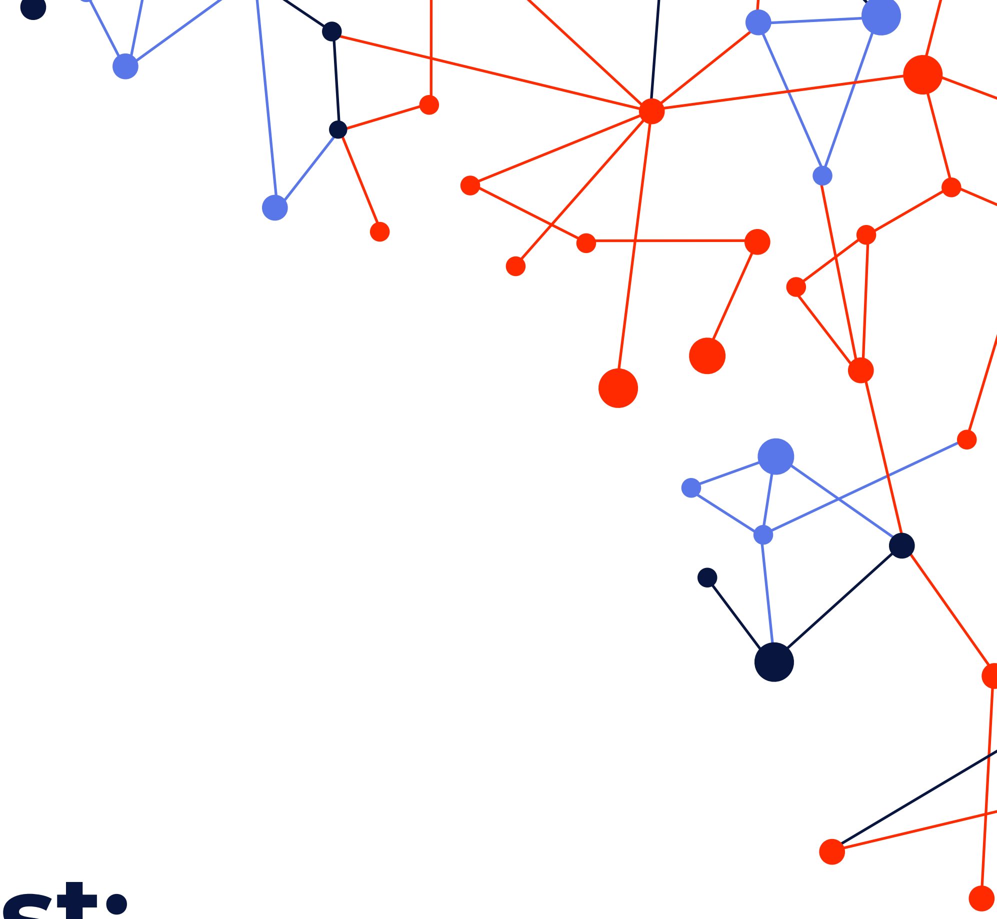
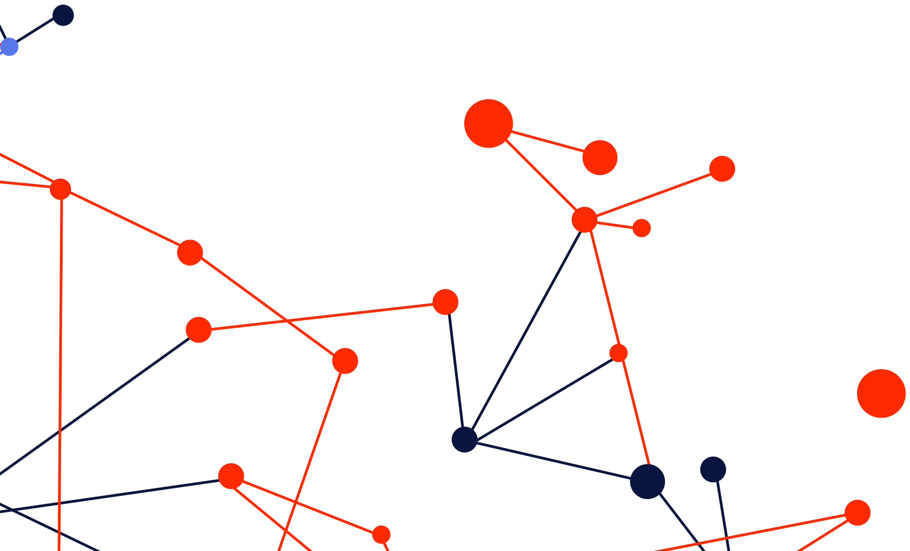
GLOBAL
LEDGER



Gone Fast: Laundering Timing Report

H1 2025



Executive summary

H1 2025 marked one of the most devastating half-years in the history of crypto hacks, with **over $3.01 billion** stolen across **119 incidents** — already **1.55 times more** than the total for all of 2024 ($1.94 billion).

But the growing volume of hacks is nothing new. **The real shift is in timing.** Attackers are moving faster, often laundering funds before the incident is even publicly known. The fastest attacker funds movement in H1'25 was just **4 seconds** — about as fast as you blink. **Speed has become the new dangerous weapon.**

The H1 2025 Crypto Hacks Report from Global Ledger is the first in the industry to analyse the **timing of funds movement** in crypto hacks at this level of detail. By breaking down timelines, we uncover patterns others miss: how fast attackers move, how long funds sit idle, and where the industry remains most vulnerable.

