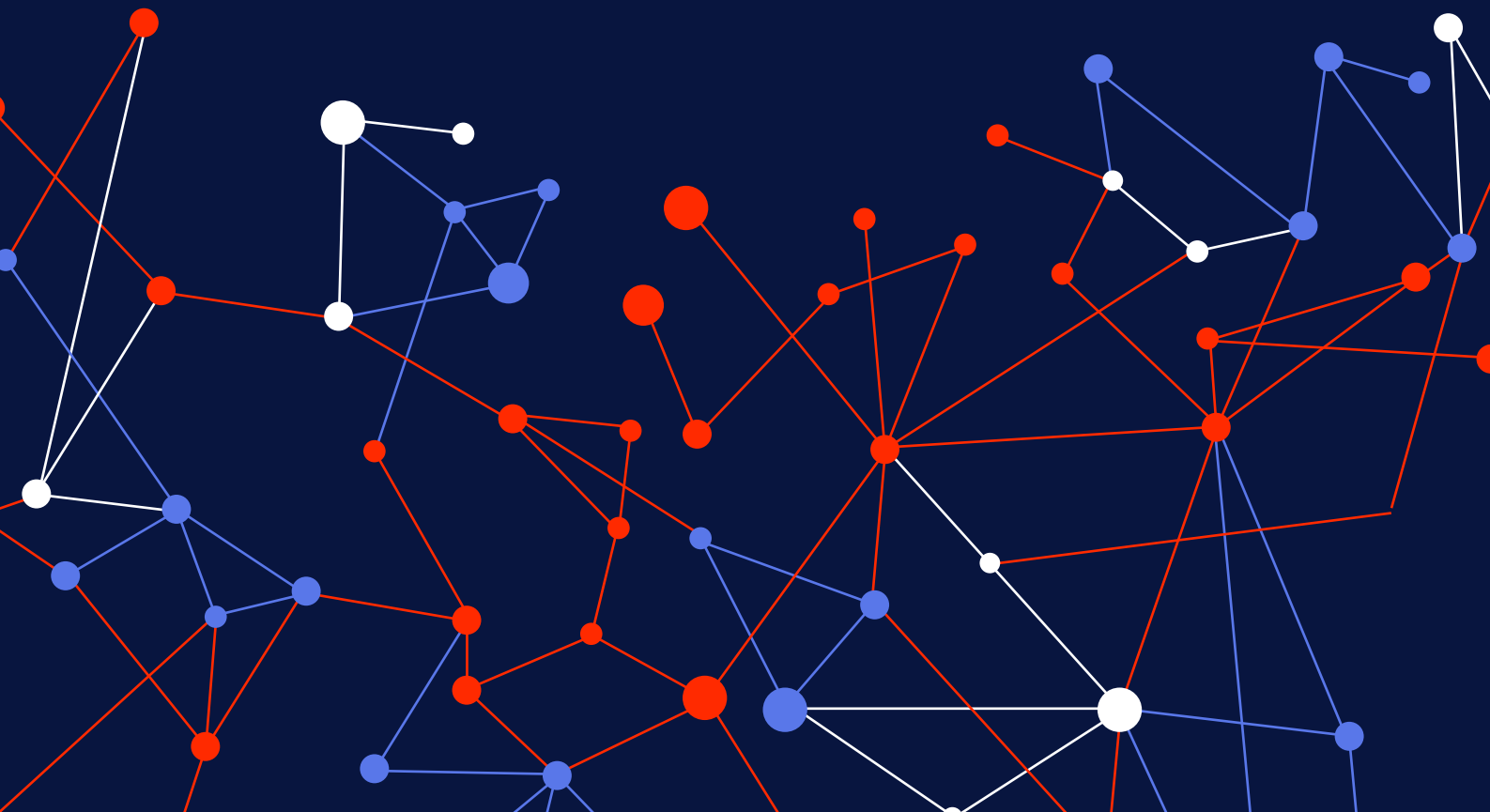
GLOBAL LEDGER

The 2026 Laundering Race Report

Cautious hackers, harder-to-trace flows: fundamental shifts in crypto crime call for a new way of managing risk



Key Takeaways

1

$4.04B

Stolen in 2025 across 255 crypto hacks — roughly half of the FTX customer shortfall.

2

2 sec

The fastest 1st funds move — faster as you can blink.

3

x2

Speed of 1st funds move in H2'25 vs H1'25 — like the same race run at double speed.

4

~76%

Or in ~195 out of 255 cases, funds moved before disclosure — before the industry could even react.

5

~2.1×

The avg. disclosure gap narrowed from ~23h to ~11h — like waiting until tomorrow vs. later today.

6

~50%

Or $1.97B of funds remain unspent — comparable in scale to the Bybit incident losses.

7

~42%

Tornado Cash used in ~ ⅖ of cases — nearly every second case.

8

~7%

Or $263.23M of funds returned — less than the amount stolen in the 2022 Wormhole hack.

Bonus: Checklist

Executive summary

An H1–H2 2025 breakdown of 255 hacks shows that hackers are getting faster. In the fastest case, the first movement of stolen funds occurred in as little as 2 seconds — 2× faster than in H1 2025, before you even have time to blink. This is also 2× faster than the quickest public incident reporting. It means illicit assets often start moving before the industry has any signal that an incident has occurred.

Across the year, in ~76% of hacks out of 255 cases, funds moved before public reporting, exposing VASPs before any disclosure. However, as public reporting accelerated in H2, funds from hacks sent to CEXs fell by 5.9× compared to H1 ($77.39 million vs $453 million). This indicates that attackers increasingly avoided direct routes from hacks into centralized exchanges due to a higher probability of transaction blocking by risk-aware compliance teams. As a result, attackers shifted toward quieter, more fragmented laundering.

During 2025, the use of Tornado Cash nearly doubled after sanctions were lifted. Its share among mixer usage grew from around 40% in H1 to nearly 75% in H2, making Tornado Cash the dominant mixer during that period. It turns out that hackers now have a legitimate way for convenient cash-outs.

At the same time, bridges overall overtook mixers as the preferred tool for laundering, likely due to their speed, liquidity, and decentralized nature. In 2025, over $2.01 billion of stolen funds were routed through bridges — nearly 49.75% of total losses and over 3× more than via mixers and privacy protocols.

This Global Ledger report presents a full-year picture of laundering speed, combining lessons from 119 hacks in H1 2025 with new findings from H2 2025. Alongside timing and laundering patterns, it offers actionable insights and a practical checklist to help compliance teams detect and prevent risk before it catches them.

Problem

Hackers set a record in the fastest cases of H2 2025, moving funds 2× faster than in H1

In 2025, public incident reporting became faster. On average, in H2 2025, attackers were 11 hours 13 minutes and 16 seconds ahead of public reporting. In H1 2025, this gap was 23 hours 14 minutes and 18 seconds, meaning the average **disclosure gap narrowed by ~2.1× in H2.**

This shift slowed post-incident laundering, as public disclosure increased the likelihood of freezes and alerts, forcing attackers to change how they move funds. In H1 2025, the fastest time from the first move to the VASP/mixer was **48 seconds**, while in H2 2025, it slowed to **2 minutes — 2.5×** slower.

A similar slowdown appears as funds approach endpoints (VASPs/mixers). In the fastest H1 case, the last funds reached a VASP/mixer in 2 minutes 57 seconds. In H2, it took 8 minutes 34 seconds to launder funds, which is **nearly 3× slower**. This was driven by larger amounts and more staged movement in H2, extending the laundering timelines, unlike the fastest case in H1, where the laundered amount was **5.6× smaller** and moved in a single step.

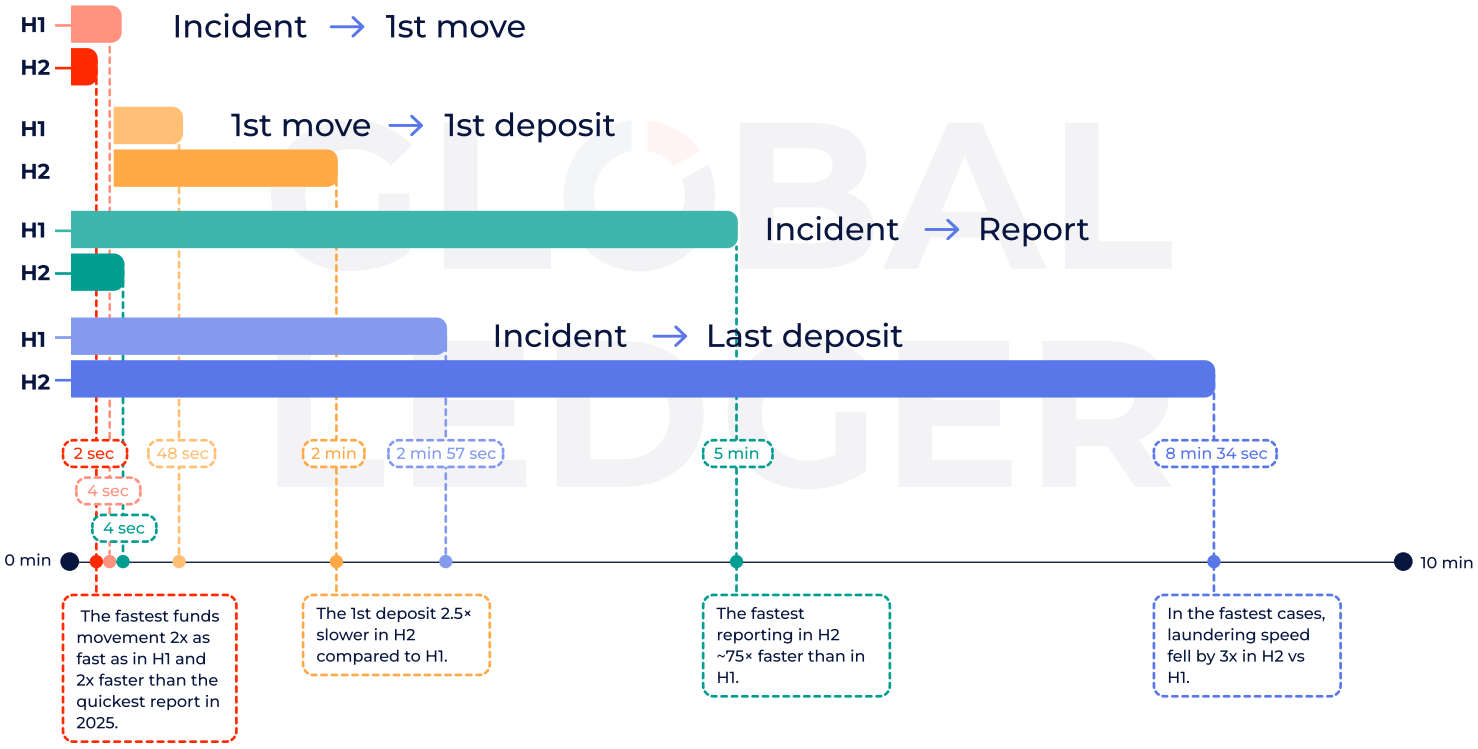
Despite slower laundering after disclosure, attackers accelerated the initial movement of stolen funds. In 2025, hackers reached a new speed threshold. In the fastest case, funds moved in just **2 seconds — twice as fast as in H1 2025**. This is also 2× faster than the quickest public incident reporting.

This speed “advantage” allowed attackers to act before the market even knew a hack had occurred. Across the year, **~76% of hacks** (around 195 out of 255 cases) saw funds move before the incident was publicly reported. The share increased sharply in H2 to 84.6%, up from 68.1% in H1 2025, representing almost **25% increase** compared to H1.

As a result, hackers take quick first moves, but then slow down, preferring to be more “cautious” once an incident becomes public.

* For this research, we define VASPs and mixers as endpoints, i.e., the points where illicit funds enter services that sharply reduce traceability. Once funds reach these endpoints, we consider further on-chain tracking unreliable due to obfuscation, custodial pooling, or jurisdictional limits. This definition ensures consistency in measuring laundering speed and behaviour across cases. While deeper tracing is technically possible, it often carries a high risk of error and falls outside the scope of this analysis.

Hackers set record in the fastest cases, moving funds 2× faster in H2



Closing the response gap requires a shift from ad-hoc reactions to continuous monitoring, standardized reporting, and proactive incident response

There are a few key steps to closing this response gap. First, Web3 projects must implement real-time on-chain and off-chain security monitoring to detect suspicious behavior and anomalies as they happen. Without internal detection and alerting, no external ecosystem response can move fast enough.

Second, the industry needs a widely adopted standard for incident reporting. Initiatives like SEAL911 already provide an effective emergency hotline for coordinating response and asset recovery, but too many projects still approach incident response reactively rather than proactively.

Closing the response gap ultimately requires a shift from ad-hoc reactions to continuous monitoring, standardized reporting, and proactive incident response, so defenders can operate at the same speed as attackers.

Yev Broshevan

CEO & Co-Founder at Hacken

What is at stake?

The risk window is becoming wider

Faster disclosure has shortened the time attackers can move unnoticed, but it has not eliminated the risk: stolen funds can still reach regulated exchanges through multi-step routes, albeit later. At the time of the research, over **$1.97 billion** (48.76% of total losses) remained **unspent**, meaning the funds didn't move or stopped moving. Some of them are likely still in the process of being laundered, as attackers may be waiting for the heat to die down.

