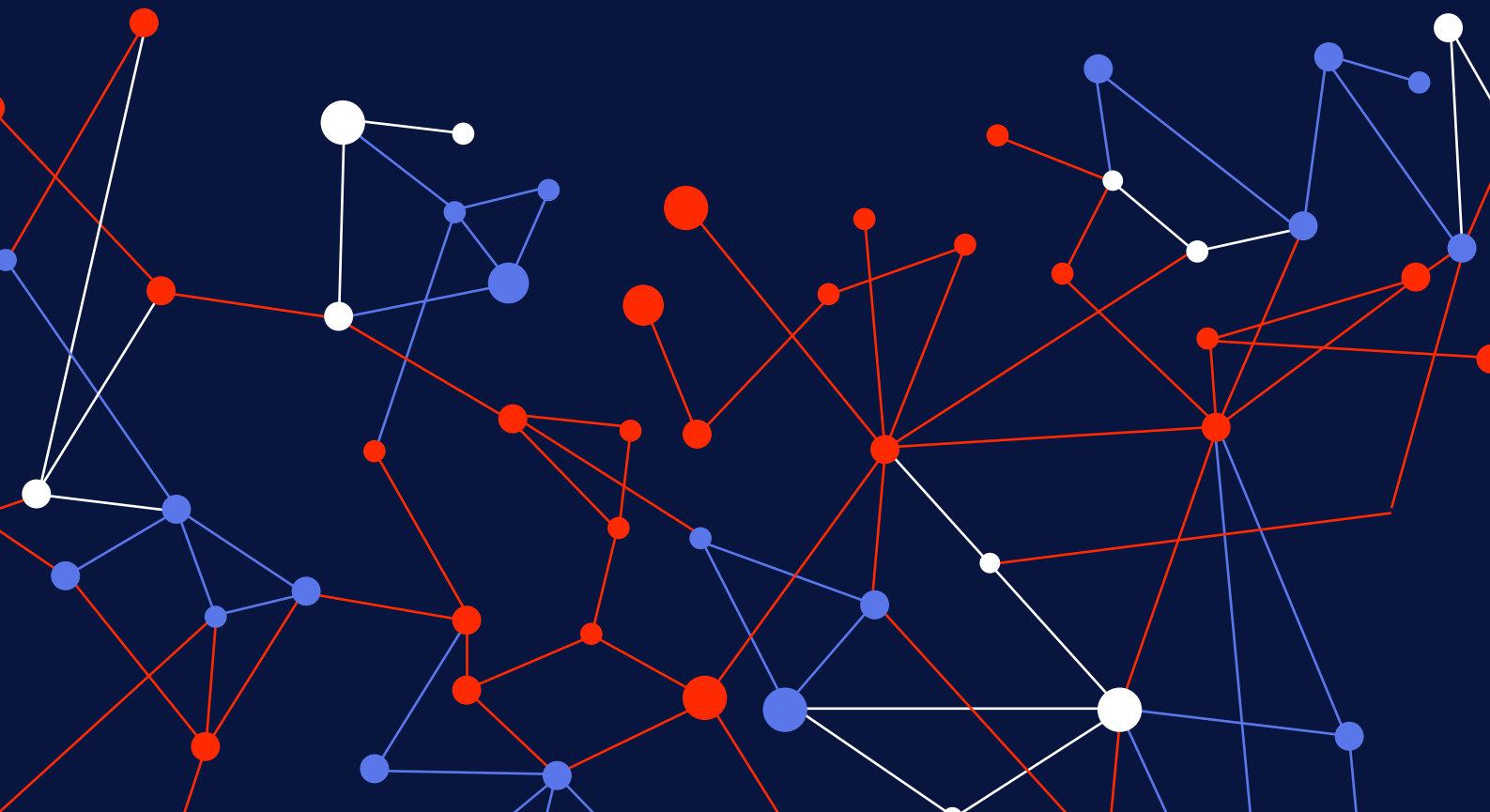
GLOBAL LEDGER

How Fast Is Crypto Laundered?

Lessons from 119 Hacks & Tips for VASPs



Key Takeaways

1

119

Hacks in H1 2025

2

$3.01B

Stolen in H1 2025

3

2 min 57 sec

The fastest laundering from incident to last deposit

4

75x

The fastest hackers can outrun AML alerts by 75x

5

20 hrs

An average head start attackers get before the public report

6

> ¼

Funds from ~ 1 in 4 hacks laundered before public disclosure

7

> 5%

Funds from fewer than 5% hacks recovered

8

10–15 min

Time for compliance teams to react to an incident

Bonus: Checklist

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**, which is already 1.55 times more than the total for all of 2024 ($1.94 billion).