Knowing these timing patterns can help **detect suspicious activity sooner** and reduce the window attackers have to launder funds. It is not just about reacting, it is about **anticipating the next move.**

Our analysis also covers the path of laundering — the methods used, sources of the funds, and final destinations. Understanding the route can help predict and spot risks earlier, react faster, and avoid becoming the next link in the laundering chain.

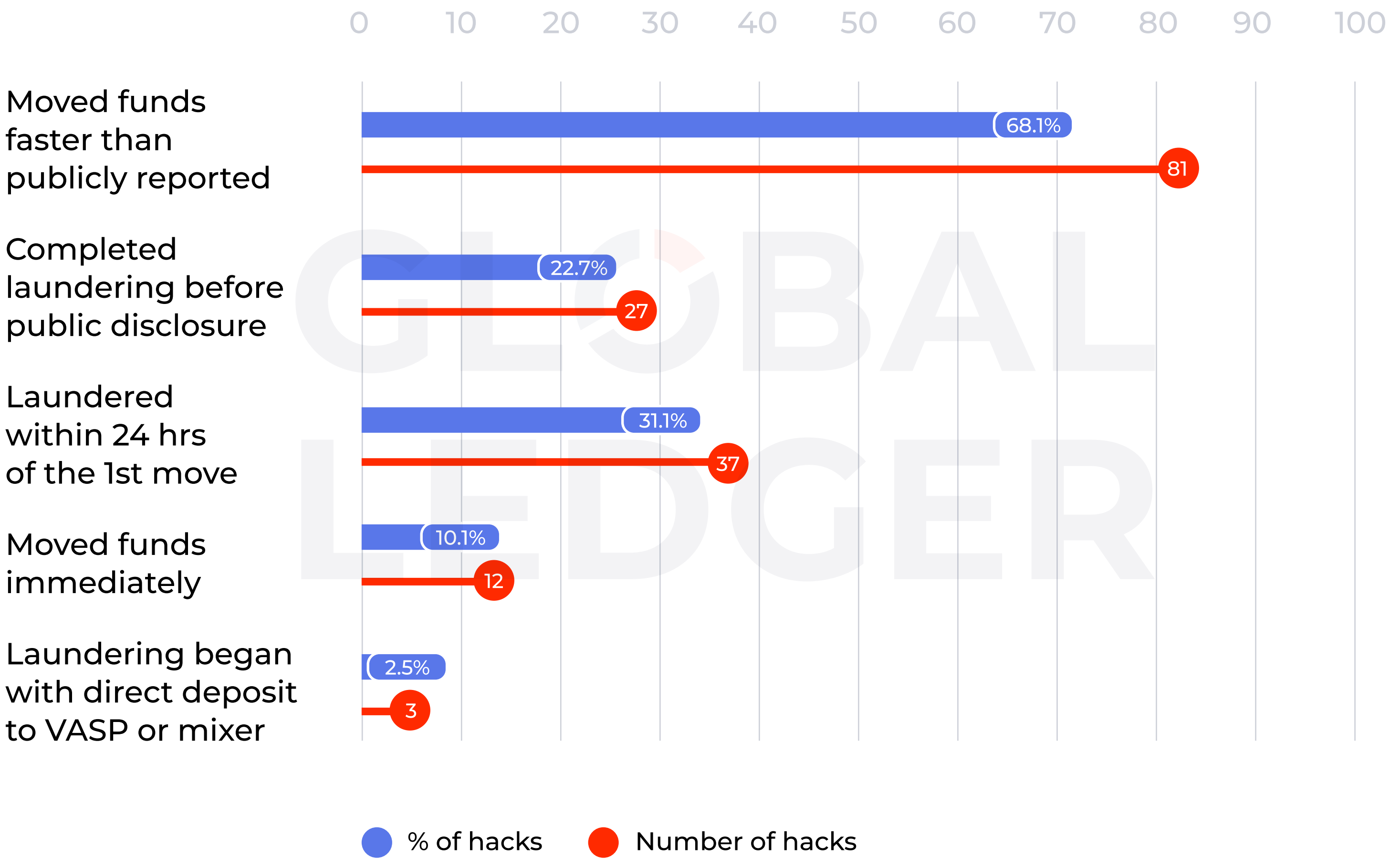
Key Takeaways

- Funds from nearly **1 in 4 hacks** were fully **laundered before public disclosure.** By the time a statement or alert is issued, the window for blocking or tracing the stolen assets has already closed, giving attackers a critical head start.
- The fastest **attacker** funds movement is 4 seconds, which is over **75 times faster** than the **alerting** system. Attackers can act almost instantly, long before any monitoring system has time to respond. Speed is no longer an advantage but a necessity for defence.
- The **fastest laundering** process, from incident to last deposit, took just **2 minutes 57 seconds,** close to a laptop screen sleep time on battery. This shows how narrow the response window really is. In the time it takes to notice something is wrong, the money may already be gone. With **stolen assets from only 4.2% of hacks** recovered in H1 2025, most funds disappear before any action can be taken.
- Hackers leverage this timing. In 31.1% of cases, illicit actors **finished laundering within a day** from the moment the funds first moved from the hacker's wallet. Once movement begins, there is a very short window to detect and act before the trail goes cold.