As laundering has slowed, the real exposure now lies beyond the first seconds after a hack — in the extended period that follows, when illicit funds move in fragmented steps. Closing this gap requires a shift from ad-hoc reactions to continuous monitoring, supported by standardized reporting and proactive incident response.

> **Integrating high-speed community alerts can be valuable if the data is verified**
>
> Integrating high-speed community alerts can be valuable, but only if the data is verified by a credible party. Otherwise, such systems risk abuse. Labels must be evidence-based or not applied — full stop. Probabilistic or insight-driven layers can exist, but they belong to investigators, not compliance workflows.

Richard Sanders

Investigator, volunteer for Ukraine

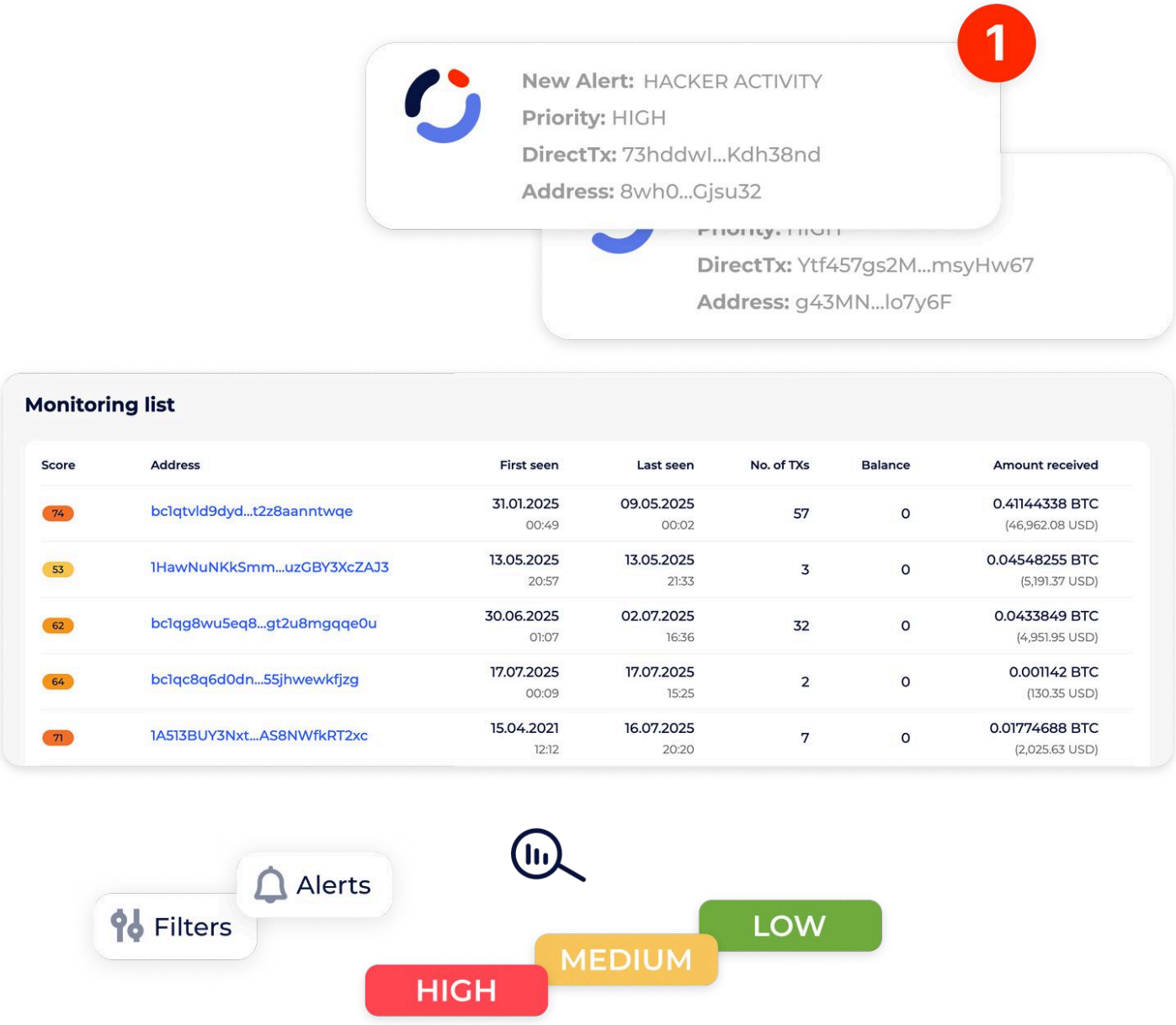
Prevent risks with Global Ledger

Real-time monitoring

When stolen funds start moving before public disclosure, the window to detect and stop illicit flows becomes extremely narrow. This is where real-time monitoring matters most — enabling VASPs to demonstrate reasonable efforts to regulators and partners, rather than just detect risk internally.

Steps compliance teams can take:

- Turn on proactive monitoring with a system that performs 500,000 AML checks each day to ensure no threats go unnoticed.
- Use AI-powered alerts to prioritise high-impact risks.
- Build procedures to return “dirty” crypto to the source before it contaminates clean funds.
- Block sanctioned or terrorist-linked assets and submit a SAR/STR response quickly.



Ready to monitor in real time? We'll walk you through it.

Schedule a Demo

Problem

Slower laundering provokes multistage exposure

In H2 2025, the average **laundering speed fell by ~25%**, driven by faster public disclosure and increased post-incident scrutiny. Rapid post-disclosure movements now raise the risk of alerts and freezes. As a result, only ~19.6% of cases (out of 255 in 2025) saw all stolen funds reach the last deposit before public disclosure, down from 22.7% in H1 to 16.9% in H2.

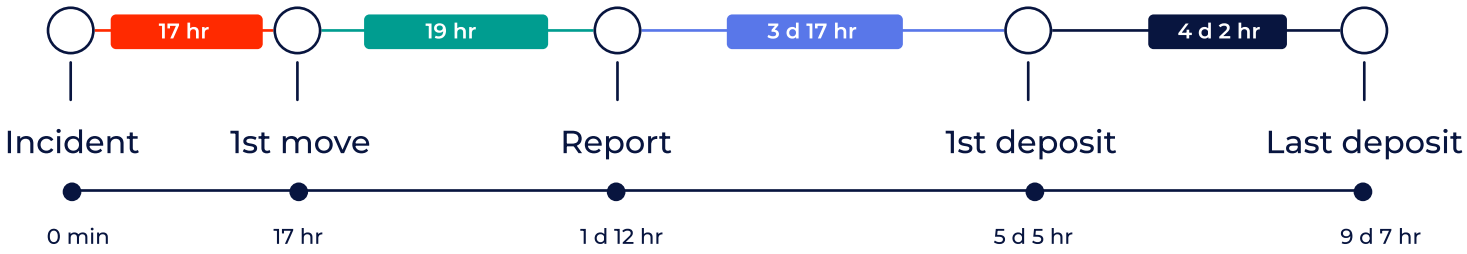
Still, **attackers remain fast at the start**, allowing them to make the first move before public disclosure and slow down to plan subsequent steps. The average time from a hack to the first movement of funds was ~17 hours (15 hours in H1 and nearly 19 hours in H2), while public disclosure followed on average ~2.1× later.

As a result, instead of rushing to cash-out, hackers increasingly wait after the first move. Stolen funds typically reach the first mixer/VASP in about 5.2 days after the incident, with H2 cases being ~1.8× slower than in H1. Cash-out is therefore often **intentionally delayed**, with portions of funds left inactive until monitoring intensity declines.

This waiting period extends through the rest of the laundering process. In ~28.2% of cases (≈72 hacks), the last deposit was made within a single day; in 41.5% (≈106 cases), within one week; and in 50.4% (≈129 cases), within 29 days, while 5.8% took longer than one month. Across all these thresholds, H2 showed a slowdown of several percentage points compared to H1.

On average, attackers needed **~9.3 days** to send all stolen funds to the last deposit, increasing from ~8 days in H1 to 10.6 days in H2.

On average, the report comes 19 hours later than the first move



As a result, with more rapid reporting and increased ecosystem visibility, attackers are increasingly relying on multistage laundering, where their traces are harder to detect.

Slower laundering favors investigators if monitoring is continuous, automated

The slowdown of illicit funds indicates a shift toward more ‘patient’ laundering strategies. This slower pace gives investigators more time to map relational networks, freeze wallets early, and coordinate actions across jurisdictions before funds are dispersed. However, taking advantage of this opportunity requires continuous, automated monitoring—something most legacy compliance frameworks lack.

Mudassar Malik

CEO and founder of Deconflict.com

What is at stake?

1 Multistage laundering “fragments” risk

While hackers may win the “sprint” at the moment of the exploit, laundering increasingly happens across multiple stages. Multistage laundering, used **in ~99% of hacks**, makes risk harder to spot. In H1 2025, there were three hacks (2.5%) where all funds went to VASP/mixer within the first move. In H2 2025, there were no such cases. It is also worth mentioning that staged and fragmented laundering was already used before, but in H2 it became more common, with funds spread across many smaller transfers. This fragmentation correlates with longer laundering timelines.

With such a laundering approach, hackers broke balances into many smaller transfers distributed across multiple unhosted wallets. Then routed through mixers, as well as decentralized infrastructure — cross-chain bridges, DEXs, and instant swap services — which significantly increases the complexity of tracing stolen funds.

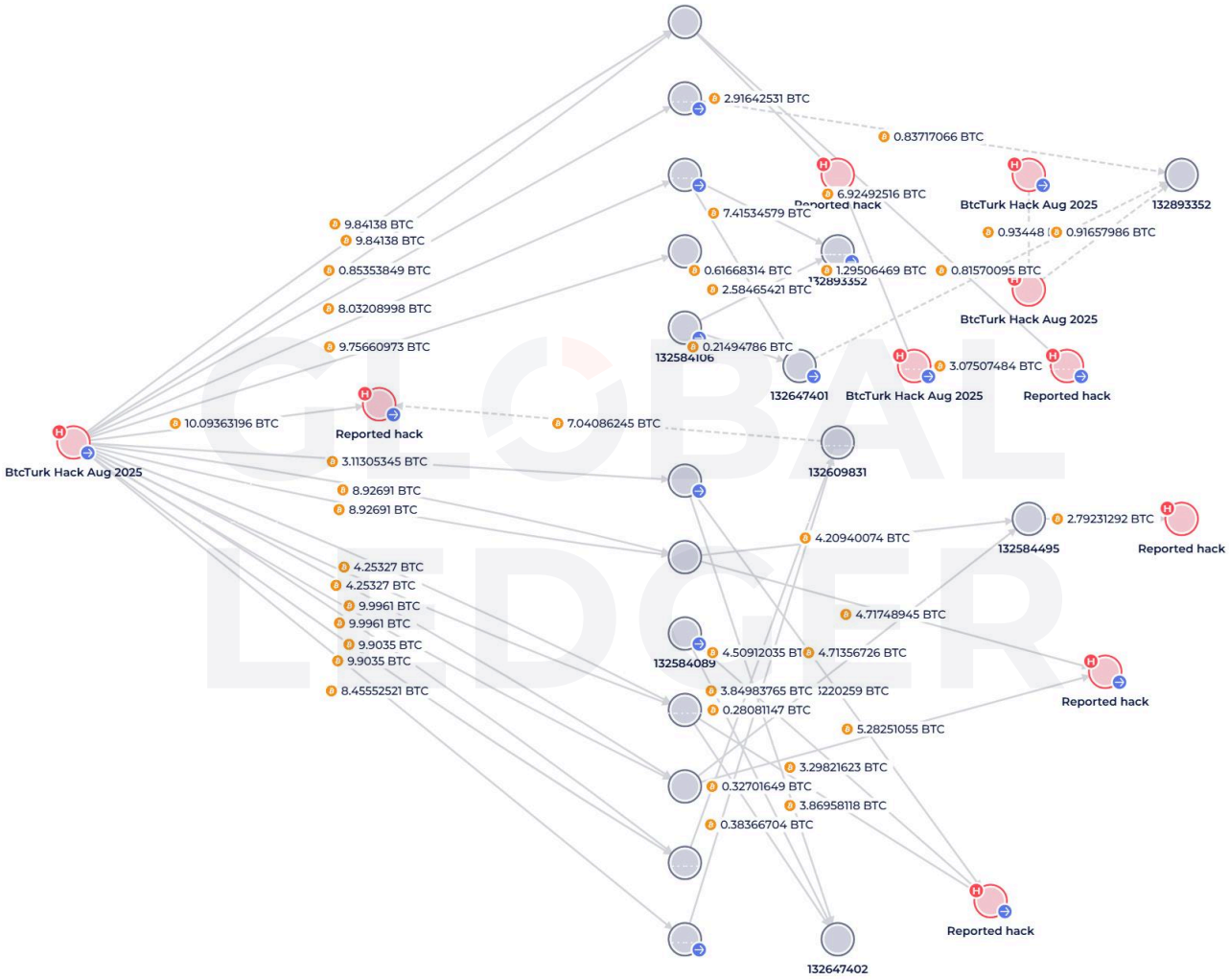
Such fragmentation helped attackers stay under the radar and avoid freezes or law-enforcement action. This fragmented pattern was clearly visible in the **BtcTurk hack**, where stolen funds were routed through unhosted wallets, CoinJoin, Wasabi Wallet, THORChain, Chainflip, and Lightning Network. Rather than a single transfer, attackers used **layered, fragmented movements** to obscure transaction trails ahead of any potential cash-out.