But the **real shift is in timing**. In H1'25, the fastest **funds movement** after a hack was just **4 seconds** — about as fast as you blink. Our findings show where every extra hour of delay erodes the chance of recovery, and how missed red flags can turn a platform into part of a laundering chain.

This extended version of The H1 2025 Crypto Hacks Report from Global Ledger goes beyond describing the problem. It translates timing and laundering patterns into actionable insights and a **handy checklist.**

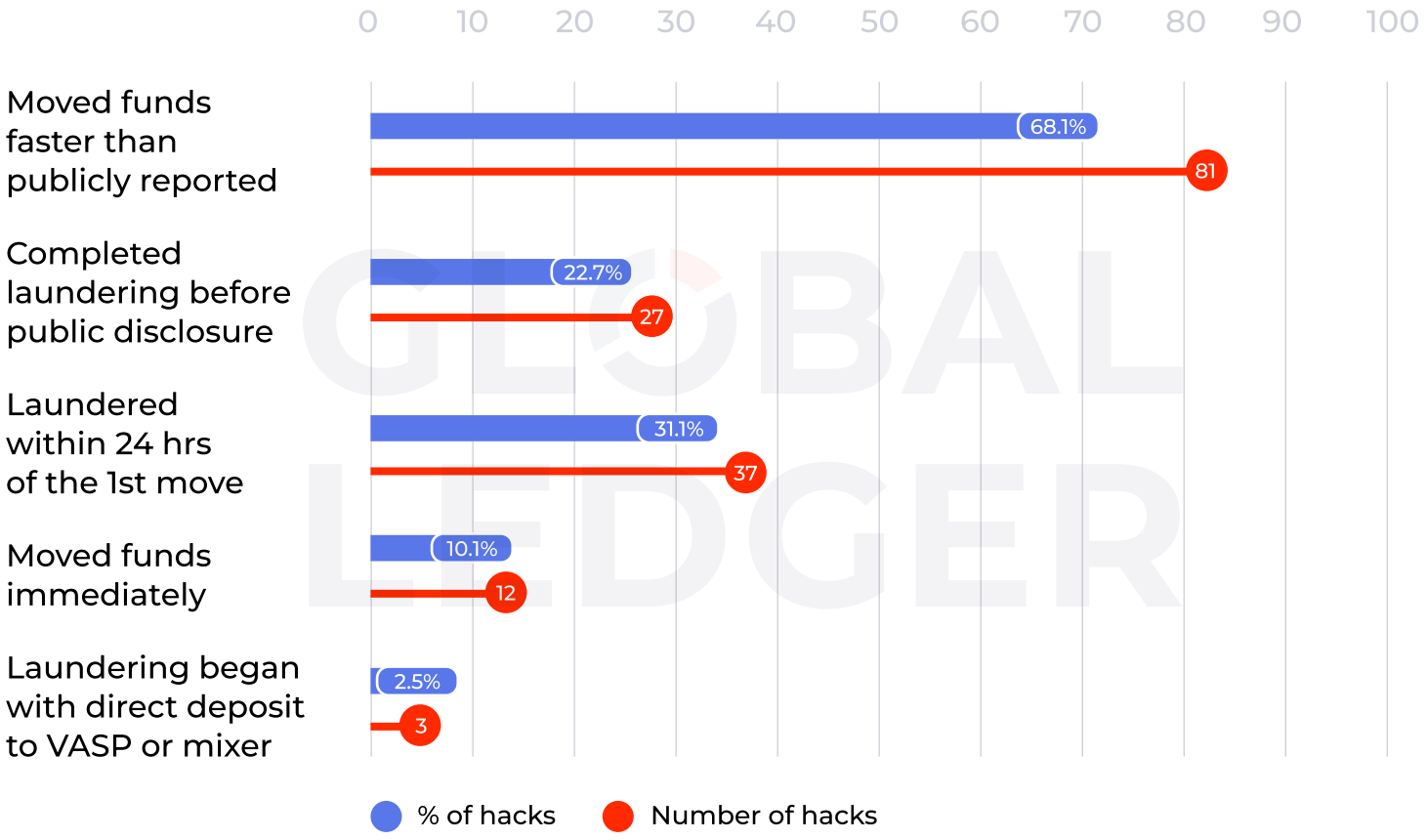
Problem

In 68% of incidents, hackers win the laundering race

Hackers don't just steal crypto but race the clock. In **68% of the hacks** we analysed in H1 2025, they were already **moving stolen funds before public disclosure**. Moreover, 10.1% showed immediate fund movement; in 64.7% of cases, funds moved within the first 24 hours.