Funds from ~ 68% of hacks were moved before the incident was even disclosed

According to the Global Ledger research, **84%** of incidents were reported **the same day** they occurred. However, this was not fast enough. In **68.1%** of hacks, the funds were moved from the hacker's wallet **faster than the incident was publicly reported.** Moreover, 10.1% showed immediate funds movement; in 64.7% of cases, funds moved within the first 24 hours.

In 68.1% of hacks, funds moved before disclosure



The data exposes a critical gap between when an incident happens and when the industry becomes aware of it. If funds are already in motion before the hack is publicly reported, then **investigators and compliance teams have no time left to react.**

Hackers leverage this gap. In **22.7%** of cases (over $34 million in total), they **completed laundering before the hack was publicly disclosed.** In 31.1% of cases, hackers laundered the funds within 24 hours of the first move. In **2.5%** of hacks, bad actors finished **laundering with just one move.**

Out of all incidents in H1 2025, only 5 (**or 4.2%**) ended with **recovered** funds despite the fact that funds end up at known, traceable addresses.

> Even with existing technical capabilities to trace and freeze digital assets, legal frameworks haven't evolved quickly enough to match the speed of illicit digital asset activities. Many public sector actors globally still struggle with how to properly classify and seize digital assets, making international cooperation slow and challenging.
>
> Unfortunately, law enforcement agencies often can't keep up with the rapid movement of blockchain-based funds. While the private sector has rapid-response tools, they lack the authority to enforce asset freezes. For example, digital asset services might voluntarily freeze suspicious funds for a few days, but law enforcement typically needs much more time to follow up. Furthermore, many services hesitate to act when victims and suspects are in different jurisdictions. Finally, the lack of clear standards for digital asset tracing methodologies leads to disagreements among these services.

Marcin Zarakowski

CEO of Recoveris

Weak public signalling allows hackers to complete laundering before disclosure

Traditional AML workflows can't keep up. In nearly a quarter of cases, funds were fully laundered before the breach was even made public. No alerts, no headlines, no warnings. If a compliance team doesn't have its own early signals, like on-chain monitoring or behavioural detection, it may never know an incident happened until it's too late.

As there is a gap between the incident and public disclosure, traditional communication channels are not effective as a defence mechanism. Without early on-chain alerting or behavioural detection, up to a **quarter of hacks may bypass AML systems** entirely, even at compliant and well-intentioned VASPs.

> To truly stay ahead, we need platform native intelligence. It can include in-house fraud intelligence and behavioural analytics, capable of platform-specific signals that third-party tools simply can't access, such as login patterns, device fingerprinting, behavioural biometrics, and internal risk markers. Also, we need AI-powered real-time detection, able to evaluate a live transaction against thousands of known fraud templates and dynamically identify anomalies or novel attack types, as well as continuous self-learning algorithms, which evolve based on emerging fraud patterns.

Max Krupyshev

CEO and co-founder of CoinsPaid

The fastest hackers can outrun AML alerts by 75x

The fastest incident-to-report time is 5 minutes and 1 second via alerting system, but our research clearly shows this is not always enough. Hackers' top speed is higher:

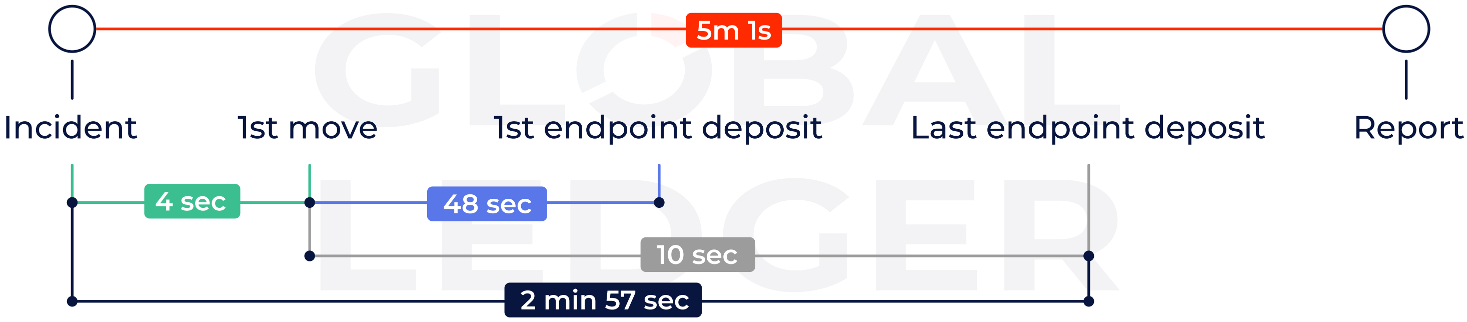
- The fastest attacker funds movement: 4 seconds, which is over **75 times faster** than the fastest incident-to-report time.
- The fastest laundering time, excluding initial hack transaction (from first movement to last endpoint[3] deposit): 10 seconds **(30× faster).** [1] [2]
- The fastest time from the first movement to the first endpoint deposit: 48 seconds **(6.3× faster)**.
- The fastest laundering time (from incident to last endpoint deposit) was 2 minutes 57 seconds **(1.7× faster**).