The BtcTurk hack case

BtcTurk ~$48 million hack is an example of deliberate, staged laundering, likely carried out by **DPRK hackers**. In August 2025, the exchange suffered a security breach that resulted in the theft of ETH, BTC, BASE, ARB, OP, POL, AVAX, zkSync, MANTLE, and Moonbeam from its hot wallets. BtcTurk reported that most user funds were safe in cold storage. At the same time, on-chain data confirmed that millions of dollars in BTC were transferred from hot wallets to attacker-controlled addresses shortly after the breach.

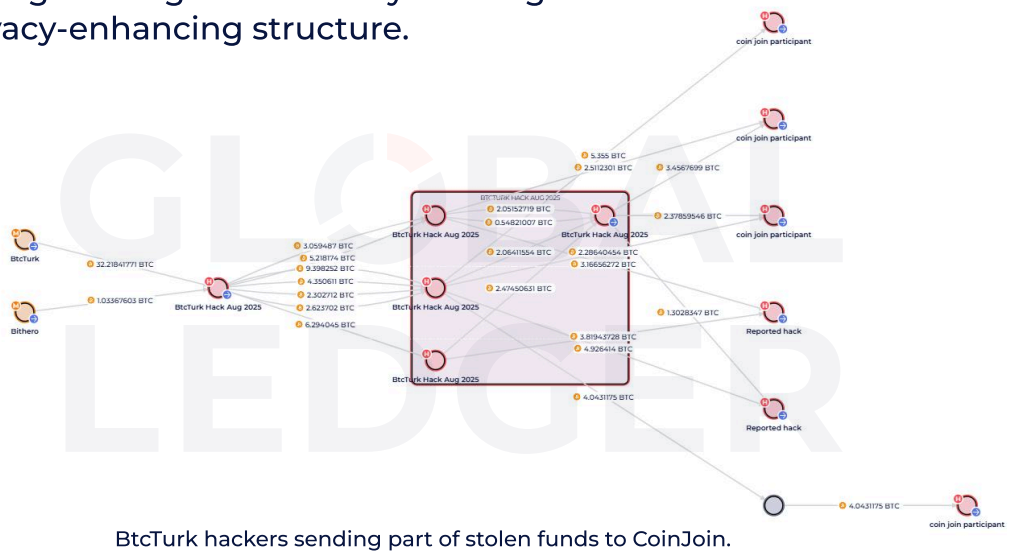
The multistage scheme used for laundering included:

- Routing funds through a chain of unhosted wallets.



BtcTurk hackers sending part of stolen funds to a chain of self-hosted wallets. Screenshot from the Global Ledger KYT tool

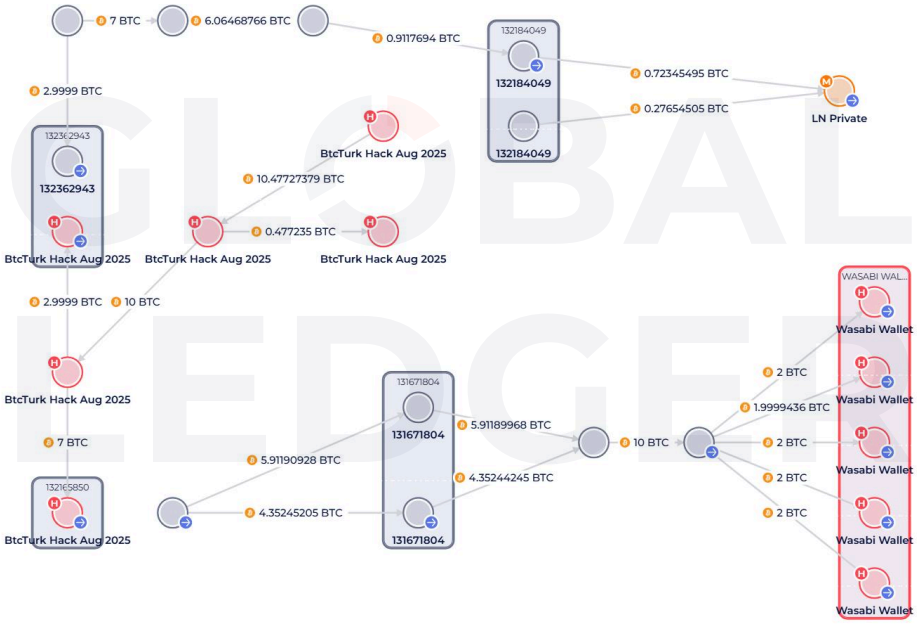
- Further concealing the origin of funds by sending them to CoinJoin—a privacy-enhancing structure.



BtcTurk hackers sending part of stolen funds to CoinJoin. Screenshot from the Global Ledger KYT tool

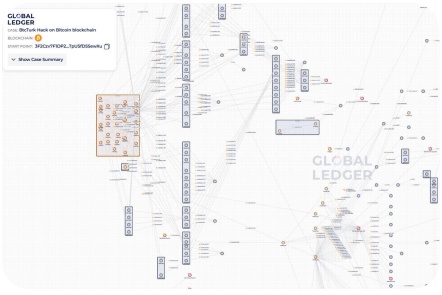
- Using THORChain, Wasabi Wallet, Chainflip, and the Lightning Network to further obscure the transaction trail.

Lightning Network is a Bitcoin Layer-2 network designed to improve transaction speed and reduce fees while enhancing user privacy. By routing payments off-chain and limiting visibility to participating nodes, it hides on-chain trails. Attackers leverage these features to further obscure transaction trails.



BtcTurk hackers sending part of stolen funds to the Lightning Network and Wasabi Wallet.
Screenshot from the Global Ledger KYT tool

These layered methods are meant to make tracing harder. They show that illicit actors understand how investigations work and deliberately act to complicate tracking and attribution.



Review how funds moved

Check the case online

2 Fragmentation obscures the trail

The BtcTurk case illustrates how attackers rely on staged execution rather than speed. The combination of self-hosted wallet chains, mixing, and cross-chain routing shows a deliberate, well-orchestrated scheme where each step is designed to gradually weaken traceability, complicate clustering and attribution.

Multistage routes weaken direct links to the original exploit. Individual deposits may look low-risk in isolation, making it harder for compliance teams to confidently attribute funds to a single incident without cross-stage visibility. And, instead of a linear path to a VASP or cash-out point, attackers construct layered routing paths that degrade analytical certainty.

Effective response to sophisticated attacks requires rapid-response protocols, cross-jurisdictional coordination, and advanced tracing capabilities

The extended timeline creates intervention opportunities, but success depends heavily on attacker sophistication. Less experienced threat actors, increasingly entering crypto crime aided by AI tools, often lack efficient laundering knowledge, giving recovery teams time to compile evidence packages and coordinate with service providers.

However, sophisticated attackers deliberately slow the process strategically. They split funds into tranches, route through privacy tools like Tornado Cash, or hold assets during unfavorable market conditions to reduce traceability and test laundering strategies.

Success requires operational readiness other than just having sufficient time: established rapid-response protocols, strategic networks spanning jurisdictions and service providers, and technical capabilities to track complex fund flows. The marathon phase alone doesn't guarantee better outcomes without proper infrastructure to exploit it.

Marcin Zarakowski

CEO of Recoveris

> Criminals learn from the controls institutions impose on suspicious behaviour, and keeping stolen funds for longer may help them avoid detection and investigative attention, enabling the laundering process to continue. However, with broader Travel Rule implementation globally, this and similar strategies are no longer valuable for attackers. Every self-hosted address needs to be verified before a regulated, Travel Rule-compliant entity interacts with it, guaranteeing the owner is identified at every transaction step.

Hannah Zacharias

Head of Regulatory Affairs at 21 Analytics

Prevent risks with Global Ledger

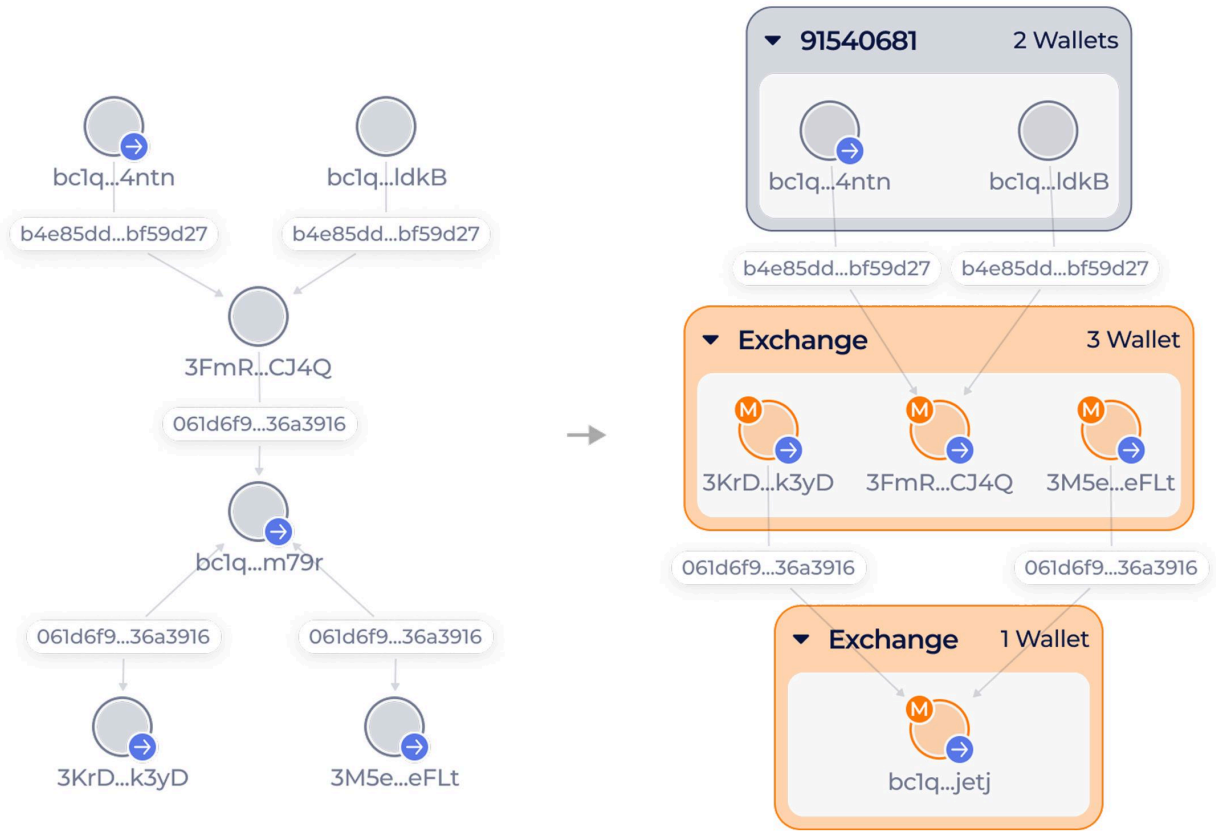
Time-based triggers and cluster analytics

When laundering routes become fragmented, single-transaction checks can no longer be enough. To respond effectively, compliance teams need to detect patterns across deposits, timing, and behaviour, not just isolated events.

To operate in this environment:

- Set up automatic triggers based on behavioural and time-based signals, rather than static rules tied to single transactions.
- Aim for a 15-minute internal SLA for reviewing suspicious flows — similar to incident response in cybersecurity. Support this with real-time alerts delivered through operational channels like Slack, Jira, or Telegram, so high-risk events trigger immediate action.
- Consider using risk bursts — clusters of similar activities within short timeframes — to identify coordinated or staged laundering attempts.
- Try to apply cluster-level analytics to identify behavioural patterns, transaction paths, and timing anomalies.

At Global Ledger, clustering algorithms can surface hidden links between wallets by combining behavioural patterns, smart contract interactions, and fund origin analysis to associate activity with specific entities or events.



Make fragmented risk visible before it turns into exposure. We'll guide you every step of the way.

Schedule a Demo

Problem

Hackers sent 3× more funds to bridges than mixers

In 2025, over **$2.01 billion** of stolen funds were routed through bridges — nearly **50% of total losses** and over 3× more than via mixers and privacy protocols. Bridge usage was notably higher in the first half of the year.

In **H1 2025**, over **$1.5 billion** of hacked assets were routed through bridges, largely driven by the Bybit incident, which alone contributed $1.38 billion, with 94.91% of stolen funds moved through bridges. In **H2 2025**, the volume routed through bridges declined by nearly **3×, to $510.64 million**, likely due to the increased use of the post-sanctioned Tornado Cash mixer and the lack of significant losses such as the Bybit hack.

While only 11.3% ($339 million) of stolen funds in H1 2025 were sent to mixers, which were used in 52% of hacks, the situation was markedly different in 2024. That year, **50% ($763.48 million)** of stolen funds across the 25 largest hacks were funnelled through mixers and privacy protocols, when mixers offered lower visibility risk and remained a more “effective” tool for obscuring large volumes before regulatory scrutiny intensified.

