2025 Crypto Crime Mid-Year Update

chainalysis.com/blog/2025-crypto-crime-mid-year-update

Chainalysis Team July 17, 2025

Key findings

Stolen funds

- With over $2.17 billion stolen from cryptocurrency services so far in 2025, this year is more devastating than the entirety of 2024. The DPRK's $1.5 billion hack of ByBit, the largest single hack in crypto history, accounts for the majority of service losses.
- By the end of June 2025, 17% more value had been stolen year-to-date (YTD) than in 2022, previously the worst year on record. If current trends continue, stolen funds from services could eclipse $4 billion by year's end.
- Personal wallet compromises now represent a growing share of total ecosystem theft, with attackers increasingly targeting individual users, making up 23.35% of all stolen fund activity YTD in 2025.
- "Wrench attacks" — physical violence or coercion against crypto holders — show correlation with bitcoin price movements, suggesting opportunistic targeting during high-value periods.

Geographic trends

- So far in 2025, significant concentrations of stolen fund victims have emerged in the U.S., Germany, Russia, Canada, Japan, Indonesia, and South Korea.
- Regionally, Eastern Europe, MENA, and CSAO saw the most rapid H1 2024 to H1 2025 growth in victim totals.
- Notable differences in the type of asset stolen have also emerged between regions, possibly reflecting the underlying pattern of regional adoption of crypto assets.

Laundering behavior

- Some differences emerge in comparing the laundering of funds stolen from services vs. individuals. Overall, threat actors who have compromised services tend to exhibit higher levels of sophistication than those targeting personal wallets.
- Stolen fund launderers consistently overspend to move funds, with average premiums fluctuating from 2.58x in 2021 to 14.5x YTD in 2025.
- Interestingly, while the average cost in dollars to move stolen funds has declined over time, the multiple over the average cost to move funds on chain has increased.
- Threat actors compromising personal wallets increasingly leave larger balances of stolen funds on-chain rather than immediately laundering stolen assets.
- Thefts targeting personal wallets currently hold $8.5 billion in crypto on-chain, while funds taken from services amount to $1.28B.

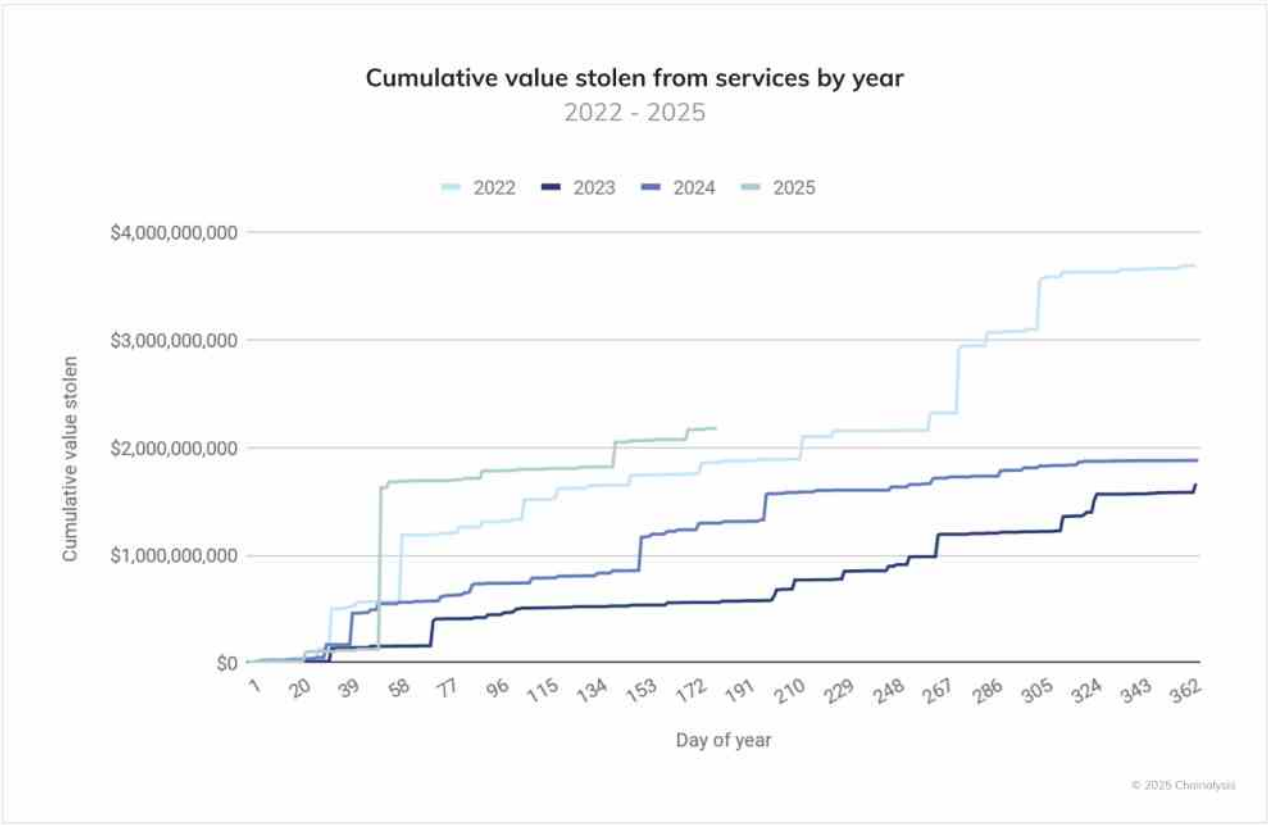
The shifting illicit landscape

Illicit volumes thus far in 2025 are on track to meet or even exceed last year's estimated $51 billion, despite significant changes to the illicit actor landscape. The closure of Garantex, a sanctioned Russian exchange, and the likely FinCEN Special Measures designation of Huione Group — a Cambodia-based Chinese language service that has processed over $70 billion in inflows — have reshaped how criminals move money through the ecosystem.

Amid this shifting landscape, stolen fund activity stands out as the dominant concern in 2025. While other forms of illicit activity have shown mixed trends YoY, the surge in cryptocurrency thefts represents both an immediate threat to ecosystem participants and a long-term challenge for the industry's security infrastructure.

Funds stolen from services: A record-breaking trajectory

The cumulative trend in value taken from services paints a stark picture of 2025's escalating threat environment. The orange line, which represents 2025's YTD activity, shows a dramatically steeper trajectory into June than any previous year in our dataset, climbing past the $2 billion mark within the first half of the year.



What makes this trend particularly alarming is its velocity and consistency. While 2022 — previously the worst year on record according to our data — required 214 days to crack $2 billion in value stolen from services, 2025 achieved comparable theft volumes in just 142 days. The 2023 and 2024 trend lines show more moderate, steady accumulation patterns.

Currently, 2025 is 17.27% worse than 2022 at the end of June. If this trend continues, we could see 2025 end with more than $4.3 billion stolen from services alone.

The ByBit breach: A new benchmark for cybercrime

The DPRK's ByBit hack fundamentally altered the 2025 threat landscape. At $1.5 billion, this single incident not only represents the largest crypto theft in history, but also accounts for approximately 69% of all funds stolen from services this year. The sophistication and scale of this attack underscore the evolving capabilities of state-sponsored threat actors in the crypto space, and comes after a notable slowdown in the second half of 2024.