[1] Initial hack transaction stands for the very first on-chain action that occurs when an attacker gains control of the funds.

[2] By the first movement, we mean the first movement of funds from the hacker's wallet when they actually start moving funds to obfuscate the trail or cash out.

[3] 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.

AML Lag Leaves 75x Head Start for Fastest Hackers



In the most critical cases, **funds are already moved before any alert is even triggered,** shrinking the response window to seconds, not minutes.

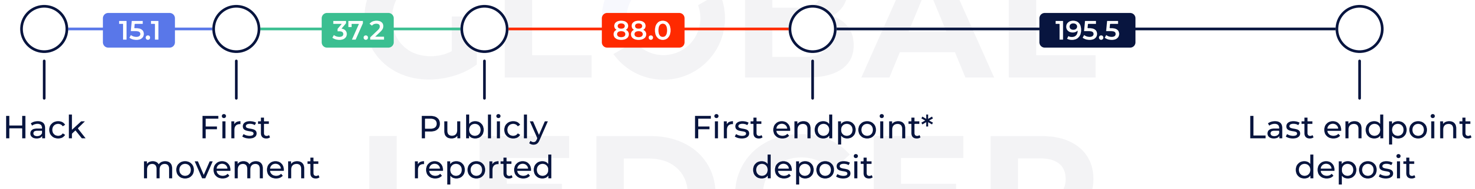
The average[4] time from the start of a hack to the first movement of funds is **15 hours**. In contrast, it takes about **37 hours on average** for the incident to become publicly known, meaning attackers usually have a **more than 20-hour head start** before anyone is aware of the breach.

On average, hackers reach their **first endpoint** within **158 hours (about 6.5 days)**, and it takes about **195 hours (just over 8 days)** to fully move funds into mixers or centralised exchanges.

However, only **68 out of 119 hacks** (57.14%) had **fully laundered** funds by the time of analysis, while funds from **12 out of 119 incidents** (10.1%) had not moved at all by that point, excluding the Nobitex case, where 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.

This suggests that in many cases, a significant portion of stolen assets is still in motion or being held for later laundering.

Attackers Get a 20-Hour Head Start on Average Before Public Report



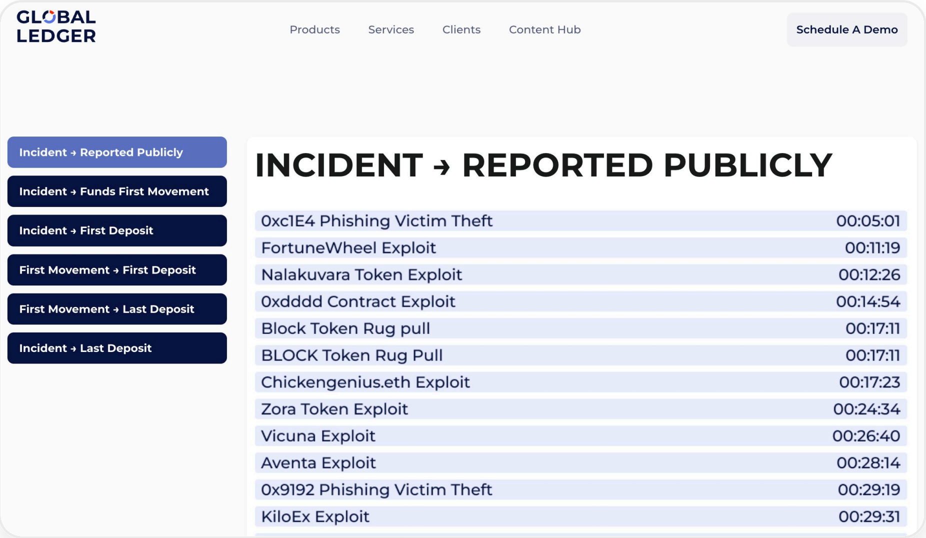
[4] In this case, we've excluded two incidents totalling $125.6K (0.00417% of total) as their timing was highly irregular and significantly skewed the overall averages. Including them would have distorted the broader trends in laundering behaviour.

While the fastest movements can be detected, the slowest laundering cases are to be identified, as the funds are still being moved, including those linked to the Bybit incident.

Larger hacks tend to move more slowly, as it often takes attackers longer to launder more funds, splitting them to obscure their tracks. As a result, the **averages don't reflect the real urgency** and may create a false sense that compliance teams and investigators have more time than they actually do.

Hack Timing Breakdown from Incident to Last Deposit

View Full Data


GLOBAL LEDGER
Products
Services
Clients
Content Hub
Schedule A Demo
Incident → Reported Publicly
Incident → Funds First Movement
Incident → First Deposit
First Movement → First Deposit
First Movement → Last Deposit
Incident → Last Deposit

INCIDENT → REPORTED PUBLICLY

0xc1E4 Phishing Victim Theft	00:05:01
FortuneWheel Exploit	00:11:19
Nalakuvara Token Exploit	00:12:26
0xdddd Contract Exploit	00:14:54
Block Token Rug pull	00:17:11
BLOCK Token Rug Pull	00:17:11
Chickengenius.eth Exploit	00:17:23
Zora Token Exploit	00:24:34
Vicuna Exploit	00:26:40
Aventa Exploit	00:28:14
0x9192 Phishing Victim Theft	00:29:19
KiloEx Exploit	00:29:31

You have a 10–15-minute window to act

If you're a VASP, and funds from a hacker-controlled address have already reached your platform, you typically have a **10–15-minute window to act.** In many cases, if a transaction exceeds the platform's internal risk threshold, it is routed for manual review and not credited to the user's balance until approved. The issue is that this only **works if ongoing monitoring is active,** not at the moment of the transaction.