The shift from mixers to bridges in 2025 is also driven by the nature of cross-chain infrastructure. Bridges are the premier tool for breaking the linear transaction trail. By moving assets cross-chain, hackers "decode" the trail, making it challenging based on what protocol was used for automated tracing systems to follow value across different ledger architectures. Most bridges operate as permissionless smart contracts that are not designed to detect or freeze illicit flows, allowing attackers to move massive volumes while evading KYC and sanctions screening.

Furthermore, attackers use bridges to reach DeFi protocols — where laundering volume grew 4.3× in H2 — allowing them to swap stolen assets into other chains to lower fees for their thousands of subsequent micro-transfers. This combination of cross-chain routing and DeFi integration creates a multi-layered barrier that degrades analytical certainty and makes investigation far more resource-intensive than tracking a simple mixer.

Moving funds cross-chain now comes with a lot more visibility and risk

Today, analytics providers are much better at pulling data across chains and understanding how bridges actually move value. From our side, we try to make this as clear as possible. We run a public explorer where anyone can see where funds are coming from and where they go. Transparency is important.

We also check transactions with several AML providers before they go through. We don't believe bridges should decide on their own which addresses are good or bad. That's a job for specialists like Global Ledger. Because of this, bridges just aren't an easy option for attackers anymore. Moving funds cross-chain now comes with a lot more visibility and risk than it used to.

Andriy Velykyy

CEO and co-founder of Allbridge

What is at stake?

Attracting launderers = attracting oversight and risking reputation

Bridges are increasingly leveraged by bad actors for large-scale laundering — not because they are inherently malicious, but because they operate in a zone between decentralisation and compliance. Many are built as permissionless smart contracts, making real-time intervention difficult. This creates a structural blind spot that sophisticated actors actively exploit.

However, the challenge isn't that bridges fail. It is that they work exactly as designed. Billions in illicit value flow through systems that aren't designed to detect or stop it in time. Without new models for cross-chain accountability, they will remain attractive tools for high-volume laundering, leaving even well-intentioned protocols exposed to reputational and regulatory risks.

Bridges are motivated to filter suspicious activity early

In reality, it's often simpler for attackers to use low-quality exchanges, OTC desks, or informal networks, where controls are weak or mostly just for show. With bridges, the cost of being associated with bad flows is much higher.

We also see a shift toward simpler ways of moving value, especially for stablecoins. Models like Circle's CCTP or LayerZero's OFT make it cheaper and more predictable to move liquidity across chains, with very little slippage. That's great for users. At the same time, these flows rely on centralized stablecoins. And that matters, because if something goes seriously wrong, issuers can step in and freeze assets. That makes these routes much less attractive for hackers, who don't want that kind of uncertainty.

Andriy Velykyy

CEO and co-founder of Allbridge

Prevent risks with Global Ledger

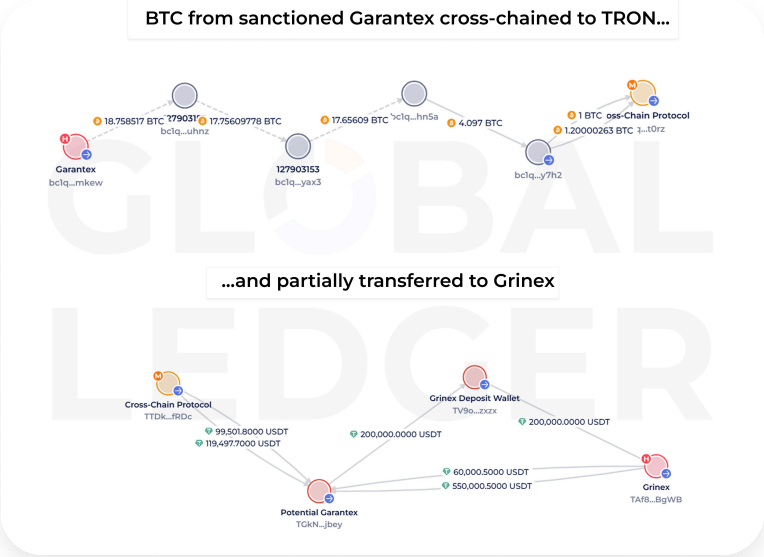
Update risk models with bridge- and mixer-specific patterns

Certain cross-chain protocols and mixers are more compliant than others. Just to name a few: Allbridge and ChangeNOW adding high-risk addresses to black lists; Mantle Network blocking Lazarus transfers; Chainflip implementing solutions to block illicit transactions; Railgun blocking illegal funds from entering the privacy pool. Additionally, many bridges offer public explorers, which support investigative continuity by allowing analysts to trace cross-chain movements.

However, relying on protocols wouldn't be enough. Protocol-level controls help but they don't replace your own. What you can do now:

To operate in this environment:

- ◯ Maintain independent monitoring.
- ◯ Flag cross-chain activity as higher risk by default.
- ◯ Update risk models with bridge- and mixer-specific patterns.



Need to trace funds across bridges? We've done it. Let's walk through a real case.

Schedule a Demo

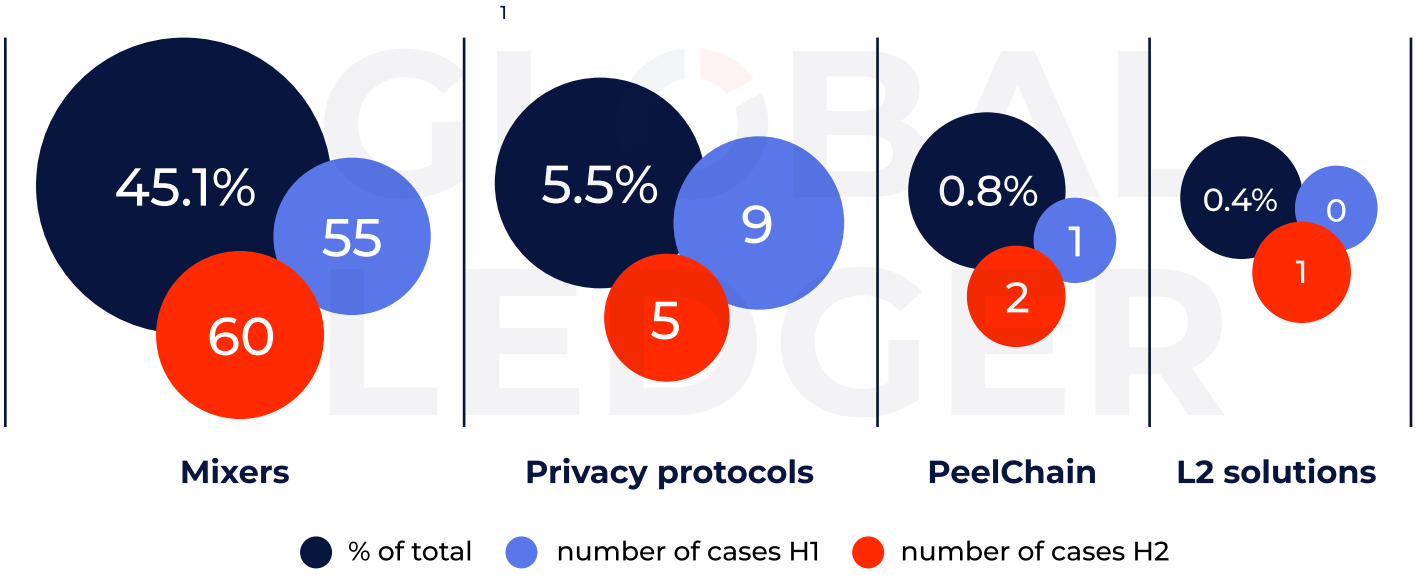
Problem

Tornado Cash became the #1 mixer in H2 2025

Mixers and privacy protocols often follow bridges as the next step in hiding final recipients. In 2025, **650.1 million** were routed via them, with a decline of roughly 8% half-over-half.

Mixers were used in 45.1% of all hacks, privacy protocols account for 5.49%, peel chains for 0.78%, and L2 solutions for 0.39%.

Mixers used in 45.1% of all hacks in 2025



Tornado Cash leads the chart in terms of popularity among crypto mixers, used in **41.57% of all hacks (115 of 255) in 2025.**

Its usage increased sharply in H2. Tornado Cash's share among mixer usage rose from 42.9% of cases in H1 to 74.3% in H2 — a 31.4 percentage-point increase, making Tornado Cash the dominant mixer during that period. The lifting of sanctions in March 2025 immediately removed the primary compliance hurdles that previously triggered automated alerts at centralized exchanges.

Hackers prefer Tornado Cash because its massive liquidity provides a level of obfuscation that smaller, fragmented mixers simply cannot match. By consolidating illicit flows into a single, high-volume pool, attackers achieve significantly higher anonymity at a lower operational cost than managing multiple smaller protocols. Ultimately, this surge reflects a return to the industry's most efficient "washing machine" as soon as the path of least resistance was reopened, prioritizing the reliability of immutable code and the anonymity provided by vast transaction volumes.

In 2025, Tornado Cash received over $2.05 billion on Ethereum

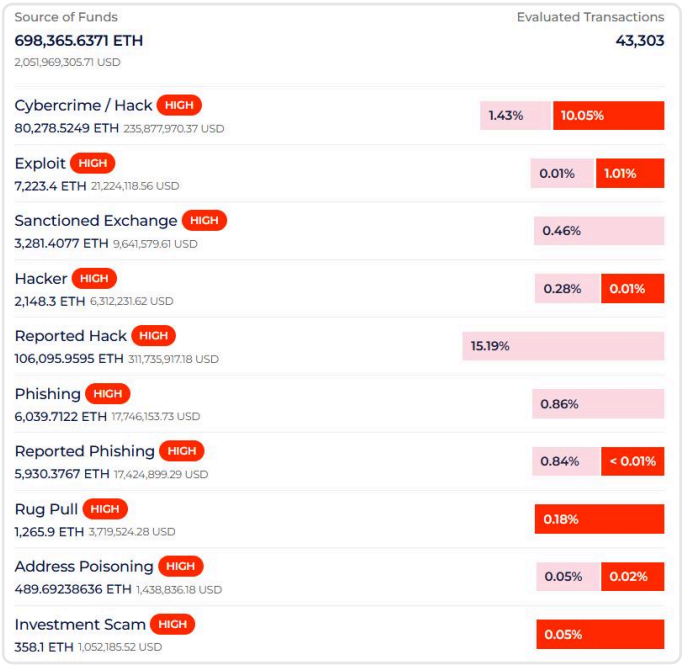
In 2025, Tornado Cash received over **$2.05 billion on Ethereum**, with ~654.98 million coming from high-risk activity, such as scams, hacks, phishing, high-risk exchanges, etc.

Tornado Cash has become a critical component of hacker infrastructure

During 2025, the total volume of outgoing transactions from the mixer reached **$1.57 billion**; about 155.55 million went to high-risk addresses. Nearly the same volume of funds (~154.2 million) was sent to low-risk addresses.

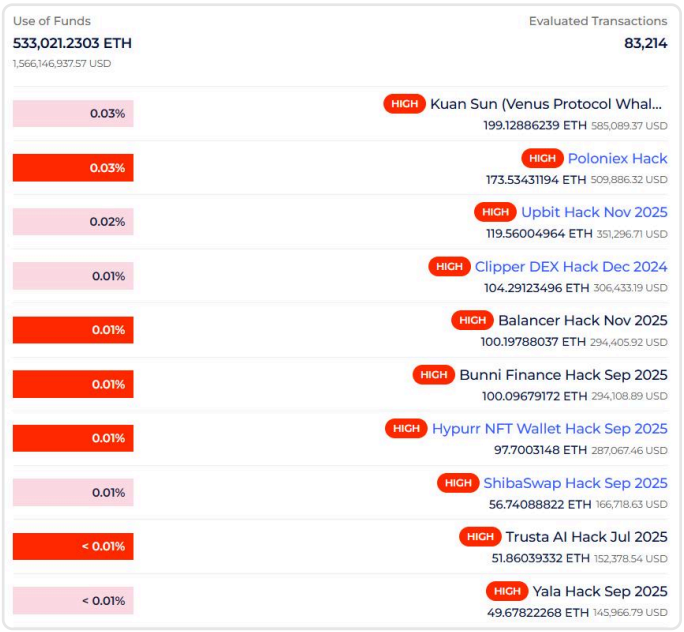
Funds leaving Tornado Cash move to wallets controlled by the same malicious actors involved in earlier hacks, e.g., incidents from 2023-2024. These include the Poloniex hack from November 2023, when ~$132 million worth of crypto was stolen (valued at the time of the incident), and the Clipper DEX hack from December 2024, with ~$450,000 in losses.

In 2025, Tornado Cash received $2.05B+ on Ethereum, with ~654.98M from high-risk activity



Screenshot from the Tornado Cash entity exposure report. Jan 1-Dec 31, 2025. Global Ledger

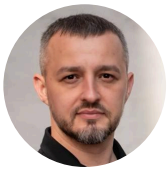
Funds from Tornado Cash went to wallets linked to hacks from 2023-2024



Screenshot from the Tornado Cash entity exposure report. Jan 1-Dec 31, 2025. Global Ledger

Attackers still rely on a single, well-known mixer instead of using several, getting sufficient obfuscation at a lower cost. Additionally, popular mixers attract more volume, making individual transactions harder to distinguish from the crowd.