This mega-breach fits within a broader pattern of North Korean cryptocurrency operations, which have become increasingly central to the regime's sanctions evasion strategies. Last year, known DPRK-related losses totaled $1.3B (heretofore the worst year on record), making 2025 already by far their most successful year to date.

The attack methodology appeared to leverage advanced social engineering tactics similar to those documented in previous DPRK operations, including the infiltration of crypto-related services through compromised IT personnel. This approach has proven

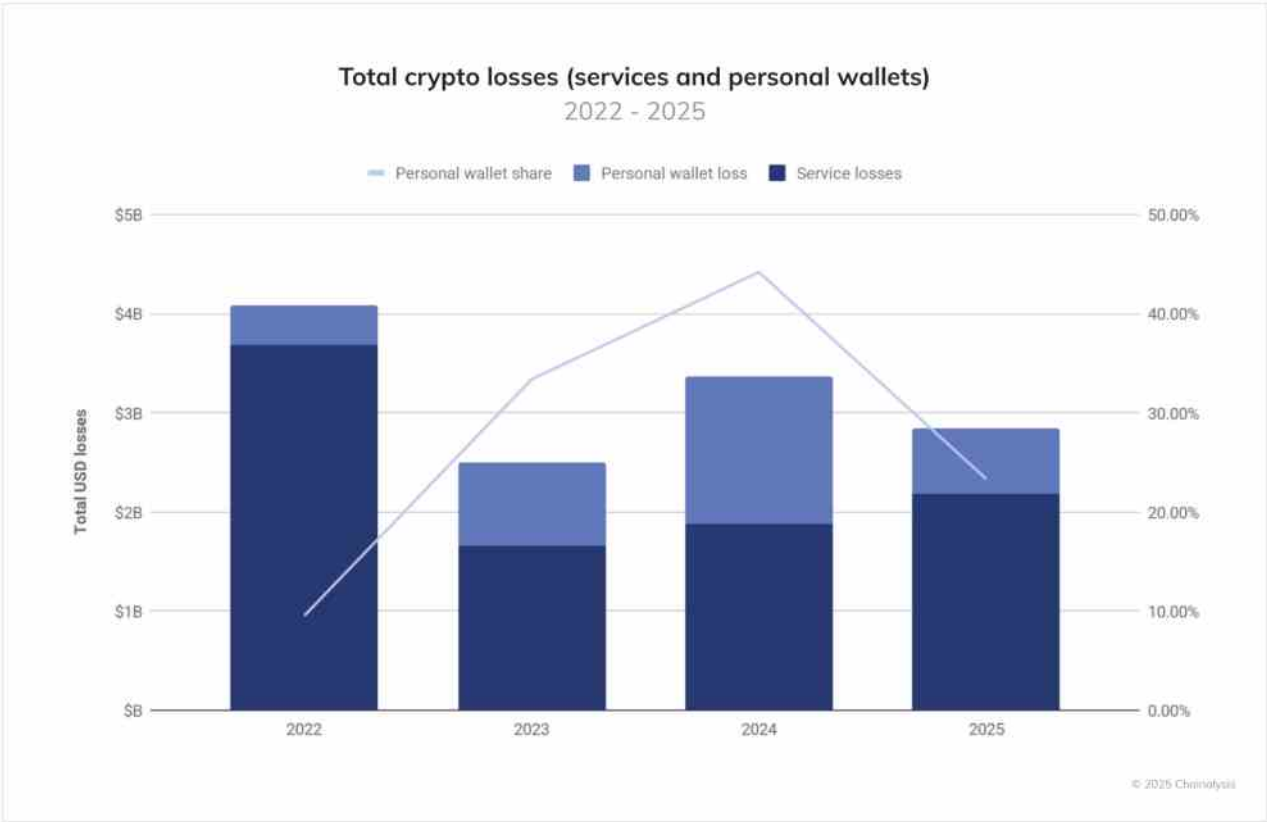
devastatingly effective, with Western tech firms having unknowingly hired thousands of North Korean workers, according to recent UN reporting.

Personal wallets: The underdocumented frontier for crypto crime

Chainalysis has developed new methodologies to identify and trace theft activity originating from personal wallets, a category of illicit activity that is by nature underreported but increasingly significant. This enhanced visibility reveals troubling trends in how attackers are diversifying their targets and tactics over time.

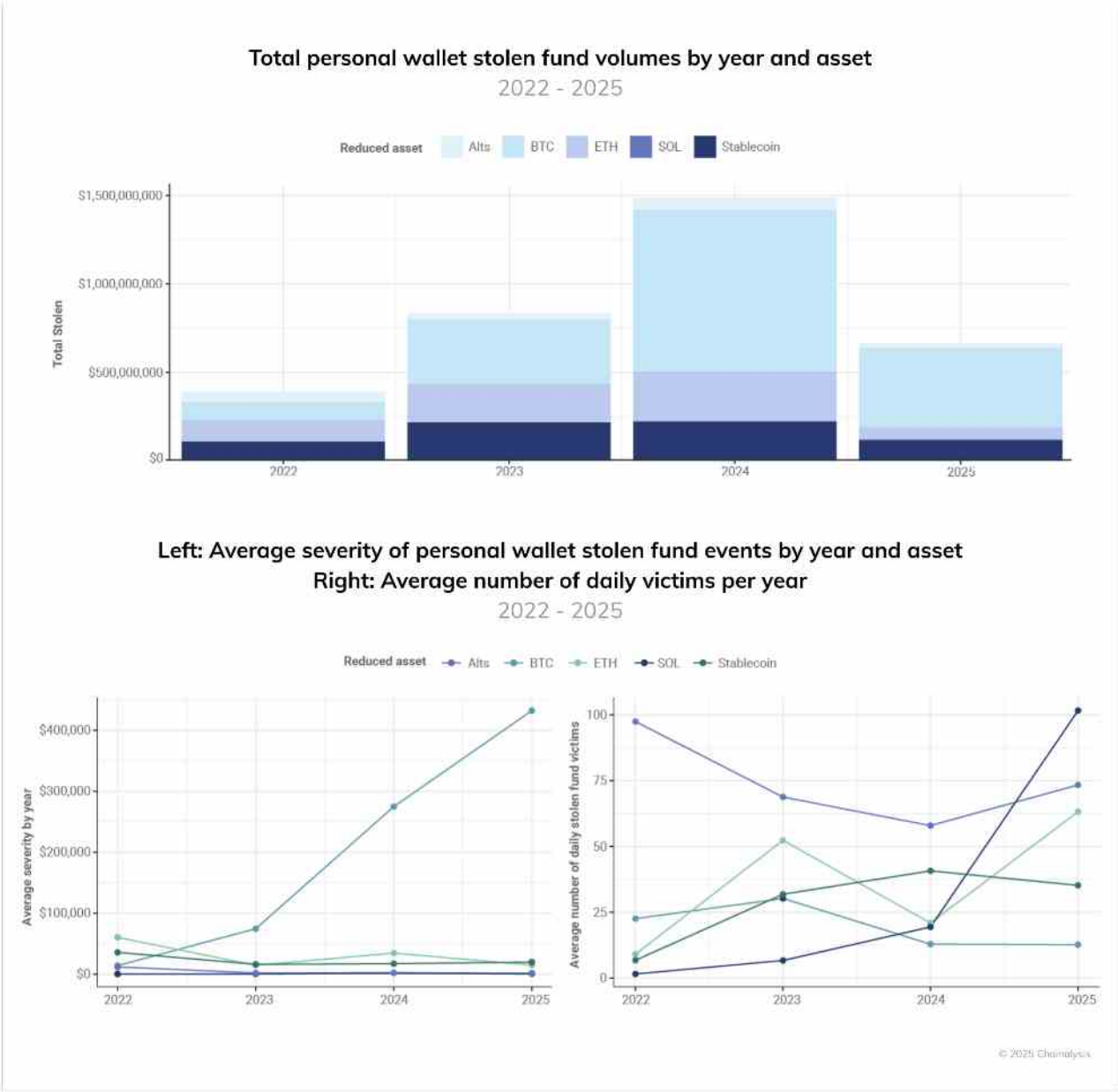
Personal wallet compromises make up a growing share of total ecosystem value stolen over time, as reflected in the chart below. The emergence of this trend likely reflects several factors:

