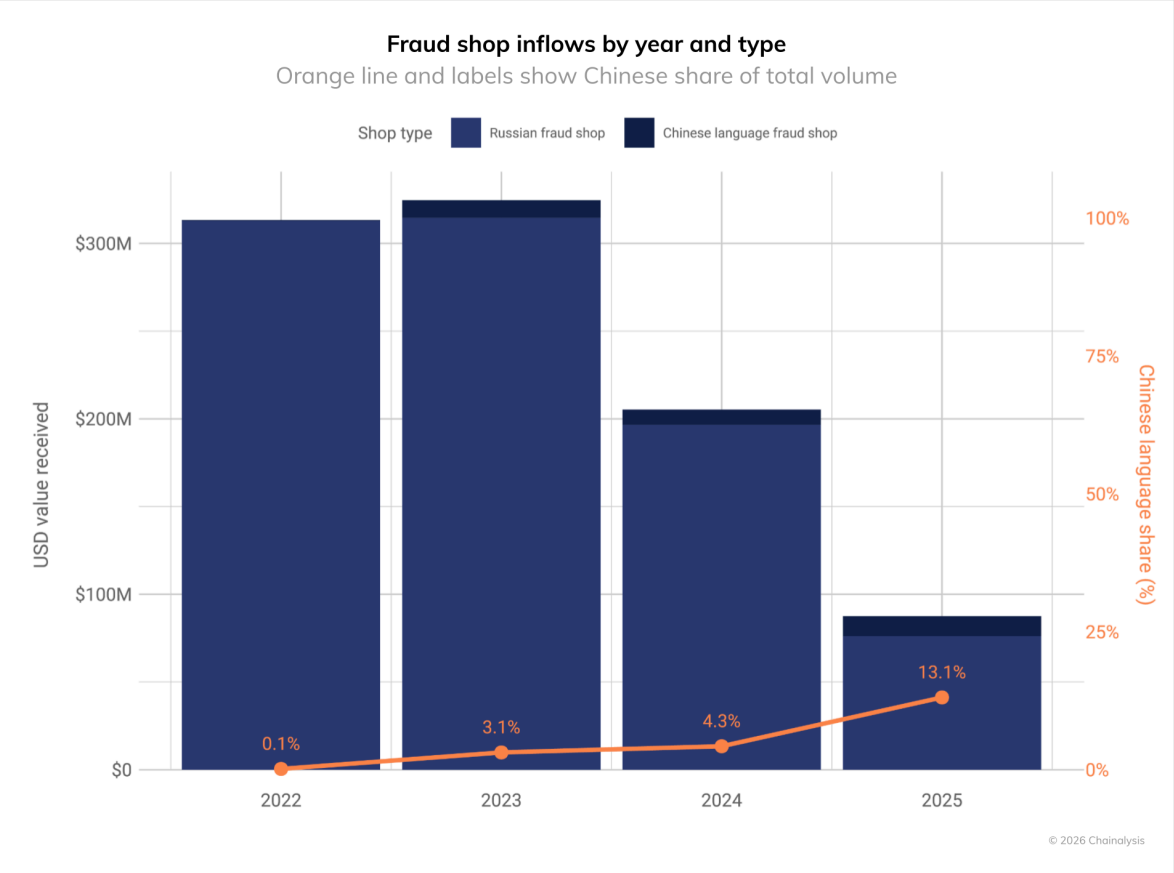
For example, after the Blacksprut hack in November 2022, which preceded the earlier shutdown of ASAP Market, we observed an immediate and substantial increase in inter-DNM sending, with the gap in net flows swinging from roughly $500,000 in favor of off-chain originating inflows to nearly -$1 million in the direction of intramarket flows. These spikes likely reflect a combination of vendor resupply, consolidation of funds, and precautionary movement of assets in anticipation of further disruptions.
At the same time, the dominant source of inflows into DNMs remains centralized exchanges, particularly in periods of relative market stability. These flows are consistent with retail purchasing behavior, where individuals acquire crypto — often via compliant exchanges — and send funds directly to DNM addresses to purchase illegal drugs.

Taken together, the DNM ecosystem continues to demonstrate both resilience and increasing structural sophistication. While individual markets rise and fall, underlying activity persists through vendor migration, inter-market resupply, and shifting payment behaviors rather than disappearing altogether. As a result, headline transaction volumes offer an incomplete picture; the greater analytical value lies in the visibility on-chain data provides into how illicit markets respond to disruption, enforcement pressure, and changes in global supply chains.

DNMs are no longer best understood as isolated retail platforms, but rather as interconnected nodes within a broader illicit supply network. Inter-DNM transfers and short-term capital movements following disruptions reveal in near real-time how supply chains adapt. Blockchain data provide an invaluable window into these dynamics, equipping analysts to identify shifts, emerging relationships, and downstream effects that can be difficult to observe otherwise — insights that will remain critical as DNMs continue to evolve.

Fraud shops contract amid enforcement, but Chinese-language networks emerge as new wholesale powerhouses

Fraud shops — markets specializing in stolen payment data, credentials, and forged documents — saw on-chain volumes plummet from approximately $205 million to $87.5 million year-over-year. This sharp contraction stems largely from successful law enforcement actions targeting key infrastructure nodes, including the takedown of payment processors like the Universal Anonymous Payment System (UAPS) and laundering services like Cryptex. These disruptions have severely hampered the liquidity and operational capacity of the traditional, largely Russia-facing ecosystem, which now exhibits smaller, more frequent transfers suggestive of a fragmented retail clientele.



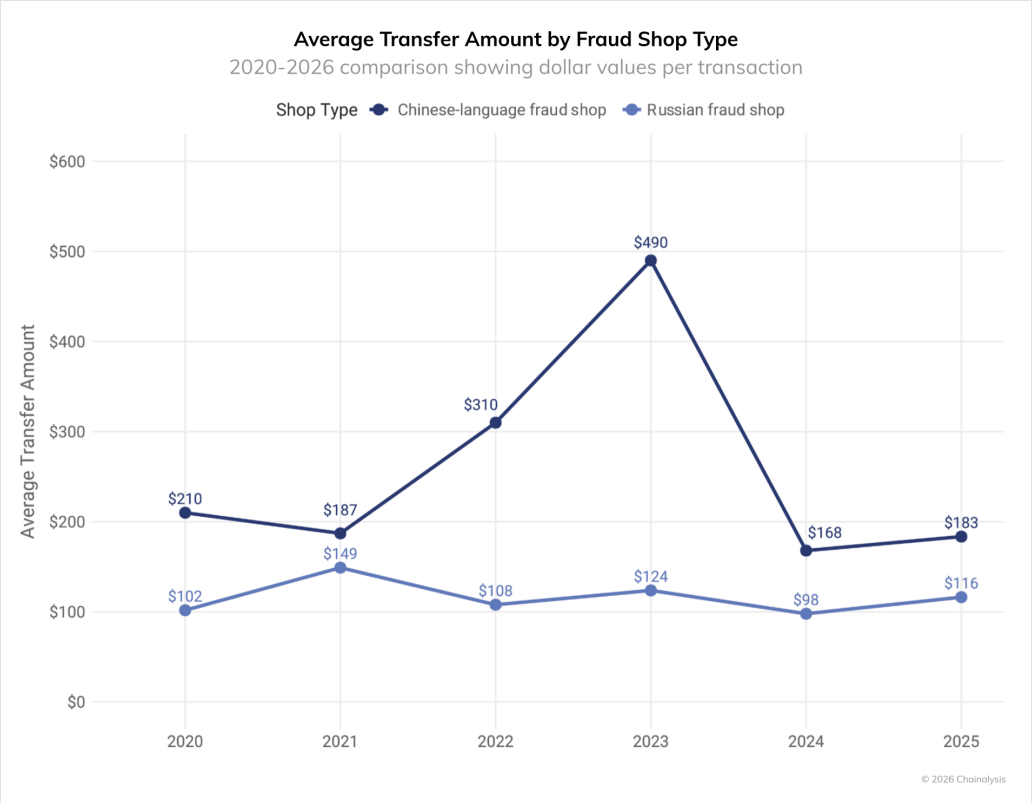
Despite these disruptions, there is still an increased pivot to custodial merchant services. It is critical to note that on-chain data of independent fraud shops operating their own wallet infrastructure only offers a partial view into the overall ecosystem, as official metrics do not capture activity that flows into broader custodial services that facilitate payments for many different types of threat actors. Another example of such a service is Sellix, which was dismantled through global law enforcement action in Operation Talent. On top of providing a payment gateway to Cracked and Nulled forums (also targeted in the Operation), they provided merchant services to fraud shops like zyzzmarket and BestCombo, as well as CSAM sites and infrastructure services. Use of a payment processor can provide “exposure laundering” to threat actors, who want to hide in the weeds of a larger service.

However, as Russian-language shops struggle, a distinct and formidable alternative has emerged: Chinese-language Telegram-based fraud networks. These entities represent a shift toward a wholesale operational model, specializing in bulk sales of compromised credit card data.

Unlike their Russian counterparts, Chinese-language shops tend to process significantly larger average transfers, indicating a focus on high-volume, B2B-style criminal transactions. With some Telegram channels boasting tens of thousands of members and offering automated English translations, these networks signal that the fraud economy is not just facing a contraction, but restructuring—moving away from traditional web-based markets toward resilient, wholesale-focused social platforms.

The screenshot below shows that for one of the many Telegram channels geared toward credit card sales, there are nearly 27,000 members. While these Telegram channels are in Chinese, the Telegram bot shops themselves often offer English translations.

Chinese-language Telegram fraud shops tend to process larger average transfers than those of Russian-language fraud shops, consistent with bulk sales of compromised payment data and wholesale-style transactions. Russian-language shops, by contrast, continue to exhibit smaller, more frequent transfers suggestive of a retail clientele.



Why visibility, not volume, matters most

Taken together, these patterns demonstrate something larger than a story about drugs or public health alone. They show that blockchain transaction data can function as a real-time barometer of illicit economic activity — one that consistently surfaces meaningful signals, sometimes months before they are visible through other reporting systems. Whether tracking fentanyl supply shocks, shifts in trafficking routes, or the downstream effects of enforcement actions, crypto flows provide an upstream view of how illicit markets adapt, contract, or expand in response to real-world pressures.

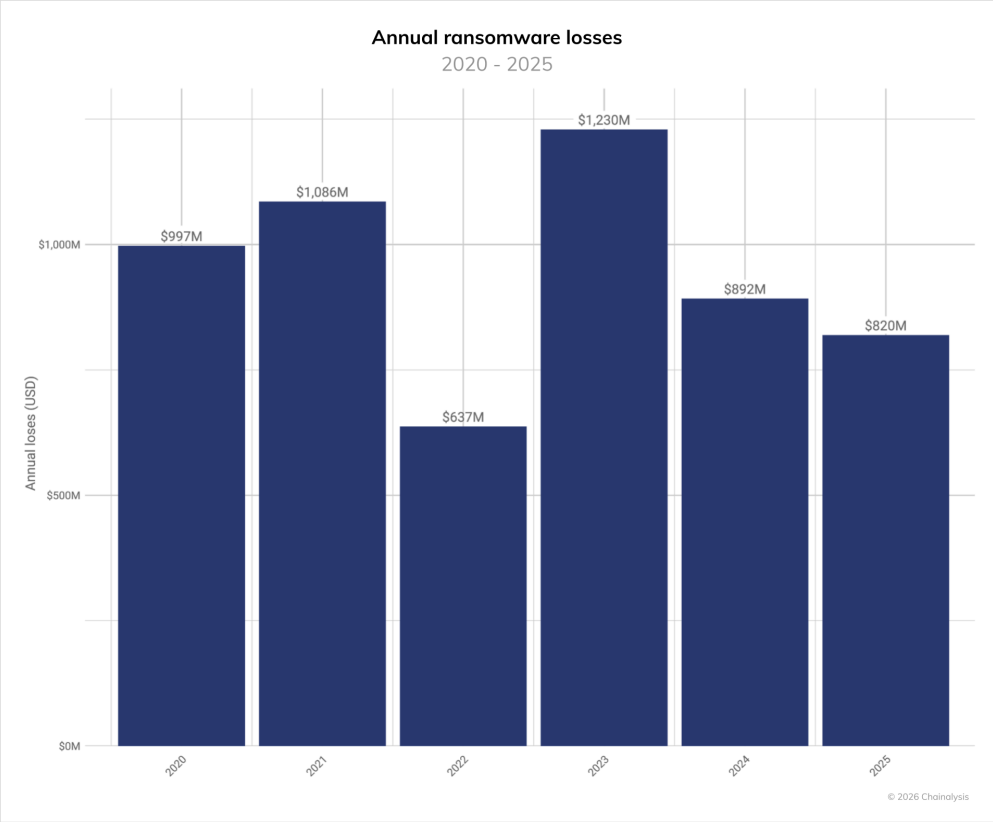
This is the strategic value of on-chain intelligence: it allows policymakers, enforcement agencies, and regulators to move from retrospective analysis to forward-looking insight. Instead of waiting for overdose statistics, seizure data, or hospital admissions to confirm that a crisis is underway — or that an intervention has worked — blockchain data can offer an early read on whether supply chains are tightening, vendors are disappearing, or capital is moving elsewhere. In this sense, crypto flows can signal not only emerging threats, but also the success or failure of policy choices in real-time.

The infrastructure to operationalize this capability already exists. Chainalysis, through its blockchain analytics platform and unrivaled Data Solutions offering, enables governments, financial institutions, and public sector stakeholders to securely translate raw blockchain data into actionable intelligence. By integrating on-chain indicators into existing analytical and decisionmaking frameworks, agencies can better anticipate crises, evaluate enforcement outcomes, and allocate resources based on what illicit actors are doing — not just what has already happened.

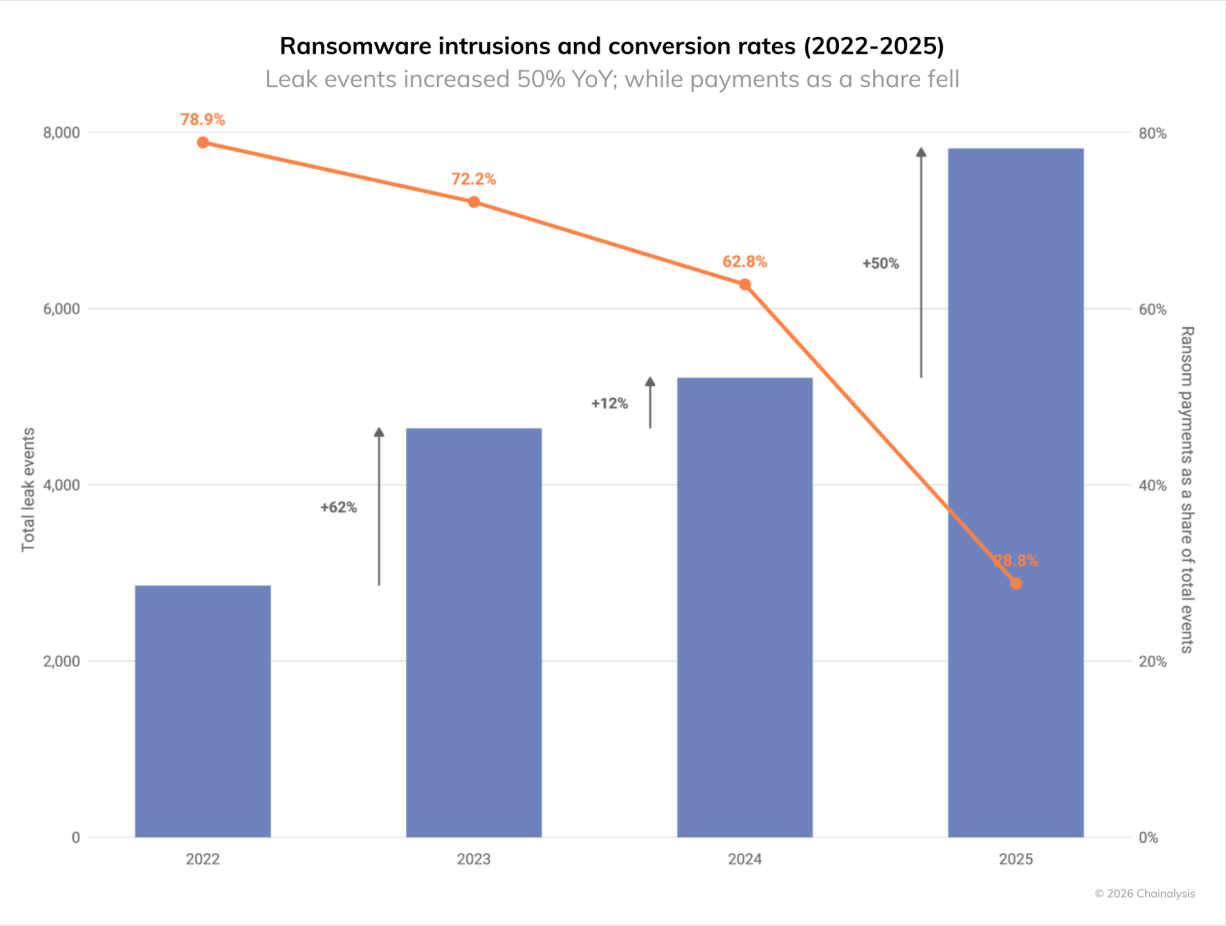
Total Ransomware Payments Stagnate for Second Consecutive Year, While Attacks Escalate

Ransomware today is best understood not as isolated attacks, but rather as an interconnected marketplace of access, infrastructure, and monetization services. In 2025, total on-chain payments remained relatively stagnant even as claimed attacks increased and median ransom sizes rose. At the same time, coordinated law enforcement actions and sanctions increasingly targeted the infrastructure layer — including bulletproof hosting providers — increasing costs across both cybercrime syndicates and state-linked actors.

In 2025, ransomware actors received more than $820 million in on-chain payments — an 8% decline year-over-year (YoY) from $892 million, our updated 2024 estimate. The 2025 total is likely to approach or exceed $900 million as we attribute more events and payments, just as our 2024 total grew from our initial $813 million estimate this time last year.



Despite the relative stability in total payments, ransomware attacks surged across multiple vectors in 2025, with eCrime.ch data showing a 50% YoY increase in claimed ransomware victims, marking the most active year on record.