If no action is taken during this narrow window, the assets will likely be moved again into a mixer, another exchange, or off-ramped entirely. At that point, **recovery becomes nearly impossible.** Once stolen funds pass through a VASP, they're often aggregated, traded, or split, losing their traceability, especially if detailed records aren't kept. From there, the assets can quickly move off-chain, beyond the reach of blockchain-based monitoring or enforcement.

“

During critical incidents, most time is lost when verifying the request, confirming authority, and assessing if urgent action is needed. To speed up information flow between law enforcement and affected platforms, we need to create fast-track channels for verified cases, standardise request templates (e.g., case ID, wallet/TxID, AML flags), establish direct contact points within law enforcement, and pre-establish memoranda of cooperation defining emergency data exchange protocols.

Oleksandr Plakhotnyuk

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

As funds movement is near-instant, and ticket-based compliance reviews are delayed by design, manual post-incident checks lose effectiveness.

“

We’re observing a growing emphasis on real-time monitoring, third-party audits, and stricter regulatory adherence as clients seek to future-proof their assets. Institutional clients are increasingly raising questions about security assurances, compliance standards, and incident response protocols, especially in light of the surge in high-profile crypto exploits. Compliance is now a baseline; institutions scrutinise how security integrates with operational workflows, such as multisig governance and hardware signing procedures

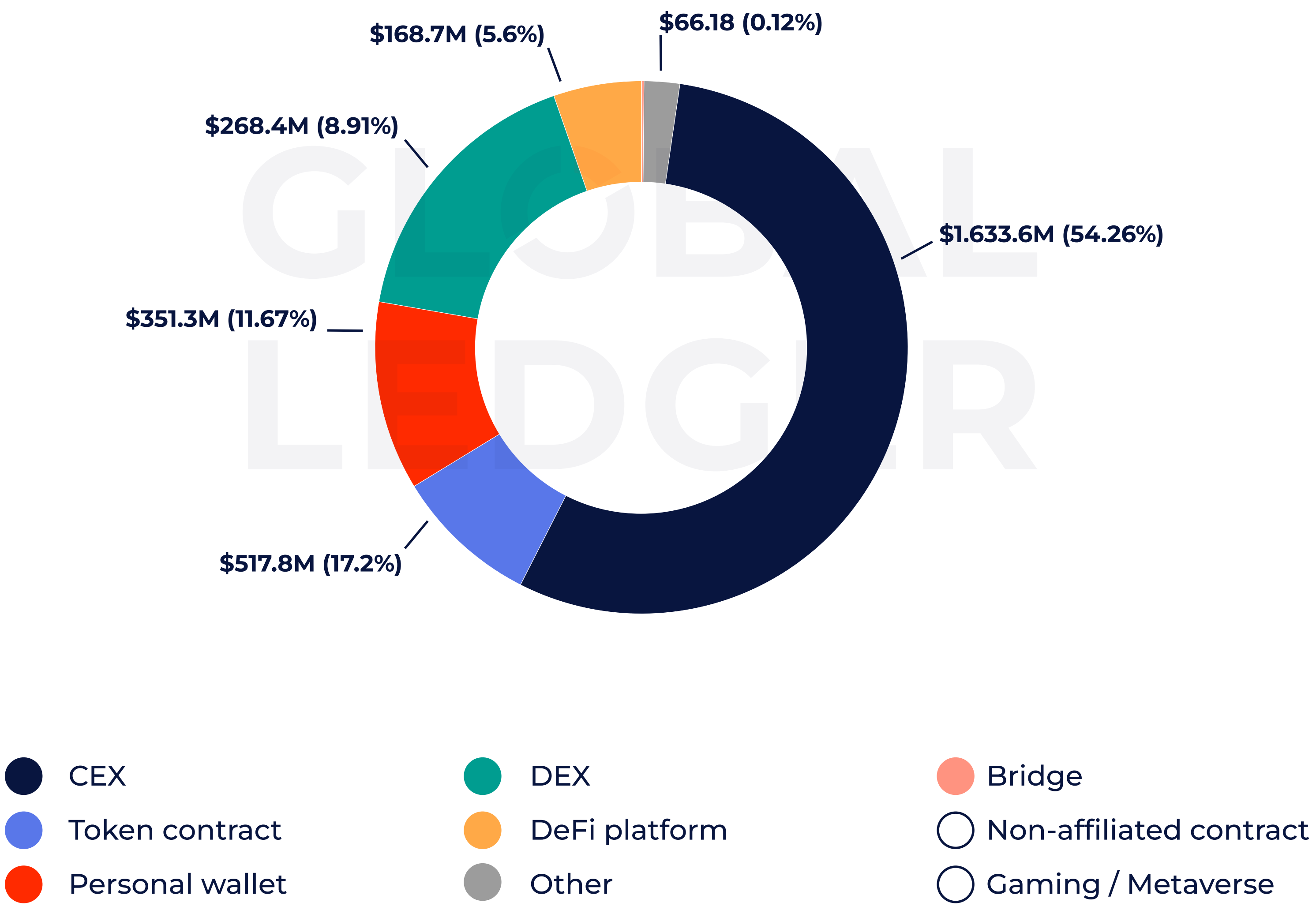
Denys Avierin

Chief Information Officer at Everstake

CEXs lost over 54% of funds stolen in H1’25

CEXs remain the most attractive as high-value, single-point-of-failure targets for attackers, contributing to **54.26%** of total losses. Token contracts are #2 in terms of money stolen, with $517.8 million, or 17.2% of all losses in H1’25. Personal wallets round out the top three, with $351.3 million (11.67%).