Hackers leverage the gap. In **22.7% of cases** (over $34 million in total), funds reached the last deposit to a VASP or mixer[1] **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, **laundering began with direct deposit** to a VASP or mixer.

In 68.1% of hacks, funds moved before disclosure



1 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.

What is at stake?

1 Losing funds for good

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

2 Up to ¼ of hacks may slip under the radar

That’s not a failure of intent. Many compliance teams are doing their best within existing frameworks. But without early detection, such as alerting or behavioural detection, **up to a quarter of hacks may unfold unnoticed.**

> 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

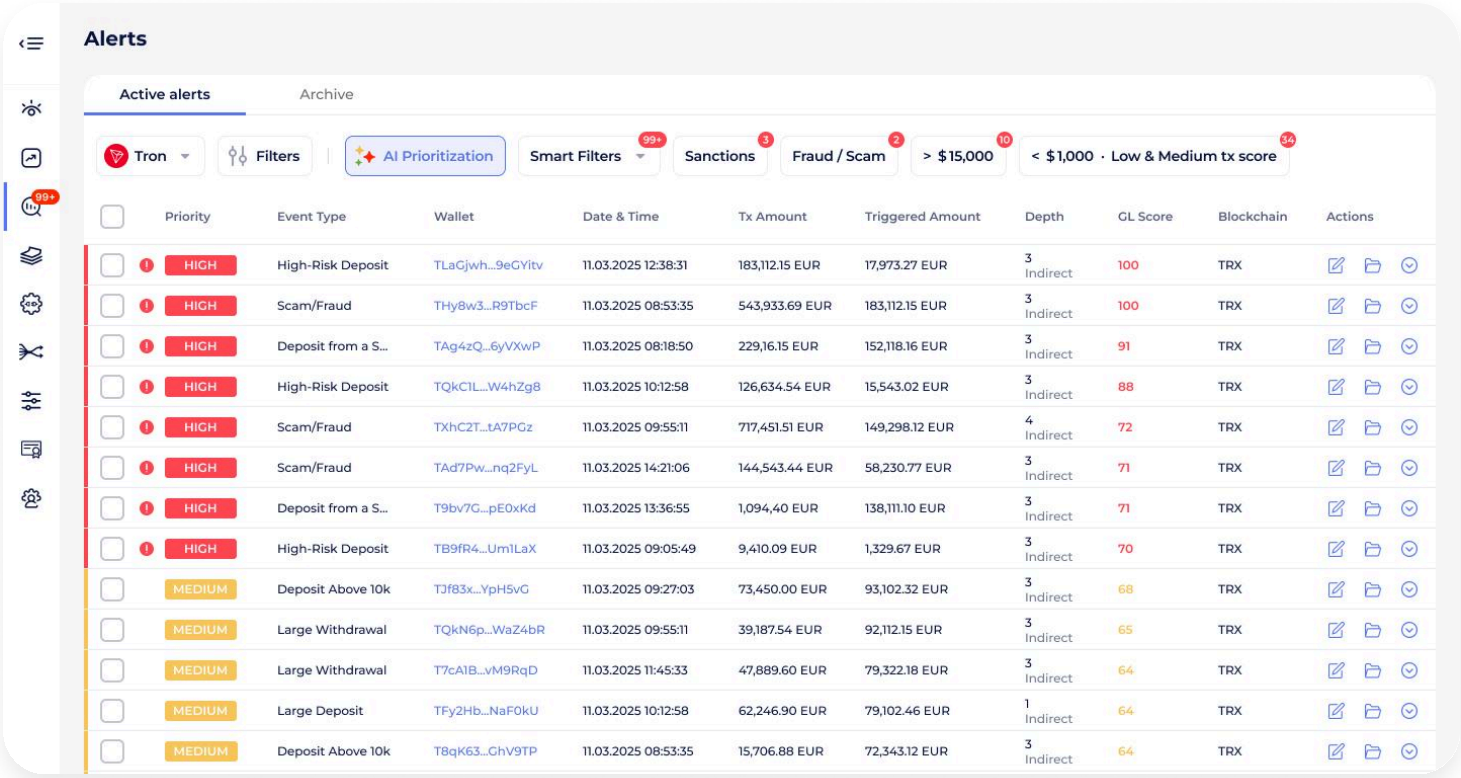
Prevent risks with Global Ledger

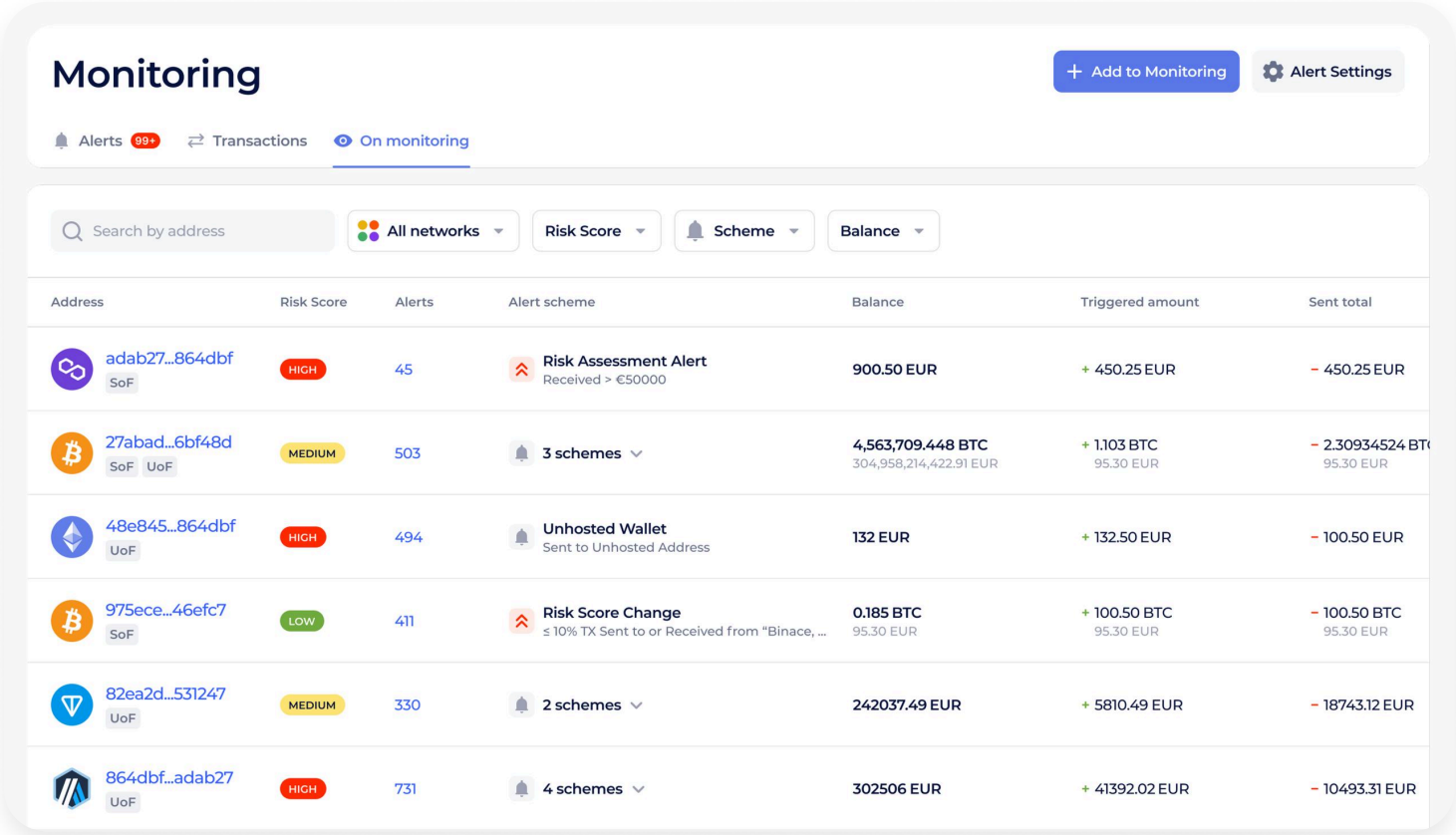
Real-time monitoring