This divergence — more claimed attacks, but fewer aggregate payments — reflects complex forces shaping the ransomware economy:

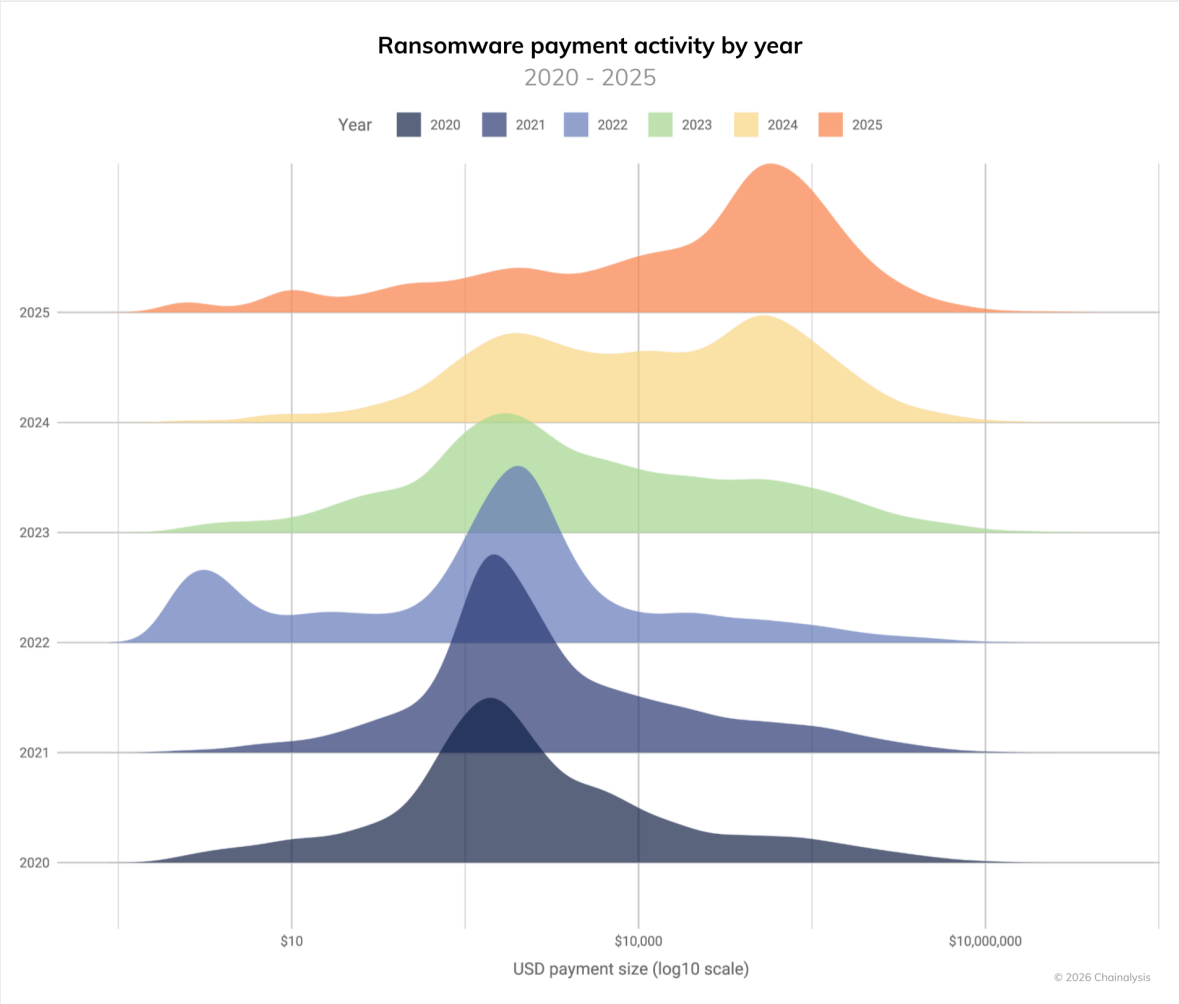
- Improved incident response and increased regulatory scrutiny have helped reduce payout frequency.
- Effective international action against ransomware operators, infrastructure, and laundering networks has constrained some revenue flows.
- In some cases, the introduction of strains like VolkLocker, notable for a cryptographic weakness that allowed free decryption in some cases, illustrates how technical vetting by defenders can occasionally disrupt a ransomware strain.
- Marked fragmentation of major ransomware-as-a-service (RaaS) operations and decreasing centralization in the ransomware market have led to a proliferation of smaller, independent ransomware actors, with some analyses tracking as many as 85 active extortion groups.

The shift from a large handful of dominant strains to a more decentralized and volatile landscape has made attribution, response, and long-term tracking as important as ever. According to the founder of eCrime.ch, Corsin Camichel, “We're seeing a structural shift in targeting: fewer large, headline-grabbing intrusions and more volume focused on small and medium enterprises. The assumption is simple — smaller victims pay faster. However, Chainalysis' data shows payments trending downward despite an all-time high in public claims. That divergence is important. It suggests attackers are working harder for diminishing returns.”

This overall trend is a major win against the ransomware ecosystem. Fewer victim payments mean more work for less for attackers, an important step in shifting the economic incentives.

Median ransom payments and shifting extortion tactics

While total payments flatlined, media payment sizes increased significantly in 2025. In particular, the median payment increased 368%, from $12,738 in 2024 to $59,556 in 2025. This dynamic mirrors reports from incident response firms that median payouts more than doubled in certain quarters.



High-impact incidents shaped the ransomware landscape

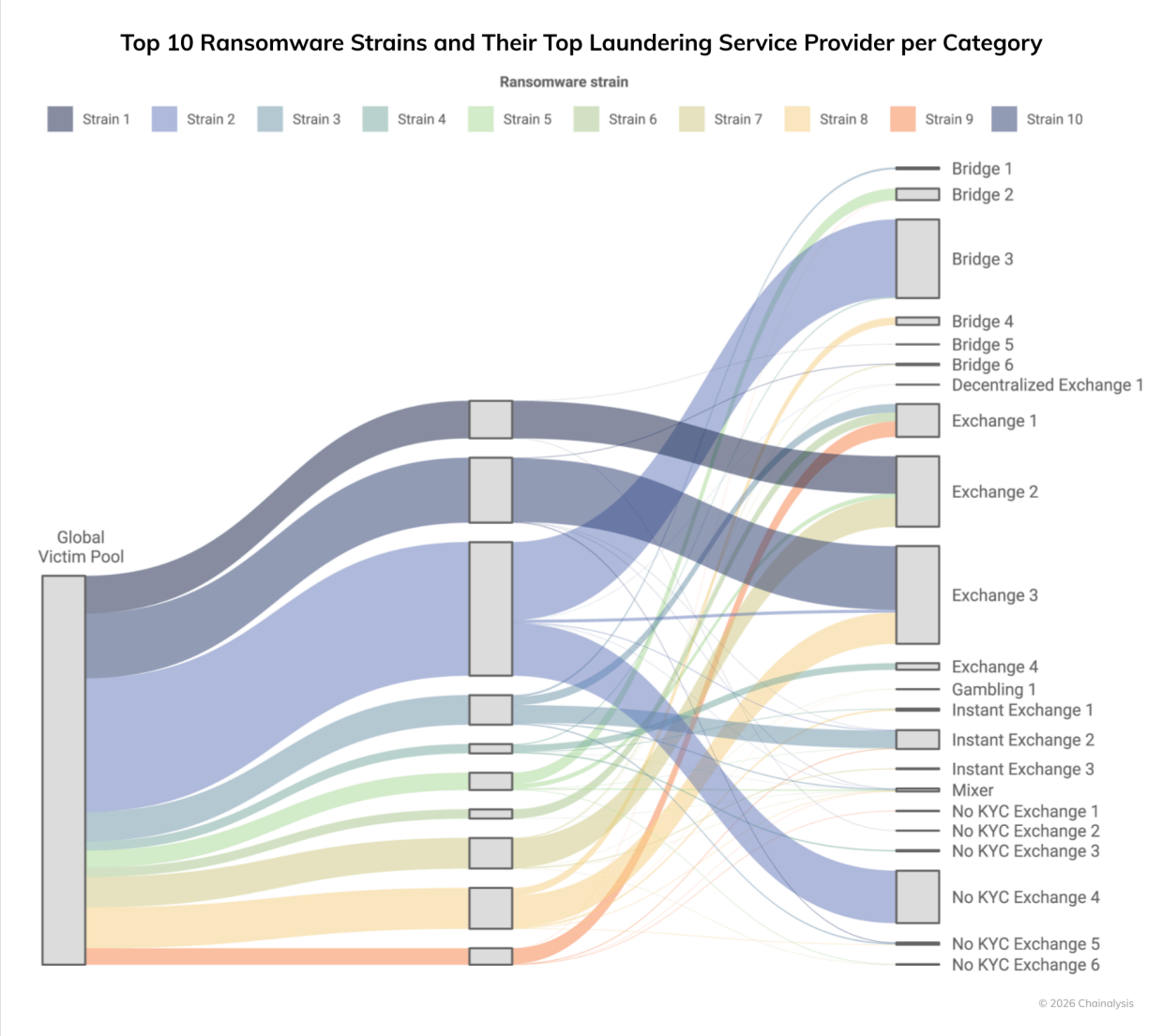
Several widely publicized trends – from zero-day exploits to social engineering – made 2025 another devastating year for ransomware's global scale and impact:

- One of 2025's most economically disruptive cyber events was the cyberattack on Jaguar Land Rover, which halted production lines across multiple countries and inflicted an estimated £1.9 billion (approximately $2.5 billion) in economic damage, the costliest cyber event in UK history.
- Retail and services sectors also felt ransomware's impact. Major British multinational retailer Marks & Spencer grappled with prolonged disruption after a breach by the Scattered Spider ransomware group forced extended operational outages and wiped hundreds of millions of pounds of market value.
- Healthcare providers remained lucrative targets. For example, kidney dialysis company DaVita Inc. experienced one of the most serious healthcare ransomware breaches, resulting in the exposure of almost 2.7 million patient records and substantial loss of allegedly 1.5 TB of clinical data.

Beyond individual companies, mass exploitation events continued to illustrate ransomware's reach. For example, Cl0p leveraged a zero-day exploit in Oracle E-Business Suite to orchestrate widespread enterprise extortion campaigns that affected hundreds of organizations.
Ransomware actors remain highly opportunistic. They do not consistently favor a specific sector at a given time of year. Instead, they exploit exposed services and misconfigurations as they arise, and capitalize on newly disclosed vulnerabilities.

Fingerprinting Strains by Financial Behavior

By isolating the primary laundering channels for the top 10 ransomware strains of 2025, we can begin to "fingerprint" these groups based on their distinct on-chain signatures. While the malware they deploy may share code or builders, their exit strategies reveal unique operational preferences.



This divergence across strains allows investigators to distinguish between groups based not only on their attack, extortion, and negotiation TTPs, but also their on-chain behavior. We can also track ransomware actors who work with multiple strains based on their unique laundering patterns.

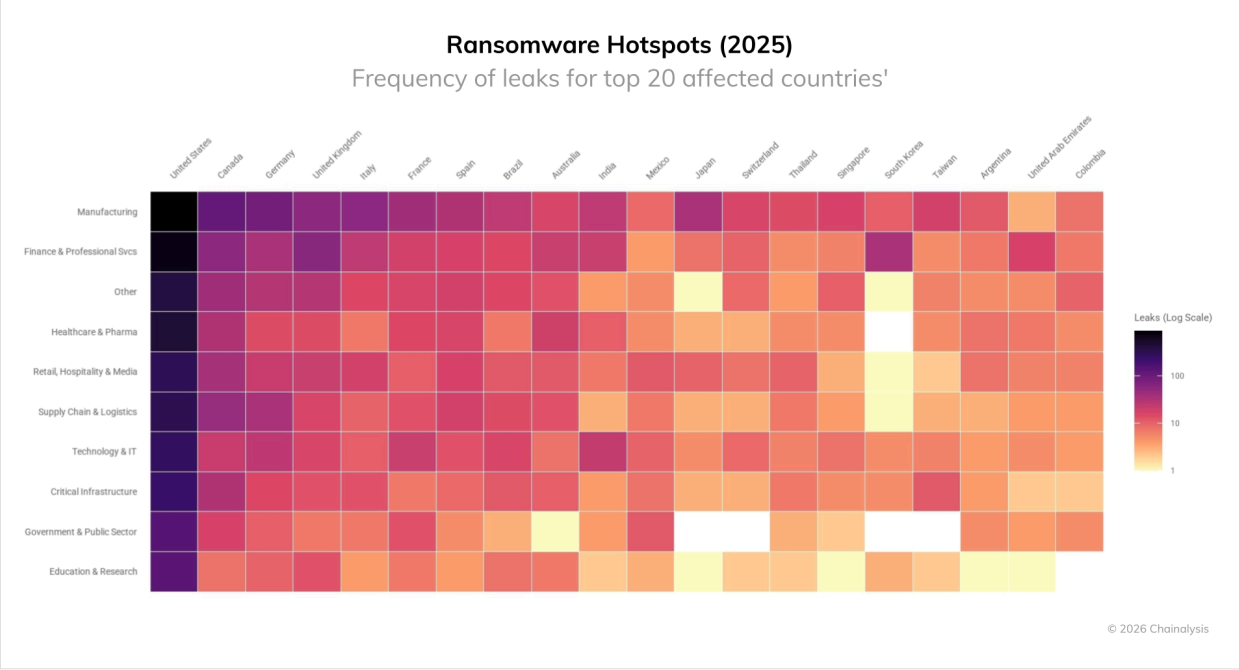
Leak site activity underscores geographic concentration

Analysis of leak site disclosures throughout 2025 shows continued disproportionate geographic concentration in developed economies. Data leak site-claimed ransomware incidents grew by 50% YoY — an all-time high.

Among the countries for which there is a clear geographical tag, the United States remains the most heavily targeted jurisdiction, followed by Canada, Germany, the UK, and other parts of Europe. Manufacturing and finance/professional services were the most heavily compromised in most of these jurisdictions, with Canada and Germany having a particularly high compromise rate within supply chains, logistics and critical infrastructure.

One important caveat is that not all data leak site claims are legitimate. Furthermore, data leak site posts may mean that a party has been victimized, but not necessarily that they failed to pay. Incident response firm Arete told us, “This year, we saw several groups reposting old victims or posting victims from other groups’ data leak sites, which skewed data leak site posting rates. However, we continue to see fewer victims making ransom payments as the adoption of security best practices improves, including better backups and the use of security technologies like endpoint detection and response, which disrupt threat groups before they can fully achieve their objectives.”

Arete elaborated that some threat groups responded to this decrease in payments by becoming more aggressive during negotiations, which has included contacting employees and even customers of victimized organizations. Other groups responded by focusing on data exfiltration and even analyzing exfiltrated data to identify what was stolen. By analyzing the exfiltrated data, the threat actors can make more specific threats about the consequences of data exposure.

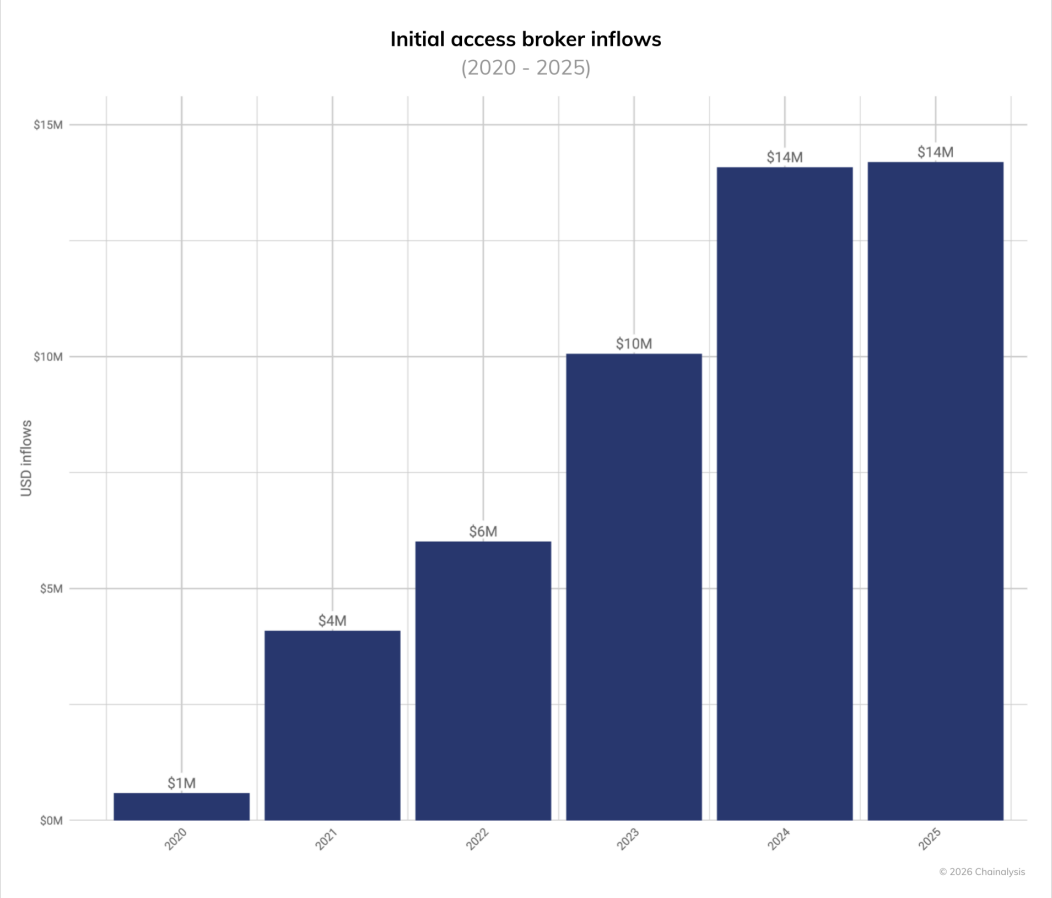


Not only was the United States hit heavily across sectors; every sector saw increased targeting YoY. Claimed victims from critical infrastructure, supply chains and logistics, and government increased YoY by between 45% and 56%. In other words, the United States is the most targeted nation globally, and the rate of intrusions has increased significantly relative to 2024. Ransomware actors continue to view U.S.-based organizations as high-value and high-liquidity targets.

The ransomware supply chain: initial access brokers (IABs)

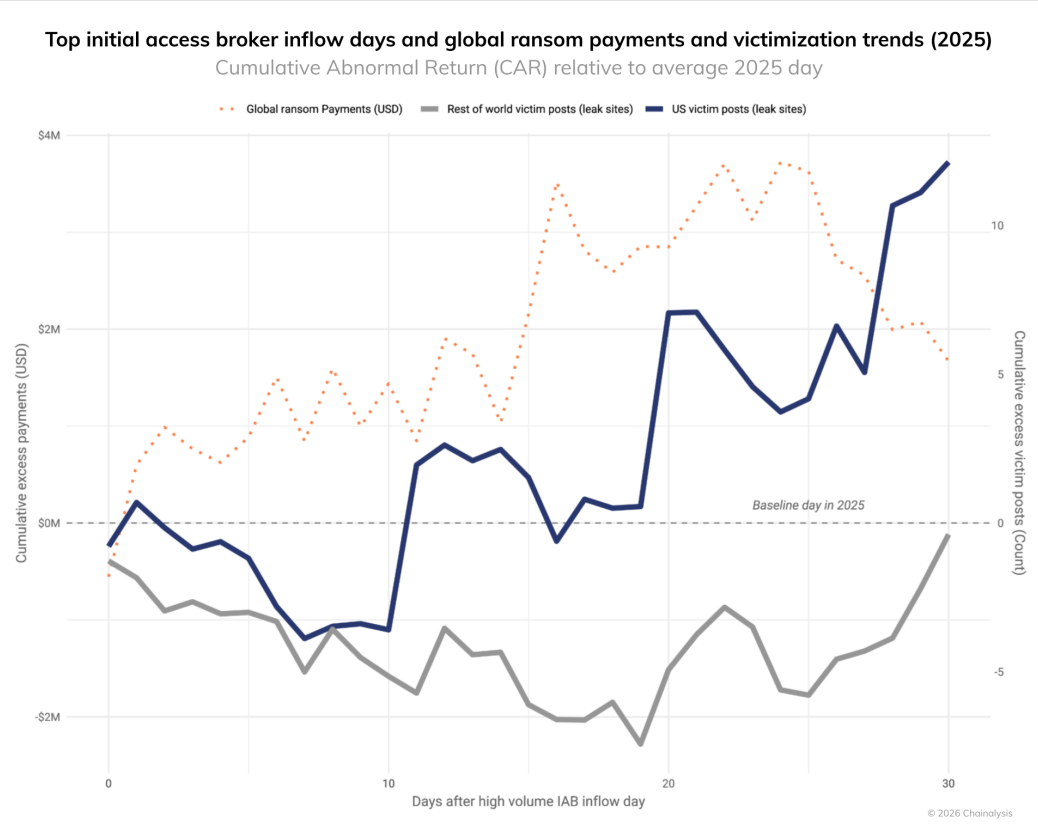
Ransomware does not occur in isolation, but rather is supported by a broader cybercrime supply chain, including Initial Access Brokers (IABs) and other specialized services. As their name suggests, IABs facilitate entry to compromised networks, enabling affiliates to deploy ransomware with relative ease.