> The dramatic surge in Tornado Cash usage—from 42.9% to 74.3% of cases following the lifting of sanctions—presents a significant national security challenge. This resurgence highlights how quickly state-sponsored actors, such as the Lazarus Group, exploit any perceived regulatory softening to smooth their laundering operations.
>
> As Ukraine aligns its legislation with MiCA (Markets in Crypto-Assets) standards, we are championing a model of 'Accountable Transparency'. We respect the right to financial privacy, but the fact remains that when a single mixer handles nearly 75% of illicit flows, it becomes a systemic risk to the integrity of the financial system. Our 2026 strategy involves implementing advanced de-anonymization tools for privacy-enhancing protocols and mandating that VASPs apply strict enhanced due diligence for any assets originating from non-compliant mixers. In the post-sanction era, our mission is to ensure that Ukraine's legalized crypto-market is a fortified environment where illicit assets are identified in milliseconds, regardless of the obfuscation layers applied.



Oleksandr Plakhotnyuk

Chief of Division for Combating Crimes Related to Virtual Assets at the Cyberpolice Department of the National Police of Ukraine

What is at stake?

Cash-out to exchanges became easier

Crucially for VASPs, the share of funds **flowing from Tornado Cash directly to centralized exchanges increased significantly** after sanctions were lifted. Before March 2025, exchanges received just $278K (0.16%) of Tornado Cash outflows. After sanctions were lifted, this figure rose to $66.7 million (4.74%), including transfers to top-tier exchanges by trading volume.

Once sanctions were officially lifted, centralized exchanges were no longer required to automatically freeze funds originating from Tornado Cash. This, in turn, allowed hackers to transfer funds directly from the mixer into centralized exchanges without relying on complex routing schemes. In effect, Tornado Cash became a shortcut to highly liquid CEXs with multiple cash-out options, ultimately simplifying both laundering and cash-out.

Tracing must shift to probabilistic and behavioral-based clustering models

The data shows that the revocation of sanctions on Tornado Cash has led to a resurgence of legacy mixers within illicit financial ecosystems. It means that tracing methodologies must shift from static blacklist-based systems toward probabilistic and behavioral-based clustering models. Investigators should incorporate temporal transaction analysis, mixer inflow–outflow correlation, and cross-protocol entity linking to map disguised capital flows. Empirical evidence supports that machine-learning–based signature detection significantly reduces false negatives, especially when integrated with real-time intelligence feeds from law enforcement and commercial APIs.

Mudassar Malik

CEO and founder of Deconflict.com

> Traditional finance has accumulated an extensive set of patterns that enable the identification of atypical user behavior and the detection of suspicious activity. Unfortunately, the cryptocurrency ecosystem is no exception in this regard. Proper configuration of triggers and the combined use of modern AML tools can deliver effective results.

Vadym Grusha

CEO and founder of Trustee Plus

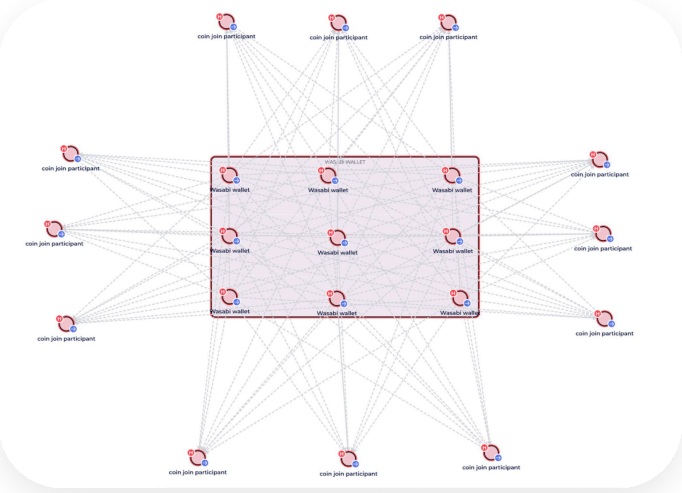
Prevent risks with Global Ledger

Identify mixer-related risk via behavioural signals

With Tornado Cash no longer sanctioned, alerts and labels are often not enough. Illicit funds can reach exchanges without automatic flags, as sanctions-based triggers no longer require blocking or escalation. As a result, mixer exposure has to be identified through behavioural signals — transaction patterns, timing, and flow analysis — rather than static lists.

What you can do now to manage mixer–related risks:

- Use alerts based on transaction behaviour — such as amounts, timing, and inflow–outflow relationships — as additional risk signals when reviewing incoming transactions.
- Consider applying probabilistic tracing after mixers to surface likely links between deposits and withdrawals when direct attribution is not possible.
- Treat post-mixer activity as higher risk by default by escalating transactions coming from mixers and connected protocols, even without sanctions signals.



Check your mixer exposure before it reaches cash-out.

We'll help you see the full picture.

Schedule a Demo

Problem

DPRK attacks on CEXs increased 2.5× in H2

In 2025, DPRK hackers stole **$1.89 billion** (~46.8% of total losses), with a sharp half-year imbalance. Five incidents in H1 accounted for over $1.55 billion, while five incidents in H2 totalled just $134.86 million, meaning H1 losses were approximately 9.04× higher than H2. This imbalance is driven largely by the Bybit exploit, where nearly $1.46 billion was stolen in a single incident.

The composition of targets also changed over the year. In H1, DPRK-linked attacks affected a wide range of targets, including major centralized exchanges (such as Bybit and Phemex), DeFi platforms, and personal wallets. In H2, activity became more concentrated, with incidents limited mainly to five CEXs and one blockchain incubator, without a large-scale exploit comparable to Bybit.

This shift reflects a move from broad, high-impact attacks in H1 to a more cautious approach in H2. While DPRK-linked hackers focus mainly on centralized exchanges as highly liquid targets, the Bybit hack has triggered increased scrutiny across the ecosystem, likely forcing a more deliberate operating tactic.

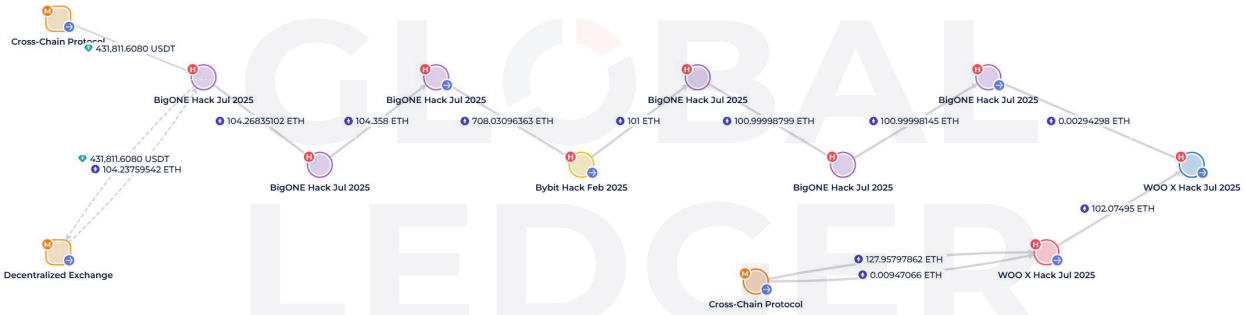
Patterns used by DPRK hackers

Our research team conducted a more in-depth analysis of six hacks allegedly connected to the DPRK hackers (WOO X and Seedify were confirmed by the exploited entity as linked to Lazarus; other cases suggest North Korean involvement):

- BigONE hack, Jul 2025: $29.7 million
- WOO X hack, Jul 2025: $13.7 million
- BtcTurk hack, Aug 2025: $48.1 million
- Seedify hack, Sep 2025: $1.7 million
- SwissBorg hack, Sep 2025: $41.5 million
- Upbit Hack, Nov 2025: $36.8 million

The analysis revealed on-chain patterns that link incidents together:

- Reusage of the same self-hosted wallets (across ByBit, Woo, and BigOne incidents).



Screenshot from the Global Ledger KYT tool

- Heavy reliance on multiple single-use wallet infrastructure, with stolen funds being split into random amounts.
- HuiOne group associated wallets identified as one of the laundering destinations of the Seedify incident.

Screenshot from the Global Ledger KYT tool

- After an incident occurs, illicit actors do not always rush to launder funds. In 58% of H2 cases, the first post-incident movement takes place within 15 minutes. By contrast, DPRK-attributed hacks show a longer average delay of **54 minutes — 3.6× longer.** Among them, the Seedify hack had the shortest delay at 13 minutes and 51 seconds, while in the WOO X case, the stolen funds were first moved only after 2 hours and 22 minutes.

For the industry, this signals that these attacks are more likely to be carried out by a coordinated group of hackers, often using automated and pre-planned processes. Unlike most opportunistic hackers, there is no rush or panic-driven movement immediately after the breach. Instead, planning comes first, followed by structured laundering — a pattern that clearly distinguishes these operations from the rapid, reactive behaviour seen in typical hacks.

A clear example of such coordinated activity: Lazarus Group

Lazarus Group-linked activity can be identified, or at minimum suspected, based on the following patterns:

1. Large-scale thefts, typically involving tens or hundreds of millions of dollars in cryptocurrency.
2. Each incident follows a highly sophisticated and premeditated intrusion, rather than opportunistic exploitation.
3. There is no evidence of an immediate laundering strategy; instead, operators often delay funds movement while developing a structured laundering plan.
4. Extensive obfuscation techniques are used, including heavy reliance on cross-chain transfers, DEX routing, and single-use wallets, with no apparent concern for transaction fee losses.
5. A hybrid laundering model is observed, combining methods such as CoinJoin, Tornado Cash, and Wasabi Wallet.
6. Targets are predominantly entities with substantial on-chain balances, indicating deliberate victim selection.
7. Centralized exchanges are frequent victims, accounting for seven out of 11 observed cases.

What is at stake?

1 High-liquidity CEXs — the primary focus of DPRK-linked operations

By consolidating large amounts of crypto in a single location, centralized exchanges create high-value single points of failure.

The share of DPRK-linked incidents targeting centralized exchanges increased from approximately **40% in H1 to over 83% in H2, representing a 2.5× increase.** Without a Bybit-scale opportunity in H2, DPRK actors concentrated on smaller CEX intrusions, indicating sustained intent while total losses remained event-driven. DPRK-linked operations prioritize scalable access-based theft and concentrate on high-liquidity targets.

Diverse timing and tactics require long-term tracking and continuous monitoring of stolen assets

North Korean cyber operations consist of multiple independent threat clusters, each with its own laundering process, timing, techniques, and preferred services. One DPRK cluster relies heavily on Tornado Cash for laundering, while another literally never uses Tornado Cash or any other mixer and instead routes funds primarily through centralized exchanges. Even when looking specifically at Tornado Cash, withdrawal behavior varies widely — some actors withdraw funds within 1–2 days after deposit, while others deliberately wait weeks or even months before proceeding.

This diversity in timing and tactics is exactly why long-term tracking and continuous monitoring of stolen assets is becoming essential for effective threat intelligence.

Yev Broshevan

CEO & Co-Founder at Hacken

2 Becoming part of the laundering chain means regulatory exposure

Instead of single large exploits, attackers shifted to repeatable hacks, primarily through private key compromise, keeping sustained pressure on exchange infrastructure.

For VASPs, this risk is not about the financial loss alone. According to the United Nations, DPRK-linked crypto theft is used to support state weapons programs, meaning any failure to detect, block, or report related flows can expose exchanges to sanctions violations and enforcement actions.

Receiving illicit funds even indirectly and unintentionally, VASPs become part of the laundering chain themselves. This exposure can attract regulatory scrutiny, especially when reporting lags behind on-chain movements.

Prevent risks with Global Ledger

Timely labeling and instant reports

Without early attribution, labeling, and fast response, even compliant VASPs can unknowingly receive illicit funds and become part of the laundering chain related to DPRK-linked crypto theft, increasing regulatory scrutiny.

In an ideal scenario, a victim report within 10 minutes, automatic labeling and clustering within ~10 minutes, a KYT transaction alert in ~1 second, and an automated block by the recipient or VASP in ~1 second could stop about 98% of cases.

In practice, fast response looks different:

- A more realistic operational target to prevent half of the incidents is: report within 24 hours, KYT labeling/clustering in <4 hours, transaction alert in <30 seconds, and blocking within 30 seconds after the alert.
- Today's industry averages are slower. Reports often come after ~1.5 days, labeling can take days (or even weeks), and manual reviews create large delays, which is why automation matters.

Global Ledger labels high-risk wallets within 1 hour and generates a report in ~1 second

Benchmarks	98% of cases	50% of cases	Current av.	Global Ledger
Hack Report	<10 min	<24 hours	~1.5 days	
Labeling	<10 min	<4 hours	1-2 weeks	<1 hour
Report / Alert	<1 sec	<30 sec	~ 3-5 min	~1 sec
Block by VASP	<1 sec	<30 sec	<30 sec	

Faster response. Lower exposure. See how it works in real time.