1. Improved security practices at major services, pushing attackers toward individuals perceived as easier targets
2. The growing number of individual crypto holders
3. The increased value of the crypto held in personal wallets over time, as crypto prices for major assets continues to appreciate
4. The development of more sophisticated individual-targeting techniques, potentially facilitated by the growth in easy-to-deploy LLM AI tools

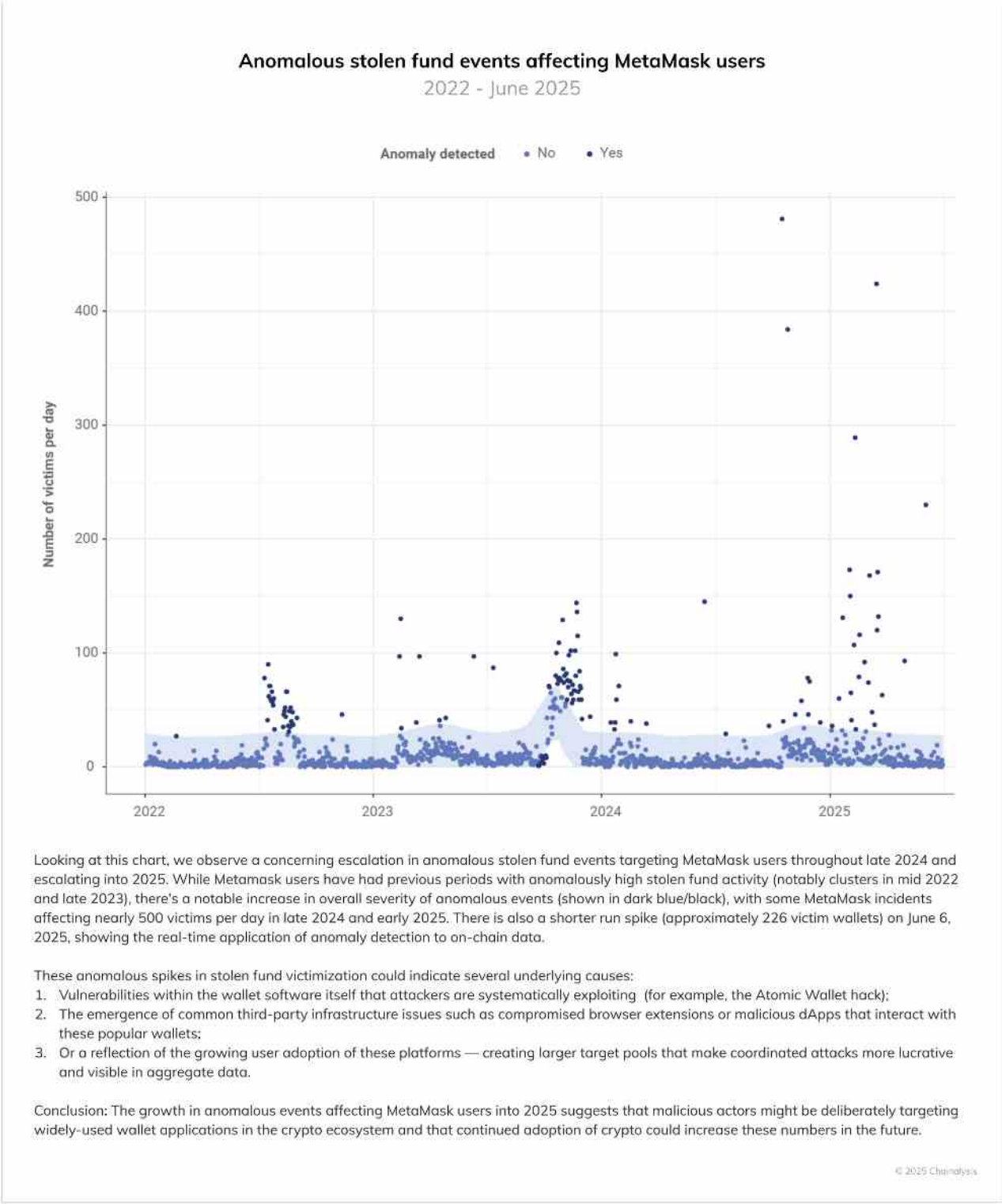


Breaking down the value stolen from personal wallets by asset is also revealing, shown in the chart below. Three key trends emerge from this expanded view. First, bitcoin theft accounts for a substantial share of stolen value. Second, the average loss resulting from

compromised personal wallets storing bitcoin has increased over time, suggesting attackers are deliberately targeting higher-value individual holdings. Third, the number of individual victims is increasing on non-Bitcoin and non-EVM chains like Solana.