The size of this enablement ecosystem is increasing over time. In 2025, we estimate that IABs received at least $14 million in on-chain payments — roughly flat YoY, although we expect this total to grow as attributions improve. Although modest relative to ransomware totals, this figure represents a critical enabling function. Total ransomware payments of approximately $820 million in 2025 represent nearly 58 times the value flowing to IABs, suggesting a substantial return on investment within this segment of the cybercrime supply chain.



It is important to note that not all IAB payments are made by ransomware operators. IABs certainly trade and buy access among themselves and some malicious actors have TTPs and objectives other than ransomware. Another important caveat is that not all ransomware incidents can be traced to IABs — there are a number of different ways to gain access to victim networks. With those caveats in mind, we can draw a connection between criminal investments and the ransomware attacks that follow.

Looking 30-days out from sizable IAB payment inflow events (days within 2025 in the top 25% of all days), we see a significant effect on both global ransomware payments and claimed US victims totals as measured by leak site posts. The chart below plots the cumulative abnormal returns relative to the average day in 2025, and shows an almost immediate and sizable growth in abnormal global ransomware payments (more payments than expected). And, after around a 10-day lull, a similar growth in leak site posts about US victims.

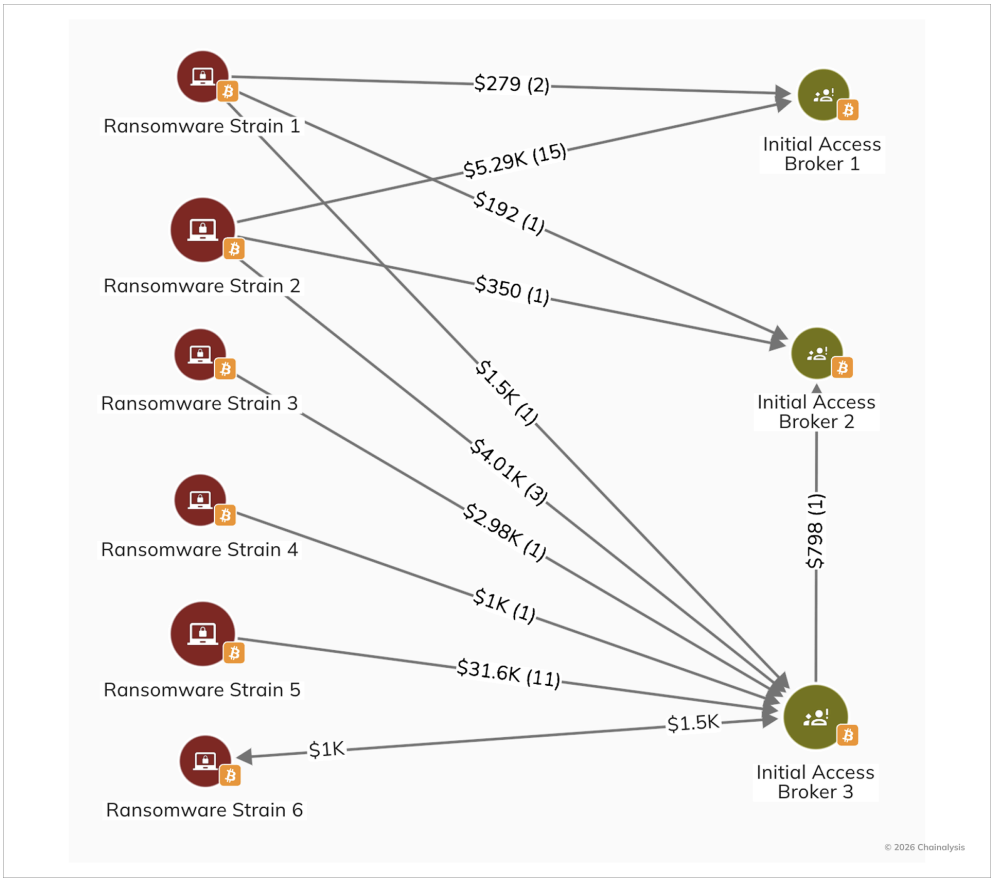


Cybercrime prevention firm Darkweb IQ told us that, from Q1 2023 to Q1 2026, the average price for victim access declined from approximately $1,427 to $439. This drop reflects a market characterized by more competitive pressure and automation as the core shaping force. “We are seeing industrialized access pipelines, AI-assisted tooling, and a proliferation of infostealer logs that lower the barrier to entry, which has resulted in an oversupply of cheap but operationally constrained inventory that floods the market and depresses pricing. While average pricing has declined due to increased volume and automation, validated, high-privilege enterprise access (e.g., domain-level control) still commands premium pricing, indicating a bifurcated and still competitive market.”

Month	Privately offered access (count)	YoY change (as stated)	MoM change
2025-01	646	+114%	–
2025-02	614	+117%	-32
2025-03	621	+201%	+7
2025-04	739	+278%	+118
2025-05	725	+87%	-14
2025-06	1,127	+154%	+402
2025-07	1,019	+48%	-108
2025-08	860	+41%	-159
2025-09	715	+1%	-145
2025-10	706	+37%	-9
2025-11	460	-35%	-246
2025-12	641	-76%	+181
2026-01	675	+4%	+34

Growth in privately offered access YoY; Source: Darkweb IQ

We can also visualize these trends on-chain, as shown in the Reactor graph below. This example illustrates both the varying prices of access being purchased by ransomware strains over time and the fact that IABs are also frequently purchasing access from other IABs.

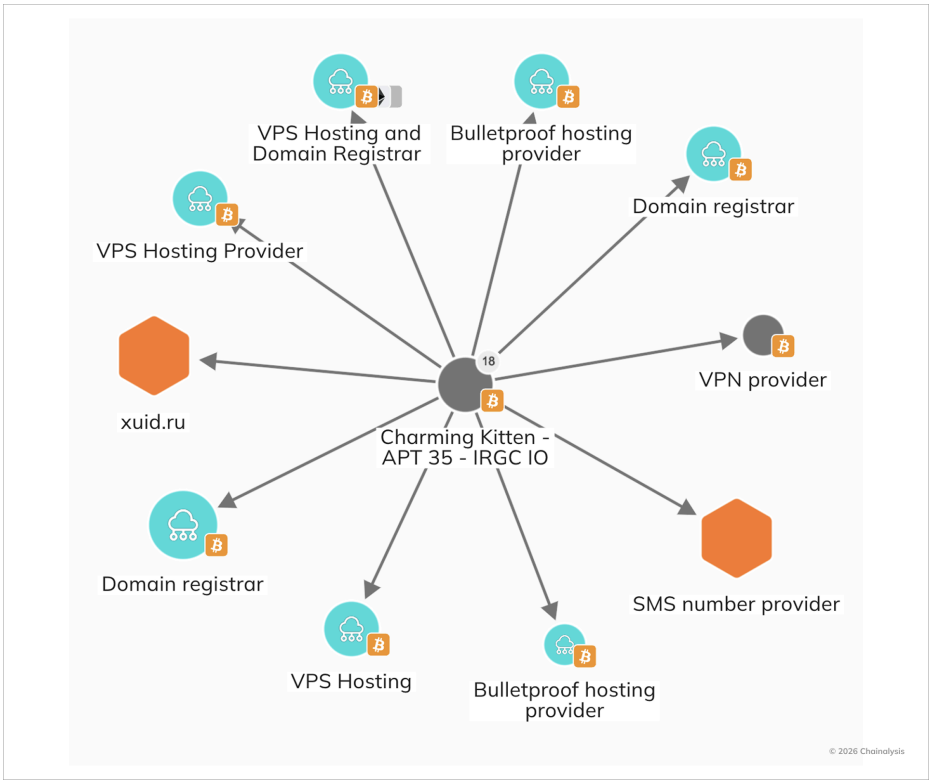


Emerging tools and frameworks hint at a future where automation not only influences price, but also accelerates compromise and extortion cycles. For example, researchers documented ransomware groups experimenting with AI-driven negotiation interfaces in mid-2025, mirroring developments in the AI-enabled scam ecosystem.

Infrastructure enables both criminal syndicates and state-linked threat actors

Ransomware infrastructure — including bulletproof hosting and residential proxy networks, and malware loaders— is not used exclusively by financially motivated criminal syndicates nor exclusively used for criminal aims. The same service-based ecosystem also supports state-linked threat actors conducting espionage, influence operations, and financially motivated campaigns.

According to data leaked in 2025, Iran-linked cyber threat actors, including groups commonly tracked as Charming Kitten, the espionage and influence operations focused branch of Iran's Islamic Revolutionary Guard Corps (IRGC) Intelligence Organization, continue to rely on commercially available hosting, proxy services, and compromised infrastructure to obscure attribution and blend into criminal traffic patterns. The increasing commoditization of access and anonymization services lowers the barrier between state and nonstate cyber operations, allowing espionage campaigns to operate within the same technical substrate as ransomware affiliates.



This blurring of lines is not unique to Iranian operations, as Russia- and China-linked actors similarly exploit these infrastructure layers to support both financial crime and state-sponsored objectives.

- In 2025, authorities sanctioned Media Land, LLC, also known as Yalishanda, a Russia-based bulletproof hosting provider associated with cybercriminal services. Sanctions targeting infrastructure providers — rather than individual operators alone — reflect a growing recognition that hosting and routing layers are force multipliers for ransomware and state-backed campaigns alike.
- Microsoft's disruption of the Russia-centric Lumma Stealer ecosystem further illustrates this convergence. While Lumma was widely used for credential theft in financially motivated campaigns, its infrastructure also enabled access brokering and downstream ransomware deployment. Targeting such tooling constrains both criminal monetization and state-aligned credential harvesting.
- As discussed in greater detail below, researchers also highlighted the role of Chinese proxy providers operating multiple residential proxy brands — including ABCProxy and 360Proxy — which offer large-scale IP rotation and anonymization services. These networks can be used to evade detection, conduct reconnaissance, and facilitate intrusion activity across both cybercrime and state-linked operations.

The overlap is significant: infrastructure providers can often advertise neutrality, serving any paying customer, although they may in some cases claim to ban CSAM. As a result, dismantling or sanctioning infrastructure nodes can generate cascading effects across ransomware affiliates, scammers, and state-aligned operators simultaneously.

This convergence reinforces a core dynamic of the modern cyber threat landscape: infrastructure is the strategic center of gravity. Disrupting it raises costs across the entire ecosystem — from extortion-driven syndicates to geopolitically motivated threat actors.

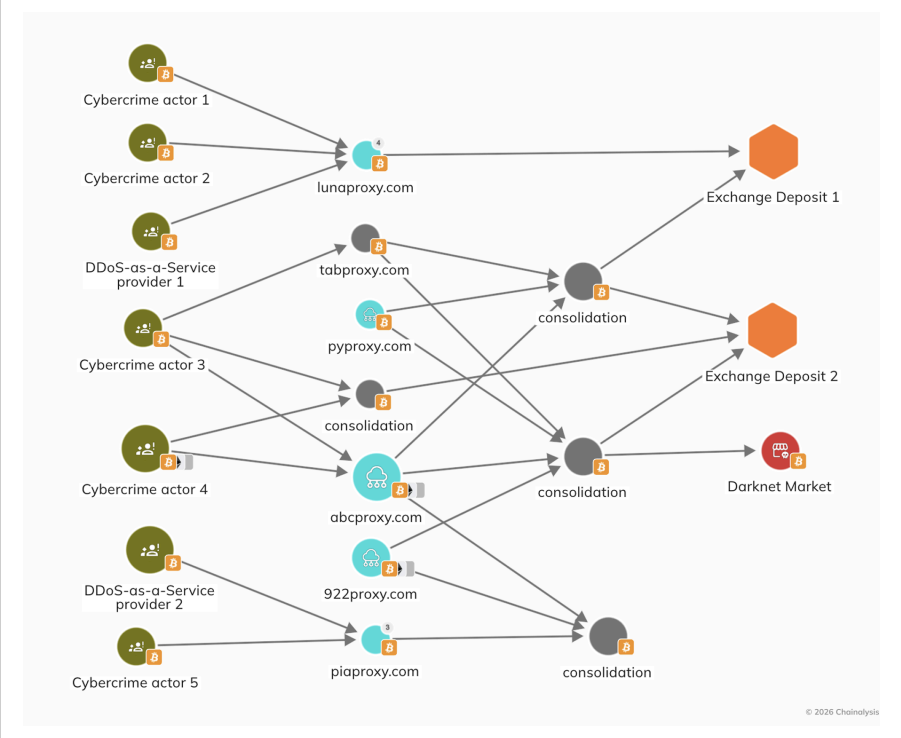
Public and private sectors making strides in disrupting ransomware's enablement layers

In 2025, the fight against ransomware moved beyond targeting specific gangs to dismantling the shared services that power the broader cybercrime economy. "Loyalty and brand names matter less than access, tooling, and negotiation capability. For defenders and policymakers, this creates a moving target — disruption of one group no longer guarantees meaningful ecosystem-wide impact. Increasingly, the most effective pressure points appear to be upstream: initial access brokers and the shared tooling relied on across actors, as recent coordinated law enforcement operations have demonstrated," says Camichel.

In May 2025, international authorities expanded Operation Endgame, a coordinated action involving Europol, the FBI, Germany's BKA, the UK's NCA, and other partners, targeting core malware loaders and ransomware infrastructure used by multiple criminal groups. The operation resulted in server seizures, arrests, and the disruption of several key malware families that functioned as entry points in some ransomware campaigns. These types of actions demonstrate that coordinated, cross-border disruption can materially degrade ransomware monetization pipelines while increasing operational friction and forcing actors to rebuild trusted tooling, hosting, and laundering relationships.

Beyond malware delivery systems, authorities also intensified pressure on the hosting environments that sustain these operations. Continued sanctions and indictments chipped away at bulletproof hosting providers (BPH) and laundering services, highlighting how these infrastructure components themselves have become targets for disruption and increasing risk for cybercriminals seeking to monetize extortion. For example, OFAC sanctions in July against AEZA Group, a BPH provider linked to high-volume abuse, demonstrated how crypto payments continue to flow through shielded infrastructure that facilitates ransomware and related attacks. Likewise, the sanctioning in February of Zservers, a provider associated with LockBit and other ransomware actors, underscored the degree to which infrastructure providers are embedded in ransomware monetization.

In parallel with sanctions and infrastructure seizures, the private sector in 2025 also drove significant disruptions of large-scale proxy services underpinning both ransomware and adjacent cybercrime activity. One notable case involved IPIDEA, a China-based residential proxy service advertising millions of proxy endpoints available for rent in any given week. Google's blog on the takedown detailed how the service facilitated botnets including Aisuru and Kimwolf, and how its infrastructure was leveraged by threat actors engaged in espionage and information operations alongside financially-motivated campaigns. Google's analysis found that several residential proxy brands shown below were controlled by the same actors behind IPIDEA reinforcing how a relatively small set of operators can service a wide range of illicit customers across the threat landscape.



On-chain data complement this technical analysis by revealing the financial interconnectedness of these services. Our analysis reveals shared consolidation wallets and deposit addresses at exchanges, suggesting overlapping ownership and coordinated fund flows. We also observed wallets connected with this network making deposits to a well-known cybercrime forum, and several proxy brands associated with this cluster maintained an advertising presence on multiple darknet markets, explicitly marketing services for anonymity and abuse.

Ultimately, this infrastructure-centric approach could change the economic calculus for attackers. While these disruptions have not translated into a drastic reduction in attack volume, they have imposed operational costs and increased friction for threat actors, who are facing coordinated pressure from governments and the private sector alike.

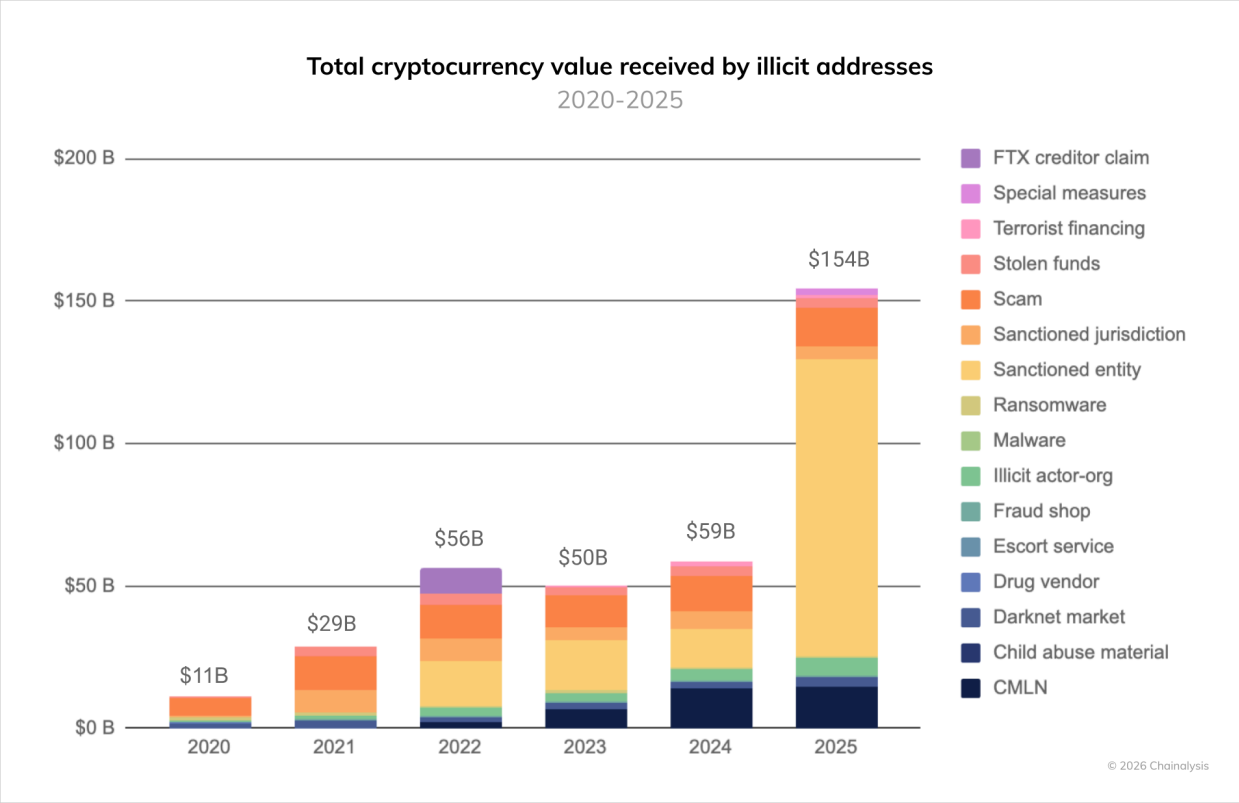
Contraction in revenue, but expansion in harm

The ransomware narrative of 2025 cannot be told through revenue figures alone. While payments declined modestly, the scale, sophistication, and strategic impact of attacks continued to expand. Organizations large and small — from global automakers to regional healthcare systems — faced extortion that disrupted operations, eroded trust, and faced systemic costs that far exceeded on-chain ransom totals.

In this context, the ransomware landscape in 2025 is best characterized by adaptation rather than retreat: extortion tactics continue to evolve, enabling actors to extract value and damage beyond traditional payment streams. For defenders and policymakers alike, this underscores a central truth of the modern ransomware era — effective response requires both robust defenses and strategic resilience to limit the total harm inflicted by these multifaceted threats.