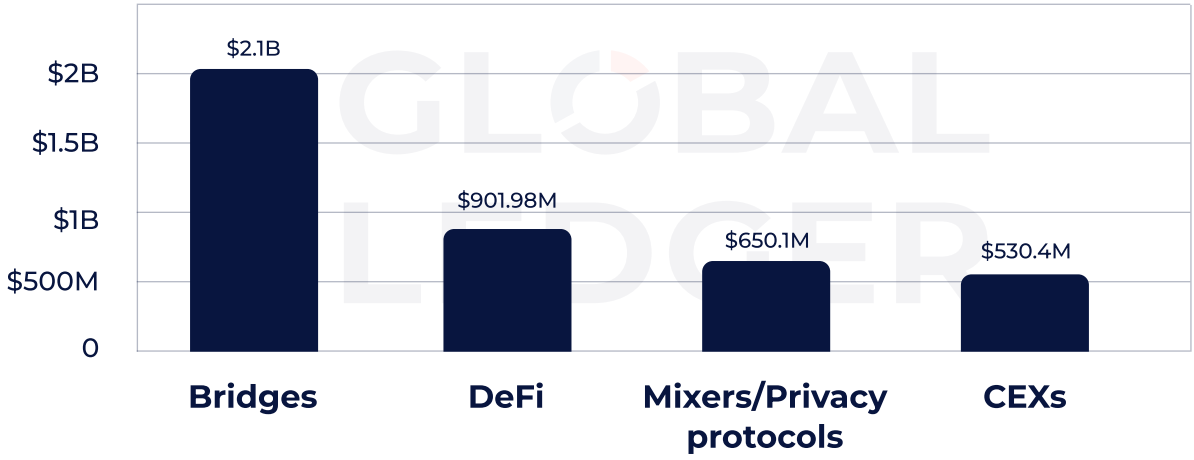
Schedule a Demo

Problem

Attackers become more cautious, waiting for cash-out

In H2 2025, inflows of stolen funds into centralised exchanges dropped sharply, falling 5.9× compared to H1 ($77.39 million vs $453 million), bringing the total sent to CEXs in 2025 to ~$530.39 million. At the same time, attackers increasingly routed funds through DeFi, with H2 volumes (~$732 million) exceeding H1 ($170 million) by more than 4.3×, making DeFi the second most used laundering route by year-end.

In 2025, ~50% of stolen funds bridged



However, this shift does not indicate reduced illicit activity. Instead, it reflects **more cautious and delayed attacker behaviour**, driven by faster public reporting and increased scrutiny. With nearly 48.76% ($1.97 billion) of stolen funds remaining unspent, attackers increasingly wait for attention to subside before attempting cash-out.

For VASPs, this can create a false sense of safety. Early reporting and visibility help reduce immediate exposure, but risk is increasingly pushed downstream, requiring continuous monitoring rather than one-off incident response.

What is at stake?

You typically have a 10–15 minute window to act

Even as stolen funds are less likely to move immediately to centralized exchanges and attackers increasingly delay cash-out, the risk does not disappear. When funds from a hacker-controlled address reach your platform, the response window is extremely narrow — typically **10–15 minutes to act**. Transactions that exceed internal risk thresholds may be routed for manual review and temporarily withheld, but this only works if continuous monitoring is already in place.

If no action is taken within this window, assets are likely to move again — into a mixer, another exchange, or off-ramped entirely. Once stolen funds pass through a VASP, they are often aggregated, traded, or split, rapidly losing traceability. From there, recovery becomes nearly impossible, and the assets can quickly move off-chain, beyond the reach of blockchain-based monitoring or enforcement.

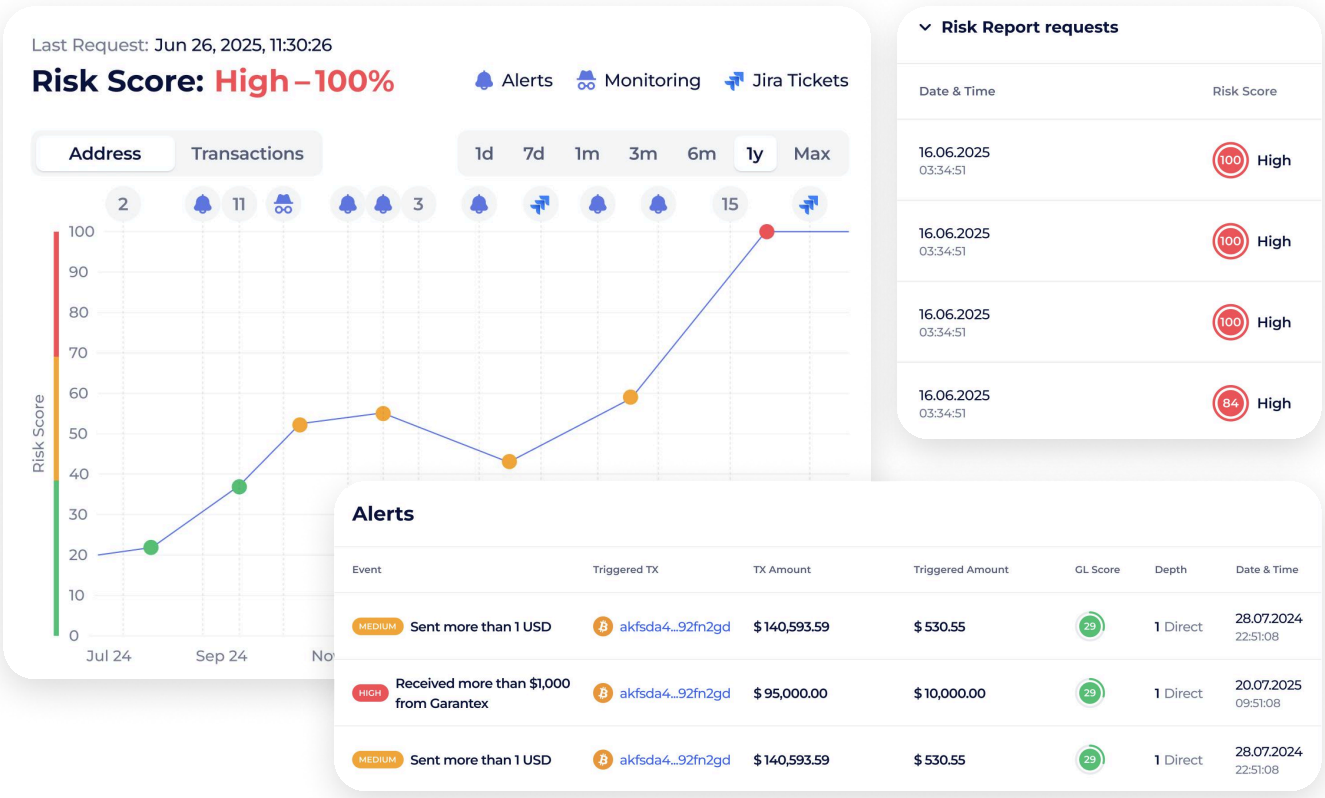
Prevent risks with Global Ledger

Compliance Memory

When stolen funds reach a CEX after a delayed cash-out, compliance teams have very limited time to act. The Compliance Memory feature ensures that critical context is immediately available during manual transaction review, enabling decisions to be made within the 10–15 minute response window.

With Compliance Memory, you can:

- Instantly access the full compliance history of an address, including alerts, risk scores, API requests, and related cases.
- Review how risk and decisions evolved over time, without digging through logs, tickets, or spreadsheets.
- Make confident compliance decisions under time pressure, relying on documented past actions instead of starting analysis from scratch.



Understand the past to make confident compliance decisions today.

Schedule a Demo

Problem

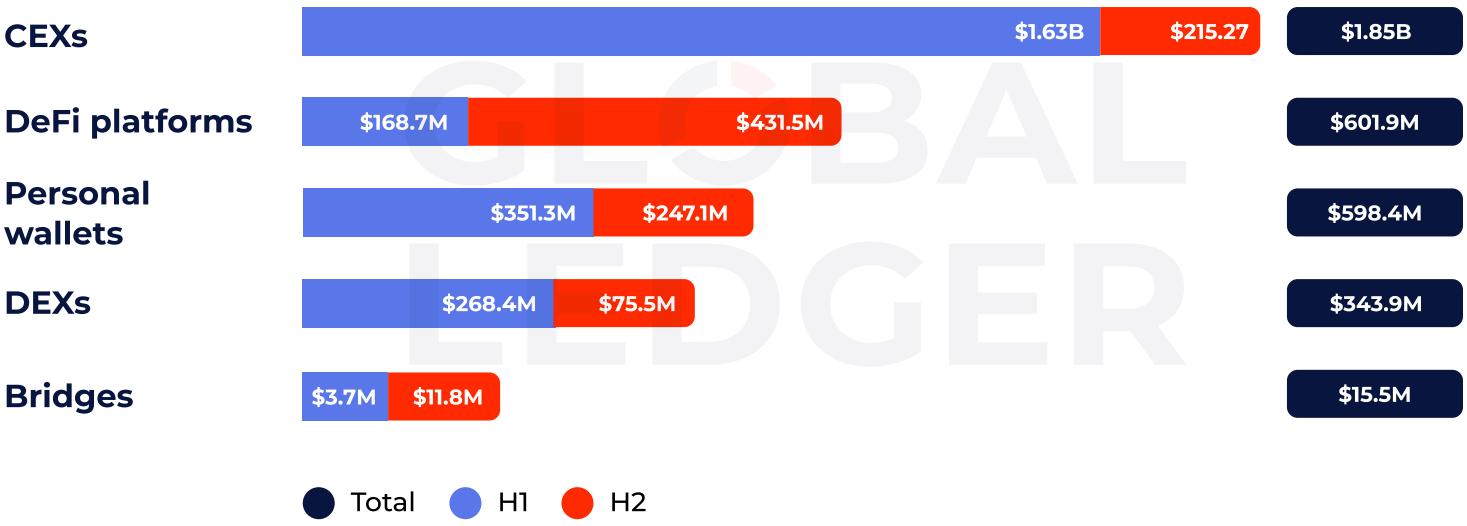
CEXs remained a primary target, accounting for $1.85B in hack losses in 2025

In 2025, centralized exchanges were the most attractive target for attackers, having lost **$1.85 billion** in hacks (45.79% of total losses). Of this amount, $1.63 billion was stolen in H1, and $215.27 million was lost in H2 — a **7.6× decline in losses in H2**.

However, these figures are heavily skewed by the $1.46 billion Bybit hack. Without this incident, centralized exchanges would have fallen behind DeFi platforms, which have lost $601.88 million (14.9% of total losses) in 2025, with a ~2.6× increase half-over-half.

Personal wallets round out the top three, with $598.4 million (14.82% of total). Losses in this category declined by approximately 29.7% in H2, falling from $351.3 million in H1 to $247.1 million in H2.

CEXs losses in hacks dropped by 7.6× in H2



What is at stake?

The decline in CEX losses is misleading

The decline in CEX losses in H2 is largely explained by the absence of a Bybit-scale incident rather than a broad shift in attacker focus. **Excluding the Bybit hack, CEX losses actually increased by approximately 21.5% compared to H1, which is quite a lot.**

At the same time, DeFi platform losses continued to rise, reaching levels nearly 2× higher than those recorded by centralized exchanges, even as DEX losses declined sharply to $75.45 million — about 3.6× lower than in H1. This means risk has not decreased but has redistributed into environments where exploitation is easier to repeat and harder to stop. DeFi can serve as a repeatable exploitation environment and an intermediate layer in attack flows. As a result, exposure may surface later on centralized exchanges, often without any obvious “red flags”.