CEXs lost over 54% of all funds stolen in H1'25



[5] Here, we refer to all losses involving token contracts, including smart contract hacks, rug pulls, and other contract-related exploits.

By the time a ticket is opened, the funds may already be gone

Centralised exchanges remain the main off-ramp for stolen funds. To their credit, many platforms already block high-risk deposits if they exceed internal risk thresholds, routing them for manual review. But again, this only works if ongoing monitoring is in place.

That delay, even just a few minutes, **gives bad actors the head start they need.** While the platform is still waiting for an alert or starting a manual review, the funds may already be split across dozens of wallets, routed through other exchanges, or off-ramped. As a result, there is nothing left to freeze, and your platform risks becoming part of a laundering trail.

This delay may no longer be defensible. Regulators increasingly expect reasonable efforts: active monitoring, automated alerts, clear escalation paths, and a working risk model. Without these, even if you have a policy on paper, you are failing your AML obligations in practice, putting your licence, partners, and reputation at risk.

> It has been widely observed throughout the industry that particular VASPs will not action alerts that could only reasonably have resulted in offboarding. However, having these wallets labelled and thus knowing these particular VASPs are receiving problematic transactions and choosing to do nothing is a precursor to enforcement actions.

Richard Sanders

Investigator,
volunteer for Ukraine

However, what exactly the concept of “reasonable effort” stands for in different jurisdictions is a question that can create confusion and inconsistent enforcement.

> The ambiguity around ‘reasonable effort’ was perhaps helpful early on — it gave companies room to interpret based on their own risk profiles. But now, as the market matures, that vagueness can actually create more confusion than clarity. What we need is a consistent baseline across regions, not a rigid checklist that stifles innovation.

Georgy Sokolov

Co-founder and Chief
Commercial Officer at Wirex

Nearly 70% of attacks were contract exploits, but malicious approvals drove ~49% of total losses

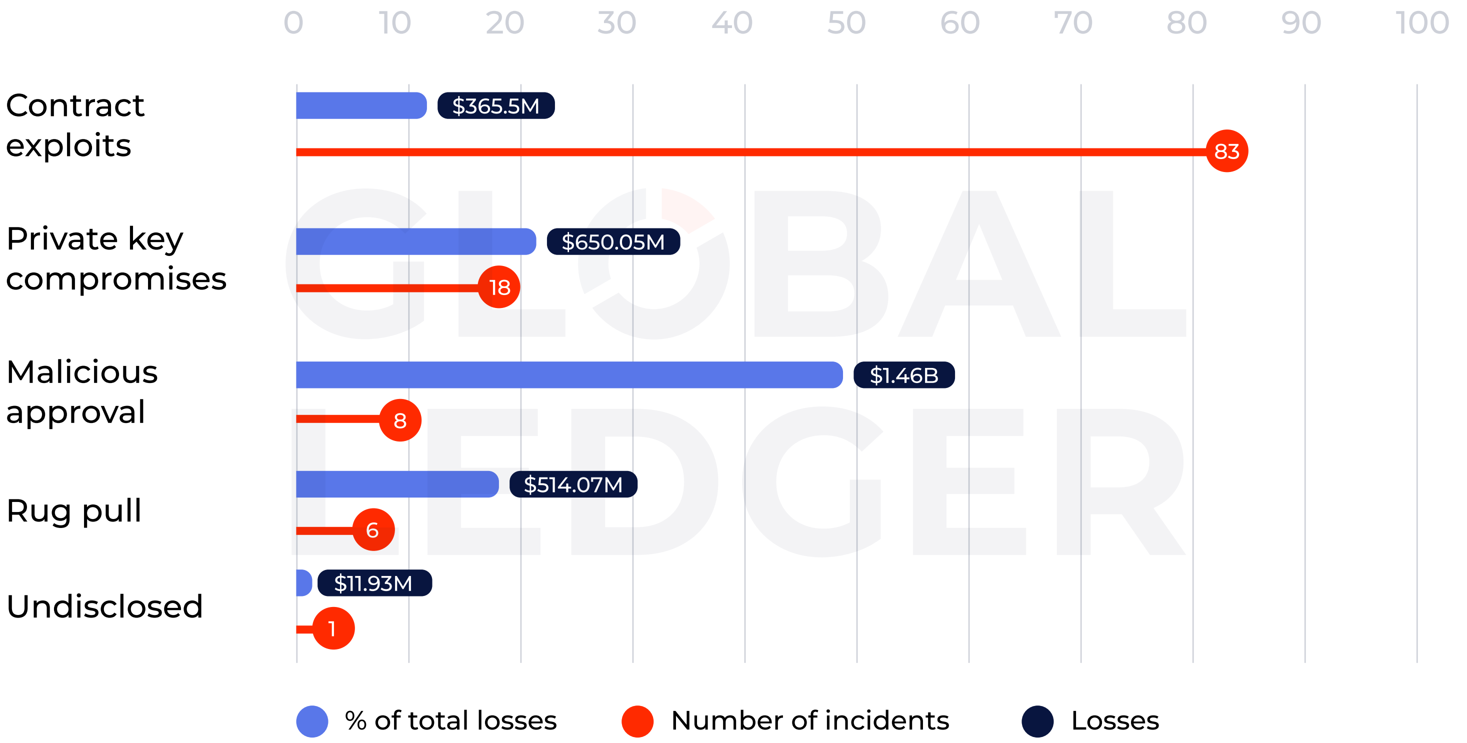
In H1’25, contract exploits were the most frequent (69.75%) but caused moderate losses ($365.5 million, or 12.15% of total losses). Meanwhile, **malicious approvals** were fewer (8, or 6.72%), yet **caused the most financial damage** ($1.46B, or 48.51% of total losses).