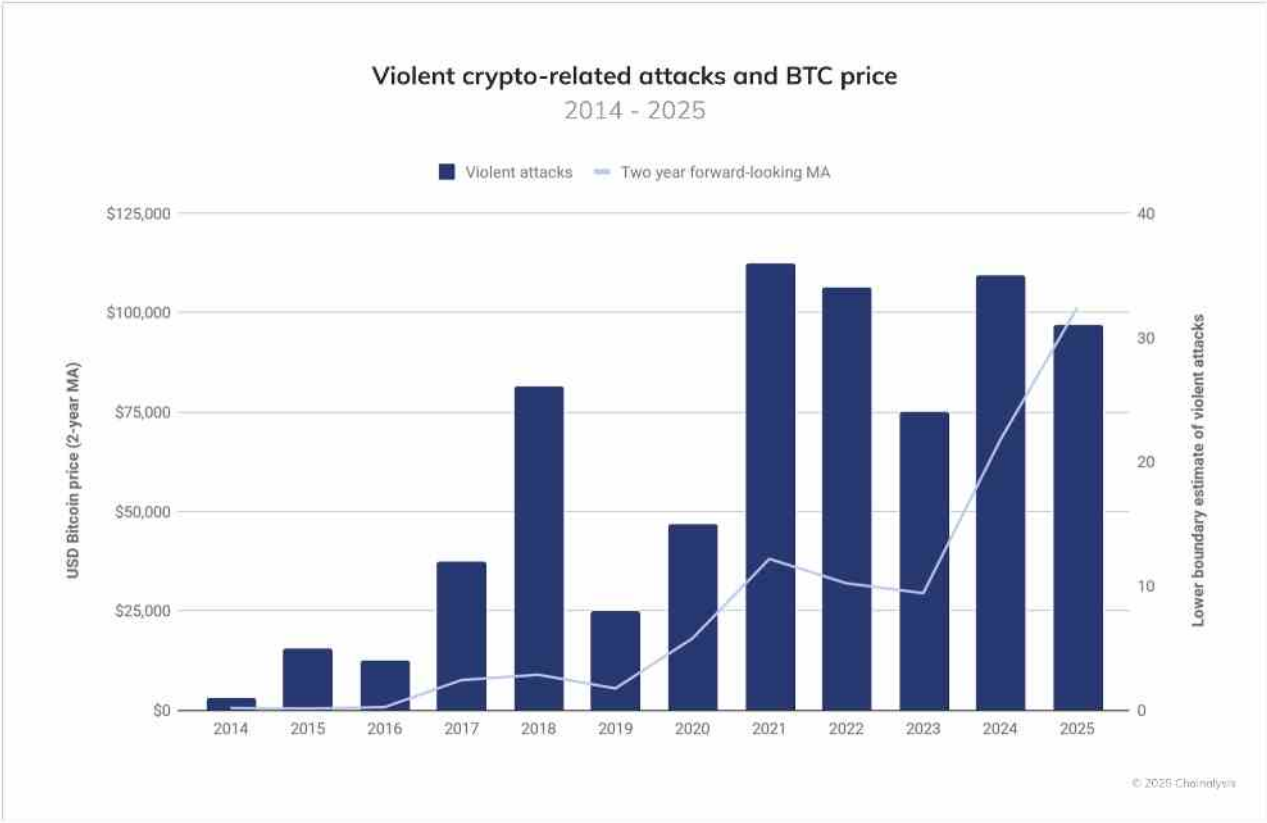
In total, these factors suggest that, while bitcoin holders are less likely to fall victim to targeted theft than individuals holding assets on chains, bitcoin holders experience more catastrophic losses in terms of value taken. The forward-looking implication is that, if the value of native assets increases, the value compromised from personal wallets will also likely rise.



The violence factor: When digital crime turns physical

One particularly disturbing subset of personal wallet theft incidents involves so-called “wrench attacks,” whereby attackers use physical violence or coercion against individuals to access their crypto holdings. Per the chart below, it is clear that 2025 is well on track to have potentially twice as many physical attacks as the next highest year on record. It is also worth noting that, since many attacks go unreported, the true number of such incidents is likely far higher.

Our analysis reveals a clear correlation between these violent incidents and a forward-looking moving average of bitcoin's price, suggesting that the future increase in asset values (and the perception of its future upward movement) may trigger additional opportunistic physical attacks against known crypto holders. Overall, while these violent attacks remain comparatively rare, the physical dimension — including maiming, kidnapping, and homicide — elevates the human impact of these cases to an extraordinary degree, as we will explore in the following case study.



Source: Jameson Lopp GitHub

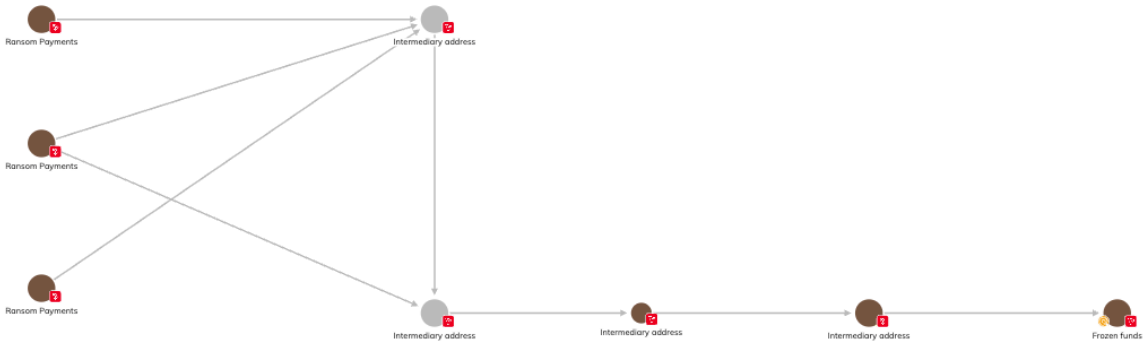
Case study: How blockchain analysis helped solve a high-profile kidnapping case in the Philippines

The intersection of violent crime and cryptocurrency laundering creates complex investigative challenges that require sophisticated analytical approaches. A recent high-profile case from the Philippines demonstrates how blockchain analysis can provide crucial investigative leads, even in the most serious criminal investigations.

In March 2024, the abduction and murder of Anson Que, CEO of Elison Steel, sent shockwaves through the Philippines business community. Que and his driver, Armanie Pabillo, were abducted on March 29 in Bulacan province. Their bodies were later discovered in neighboring Rizal province, bound and showing clear signs of assault. Initially believed to be a ₱20 million kidnapping case, the investigation revealed that approximately ₱200 million had been paid in ransom in the hope that Que would be released.

The Philippines National Police (PNP) alleged that junket operators 9 Dynasty Group and White Horse Club facilitated an elaborate money laundering operation following the abduction. The scheme involved converting the ransom payments — originally made in Philippine Pesos and US Dollars — into cryptocurrency using e-wallets meant exclusively for casino gaming, shell accounts, and digital assets to obscure the money trail.

Using Chainalysis Reactor, our Global Services team worked alongside PNP investigators to map the flow of the ransom payments. Blockchain analysis revealed how the separate ransom payments moved through a series of intermediary addresses, where the funds were collated and further laundered through additional intermediary addresses. With PNP support, Chainalysis notified Tether and worked with them to successfully freeze a portion of the funds held in USDT.