Prevent risks with Global Ledger

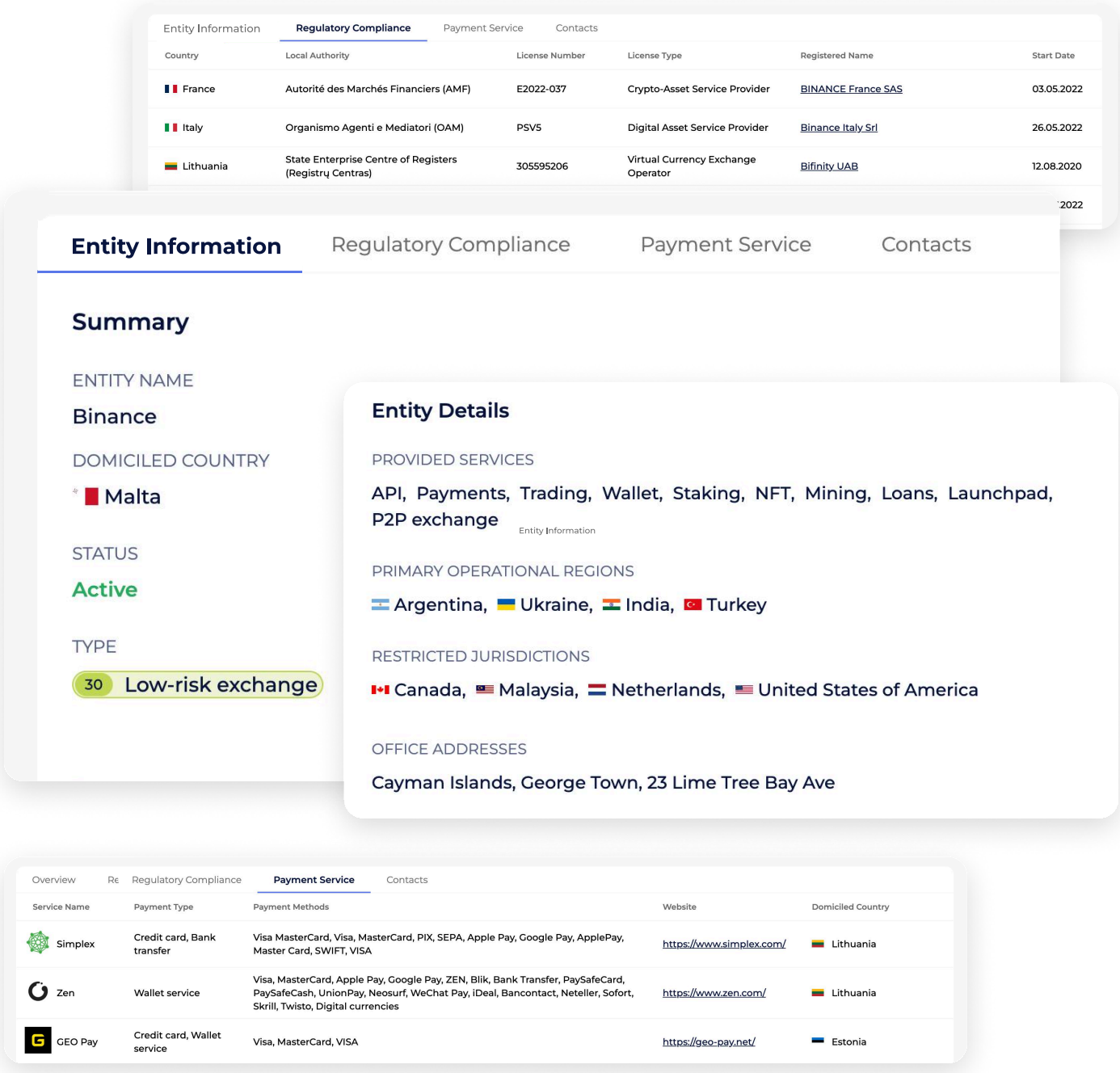
Enhanced due diligence (EDD)

As attack activity becomes more fragmented and funds increasingly pass through multiple intermediaries — such as bridges, mixers, or services with limited or no KYC controls — deposits coming from unclear or high-risk sources to centralized exchanges require closer scrutiny.

3 ways EDD helps protect your platform:

- Apply stricter rules for deposits from instant, non-KYC sources.
- Trigger EDD reviews for flows linked to mixers, bridges, or sanctioned wallets.
- Use hold-and-review policies to freeze funds while the investigation unfolds.

To identify non-KYC and other high-risk services quickly, compliance teams can rely on the Entity Database, covering 92K+ entities with detailed information on ownership, service type, jurisdictional restrictions, and risk indicators.



View who you're dealing with. Request a demo report for any entity.

Schedule a Demo

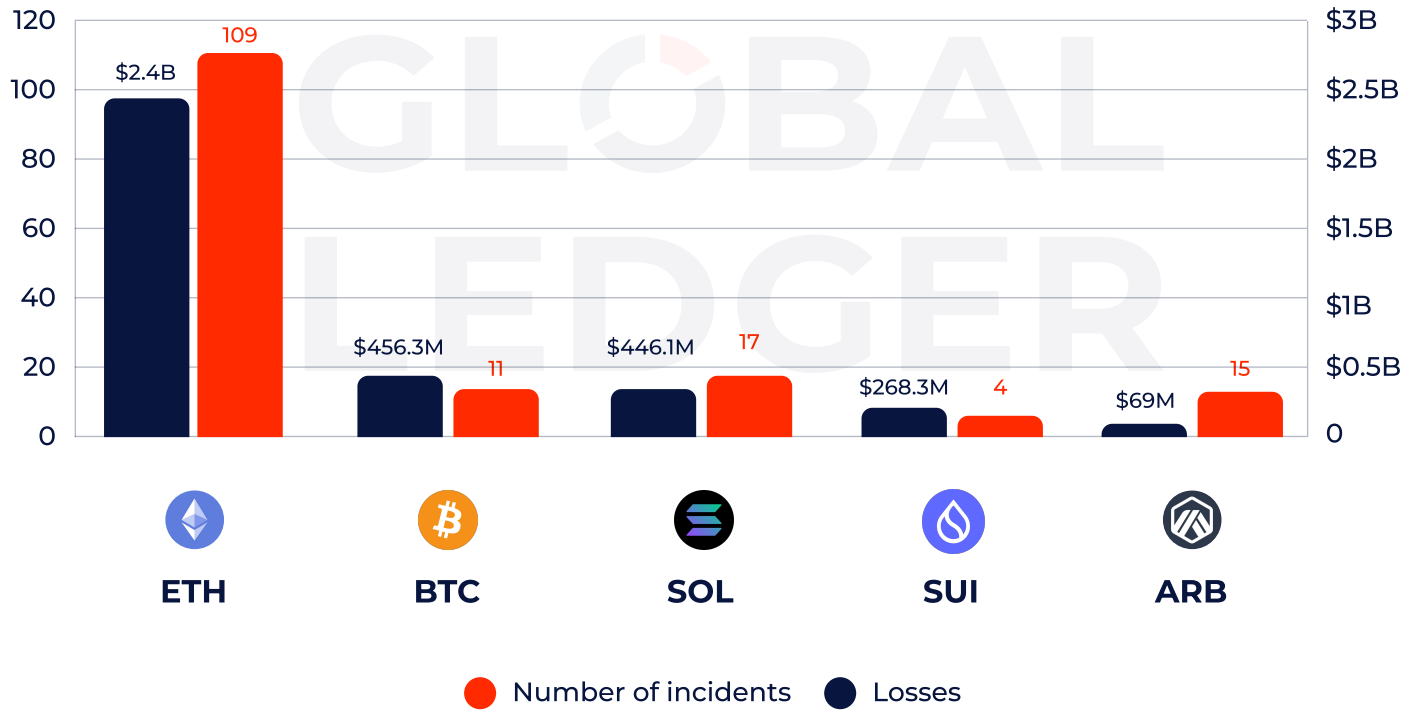
Problem

Ethereum leads the chart in terms of stolen value, with $2.4B stolen in 2025

Ethereum accounts for the majority of stolen value in 2025, with **$2.44 billion** — over 60% of total losses — across 109 incidents. Losses were heavily front-loaded, with H1 volumes about 3.6× higher than in H2 ($1.91 billion vs. $537.8 million). The gap is largely driven by the Bybit hack, which concentrated a significant share of Ethereum losses.

Bitcoin and Solana follow at a distance, each accounting for around 11% of stolen value (11.31% and 11.05% respectively). This underscores that **high-value risk is heavily concentrated around Ethereum-based activity**, rather than being evenly distributed across blockchains.

Ethereum leads in stolen value: $3.8B in 2025



What is at stake?

Limited visibility slows response where risk is highest

High-value illicit flows often originate in complex smart-contract environments and move across multiple chains before reaching VASPs.

When transaction visibility is split across multiple blockchains and monitoring systems, it takes longer to reconstruct the full laundering path and make evidence-based decisions. Besides, it can delay response and make coordination with counterparties more difficult. As a result, risk increases while there is less time to intervene and recover funds.

Prevent risks with Global Ledger

Get visibility across major blockchains

When high-value illicit funds move across chains, visibility determines how quickly you can respond.

- Continuous transaction tracking across major blockchains: Monitor activity across Bitcoin, Ethereum, Tron, BNB, Solana, and other leading networks in one place — covering 98% of total market cap.
- Analyzing tokens, stablecoins, and smart-contract activity to understand the full transaction context.

Blockchain

Bitcoin	BTC	Polygon	MATIC
BSV	BSV	Arbitrum	ARB
Litecoin	LTC	Base	ETH
Ethereum	ETH	Avalanche	AVAX
Tron	TRX	Moonbeam	GLMR
Binance Coin	BNB	Polkadot	DOT
		Solana	SOL

Token

USDT	DAI	**...and all other tokens**
USDC	BUSD	
	USDP	

Get a full view of cross-chain risk. We'll help you walk through it.

Schedule a Demo

Problem

Contract exploits accounted for ~64% of incidents — damage increased by ~36% in H2

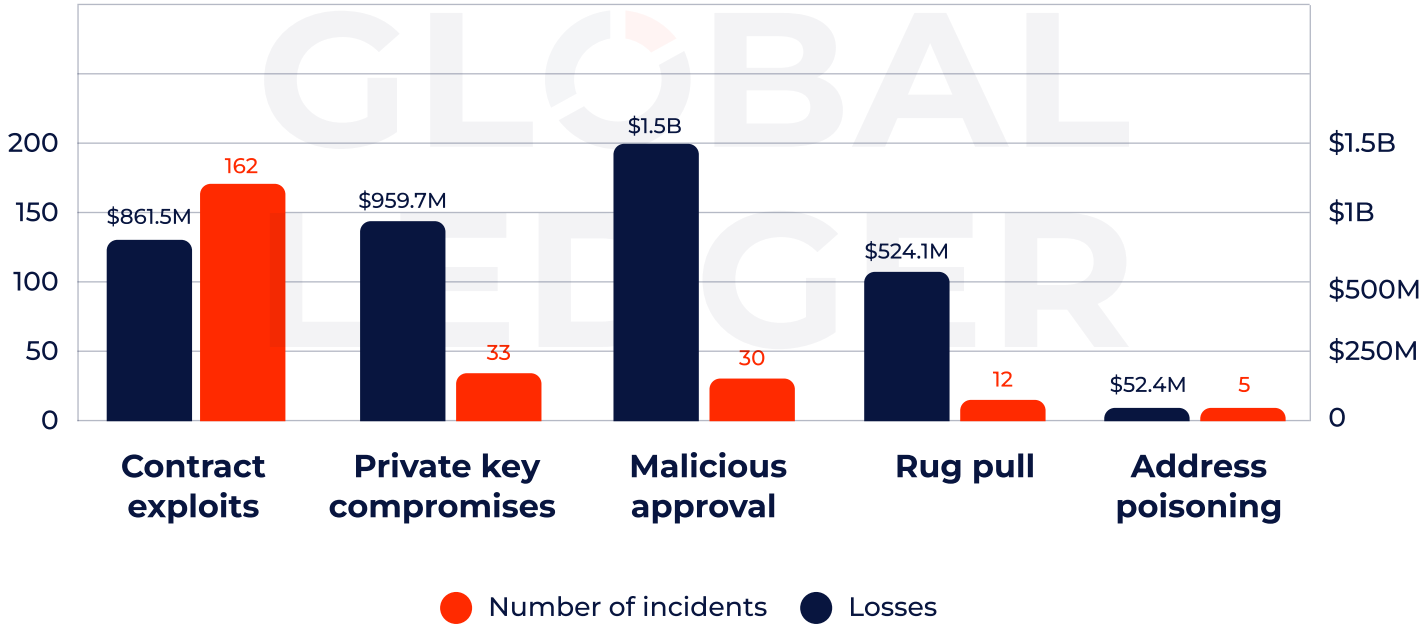
Throughout 2025, **contract exploits** accounted for 63.53% of incidents, making them the most common way funds were stolen. While the share of such incidents declined in H2, **the total damage increased by 35.69%**, with losses from contract exploits reaching $861.54 million for the year.

At the same time, some attack types caused large financial losses even though they were less common. For example, **malicious approvals** accounted for ~12% of cases, yet resulted in $1.51 billion in losses, largely due to high-impact incidents like Bybit. **Private key compromises**, accounting for 13.33% of hacks, led to $959.68 million in stolen funds.

The data reveals a trend: attackers are shifting from technical bugs to systemic weaknesses in key management, signer behaviour, and user interfaces. Focusing only on common threats (e.g., smart contract bugs) can be misleading. Low-frequency but high-impact attacks — like malicious approvals or private key leaks — represent systemic vulnerabilities, especially in CEX environments.

Smaller but evolving attack types also matter. **Rug pulls** accounted for $524.10 million in losses, and while their impact dropped more than 5× in H2, the number of incidents remained unchanged. Meanwhile, **address poisoning** emerged only in H2, with five incidents resulting in $52.41 million in losses — enough to make it the fourth-largest attack type by stolen volume.

Contract Exploits = 64% of Cases. Malicious Approvals = $1.5B Losses



Criminals learn from the controls institutions impose on suspicious behaviour, and keeping stolen funds for longer may help them avoid detection and investigative attention, enabling the laundering process to continue. However, with broader Travel Rule implementation globally, this and similar strategies are no longer valuable for attackers. Every self-hosted address needs to be verified before a regulated, Travel Rule-compliant entity interacts with it, guaranteeing the owner is identified at every transaction step.

Hannah Zacharias

Head of Regulatory Affairs at 21 Analytics

Smart contract security is no longer enough. Operational security is where the billion-dollar risks now sit

Access control and authorization failures have become some of the most damaging threats in Web3, often surpassing smart contract exploits in financial impact, underscoring why security must evolve from point-in-time audits to continuous, end-to-end protection across infrastructure, operations, and human processes.

Hacken's 2025 Yearly Security Report shows over $2 billion stolen by North Korean threat actors in 2025 alone, primarily through phishing and credential compromise, with centralized exchanges remaining the main targets. This highlights that operational security, not just code, is now the weakest link.