Crypto Crime in 2025 Was Primarily Driven by 694% Surge in State-Driven Sanctions Evasion Volume

Sanctions evasion has traditionally been viewed as a game of financial shell companies and hidden bank accounts. While those opaque traditional structures remain the bedrock of illicit finance, the mechanism has expanded to the blockchain at scale. Nation-states have upgraded their capabilities not just to launder on-chain, but also to execute cross-border trade. The data support this shift toward large-scale evasion. In 2025, illicit addresses received at least $154 billion, a 162% increase year-over-year. The primary driver of this surge was a 694% increase in value received by sanctioned entities, totaling a staggering $104 billion throughout the year.



At the same time, cryptocurrency's role in nation-state strategy extends well beyond evasion. States are using blockchain infrastructure for a spectrum of licit and illicit objectives: trade settlement, reserve diversification, procurement of dual-use goods, ransomware enablement, cyber operations, and financial

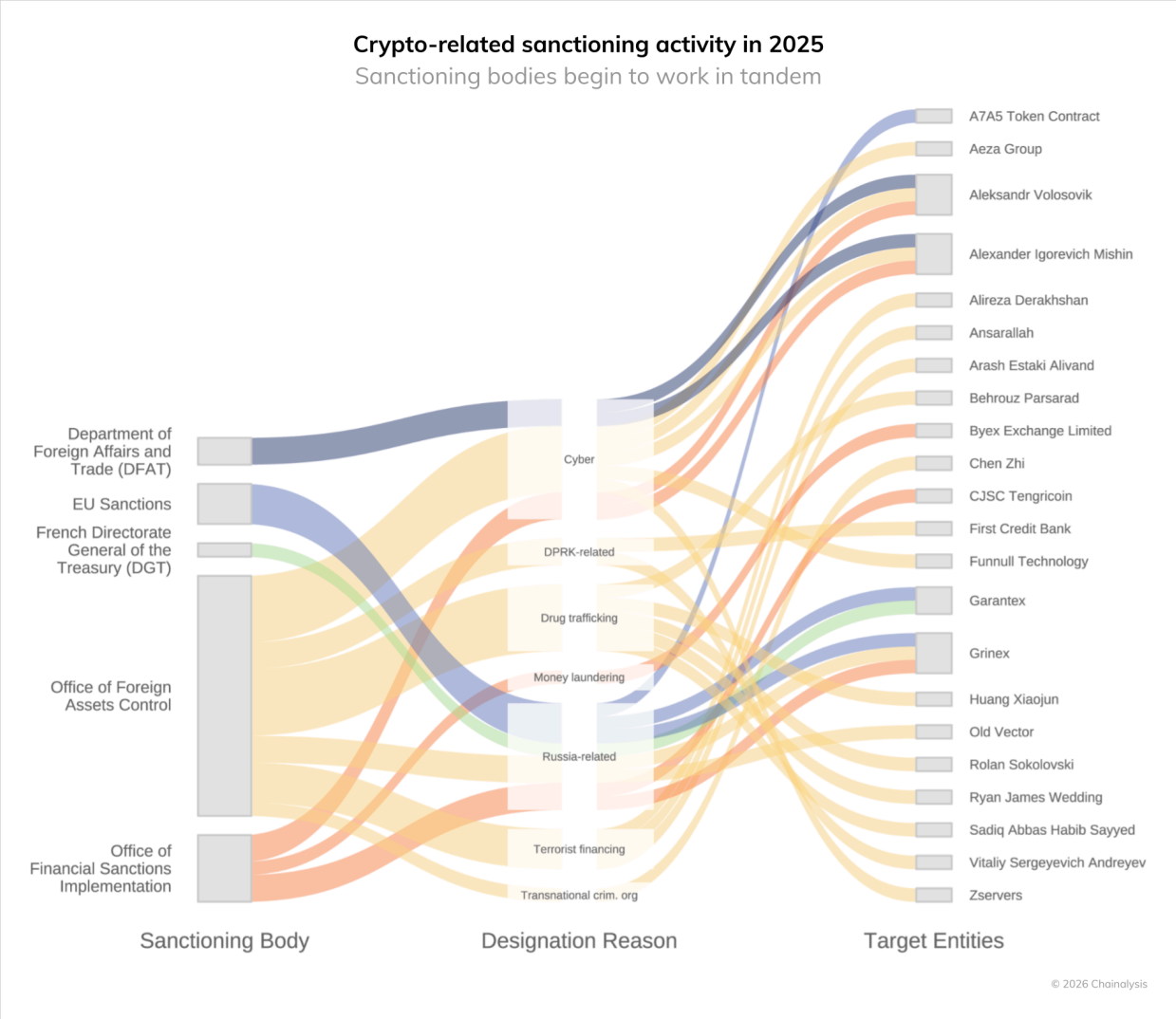
innovation. As we noted in the introduction of our report, crypto adoption continues to expand globally across legitimate and illicit markets, creating a parallel environment in which the same stablecoin rails that facilitate remittances or cross-border commerce can also enable sanctioned trade flows. This convergence can complicate enforcement; the focus is no longer solely on isolating bad actors, but also on identifying when large-scale use of crypto crosses into sanctions violations or national security risk. Against that backdrop, the remainder of this section examines how sanctioned entities — which often include the states that host, fund, and provide them with material support — are operationalizing the blockchain.

In 2025, international regulatory bodies significantly stepped up coordinated sanctions efforts targeting cryptocurrency-related financial activity perceived as facilitating illicit finance and sanctions evasion, with key actions from the U.S. Office of Foreign Assets Control (OFAC), the European Union, the U.K.'s Office of Financial Sanctions Implementation (OFSI), and allied Western nations. OFAC continued to designate crypto actors and infrastructure tied to ransomware, state-linked evasion networks, and sanctions-circumvention services. This illustrates a consistently evolving regulatory approach to blockchain-native illicit activity.

Meanwhile, the EU adopted sweeping sanctions packages, including measures explicitly targeting Russian crypto providers and a ruble-backed stablecoin, A7A5. A7A5 facilitated $93.3 billion in transactions in just 10 months, reflecting the growing use of digital assets to circumvent sanctions and facilitate cross-border trade. These efforts underscore an increasingly multilateral sanctions regime that blends traditional financial controls with blockchain-specific actions to disrupt the use of digital assets for circumventing economic sanctions.

The chart on the following page visualizes this expanding web of enforcement, mapping sanctioning bodies to their specific designations. It highlights the heavy concentration of coordinated actions in the Russia and Cyber sectors, as well as the growing roster of international agencies now actively policing the crypto ecosystem.

In March 2025, OFAC formally delisted decentralized, non-custodial mixer Tornado Cash from its Specially Designated Nationals (SDN) List following a court ruling that its autonomous smart contracts could not be treated as property subject to sanctions, reflecting ongoing legal and regulatory debates about decentralized protocols. Beyond the delisting, national and international authorities remain vigilant about the risks posed by privacy-enhancing tools to obfuscate transactions, which are not inherently illicit, but are often abused by sanctioned and other malign actors.



A diversifying threat: From $2 billion in DPRK hacks to state-backed procurement

In 2025, nation-state use of cryptocurrency moved decisively into the billions. What were once experimental and opportunistic tactics have matured into institutionalized strategies embedded within national economic and security policy. Russia, Iran, and North Korea each operate with distinct objectives and tradecraft, yet despite differing operational models, the three states have collaborated across a number of military, technological, and economic domains in recent years. Collectively, their on-chain behavior demonstrates the same underlying shift: crypto is no longer peripheral to their sanctions evasion, but rather one of its critical elements.

Iran continued integrating crypto into its strategic priorities and financing for proxies, even as the regime faced internal and external pressures not seen since the early days of the Islamic Republic. In Q4 2025,

IRGC-linked addresses accounted for over half of all value received by Iranian entities, moving more than $3 billion to support regional militia networks, facilitate oil sales, and procure dual-use equipment. Meanwhile, for Russia, once ambivalent about cryptocurrency, legislation passed in 2024 crystallized into operational reality in 2025, as cross-border trade began settling on-chain at industrial scale. The ruble-backed A7A5 stablecoin processed more than $93 billion in less than a year, functioning as a purpose-built settlement rail for sanctioned actors seeking access to the international financial system.

As the most dramatically isolated of this group from the international community, North Korea remains as aggressive and sophisticated as ever. In 2025 alone, DPRK-linked actors stole over $2 billion in cryptocurrency while continuing to embed IT workers globally to generate revenue for the Kim regime. In addition, many categories of illicit on-chain activity, from money laundering networks to OTC brokers to infrastructure providers, increasingly intersect with actors operating in or connected to China, which maintains economic, diplomatic, and military relationships with all three states. Taken together, these examples illustrate a diversifying threat landscape where on-chain activity serves as a strategic instrument of state power.

Iran's $3 billion+ proxy network

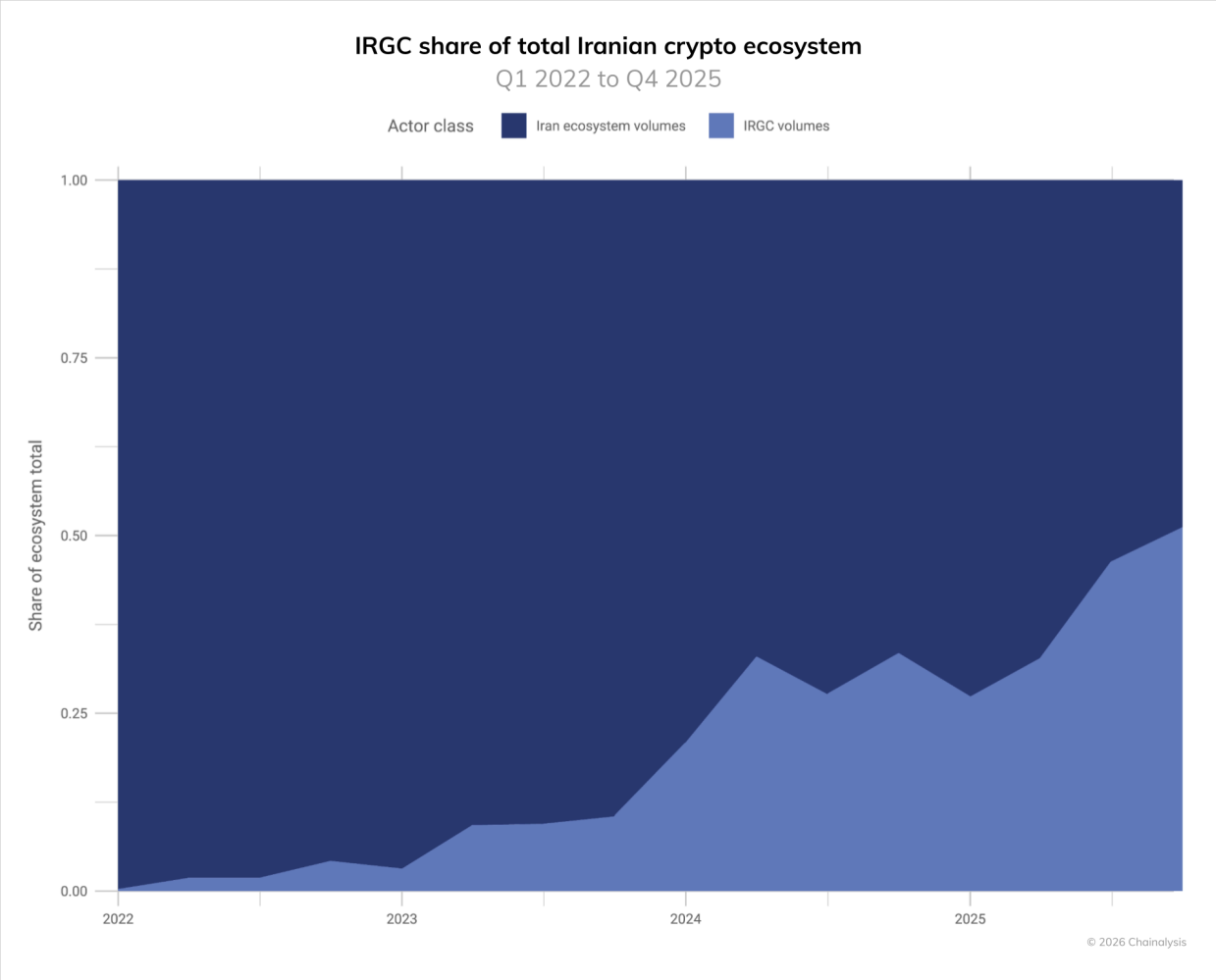
In Iran, the integration of cryptocurrency into state strategy grew in 2025. In 2026, Iran stands as a primary example of how geopolitical upheaval and economic pressure can drive expanded crypto use both as a tool to safeguard economic activity and as a parallel financial system, with its multibillion-dollar on-chain ecosystem reacting to domestic unrest and external military attacks against it in near real-time. The Iranian crypto ecosystem reached over $7.78 billion in 2025, growing amid domestic instability and external military pressure. From nearly 75 identified mainstream cryptocurrency exchanges in Iran, to the Islamic Revolutionary Guard Corps (IRGC) use of crypto, to leaked data around the Central Bank of Iran's use of crypto, it is clear that crypto — and more specifically stablecoins — are top of mind for the financial operations of the regime and Iranians writ large.

The IRGC's 50% market share

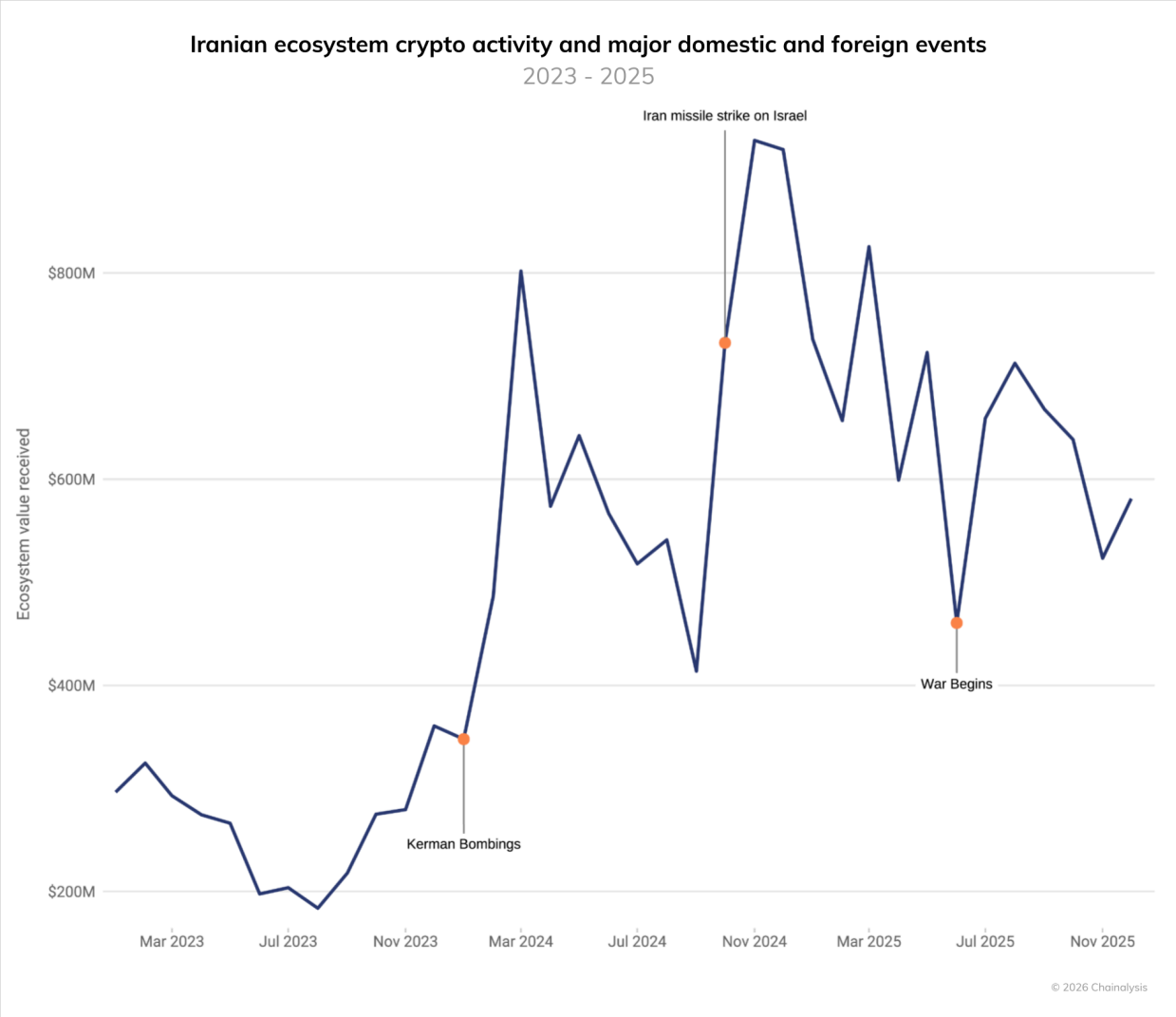
Addresses associated with IRGC facilitation networks rose steadily throughout the year, accounting for over 50% of the total value received by Iranian services by Q4 of 2025. In 2025 alone, the volume of funds received by these IRGC-associated addresses spiked to more than $3 billion (up from $2 billion the previous year). Crucially, this $3 billion total is a lower-bound estimate that excludes volumes from major entities like the UK-registered exchanges Zedcex and Zedxion, as these services were not designated until January 2026. When OFAC finally sanctioned these platforms for facilitating transactions on behalf of IRGC-linked networks, it revealed they had processed tens of billions of dollars' worth of transactions tied to Iran-aligned actors, highlighting how exchange infrastructure can serve as critical nodes in state-backed crypto activity.

In February 2026, the US and Israel launched coordinated military strikes on Iran that targeted defense infrastructure and strategic leadership, and killed the Supreme Leader. Crypto markets responded with visible on-chain asset movements in near real time. Our data can capture the dynamic ebbs and flows of wallet activity of Iranian exchange counterparties, illustrating that major geopolitical events often manifest quickly on public ledgers and provide useful analytic indicators.

Beyond the immediate market reaction to conflict, however, a primary objective of this state-sponsored financial architecture remains the sustained support of external operations. These funds are used to finance a web of regional militia proxies, including Lebanese Hezbollah, Hamas, and the Houthis, facilitating the movement of commodities, illicit oil, and arms at scales not seen on the blockchain before.



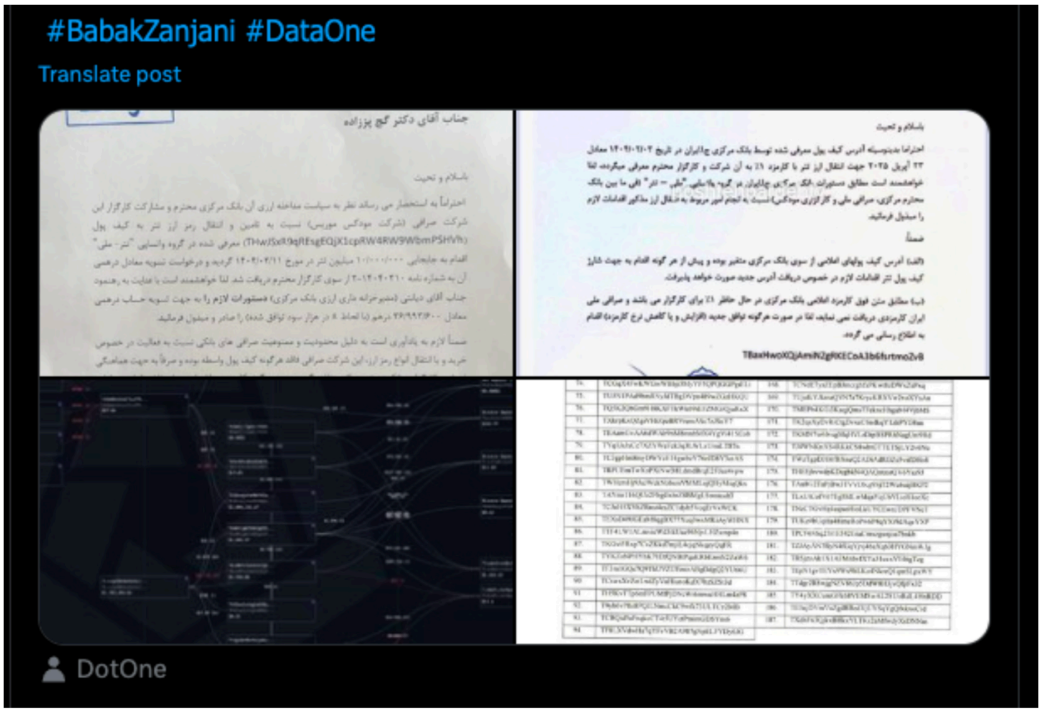
Crucially, blockchain data have become a barometer for kinetic conflict. We observed significant spikes in Iranian on-chain volume corresponding directly to major geopolitical events, including the Kerman bombings, missile strikes in October 2024, and the 12-day war in June 2025. In the same month, cyberattacks targeted Nobitex, Iran's largest exchange, draining its reserves for over $90 million; however, the exchange has largely recovered since.