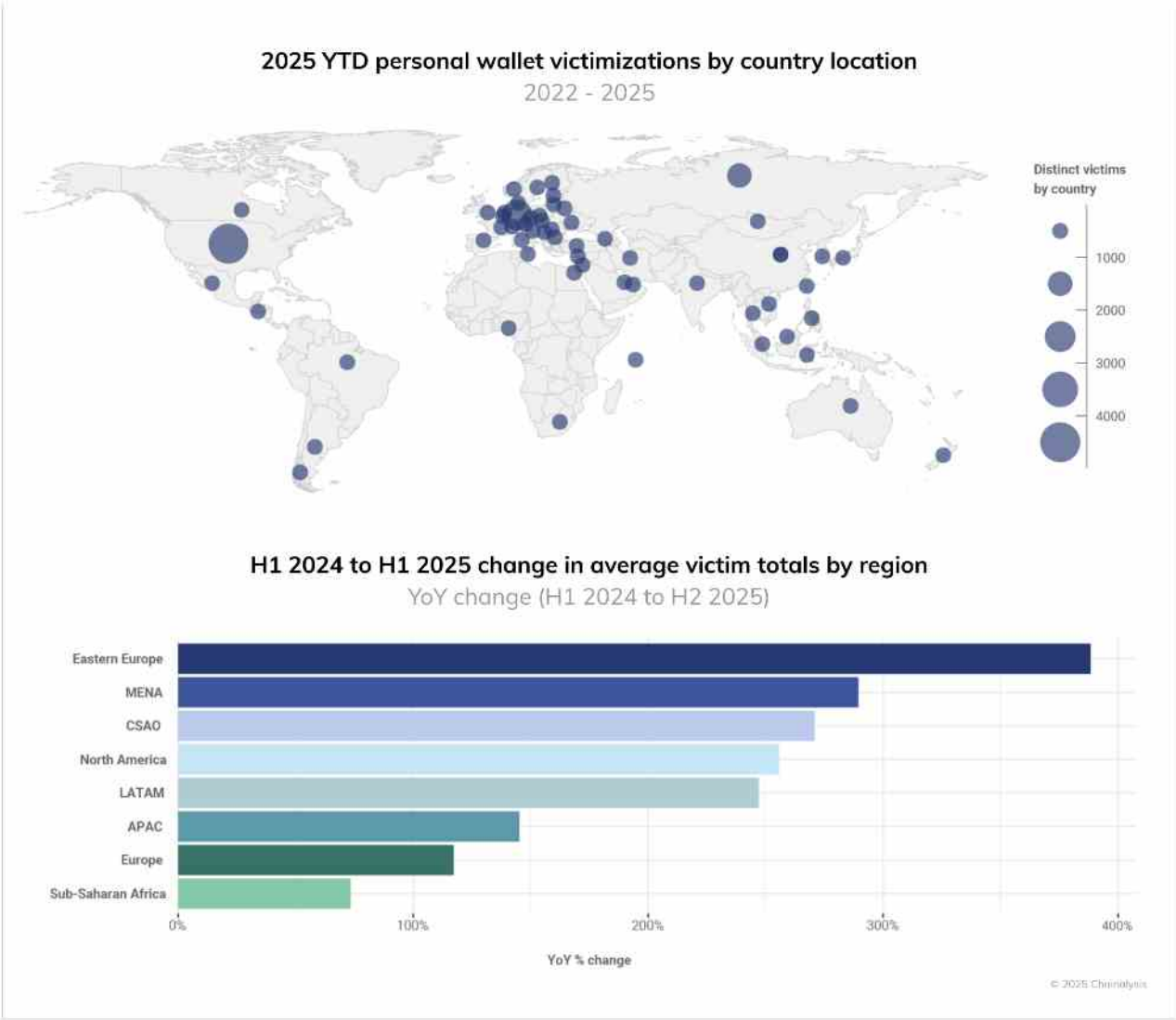
Notably, the laundering techniques employed were relatively unsophisticated — a pattern consistent with many organized crime groups that adopt cryptocurrency for its speed and perceived anonymity but lack deep technical expertise. Unlike traditional financial investigations where evidence is often scattered across different institutions, the blockchain provides a single, authoritative, and immutable ledger. This enables investigators to follow movements in real time, map networks, and generate leads that span continents.

The tragic loss of Anson Que and Armanie Pabillo reminds us of the real human cost behind these crimes. But their case also demonstrates that the immutable nature of blockchain technology can serve as a powerful tool for justice — ensuring that those who exploit others cannot simply disappear into the digital shadows.

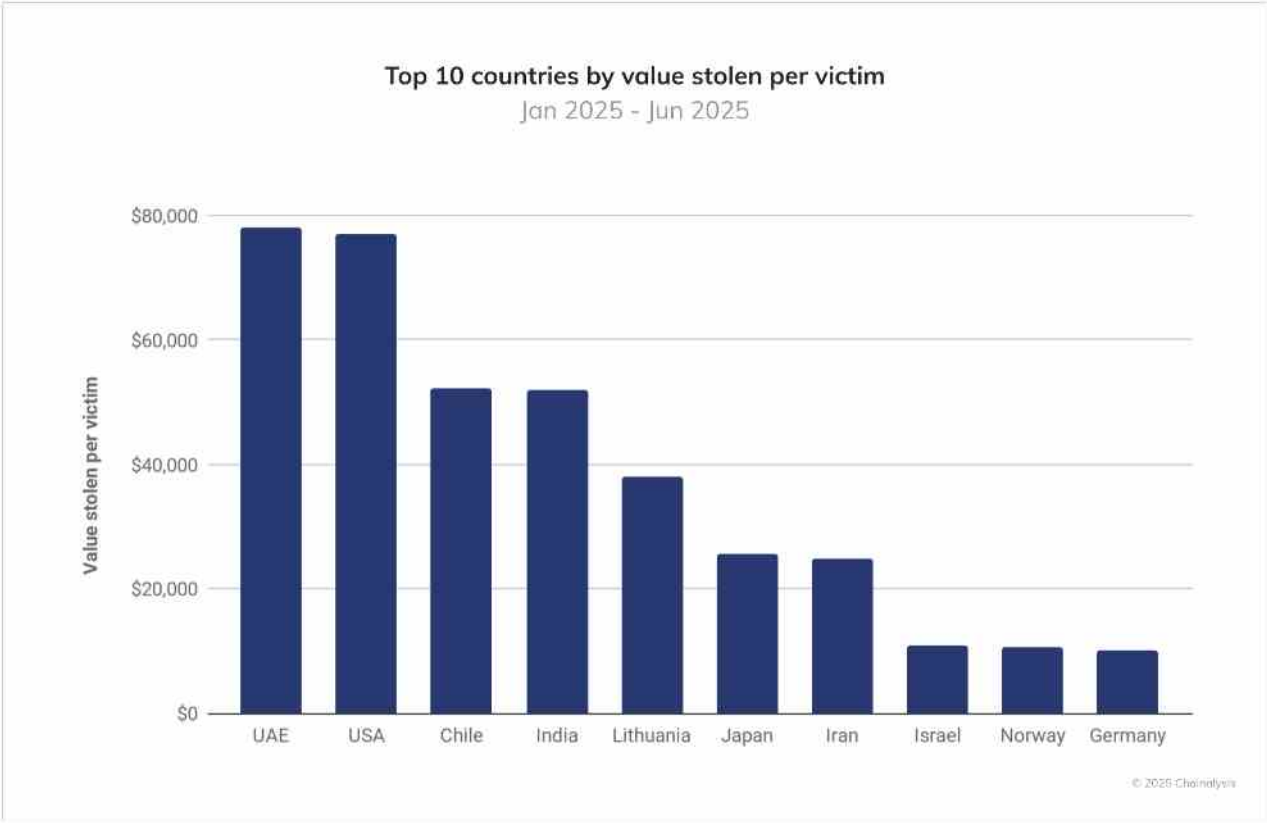
Geographic patterns: Victimization around the world

Leveraging Chainalysis' geolocation data intersected with reported cases of stolen funds, we can estimate the global distribution of personal wallet victimizations. Note: these data include only known stolen fund events affecting personal wallets that have reliable geolocation data. They are therefore not a comprehensive view of all global stolen fund activity in 2025.