Private key compromises were #2 in terms of the number of incidents and caused $650.05 million of losses (21.61% of total). Rug pulls, though less common (6), resulted in $514.07 million lost (17.08% of total).

However, these figures are skewed by the volume of the Bybit exploit, which significantly inflated the impact of the malicious approval category. Without the Bybit case, **private key compromises would be the leading source of losses** in H1 2025, continuing the pattern from 2024, when they accounted for 48.03% of total stolen funds ($930 million).

[6] Bybit hack accounted for nearly all the total losses in this category, with $1.456 billion stolen.

Contract Exploits Account for Most Attacks. Malicious Approvals Cause Biggest Losses



High frequency ≠ high risk. Your priorities might need correction

While contract exploits made up the majority of attacks, they accounted for only a fraction of total losses. In contrast, malicious approval attacks, though less frequent, were responsible for nearly half of the stolen funds in H1'25.

The data reveals a clear trend: attackers are shifting from technical bugs to **systemic weaknesses in key management, signer behaviour, and user interfaces.** The Bybit hack skewed the entire dataset and illustrates how **low-frequency attacks can cause a disproportionate impact.**

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.

Sharp spikes in activity, such as large transactions or multiple transactions with the same pattern, will always be the main trigger for security systems to operate and for additional verification. However, attackers use new methods for their activities every time, so updating security rules is an ongoing process that requires constant monitoring. Most likely, building a basic model of client behaviour and monitoring deviations will be the most acceptable option in the future.

Vadym Grusha

CEO and founder of Trustee Plus

Hackers routed 4.4x more stolen funds through bridges than mixers

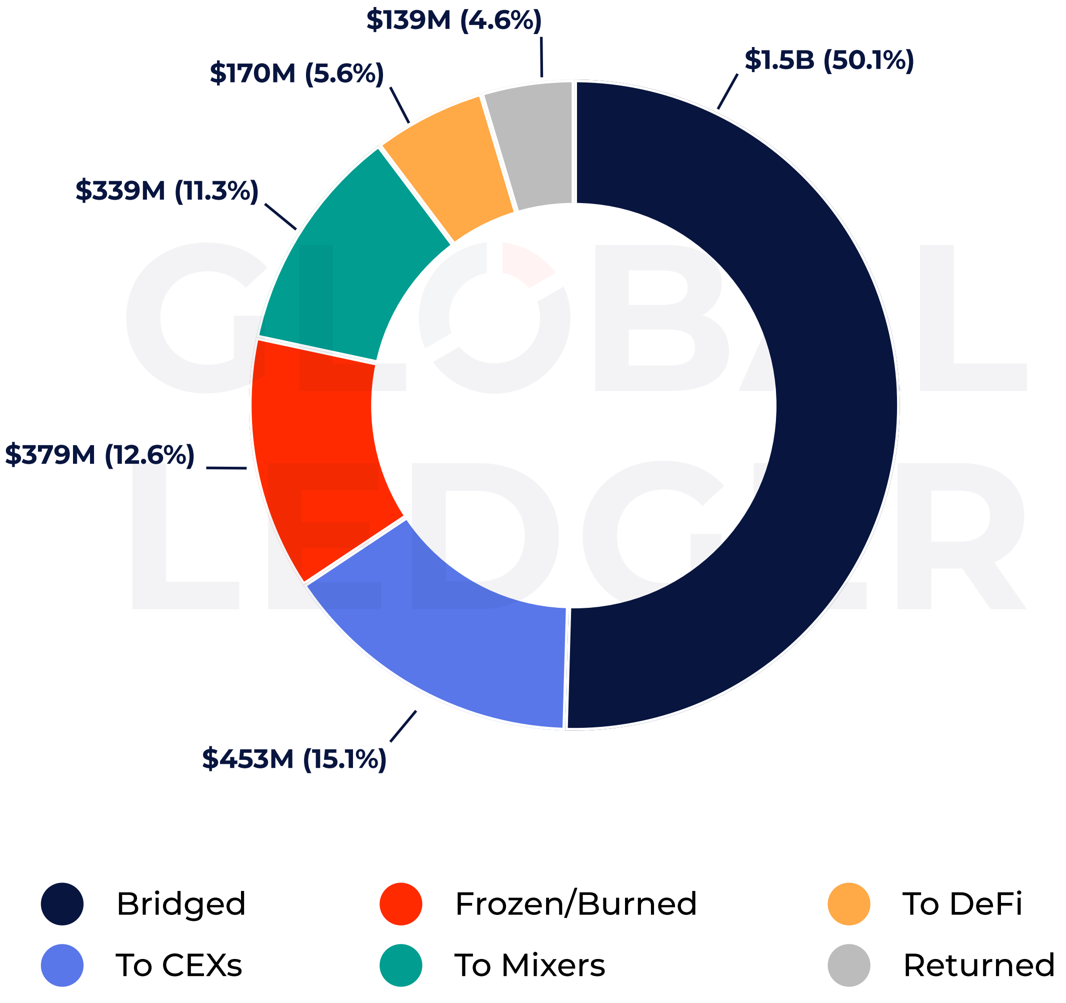
At the time of the research, over **$1.6 billion** (53.6% of total losses) remained **unspent**, meaning the funds didn't move or stopped moving. Some of them are likely still in the process of being laundered, as attackers may be waiting for the heat to die down.