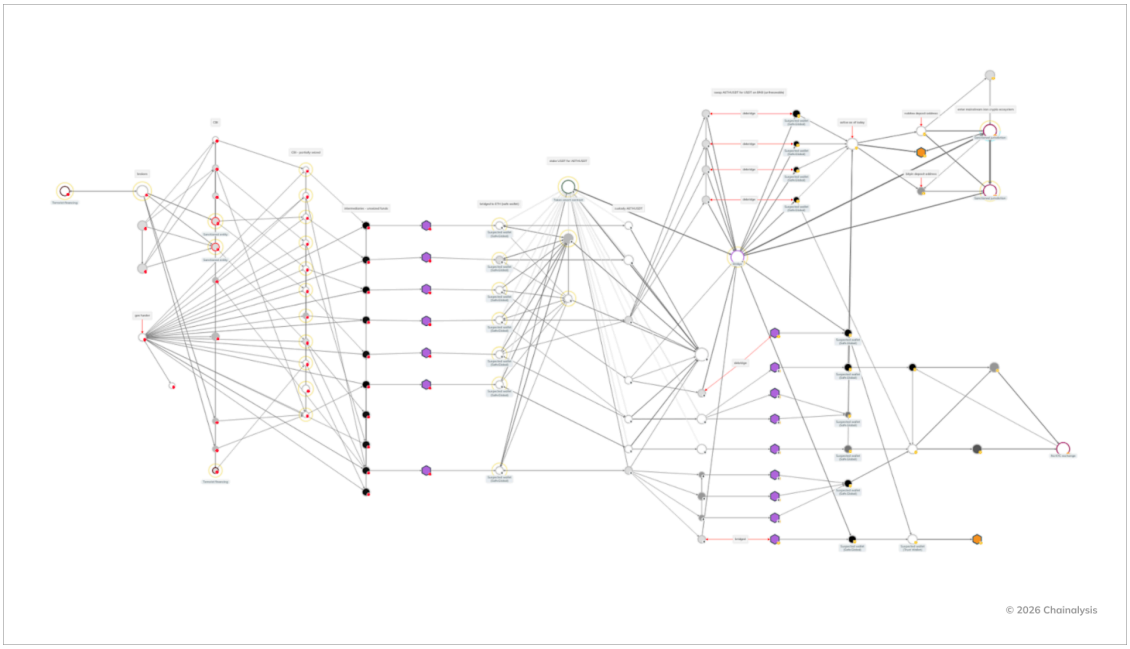
Central Bank of Iran: A shift to the blockchain

In late 2025 Iranian businessman and OFAC SDN Babak Morteza Zanjani – who was initially listed as Zedxion's director in 2021 – posted leaked documents with addresses belonging to the Central Bank of Iran in a social media post. The documents indicated that the regime was using a broker to facilitate the purchase of stablecoins from fiat currency deposits, unraveling a network of coordinated central bank laundering that is unprecedented in its organization and scale.

Blockchain analysis reveals that the broker hired by the regime to purchase stablecoins has exposure to other regime proxies, including Iranian national and OFAC SDN Alireza Derakhshan, who coordinated the purchase of over $100 million worth of cryptocurrency related to Iranian oil sales between 2023 and 2025. Further, the analysis demonstrates how regime actors laundered the central bank funds through several bridges and DeFi protocols before moving the funds back into the mainstream Iranian crypto ecosystem and IRGC-affiliated entities.



Central Bank of Iran documents leaked on the social media account of OFAC SDN and Iranian businessman Babak Morteza Zanjani, revealing cryptocurrency addresses belonging to the regime.



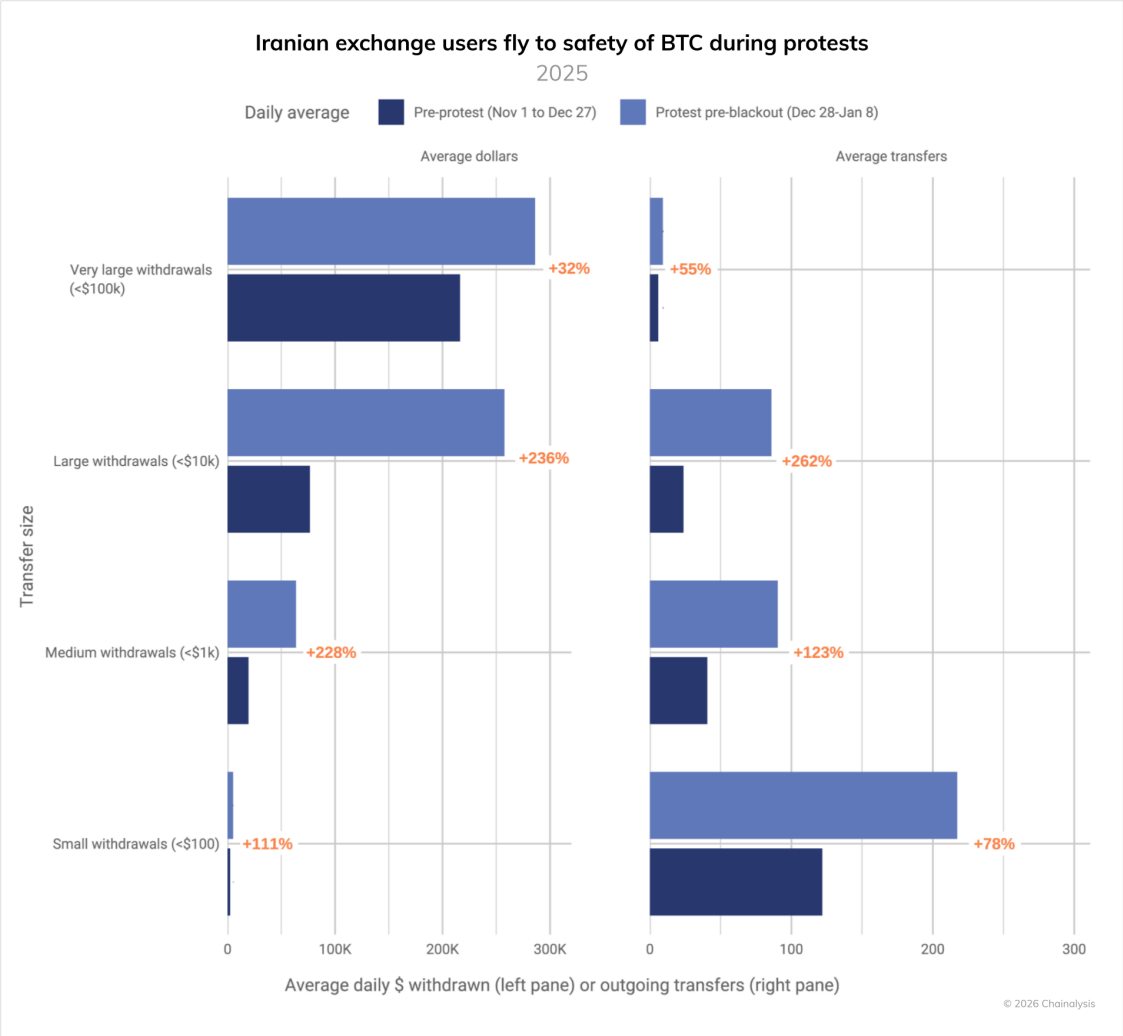
Central Bank of Iran funds were laundered through several bridge and DeFi protocols before being cycled back into the mainstream Iranian crypto ecosystem.

This analysis underscores the extent to which nation states like Iran, subject to heavy sanctions prohibiting the movement of fiat funds, have turned to crypto to facilitate foreign trade activities and have skillfully learned how to obfuscate their activity on the blockchain. Notably, blockchain analysis has evolved to track this activity in real-time.

Bitcoin as protest: The civilian flight to self-custody

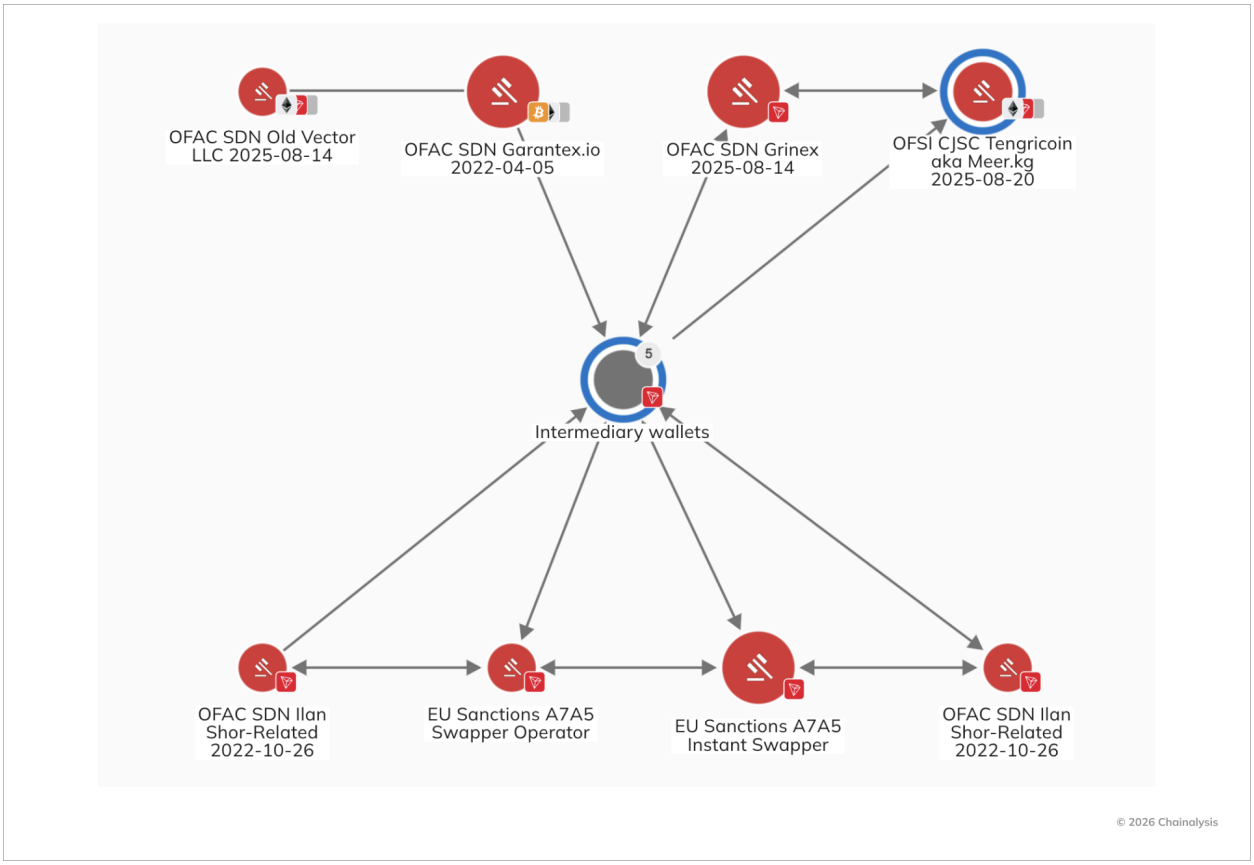
While the state uses crypto for warfare, Iranian citizens have used it for survival. Facing inflation rates of 40-50% and a collapsing rial, civilians have turned to cryptocurrency as an alternative mechanism.

Comparing the pre-protest window (Nov–Dec 2025) to the period of the internet blackout (Jan 2026), we observed a surge in withdrawals from Iranian exchanges to personal Bitcoin wallets. Unlike the state, which favors stablecoins for settlement, civilians are taking possession of bitcoin at markedly higher rates. This "flight to self-custody" indicates that for the average Iranian, bitcoin has become a censorship-resistant asset that offers financial flexibility in an authoritarian and highly volatile environment.



The $93 billion bridge: How A7A5 industrialized Russian sanctions evasion

A prime example of the landscape's complexity is the role of the A7A5 token network. In August 2025, OFAC and OFSI designated entities tied to A7A5, a Russian ruble-backed token, along with its affiliated exchange Grinex and Kyrgyzstani issuer Old Vector. This was followed by the European Commission's 19th sanctions package in October 2025, which enacted a transaction ban on A7A5 itself and the tokens' related entities.



A7A5 represents an evolutionary step in sanctions evasion: a token expressly designed to bypass the traditional financial system entirely. Our on-chain analysis reveals several critical features of this network:

- Grinex is the direct successor to Garantex, the notorious Russian exchange sanctioned in 2022 that has processed hundreds of millions of dollars' worth of illicit transactions. Following the disruption of Garantex's online infrastructure in March 2025, on-chain data showed a massive transfer of user funds and newly minted A7A5 tokens moving directly from Garantex wallets to Grinex via Old Vector. This was a clear "rebranding" effort to maintain liquidity for sanctioned entities.
- Unlike retail tokens, A7A5 trading volumes surge Monday through Friday and drop precipitously on weekends. This pattern suggests the token is being used primarily as a settlement layer for the Russian government and businesses to settle cross-border accounts during business hours, rather than for retail use which typically operates 24/7.

- Perhaps most concerning is the A7A5 Instant Swapper service. This instant exchange service operates without meaningful or no KYC, and converts the sanctioned A7A5 token into mainstream USD-pegged stablecoins. To date, over $2.2 billion in value has moved through this service, effectively allowing sanctioned Russian entities to transfer assets from sanctioned Russian banks, through a now sanctioned ruble-backed stablecoin into the broader global crypto economy, in an effort to allow the ability to facilitate cross-border trade outside of the traditional fiat ecosystem.
- Dozens of addresses with high activity within the A7A5 network belonging to sanctioned Moldovan oligarch Ilan Shor were leaked in 2025, revealing key sources of liquidity for the A7A5 Instant Swapper. Prior to the joint law enforcement takedown of Garantex in March 2025, Shor representatives met with Garantex administrators to set up A7A5 trading.

Russia's use of A7A5 illustrates not only how sanctioned states are building parallel financial rails, but also how enforcement authorities are adapting in response. Sanctions against entities like bulletproof hosting providers Zservers, AEZA, and Yalishanda and IP infrastructure provider Funnull Technology demonstrate a growing regulatory focus on the infrastructure layer that enables on-chain illicit activity. Authorities are no longer just targeting the wallets receiving illicit funds; they are dismantling the Infrastructure as a Service (IaaS) providers that allow state-sponsored hackers and ransomware gangs to operate. This "infrastructure-centric" approach aims to disrupt the operational capacity of sanctioned entities at its foundation – restricting hosting services, liquidity pathways, and technical backbones that keep networks online. By targeting these service providers, regulators increase costs, fragment ecosystems, and force sanctioned actors to rebuild in less stable and more exposed environments.

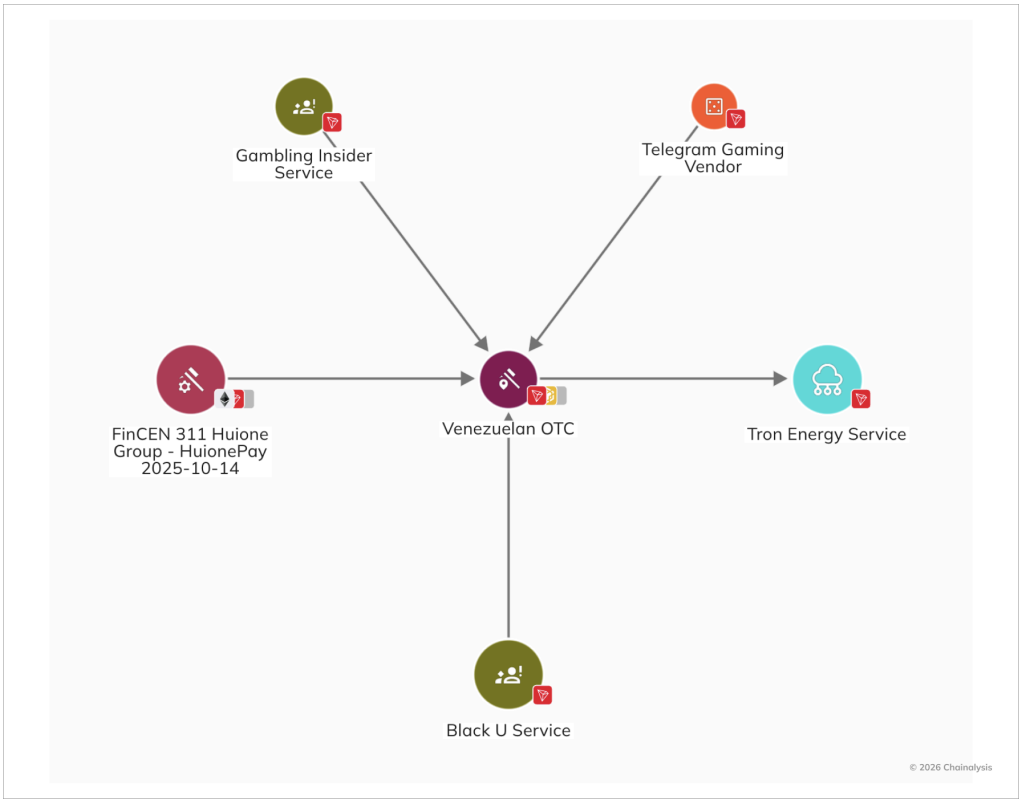
From Survival to Statecraft: Cryptocurrency's Split Reality in Venezuela

Venezuelan nationals were early adopters of crypto, using it as a hedge against hyperinflation, and sustained instability in the domestic banking sector under the Maduro regime. In 2025, we identified an estimated $44.6B in transaction flows in Venezuela. While the Government of Venezuela (GoV) sought to formalize and oversee the sector through the creation of Superintendencia Nacional de Criptoactivos (SUNACRIP) and a network of state-run exchanges — including support for the now-defunct state-backed crypto asset, the Petro — Venezuelans instead flocked to international cryptocurrency exchanges, in large part reflecting limited confidence in the regime's offerings. The state-run exchanges ultimately had limited success, conducting transactions totaling in the tens of millions until their eventual shut down, a far cry from broad adoption. As the sanctions targeted the GoV rather than ordinary citizens, many global exchanges permitted Venezuelan nationals on their platforms, creating a critical financial lifeline to the global financial system amid domestic constraints.

At the same time, informal networks, potentially linked to the regime, operate alongside mainstream usage. Beyond the formalized ecosystem under SUNACRIP, reports indicate the Maduro regime has engaged in stablecoin-for-oil trade. These typologies suggest these regime-aligned financier networks may mirror models observed in other sanctioned jurisdictions, such as Iran and Russia, facilitating cross-border trade and evading sanctions all at once.