So far in 2025, the U.S., Germany, Russia, Canada, Japan, Indonesia, and South Korea top the list of highest victim counts per country, whereas Eastern Europe, MENA and CSAO saw the most rapid H1 2024 to H1 2025 growth in victim totals.



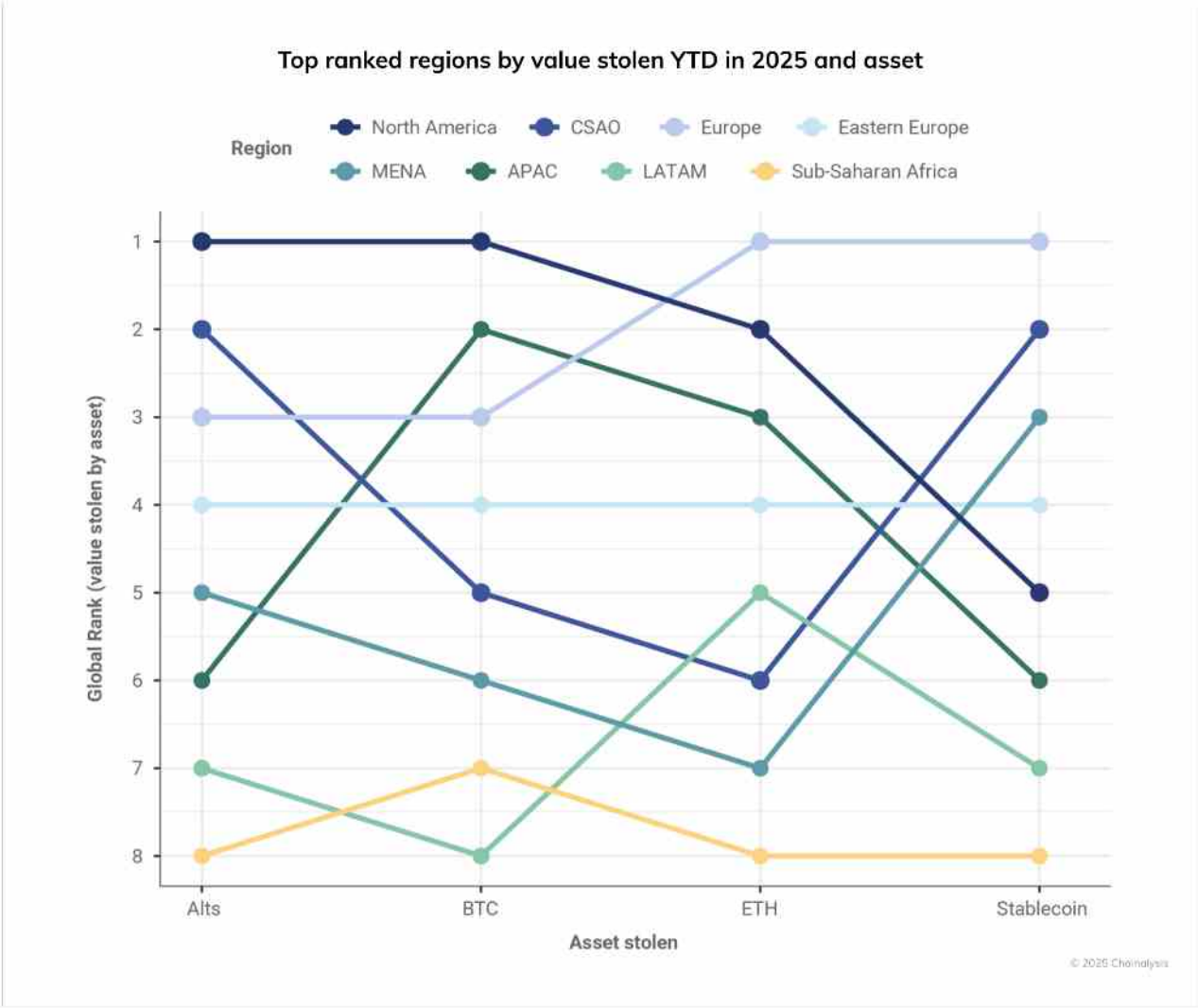
A somewhat divergent list of countries emerges when plotting the value stolen per victim in 2025. As shown in the chart below, the U.S., Japan and Germany remain in the top 10, but the UAE, Chile, India, Lithuanian, Iran, Israel, and Norway have some of the highest victimization severity rates globally.



Regional variation in assets stolen from personal wallets

Our 2025 data reveal emerging patterns of regional concentration in crypto thefts. The chart below ranks regions based on the total values stolen YTD by asset.

North America dominates both bitcoin and altcoin theft, ranking first in both categories. This concentration likely reflects the region's high crypto adoption rates and the operation of threat actors capable of targeting large individual holdings. Europe leads the world in ether and stablecoin theft, potentially indicating some combination of either adoption rates for these assets or an attacker preference for more liquid, easily transferable assets.