The functionality of cross-chain protocols (**bridges**) is heavily **leveraged** by illicit actors, making them a key tool for obfuscating stolen funds origin. In H1'25, **over $1.5 billion (50.1%)** of hacked assets were routed through them. This data shows a sharp difference compared to **$339M (11.3%)** sent to **mixers**, which were used in 52% of hacks. This indicates that bridges are overtaking mixers as the preferred tool for laundering at scale for hack cases, likely due to their speed, liquidity, and lower regulatory scrutiny.

About 15% of the hacked funds ($453 million) were sent to **CEXs**, which are highly likely to be used for further cash-out. Interestingly, **DeFi** received about ⅓ of what centralised exchanges got—$170 million, or **5.6%**. This suggests that, despite growing usage, DeFi is still not the primary off-ramp for stolen funds, and centralised platforms remain the main target for cashing out.

Nearly **13%** ($379 million) got **frozen/burnt**, while just a small portion ($139 million, or **4.6%**) was **returned**. Enforcement efforts are making some impact, but voluntary returns remain rare, and most recovery still depends on rapid intervention, not goodwill.

Hackers laundered 4.4x more via bridges than mixers in H1`25



Bridges are not the problem, but they are the surface

This trend highlights how b**ridges 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.

The **Bybit incident alone** contributed **$1.38 billion** to bridge-related laundering, **94.91%** of the total funds stolen in that attack, underscoring just how central cross-chain movement has become in high-value laundering operations.

Certain cross-chain protocols are already more compliant than others, adding high-risk addresses to black lists and blocking illicit transactions, but they are still caught between **preserving openness and addressing regulatory expectations.** Additionally, many bridges offer public explorers, which support investigative continuity by allowing analysts to trace cross-chain movements.

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 fallout.

> The real challenge lies in the structure of the wider ecosystem. While real-time intervention at the protocol level can be limited due to decentralization, coordinated action between infrastructure providers, analytics platforms, and token issuers is key to improving resilience. That's why we work with regulated stablecoins like USDC and USDT, which include built-in controls around funds usage. We also collaborate with analytics and security partners to integrate risk signals into the user interface. If a wallet is flagged by trusted partners, we can prevent a transaction from being initiated through the front-end.

Andriy Velykyy

CEO and co-founder of Allbridge.io

Conclusion: With slow signals and fast laundering, 2025 is a wake-up call for VASP defences

The data from H1 2025 paints a clear and urgent picture: crypto hacks are no longer just growing in number, they are also evolving in **speed**.

1 Slow public disclosure → Hackers complete laundering before the news

If the current disclosure pace (~37 hours) continues, **30–40% of incidents** will be completed before AML teams even become aware of the attack.

This will make any response purely formal and retrospective. In many cases, even well-intentioned VASPs are not enablers but victims themselves drawn into laundering schemes. Yet in the eyes of the ecosystem and regulators, involvement, even passive, can still carry reputational and compliance consequences.

2 Laundering can take minutes → Manual compliance doesn't keep up

Because funds often begin moving and reach VASPs within minutes or hours, while compliance procedures still rely on ticket-based reviews, manual case-by-case checks are quickly becoming ineffective. Without automated and up-to-date AML and anti-fraud procedures and integrations, VASPs will always learn about the hack **after the funds are already gone.**

3 Laundering often happens in small batches → Victims can lose the trail

VASPS' monitoring systems often focus on individual transactions or large amounts, while hackers deliberately structure their activity and break funds into smaller parts (Garantex moving its untouched reserves is just one example).

As a result, structured laundering activity frequently slips through unnoticed. Without analysing behavioural patterns and cluster-level activity, **most attacks will continue to fly under the radar.**

4 Lack of a real-time AML → Compliance remains retrospective rather than predictive

The lack of a real-time AML is turning compliance into an archival function rather than a protective one. In H1 2025, funds from only 5 incidents (just 4.2%) were recovered. The average laundering duration was 15.4 days, yet half of the cases were completed before that point.

Because most AML teams respond retrospectively and lack a framework for immediate action, **even preventable incidents can go unaddressed.** Without finding a balance between implementing real-time processes and user experience, AML remains a post-incident reporting tool, not an active line of defence.