Furthermore, informal over-the-counter (OTC) brokers, whether operating physical storefronts or offering services tailored to Venezuelan nationals, continue to function as on- and off-ramps. Certain brokers have enabled swaps into crypto from bolivars held at sanctioned Venezuelan banks.

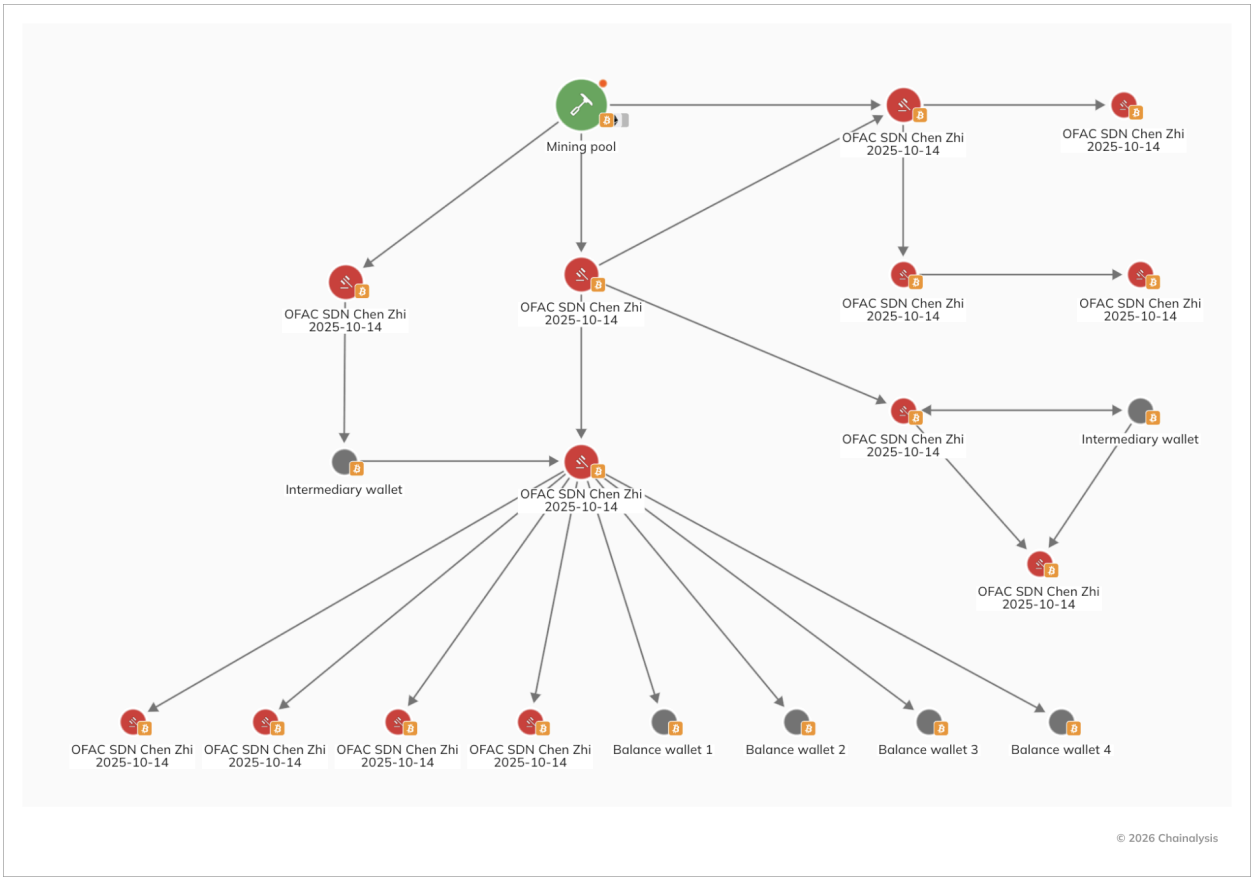
In one example (depicted below), an OTC broker shows direct on-chain exposure to Chinese-language money laundering networks (CMLNs) and the recently FinCEN 311-designated Huione Group. Such exposure underscores the risk that these intermediaries may facilitate the laundering of illicit proceeds, whether related to state-linked actors, transnational organized crime, or unrelated independent actors. These services therefore represent informal, largely unregistered conduits between Venezuela's highly turbulent domestic financial system and the global crypto ecosystem.



Overall, Venezuela's relationship to cryptocurrency reflects a dual dynamic. For individual citizens, crypto primarily provides access to global exchanges and a mechanism to preserve value amid persistent macroeconomic volatility. For the GoV, attempts at institutionalizing and controlling domestic adoption have largely failed; however, the strategic use of crypto by the regime to facilitate cross-border trade and evade sanctions, especially in the oil sector, has found success. This tension highlights the dynamic push and pull we observe in heavily sanctioned environments: crypto can simultaneously function as an instrument of state-level sanctions evasion and as a stabilizing financial outlet for beleaguered populations navigating prolonged economic distress and illicit finance risk. While Venezuela's crypto ecosystem continues to reflect the interplay between economic hardship and sanctions pressure, global enforcement efforts have also intensified against other complex networks that leverage crypto to facilitate fraud and laundering at scale.

Regulatory bodies target Southeast Asian scam networks

2025 also saw coordinated actions by U.S. and allied authorities against crypto-enabled scam and laundering networks in Southeast Asia. In October 2025, the designation of Huione Group under FinCEN's Special Measures as a primary money laundering concern under Section 311 of the USA PATRIOT Act highlighted in particular how cross-border enforcement is adapting to confront highly automated, high-volume on-chain illicit activity. Huione Group has processed over $98 billion of total cryptocurrency inflows between August 2021 and January 2025, including over $4 billion in confirmed illicit proceeds. Huione Group has long been used by a host of illicit actors, ranging from money launderers, scam technology vendors, escort services, and more. Along with Huione's designation, the transnational criminal organizations Prince Group and its frontman Chen Zhi were targeted with sanctions in multiple jurisdictions for their role in facilitating cryptocurrency scams, mining operations, money laundering, and forced labor at scam compounds in Cambodia and beyond. Additionally, OFAC designated Jin Bei, a guarantee platform facilitating activity similar to Huione Group, and OFSI also sanctioned Byex, a cryptocurrency exchange platform with links to Prince Group. Over $15 billion of Chen Zhi's money was seized by the U.S. government, a landmark disruption; however, following his designation, addresses affiliated with and controlled by Chen Zhi continued to launder his remaining stored value on-chain prior to his arrest in Cambodia and extradition to China in January, as shown in the graph below:



Looking ahead

Sanctions evasion involving cryptocurrency is likely to remain concentrated in a relatively small number of highly capable state actors and their transnational facilitation networks. As we have shown throughout 2025 — from designations tied to A7A5 and Grinex to actions against infrastructure providers like Zservers and AEZA — enforcement is increasingly focused on the service layer that enables illicit activity, not just individual wallets. It is also important to remember that the billions of dollars attributed to IRGC-linked wallets, DPRK hacking groups, and other state actors ultimately move through networks of individual brokers, facilitators, IT workers, and other operators whose activity in the aggregate gives state-backed campaigns their breadth and depth. Even at billion-dollar volumes, these ecosystems are run by human beings making operational decisions, leaving behavioral patterns and infrastructure dependencies that can be traced and disrupted. Targeting exchanges, hosting providers, OTC brokers and other facilitators can thus have outsized impact by disrupting liquidity and operational continuity for complex, multijurisdictional sanctioned networks.

At the same time, sanctioned actors are likely to continue to rely on stablecoins and centralized services, because they offer the liquidity, global presence, and interoperability needed for cross-border trade. While tactics such as chain-hopping and rapid rebranding (e.g., Garantex-to-Grinex) are likely to persist, the blockchain's transparency will remain a structural advantage for investigators, compliance teams, regulators, and policymakers. 2025 provided clear examples across a range of geopolitical challenges that real world risk manifests on-chain, with observable changes in trading patterns and large-scale flows, as regimes and the citizens living under their yoke responded to heightened uncertainty. This underscores the utility of our data not only for tracking illicit finance, but also for providing real-time insight into how macro developments influence risk sentiment across digital asset markets. Stronger analytics, more comprehensive data, closer public-private collaboration, and coordinated designations have made large-scale evasion more visible — even when it is moving at a billion-dollar scale.

Looking to the longer-term, as economies such as Venezuela and Iran eventually confront the prospect of reconstruction and reintegration into the international system, crypto and on-chain infrastructure could play an important role in rebuilding trust in repairing badly damaged financial systems and expanding access to basic services. Stablecoins and on-chain settlement mechanisms in particular offer low-cost, borderless avenues for remittances, payments, and savings for populations underserved by the formal banking sector and plagued by corruption, opaqueness, and AML/CFT risk. If coupled with sound regulation and inclusive policy frameworks, these tools could help governments leverage crypto not just for resilience, but also for broader financial inclusion as part of economic recovery.

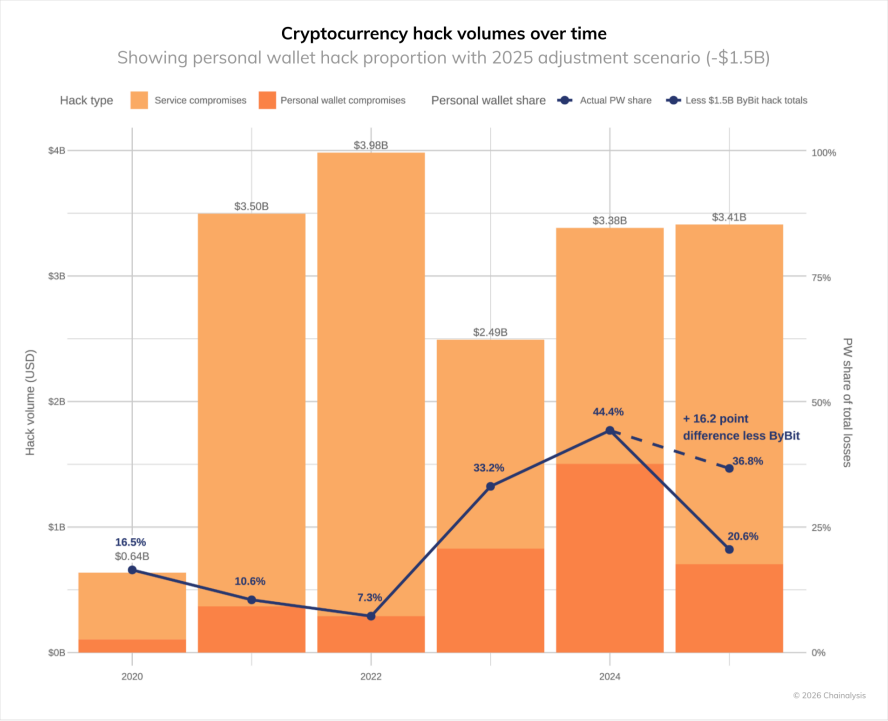
North Korea Drives Record $2 Billion Crypto Theft Year, Pushing All-Time Total to $6.75 Billion

The cryptocurrency ecosystem faced another challenging year in 2025, with stolen funds continuing their upward trajectory. Our analysis reveals a shift in crypto theft patterns, characterized by four key developments: the persistence of the Democratic People's Republic of Korea (DPRK) as a primary threat actor, the growing severity of individual attacks on centralized services, a surge in personal wallet compromises, and an unexpected divergence in decentralized finance (DeFi) hack trends.

These patterns emerge clearly from the data and reveal significant changes in how crypto theft is occurring across different platform types and victim categories. As digital asset adoption expands and valuations reach new heights, understanding these evolving security threats has become increasingly critical.

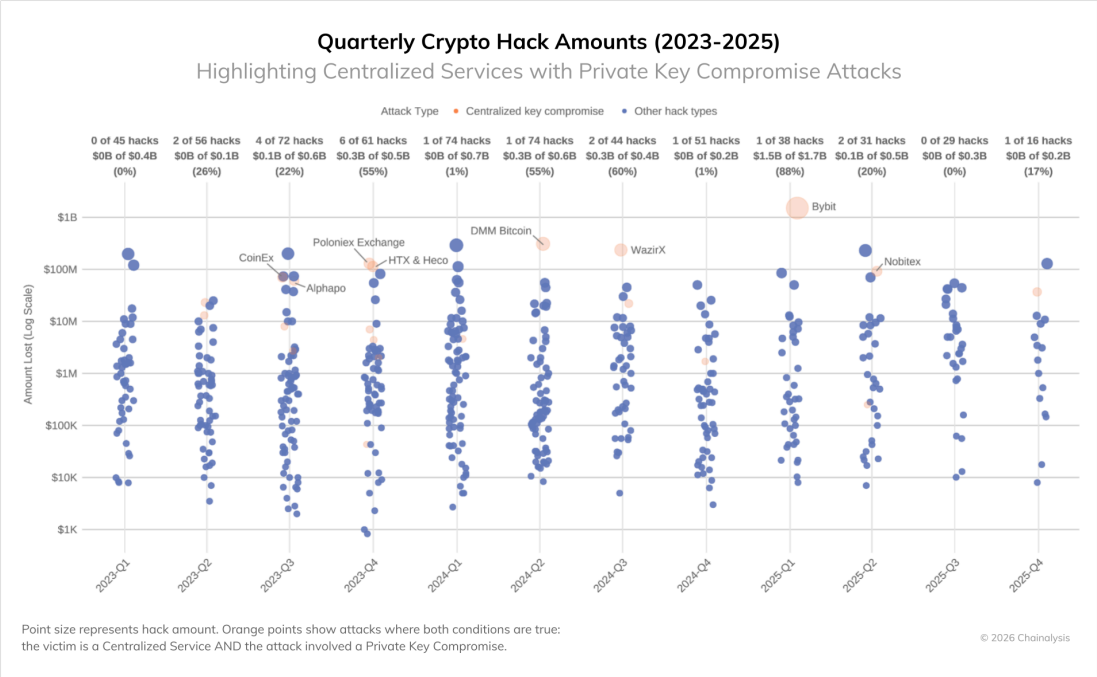
The big picture: Over $3.4 billion stolen in 2025

The cryptocurrency industry witnessed over $3.4 billion in theft from January through early December 2025, with the February compromise of Bybit alone accounting for $1.5 billion of that total.



Beyond the headline figure, the data reveal important shifts in the composition of these thefts. Personal wallet compromises have grown substantially, increasing from just 7.3% of total stolen value in 2022 to 44% in 2024. In 2025, the share would have been 37% if it weren't for the outsized impact of the Bybit attack.

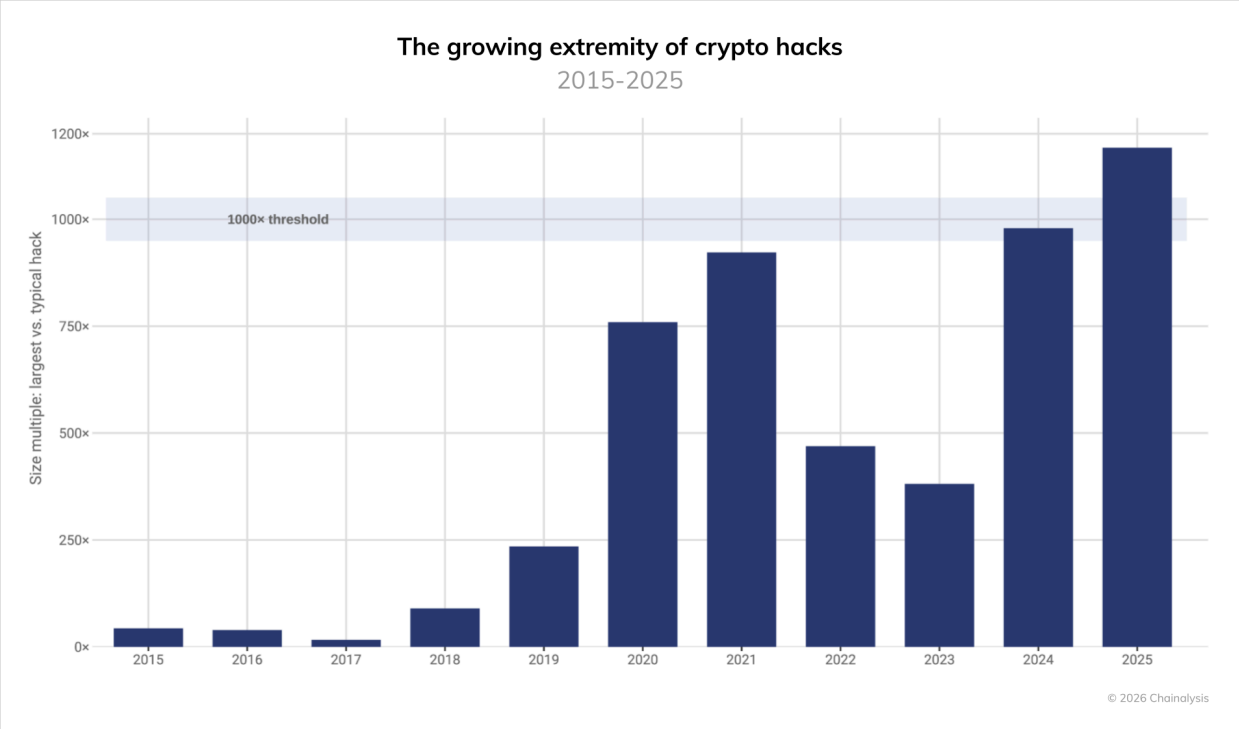
Meanwhile, centralized services are experiencing increasingly large losses due to sophisticated attacks on private key infrastructure and signing processes. Despite their institutional resources and professional security teams, these platforms remain vulnerable to advanced threats that can circumvent cold wallet controls. While such compromises are infrequent (as shown in the chart below), their scale still drives enormous shares of stolen volumes when they do occur, accounting for 88% of losses in Q1 2025. Many attackers have developed methods to exploit third-party wallet integrations and trick legitimate signers into authorizing malicious transactions.



The persistence of high theft volumes indicates that while some areas of crypto security may be improving, attackers continue to find success across multiple vectors.

Top three hacks account for 69% of losses as outliers reach 1,000 times the median

Stolen fund activity has always been outlier-driven, with most hacks relatively small and some immense. But 2025 reveals a striking escalation: the ratio between the largest hack and median of all incidents has crossed the 1,000x threshold for the first time. Funds stolen in the largest attacks are now 1,000 times larger than those stolen in the typical incident, surpassing even the 2021 bull market peak. These calculations are based on the USD values of funds stolen at the time of their theft.