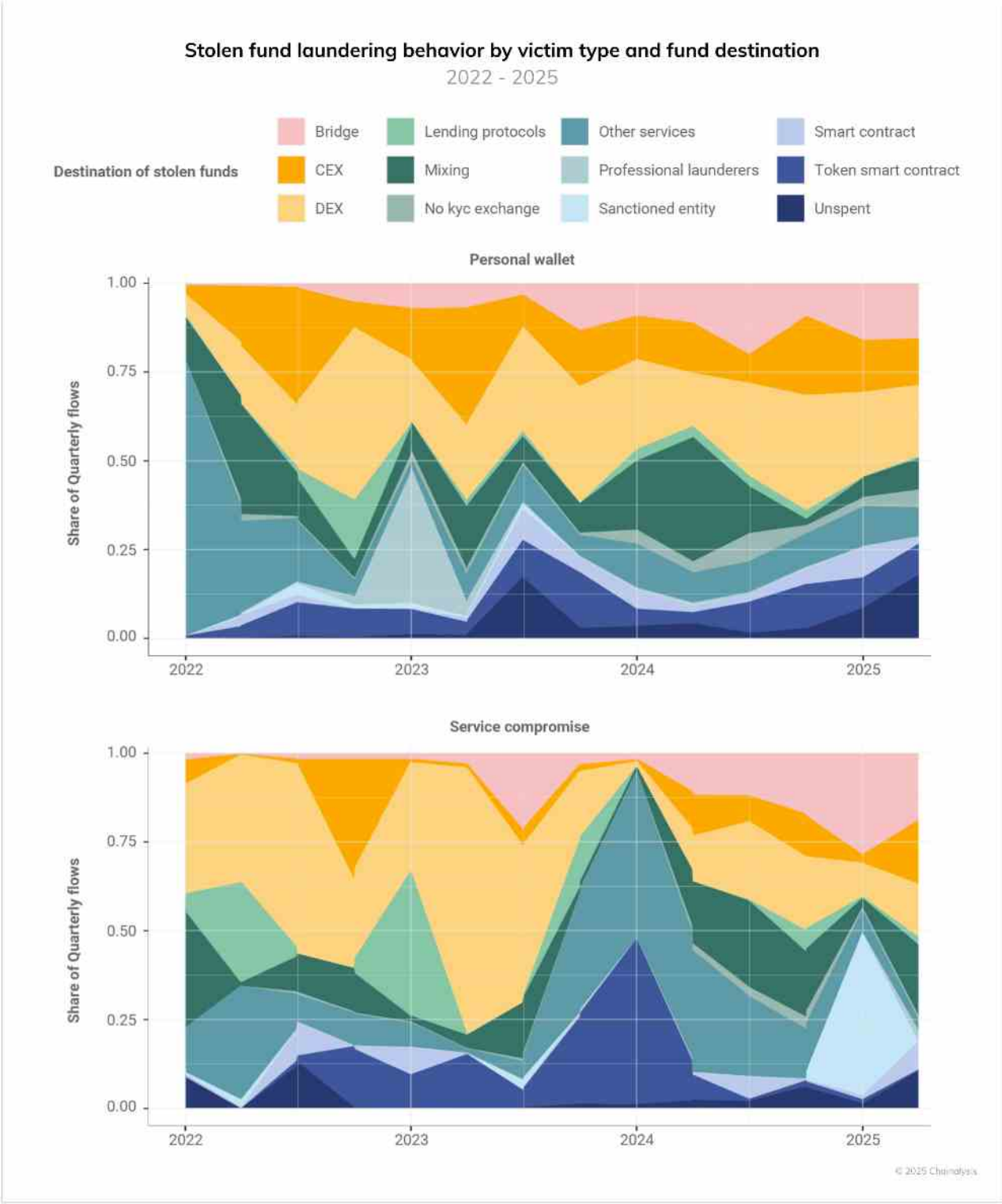


APAC ranks second in terms of total BTC stolen and third in terms of stolen ETH, whereas CSAO ranks second in terms of stolen altcoin and stolen stablecoin value. Fairly consistently, Sub-saharan Africa ranks the lowest in terms of value stolen (second to last in terms of compromised BTC), which is most likely indicative of lower wealth levels in this region and not necessarily a signal of lower victimization rates among crypto users.

The economics of crypto laundering

Understanding how stolen funds move through the crypto ecosystem provides crucial insights for both prevention and enforcement efforts. Our analysis reveals that laundering behavior differs significantly between personal wallet compromises and service attacks, reflecting different risk profiles and operational requirements.

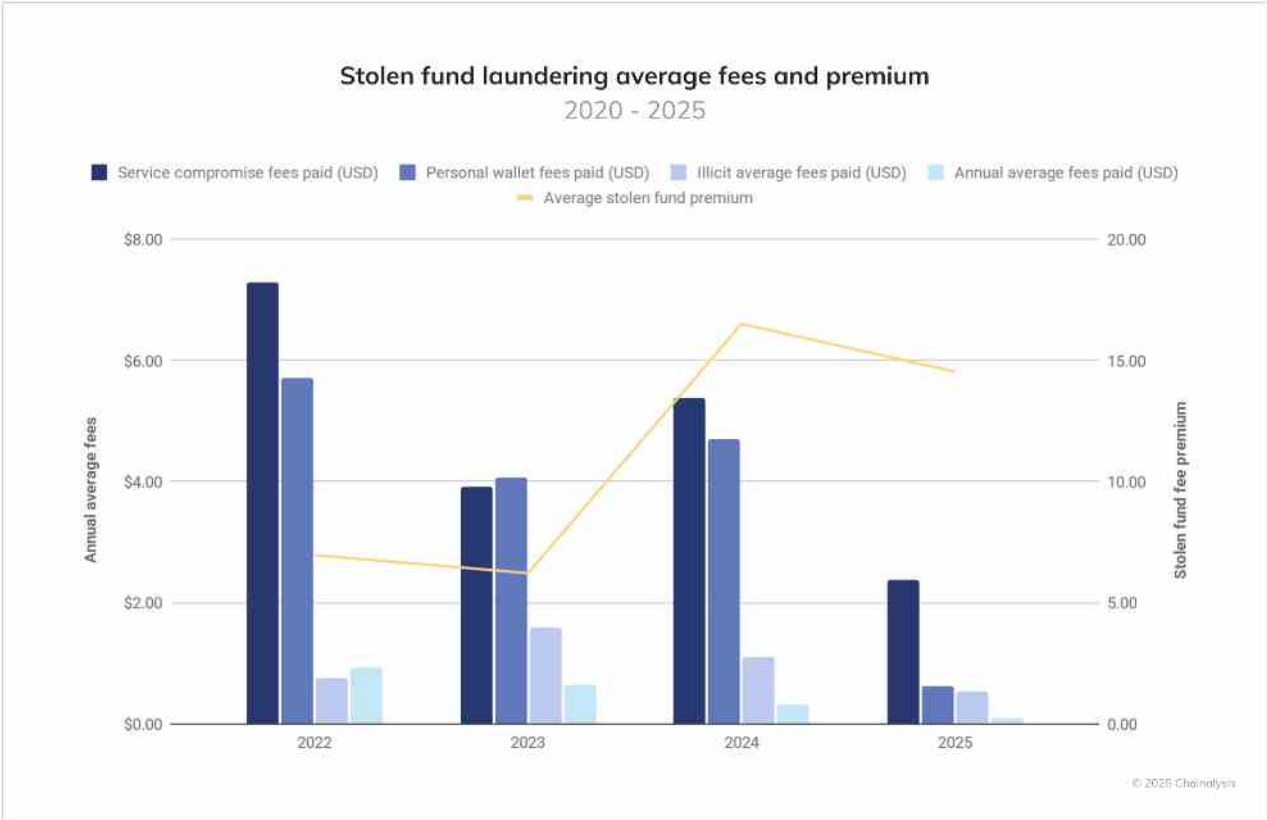
For example, in 2024 and 2025, threat actors targeting services made significant use of bridges as a means of laundering funds by chain hopping. Mixer use also figures more prominently into thieves targeting services than for those targeting personal wallets. By contrast, funds stolen from personal wallets tend to interact more with token smart contracts (potentially suggesting a swap); send value into sanctioned entities (notably Garantex), which might suggest a Russian perpetrator intersection; and flow to centralized exchanges (CEXs), suggesting less sophisticated laundering techniques.