In DeFi, operational security breaches already rival smart contract hacks in total losses, yet the industry still treats security largely as a contract audit problem. In 2026, security firms must evolve from point-in-time audits to continuous, protocol-wide security — strengthening access controls, enforcing multisig and timelocks, deploying monitoring and EDR, and hardening teams against social engineering.

Yev Broshevan

CEO & Co-Founder at Hacken

What is at stake?

The real losses come from overlooked risks

In 2025, smart contract exploits dominated by volume, but **malicious approvals caused ~1.8× more losses**, revealing a gap between how often risks occur and how costly they are when missed.

Contract exploits are frequent but often capped by protocol-level limits or rapid mitigation. In contrast, malicious approvals and private key compromises directly target user wallets and signing authority, allowing attackers to access large balances in a single step. Address poisoning similarly exploits user behavior rather than technical vulnerabilities. Together, these patterns show that systemic and behavioral weaknesses pose greater financial risk than smart contract exploits.

Malicious approval scams require rapid response from recovery teams

Unlike contract exploits with immutable on-chain proof, malicious approval scams rely on Web2 infrastructure, like fake websites, fraudulent channels, manipulated interfaces. This evidence typically disappears within days, creating urgent preservation challenges.

Recovery teams must rapidly deploy web-forensics tools that capture and preserve this ephemeral evidence in court-admissible formats. When properly documented, this evidence shifts responsibility from victim to perpetrator. Success depends on timing: capturing deception infrastructure before it vanishes, and proper forensic methodology meeting evidentiary standards.

Marcin Zarakowski

CEO of Recoveris

Prevent risks with Global Ledger

4-eyes principle + segregation

Some of the most damaging attacks aren't frequent; they target operational blind spots. That's why basic controls matter.

- The four-eyes principle states that no sensitive action (like fund transfers, whitelist changes, or key access) should be performed by one person alone.
- Enforce multi-party approval and role separation for all sensitive operations — including smart contract upgrades, whitelist changes, fund movements, etc. — ensuring that no single role or system can execute high-impact actions end to end.
- Regularly review multisig and MPC configurations to ensure signing thresholds, role assignments, and emergency procedures align with current risk exposure and operational realities.

A second pair of eyes helps. We know what to look for.

Schedule a Demo

Problem

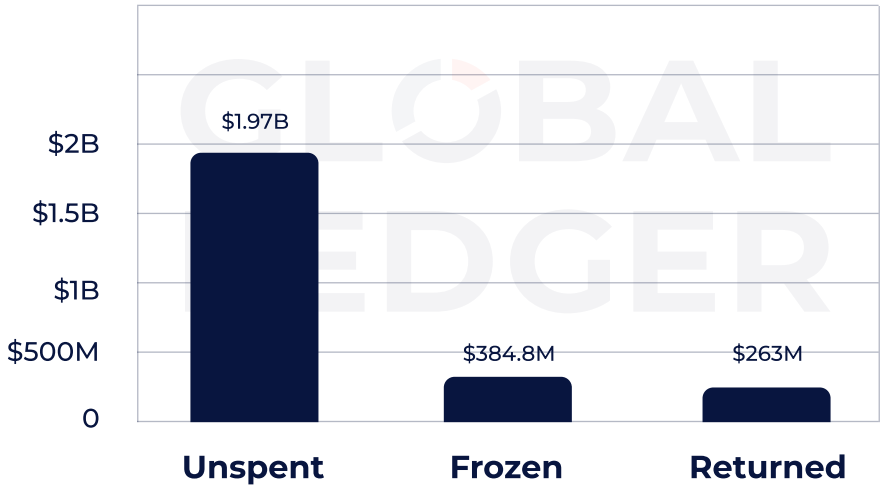
Nearly half of stolen funds remain unspent — likely “tomorrow’s” VASP exposure

Nearly **$2 billion** — 48.76% of total losses — **remain unspent**, meaning they either never moved or stopped moving shortly after the hack. In many cases, attackers delay laundering and re-enter the ecosystem at a later stage, when attention wanes.

Only **~ 9.52% of total losses** ($384.79 million) were frozen. The volume of funds frozen in H1 was ~65× higher than in H2, with Cetus ($162 million), Nobitex* ($83.89 million), and Bybit ($72.46 million) leading the list.

At the same time, **just 6.52%** ($263.23 million) of stolen funds were returned, showing a 10.79% decrease in H2 compared to H1 2025. Here, the Bybit incident, with $38.44 million recovered, is not leading the chart. Higher recovery volumes were recorded for the UPCX hack ($72.97 million) and the Balancer hack ($55.1 million).

~50% of stolen funds remain unspent



* In the Nobitex hack, funds were deliberately sent to burn addresses as a symbolic act. In that incident, $83.89 million was hacked and burned, effectively a public execution of the assets.

What is at stake?

1 Recovery remains the exception

Enforcement actions show some effect, but voluntary returns are rare, and most recoveries depend on rapid intervention rather than cooperation. In some cases, projects have negotiated directly with attackers to recover funds, typically by offering bounties. While this can lead to high recovery rates — up to ~90% in exceptional cases like GMX — such outcomes are uncommon and not scalable.

By contrast, enforcement pressure alone is often less effective, even though there are rare exceptions, such as the Loopscale case, where funds were returned after assurances of no legal action.

In practice, most illicit assets are far **more likely to circulate than to be recovered**, making late detection a much bigger risk than successful recovery.

Investigators need more interoperability, with tracing APIs, compliance data, and law enforcement work

Asset recovery remains limited due to two core issues: slow cross-border legal processes and fragmentation of laundering pathways. On the legal side, delays in data sharing, asset-freeze authorization, and evidence standardization make real-time cooperation difficult. Technically, attackers now exploit micro-laundering techniques, leveraging cross-chain bridges, privacy-preserving DeFi protocols, and rapid asset conversions to overwhelm manual tracing and reporting systems. This means the investigative community should focus on interoperability, integrating law enforcement casework, compliance data, and industry-grade tracing APIs.

Mudassar Malik

CEO and founder of Deconflict.com

2 Dormant funds become delayed exposure

Nearly **half of stolen funds remain unmoved**, suggesting that attackers are deliberately delaying laundering through further fragmentation. When activity resumes weeks or months later, these assets rarely move directly to exchanges. Instead, they pass through multiple intermediary wallets, protocols, and services, reaching regulated platforms multiple hops removed from the original hack. As a result, exposure becomes harder to spot, and illicit origins can go unnoticed without the ability to reconstruct the full transaction path.

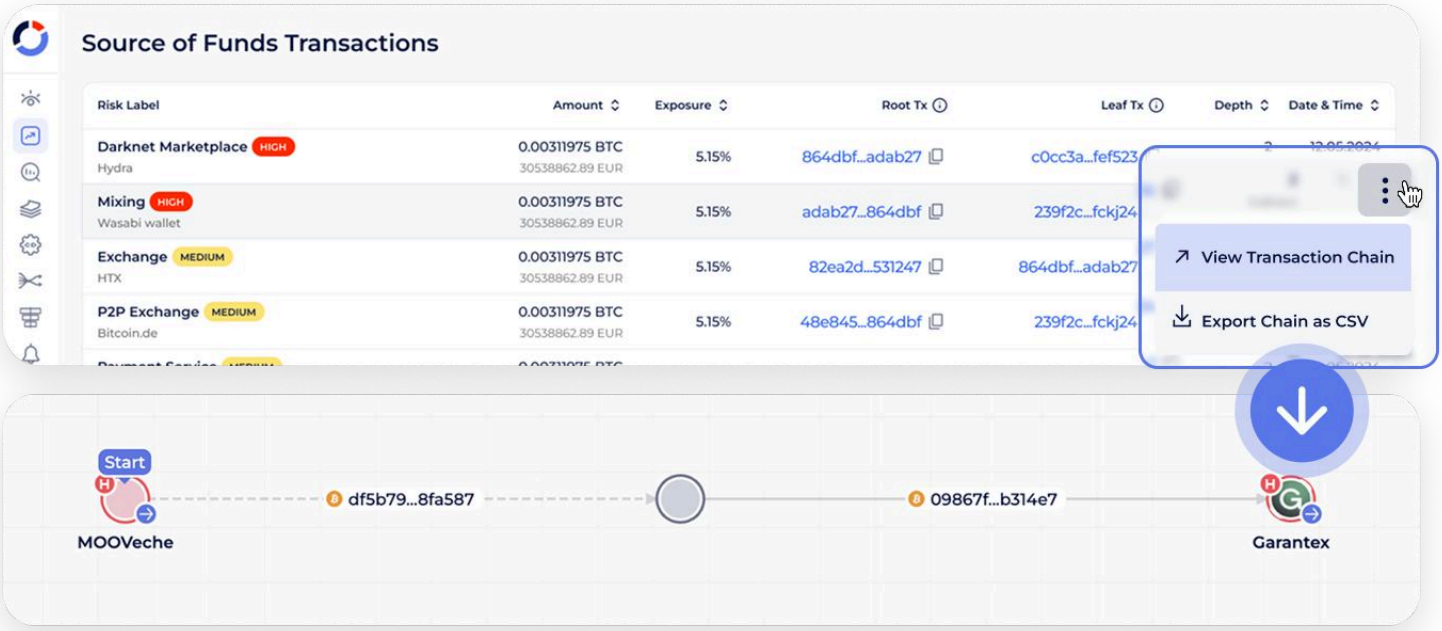
Prevent risks with Global Ledger

Reconstruct exposure across multiple hops

When stolen funds reach exchanges several hops after a hack, their origin is harder to trace. With **Transaction Tree on Demand**, you can link incoming funds to illicit sources even when you weren't the first stop.

What this enables:

- Trace the full path of funds across multiple hops.
- Identify exposure to hacks and stolen assets deep in the transaction flow.
- Create ready-to-share visuals for compliance audits and legal case files.



Make sure your exchange isn't part of a laundering cycle.

Schedule a Demo

Conclusion

Fragmented Laundering — Delayed Exposure for VASPs

The way illicit funds move has changed. Despite fast initial movements, subsequent laundering has slowed due to quicker disclosure. For VASPs, this means less time to react at the start and greater exposure later in the flow.

1 Faster first funds movement leaves little time to react

In the fastest cases, the first movement of stolen funds occurred in 2 seconds. It leaves minimal time for early intervention.

2 Laundering is increasingly fragmented

Multistage laundering dominates in ~99% of cases. Instead of single transfers, hackers move illicit funds through multiple hops, making risk harder to detect.

3 Tornado Cash is actively used in laundering schemes

Tornado Cash was used in ~41.6% of all hacks, with its share rising sharply in H2 to ~74% of cases, following the lifting of sanctions.

4 Attackers are more patient — exposure is delayed

Attackers are more cautious and appear to be waiting out initial scrutiny before taking the next steps. The high level of unspent funds (~50%) also suggests hackers wait for the heat to die down.

1

Reputation hit

Funds slip in unnoticed until an investigation or headline puts your name in the story.

2

Regulatory pressure

Without alerts, visibility, and a response plan, regulators treat it as failure, not oversight.

3

Loss of partners

Banks and providers can cut ties. Losing a single partner can mean losing the business.

Use our checklist to avoid costly blind spots.

Bonus

Checklist: Top 6 Laundering Race Issues & How to Keep Up

Issue	How to Solve It
First fund movements are faster	◯ Set up behaviour- and time-based triggers (not only static rules). ◯ Aim for a 15-minute internal SLA for reviewing suspicious flows. ◯ Set up an alerting system that integrates with your team's real channels like Slack, Jira, Telegram. ◯ Consider using risk bursts: clusters of similar incidents in short timeframes that may point to coordinated laundering attempts. ◯ Trigger EDD reviews for flows linked to mixers, bridges, or sanctioned wallets. ◯ Apply stricter rules for deposits from non-KYC sources. ◯ Use hold-and-review policies to freeze funds while the investigation unfolds.
Laundering has become fragmented	◯ Use cluster-level analytics to identify behavioural patterns, transaction paths, and timing anomalies. ◯ Escalate patterns across hops (repeat routes, counterparties, timing).

GLOBAL LEDGER

Issue	How to Solve It
Cross-chain bridges create blind spots	○ Create scenarios with bridge-specific patterns (routing, aggregation). ○ Maintain continuous monitoring and real-time alerts.
Tornado Cash as № 1 post-sanctions mixer	○ Treat post-mixer inflows as higher risk by default, even without sanctions flags. ○ Use behavioural and probabilistic analysis to link mixer inflows and outflows when direct attribution breaks.
Misplaced focus on the most popular risks	○ Enforce multi-party approval and role separation for all sensitive operations — including smart contract upgrades, whitelist changes, fund movements, etc. — ensuring that no single role or system can execute high-impact actions end to end. ○ Regularly review multisig and MPC configurations to ensure signing thresholds, role assignments, and emergency procedures align with current risk exposure and operational realities.
½ of stolen funds still unspent, likely to be laundered	○ Use AI-powered alerts and continuous monitoring ○ Trace the full transaction path to identify deep exposure if funds resurface on your platform. ○ Document clear evidence for audits or investigations.

Quiet risk is harder to spot. Preparation helps — and you don't have to do it alone.

Schedule a Demo

Subscribe to the Global Ledger newsletter for upcoming reports

Subscribe