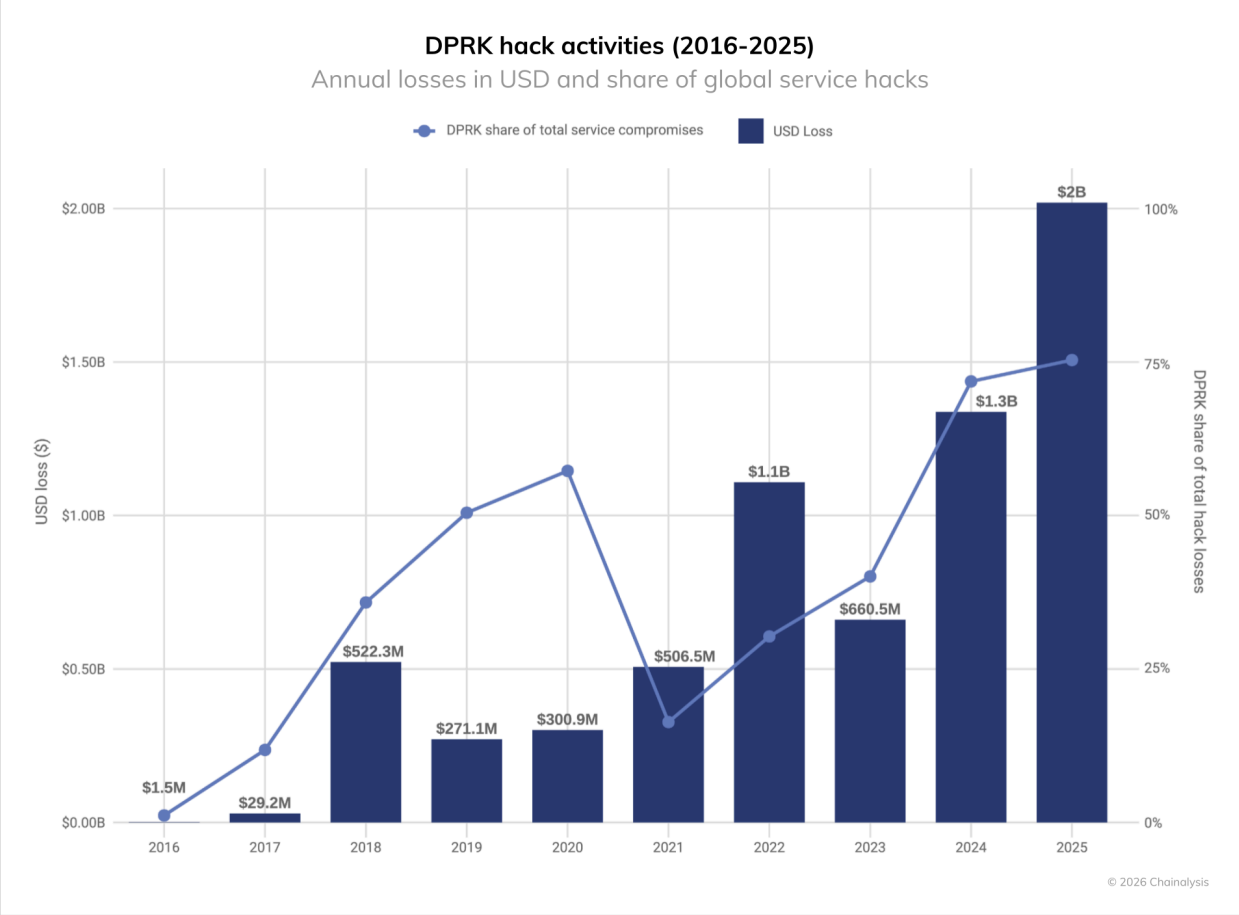
This growing discrepancy has concentrated losses dramatically. The top three hacks in 2025 account for 69% of all service losses, creating a landscape where individual incidents have an outsized impact on yearly totals. While the number of incidents may fluctuate and median losses grow with asset prices, the potential for catastrophic individual breaches is escalating faster still.

North Korea remains dominant crypto threat actor, despite fewer confirmed incidents

The Democratic People's Republic of Korea (DPRK) continues to pose the most significant nation-state threat to cryptocurrency security, achieving a record-breaking year for stolen funds despite an assessed dramatic reduction in attack frequency. In 2025, North Korean hackers stole at least $2.02 billion in cryptocurrency ($681 million more than 2024), representing a 51% increase year-over-year. This marks the most severe year on record for DPRK crypto theft in terms of value stolen, with DPRK attacks also accounting for a record 76% of all service compromises. Overall, 2025's numbers bring the lower-bound cumulative estimate for cryptocurrency funds stolen by the DPRK to $6.75 billion.

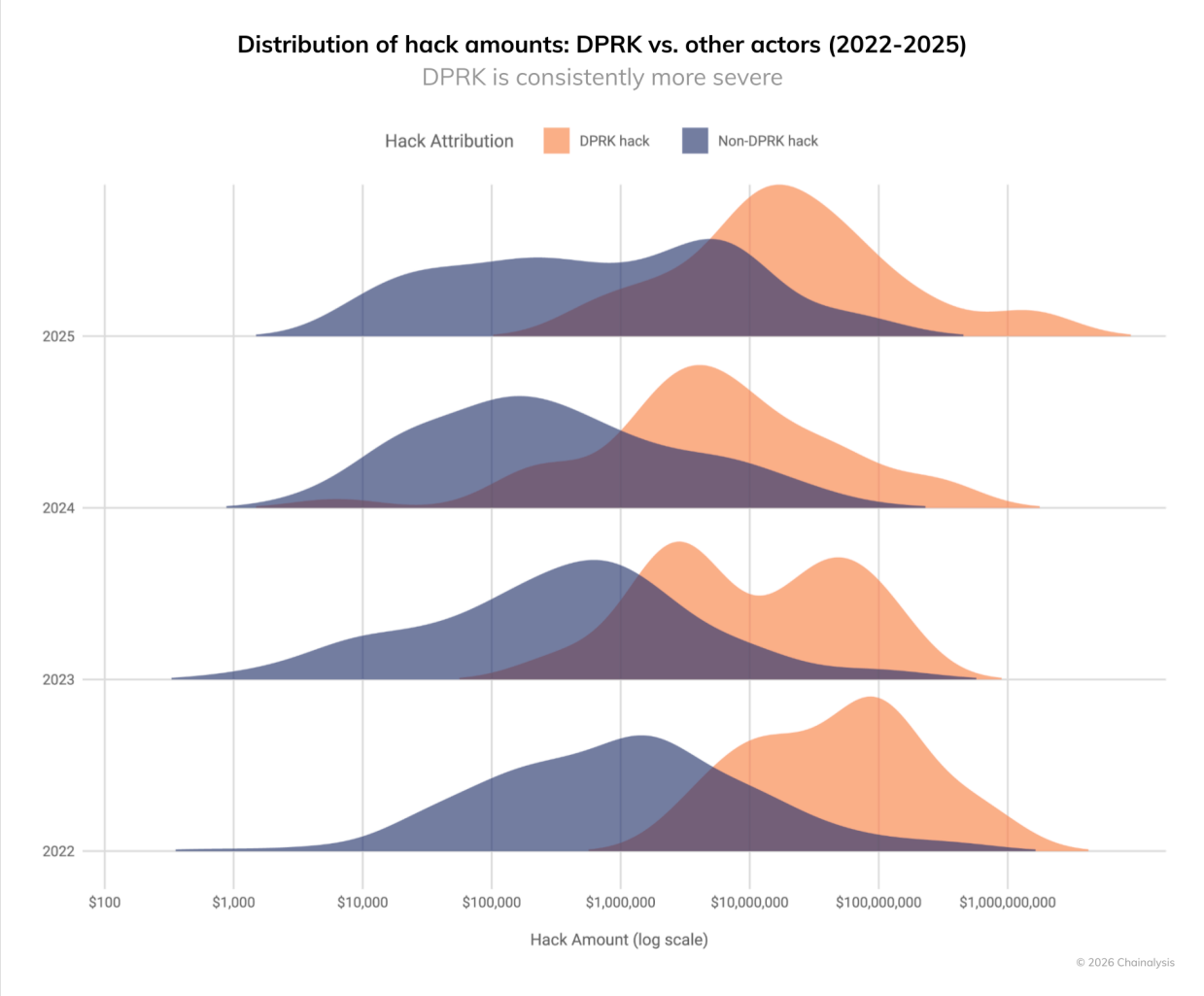
North Korean threat actors are increasingly achieving these outsized results often by embedding IT workers – one of DPRK's principal attack vectors – inside crypto services to gain privileged access and enable high-impact compromises. Part of this record year likely reflects an expanded reliance on IT worker infiltration at exchanges, custodians, and web3 firms, which can accelerate initial access and lateral movement ahead of large-scale theft.

More recently, however, DPRK-linked operators have flipped this IT worker model on its head. Instead of merely applying for roles and embedding themselves as employees, they are increasingly impersonating recruiters for prominent web3 and AI firms, orchestrating fake hiring processes that culminate in “technical screens” designed to harvest credentials, source code, and VPN or SSO access to the victim’s current employer. At the executive level, a similar social-engineering playbook appears in the form of bogus outreach from purported strategic investors or acquirers, who use pitch meetings and pseudo–due diligence to probe for sensitive systems information and potential access paths into high-value infrastructure — an evolution that builds directly on the DPRK’s IT worker fraud operations and their focus on strategically important AI and blockchain companies.



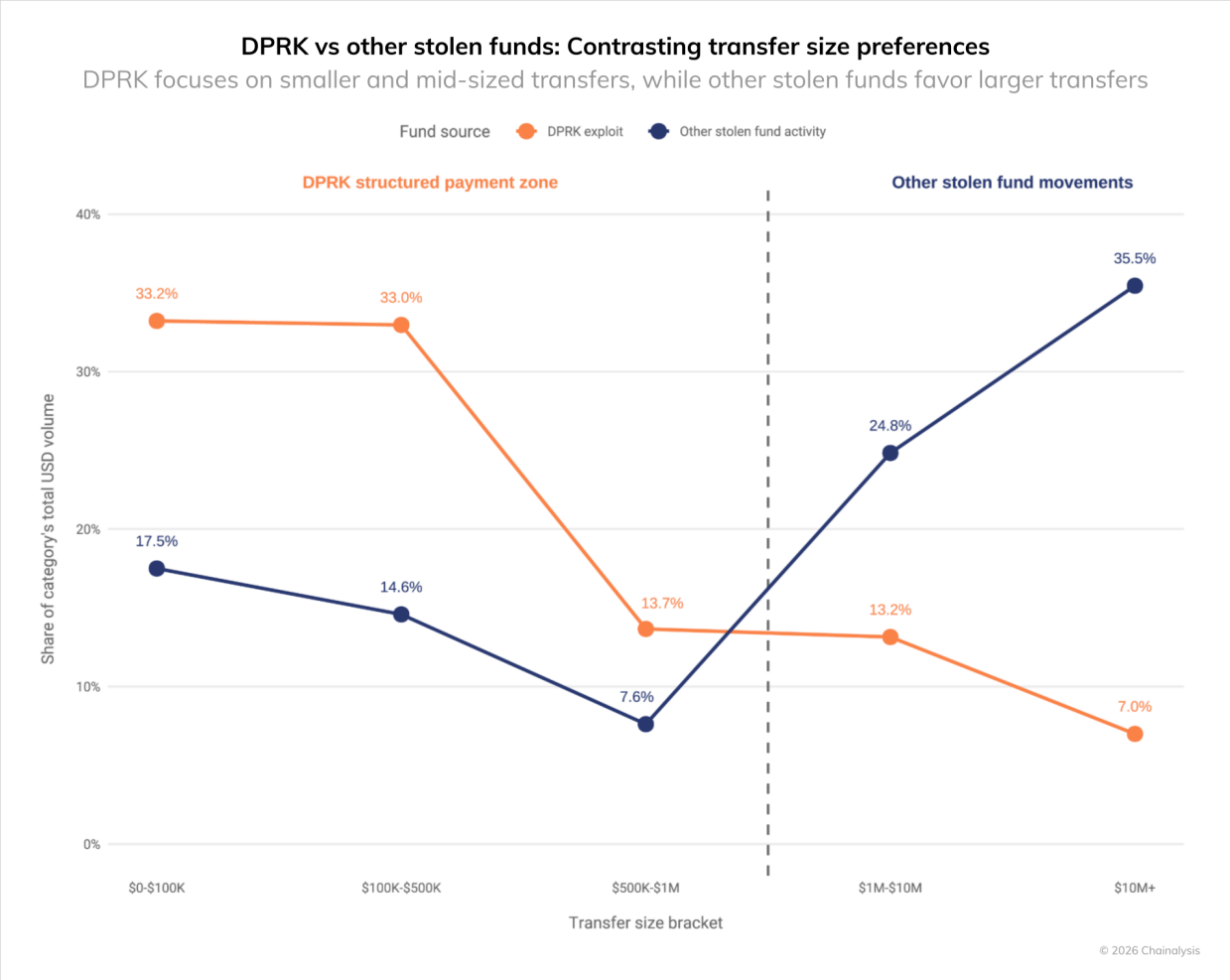
As we have seen in years past, the DPRK continues to undertake significantly higher-value attacks than other threat actors. As shown in the chart below, from 2022-2025, DPRK-attributed hacks occupy the highest value ranges, while non-DPRK hacks show more normal distributions across all theft sizes. This pattern reinforces that when North Korean hackers strike, they target large services and aim for maximum impact.

This year’s record haul came from significantly fewer known incidents. This shift — fewer incidents yielding far greater returns — reflects the impact of the massive Bybit hack in February 2025.



The DPRK's distinctive laundering patterns

The massive influx of stolen funds in early 2025 provides unprecedented visibility into how DPRK-linked actors launder cryptocurrency at scale. Their patterns differ markedly from those of other cybercriminals and evolve over time, revealing current operational preferences and potential vulnerabilities.



DPRK laundering shows distinctive bracketing patterns, with slightly over 60% of volume concentrated below a $500,000 transfer value. In contrast, other stolen fund actors send over 60% of their funds on-chain in tranches in the $1M to $10M+ range. Even while the DPRK consistently steals larger amounts than other stolen fund threat actors, they structure on-chain payments in smaller tranches, speaking to the sophistication of their laundering.

Compared to other stolen fund actors, the DPRK shows clear preferences for certain laundering touchpoints:

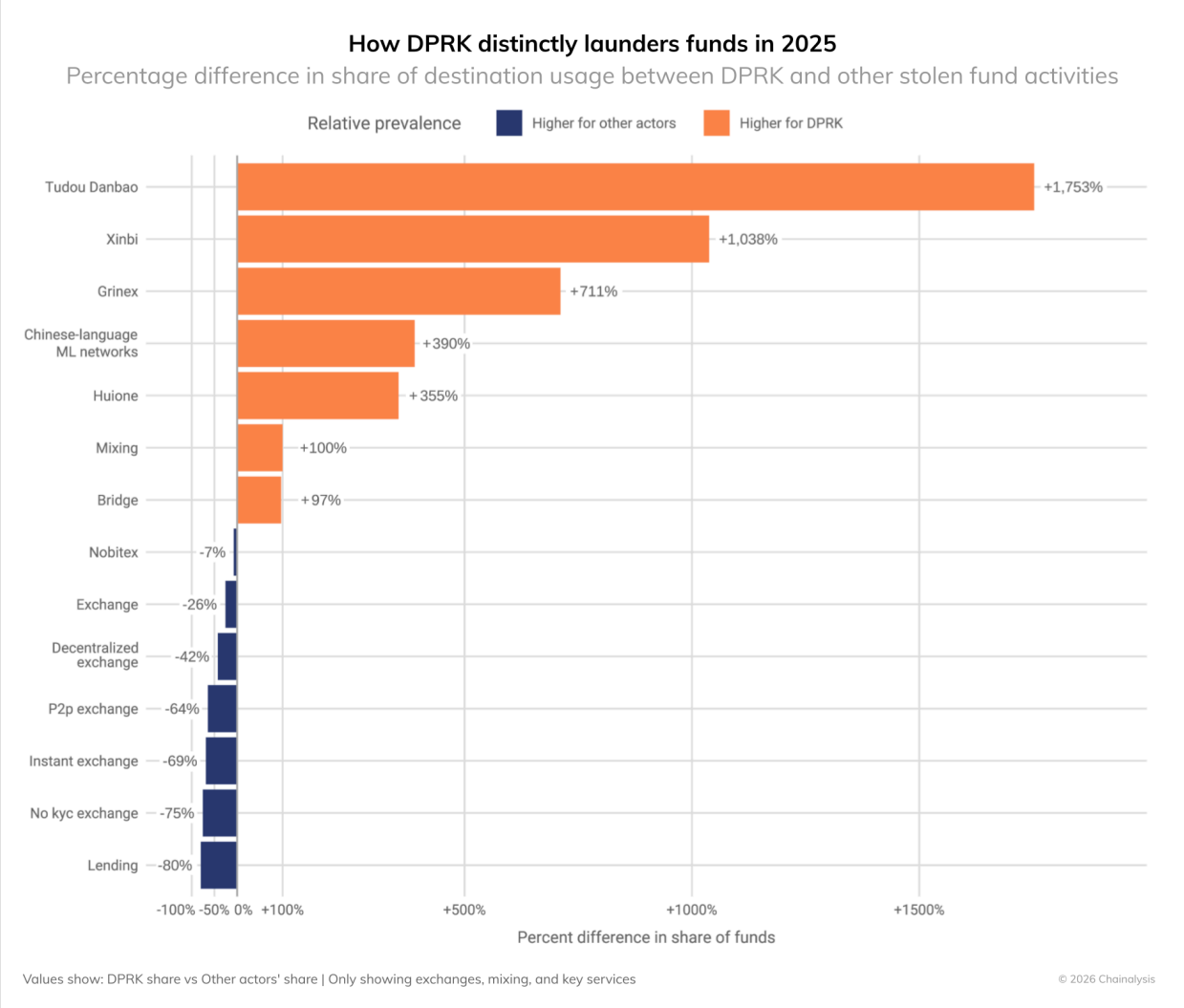
DPRK hackers tend to strongly prefer:

- Chinese-language money movement and guarantee services (+355% to +1000%+): Their most distinctive characteristic, showing heavy reliance on Chinese-language guarantee services and money laundering networks comprised of many different laundering operators that may have weaker compliance controls
- Bridge services (+97% difference): Heavy reliance on cross-chain bridges to move assets between blockchains and attempt to complicate tracing

- Mixing services (+100% difference): Greater use of mixing services to attempt to obscure the flow of funds
- Specialized services like Huione (+356%): Strategic use of specific services that facilitate their laundering operations

Other stolen fund actors tend to strongly prefer:

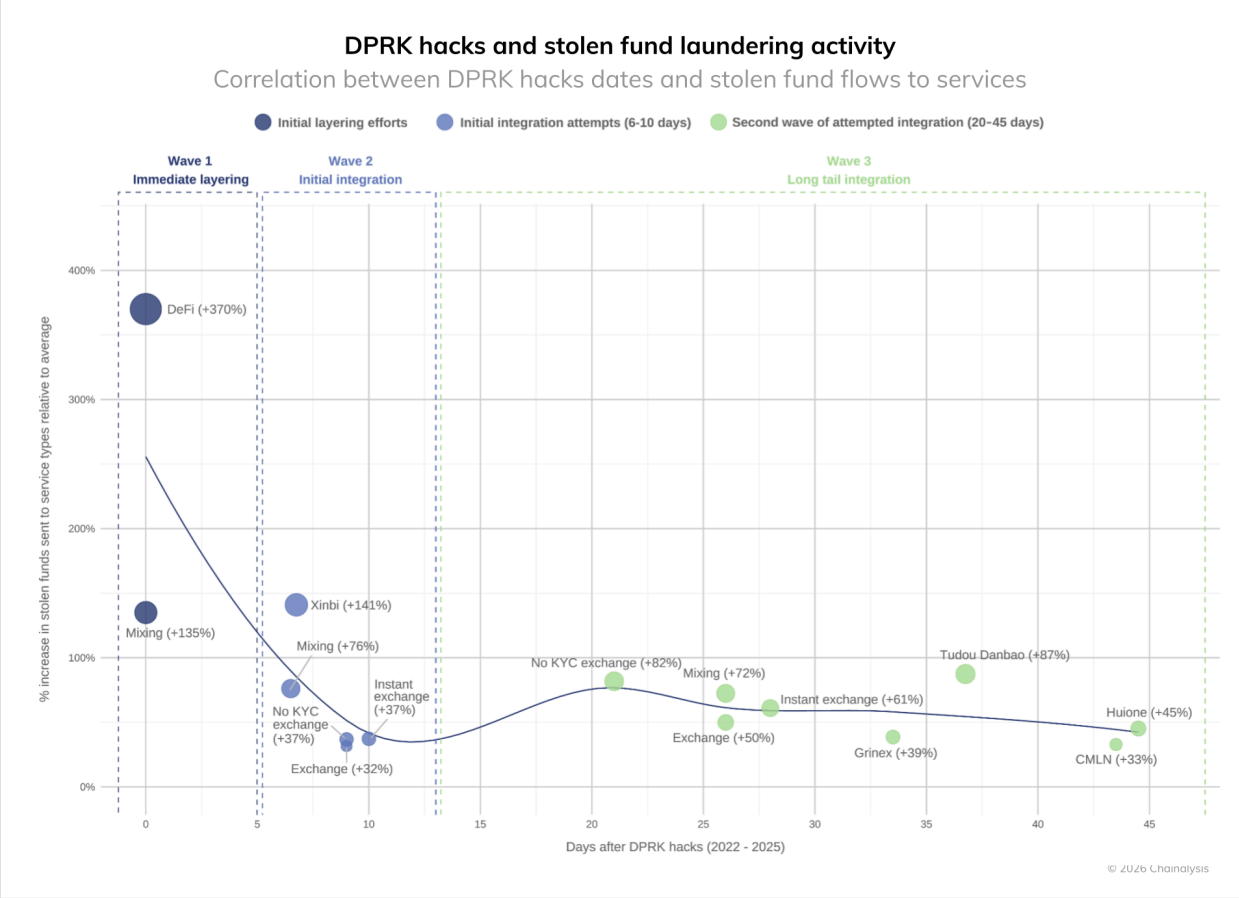
- Lending protocols (-80% difference): DPRK avoids these DeFi services, showing limited integration with the broader DeFi ecosystem
- No KYC exchanges (-75% difference): Surprisingly, other threat actors use KYC-free exchanges more than DPRK
- P2P exchanges (-64% difference): DPRK shows limited interest in peer-to-peer platforms
- Centralized exchanges (-25% difference): Other criminals display more direct interactions with conventional exchange platforms
- Decentralized exchanges (DEXs) (-42% difference): Other threat actors strongly prefer DEXs for their liquidity and pseudonymity



These patterns suggest that the DPRK operates under different constraints and objectives than those of non-state-backed cybercriminals. Their heavy use of professional Chinese-language money laundering services and over-the-counter (OTC) traders suggests that DPRK threat actors are tightly integrated with illicit actors across the Asia-Pacific region, and is consistent with Pyongyang's historical use of China-based networks to gain access to the international financial system.