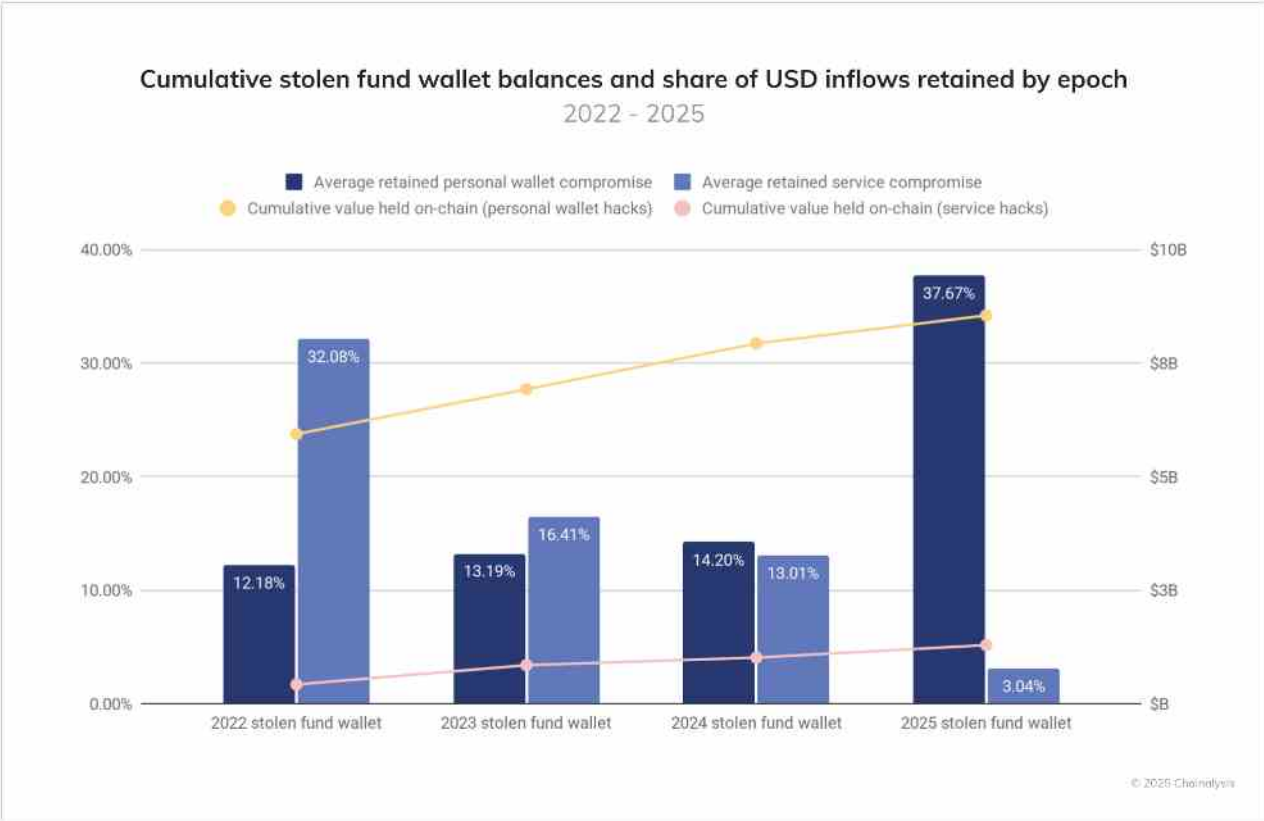
In the course of this laundering activity, stolen fund actors consistently pay premium fees to move their illicit proceeds, with costs varying dramatically over time. Interestingly, as adoption of blockchains like Solana and various layer 2s have driven down the cost of transactions overall, stolen fund actors are, on average, paying a higher premium over this same period. So, while the average fee has declined 89% from 2022 to 2025 YTD, the premium paid by stolen fund actors over this base rate has increased by 108% over the same timeframe. It is also notable that threat actors targeting services typically pay

higher premiums than those conducting personal wallet thefts, likely reflecting the urgency of moving large sums before detection and freezing measures can be implemented.

These patterns also broadly suggest that, while the vast majority of hacking is financially motivated (the June 19 hack of Nobitex being an obvious recent exception), stolen fund actors do not optimize on the cost of transactions on-chain, but instead heavily prioritize speed and transaction finality.



Interestingly, not all stolen funds enter into immediate laundering cycles. Personal wallet compromises in particular increasingly remain on-chain, with significant balances remaining stationary on attacker-controlled addresses, rather than quickly being laundered on chain or converted into fiat currency. This “HODLing” behavior among criminals may reflect confidence in their operational security, or simply mirror broader crypto investment strategies.



Prevention and mitigation strategies

The surge in both service and personal wallet compromises demands a multi-layered approach to crypto security. For service providers, the lessons from 2025's major breaches underscore the continued importance of robust security cultures, regular security audits, and employee screening processes that can detect social engineering attempts. Code audits have become increasingly critical, with smart contract vulnerabilities representing a growing attack vector. Technical wallet infrastructure improvements, particularly the implementation of multisignature hot wallet addresses, have proven essential for institutional security, providing additional layers of protection even when individual keys are compromised.

For individuals, the growing threat to personal wallets requires a fundamental reassessment of security practices. The correlation between violent attacks and bitcoin price movements suggests that operational security, such as keeping cryptocurrency holdings private, may be as important as technical security measures (such converting holdings into privacy coins or using cold storage wallets). Users in high-growth victimization countries should be particularly vigilant about their digital footprint and physical security.

Additionally, personal security in the physical world has become an urgent concern as crypto-related kidnappings and violent crimes escalate. High-profile cases, including families targeted for their known cryptocurrency wealth, demonstrate that digital asset holders must now consider traditional personal security measures. This includes being cautious about public displays of wealth, avoiding social media posts that reveal crypto

holdings or trading activities, and implementing physical security protocols such as varying daily routines and being aware of surveillance. For substantial holders, professional security consultation may be warranted, as the intersection of digital wealth and physical vulnerability creates unprecedented risks that traditional security frameworks have yet to fully address.

Looking ahead: A critical inflection point

Thus far, 2025 data present a sobering picture of how crypto crime is evolving. While the ecosystem has matured in terms of regulatory frameworks and institutional security practices, threat actors have correspondingly upgraded their capabilities and expanded their range of targets.

The ByBit hack demonstrates that even sophisticated industry entities remain vulnerable to advanced persistent threats, while the surge in personal wallet compromises shows that individual holders of cryptocurrency face unprecedented risks. The geographic expansion of crypto crime, and the correlation between asset prices and violent attacks add additional complexity to an already challenging security environment.

However, the detailed blockchain analysis that enables this reporting also provides the foundation for more effective countermeasures. Law enforcement armed with comprehensive transaction analysis can follow the money more effectively than ever before, while service providers can implement more targeted security measures based on observed attack patterns.

The crypto industry stands at a critical inflection point. The same transparency that enables unprecedented criminal behavior analysis also provides the tools for more effective prevention and enforcement. The challenge lies in implementing these capabilities quickly enough to stay ahead of rapidly evolving threats.

As we move into the second half of 2025, the stakes for cryptosecurity have never been higher. With stolen funds projected to potentially reach $4 billion by year’s end, the industry’s response in the coming months will likely determine whether crypto crime continues its concerning trajectory or begins to plateau as defensive measures mature.

See how you can stay ahead of emerging threats

Request a personalized demo

This website contains links to third-party sites that are not under the control of Chainalysis, Inc. or its affiliates (collectively "Chainalysis"). Access to such information does not imply association with, endorsement of, approval of, or recommendation by Chainalysis of the site or its operators, and Chainalysis is not responsible for the products, services, or other content hosted therein.

This material is for informational purposes only, and is not intended to provide legal, tax, financial, or investment advice. Recipients should consult their own advisors before making these types of decisions. Chainalysis has no responsibility or liability for any decision made or any other acts or omissions in connection with Recipient's use of this material.

Chainalysis does not guarantee or warrant the accuracy, completeness, timeliness, suitability or validity of the information in this report and will not be responsible for any claim attributable to errors, omissions, or other inaccuracies of any part of such material.