The timeline of stolen fund laundering post-DPRK hacks

Our analysis of on-chain activity following DPRK-attributed hacks reveals a consistent pattern in how these events are associated with the movement of stolen funds throughout the cryptocurrency ecosystem. Following major theft events between 2022-2025, stolen funds follow a structured, multi-wave laundering pathway that unfolds over approximately 45 days:



Wave 1: Immediate layering (days 0-5)

During the initial days after a hack, we observe an extraordinary spike in activity focused on immediate distancing of funds from the theft source:

- DeFi protocols see the most dramatic increase (+370%) in stolen fund flows, serving as the primary entry point
- Mixing services experience substantial volume increases (+135-150%), creating the first layer of obfuscation
- This phase represents urgent "first-move" efforts to establish distance from the original theft

Wave 2: Initial integration (days 6-10)

As the second week begins, the strategy shifts toward services that can help integrate funds into the broader ecosystem:

- Exchanges with limited KYC (+37%) and centralized exchanges (+32%) begin receiving flows
- Second-tier mixing services (+76%) continue the laundering process at reduced intensity
- Cross-chain bridges like XMRt (+141%) help fragment and obscure fund movement across blockchains
- This phase represents the critical transitional period where funds begin moving toward potential off-ramps

Wave 3: Long tail integration (days 20-45)

The final phase shows clear preference for services that can facilitate ultimate conversion to fiat or other assets:

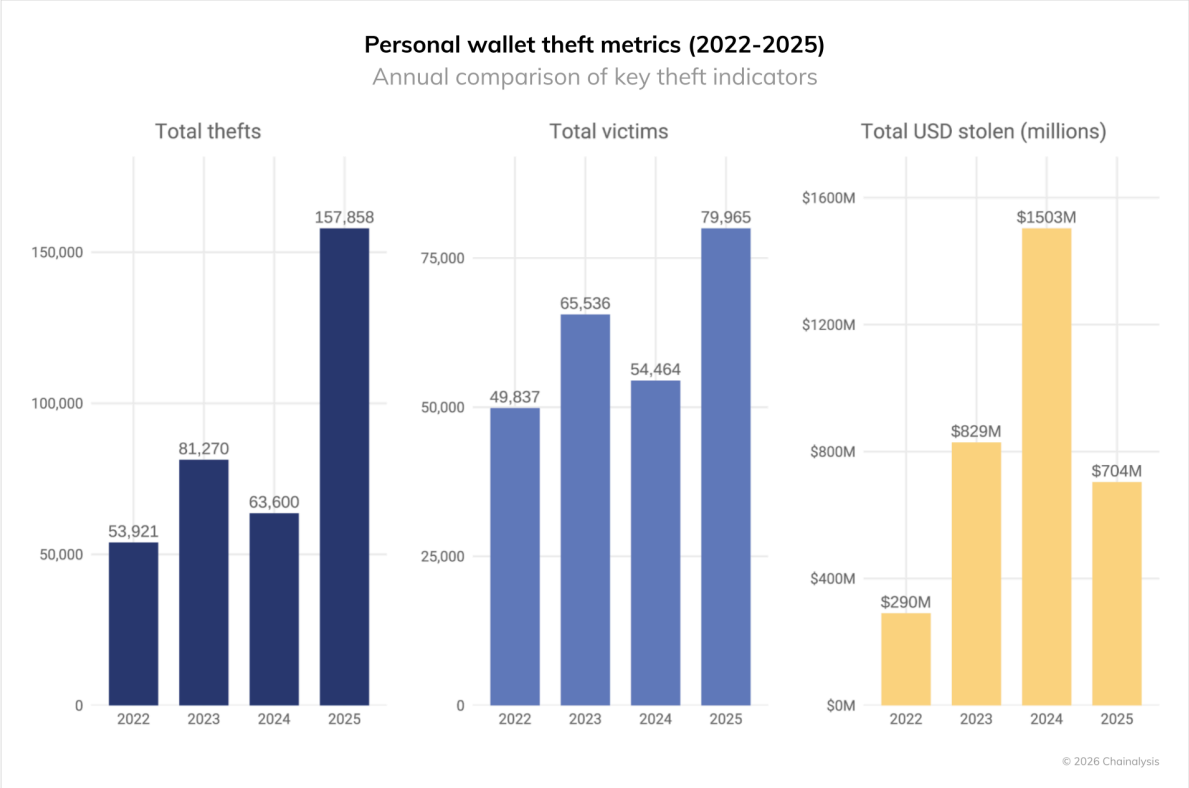
- No-KYC exchanges (+82%) and guarantee services like Tudou Danbao (+87%) see significant increases
- Instant exchanges (+61%) and Chinese-language platforms like Huione (+45%) serve as final conversion points
- Centralized exchanges (+50%) also receive funds, suggesting sophisticated attempts to mix with legitimate flows
- Less regulated jurisdictions represented by platforms such as Chinese-language money laundering networks (+33%) and Grinex (+39%) complete the pattern

This general 45-day window for laundering operations provides crucial intelligence for law enforcement and compliance teams. The pattern's persistence across multiple years indicates operational constraints facing DPRK-linked actors, likely related to their limited access to financial infrastructure and need to coordinate with specific facilitators.

While these actors don't always follow this exact timeline—some stolen funds remain dormant for months or years—this pattern represents their typical on-chain behavior when actively laundering proceeds. It's also important to acknowledge potential blind spots in this analysis, as certain activities like private key transfers or OTC crypto-for-fiat sales wouldn't be visible on-chain without corroborative intelligence.

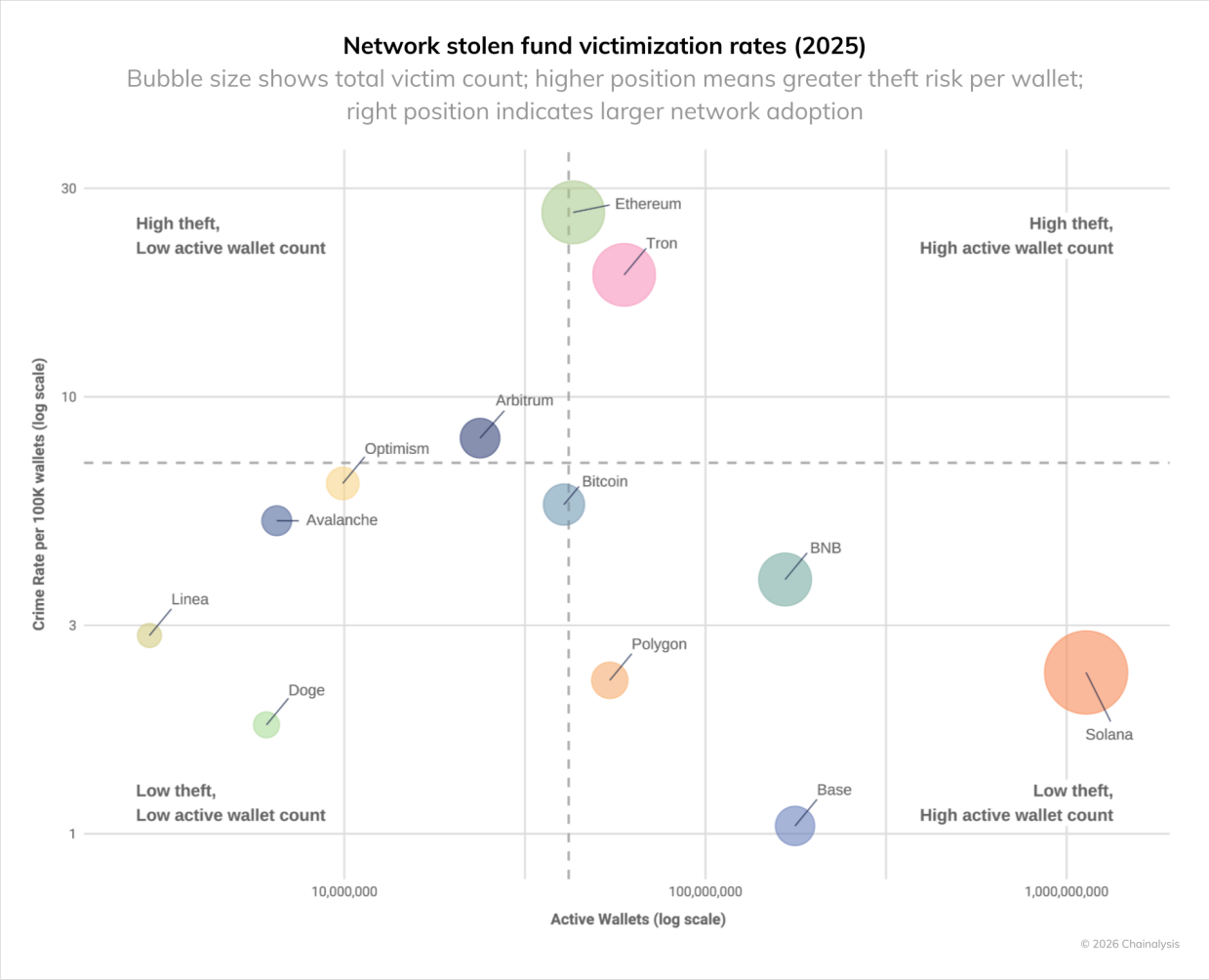
Personal wallet compromises: The escalating threat to individual users

Through analysis of on-chain patterns, in addition to reporting from victims and industry partners, we can gain an understanding of the magnitude of personal wallet compromises, although the true number of compromises is likely far greater. Based on our lower bound estimates, personal wallet compromises now account for 20% of all value stolen in 2025, down from 44% of the total in 2024, representing an evolution in both scale and pattern. Total theft incidents surged to 158,000 in 2025, nearly triple the 54,000 recorded in 2022. Unique victims increased from 40,000 in 2022 to at least 80,000 in 2025. These dramatic increases are likely due to greater crypto adoption. For example, Solana, one of the blockchains with the greatest number of active personal wallets, had by far the largest number of incidents (~26,500 victims).



Yet despite more incidents and victims, the total USD value stolen from individual victims actually declined from 2024's peak of $1.5 billion to $713 million in 2025. This suggests that attackers are targeting more users, but stealing smaller amounts per victim.

Network-specific victimization data provides additional insight into which domains present the greatest risk to crypto users. The chart below presents victimization data adjusted for active personal wallets across networks. When measuring crime rates per 100K wallets in 2025, Ethereum and Tron show the highest rates of theft. Ethereum's large size indicates both high rates of theft and high victim count, while Tron's position shows elevated rate of theft despite a smaller active wallet base. In contrast, Base and Solana show lower victimization rates despite significant user bases.



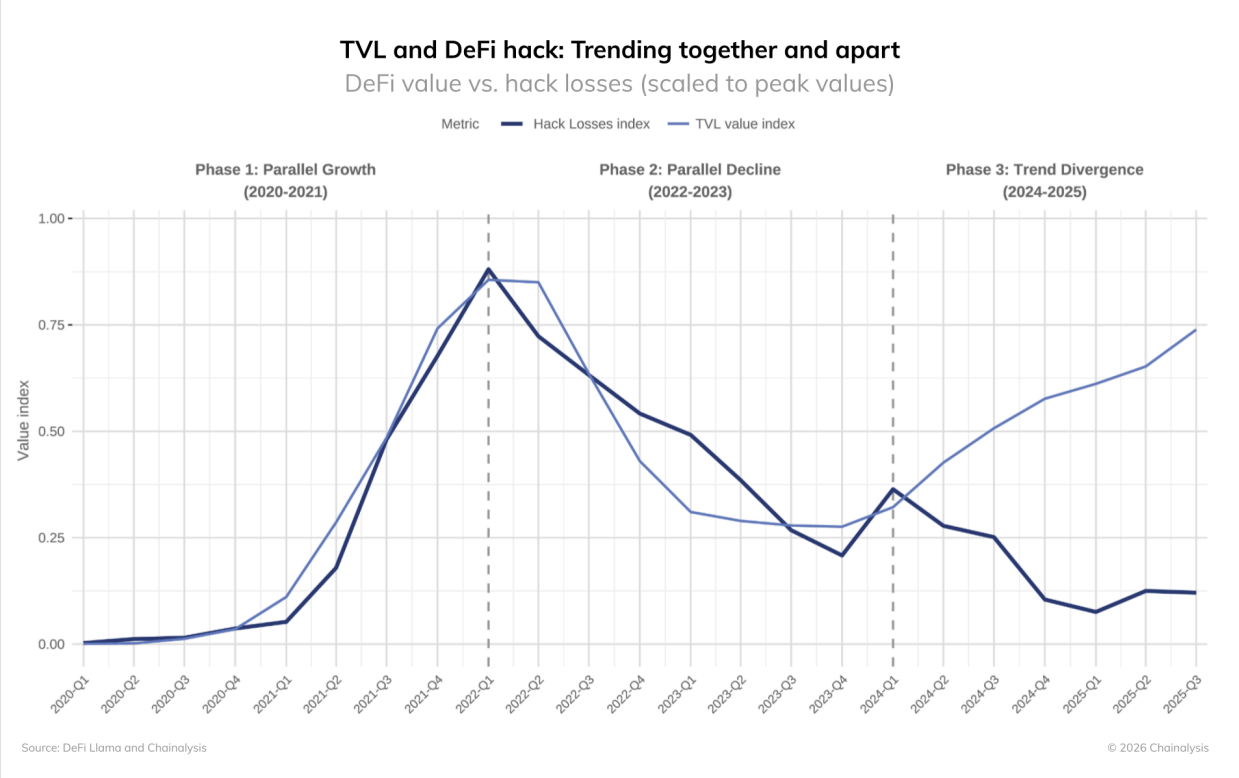
These measurable differences highlight that personal wallet security risks are not uniform across the crypto ecosystem. The variation in victimization rates across chains with similar technical architectures suggests that factors beyond technology — such as user demographics, popular applications, and criminal infrastructure — play important roles in determining theft rates.

DeFi hacks: A diverging pattern signals market shift

The DeFi sector presents a unique pattern in 2025's crime data, showing a clear divergence from historical trends.

The data reveal three distinct phases:

- Phase 1 (2020-2021): DeFi total value locked (TVL) and hack losses grew in parallel
- Phase 2 (2022-2023): Both metrics declined together
- Phase 3 (2024-2025): TVL recovered while hack losses remained suppressed



The first two phases follow an intuitive pattern: greater value at risk means both more value to steal and greater criminal effort targeting high-value protocols. As the infamous bank robber Willie Sutton supposedly said: "Because that's where the money is."

This makes Phase 3's divergence from historical precedent all the more notable. DeFi TVL has recovered significantly from its 2023 lows, yet hack losses have not followed suit. The sustained lower level of DeFi hacks even as billions of dollars have returned to these protocols represents a meaningful change.

Two factors may explain this divergence:

- **Improved security:** Consistently lower hack rates despite growing TVL suggest that DeFi protocols may be implementing more effective security measures compared to the 2020-2021 period.
- **Target substitution:** The concurrent rise in personal wallet thefts and centralized service compromises suggests that attacker attention may be shifting to alternative targets.

Case study: Venus Protocol's security response

The Venus Protocol incident of September 2025 exemplifies how improved security practices are making a tangible difference. When attackers used a compromised Zoom client to gain system access and manipulate a user into granting delegate status over a $13 million account, the outcome could have been catastrophic. However, Venus had onboarded Hexagate's security monitoring platform just one month prior.

The platform detected suspicious activity 18 hours before the attack and generated another alert as soon as the malicious transaction occurred. Within 20 minutes, Venus had paused its protocol, preventing any fund movements. The coordinated response demonstrated the evolution of DeFi security:

- **Within 5 hours:** Partial functionality restored after security checks
- **Within 7 hours:** Force-liquidation of the attacker's wallet
- **Within 12 hours:** Full recovery of stolen funds and service resumption

Most remarkably, Venus passed a governance proposal to freeze $3 million in assets still controlled by the attacker; the attacker not only failed to profit, but actually lost money, as well.
This incident illustrates tangible improvements in DeFi security infrastructure. The combination of proactive monitoring, rapid response capabilities, and governance mechanisms that can act decisively has made the ecosystem more agile and resilient. While attacks still occur, the ability to detect, respond, and even reverse them represents a fundamental shift from the early DeFi era when successful hacks often meant permanent losses.

Implications for 2026 and beyond

The 2025 data present a complex picture of DPRK's evolution as a crypto threat actor. The nation state's ability to execute fewer but far more damaging attacks demonstrates increasing sophistication and patience. The Bybit incident's impact on its yearly activity patterns suggests that when DPRK successfully executes a major theft, it reduces operational tempo to focus on laundering the proceeds.

For the cryptocurrency industry, this evolution demands enhanced vigilance around high-value targets and improved detection of DPRK's specific laundering patterns. Their consistent preferences for certain service types and transfer amounts provide detection opportunities, distinguish them from other criminals, and can help investigators identify their on-chain behavioral footprint.

As North Korea continues to use cryptocurrency theft to fund state priorities and circumvent international sanctions, the industry must recognize that this threat actor operates by different rules than typical cybercriminals. The country's record-breaking 2025 performance — achieved with 74% fewer known attacks — suggests we may be seeing only the most visible portion of its activities. The challenge for 2026 will be detecting and preventing these high-impact operations before DPRK-affiliated actors inflict another Bybit-scale incident.

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 in the public and private sectors use our solutions to prevent hacks and fraud, investigate illicit activity, manage risk exposure, and develop innovative market solutions. Our mission is to build trust in blockchains, blending safety and security with a commitment to growth and innovation.

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