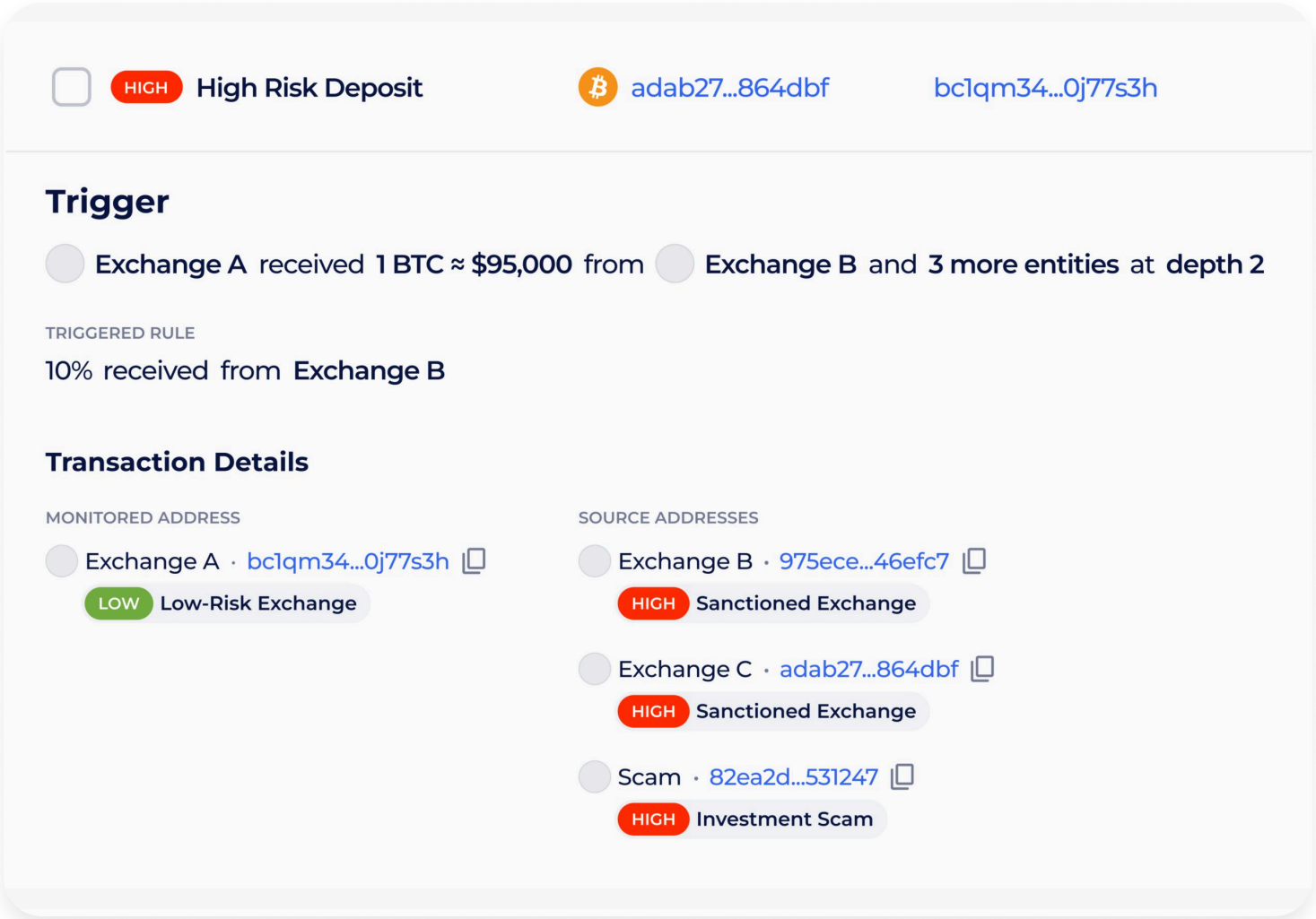
The gap between attack and disclosure is where real-time monitoring becomes critical. When signals are visible before the headlines hit, VASPs have a chance to act before the funds are laundered.

Steps to real-time monitoring that works when it matters most:

- Turn on proactive monitoring with a system that monitors 30 million wallets daily.
- Use AI to prioritise true high risks and resolve 1,000 alerts a day.
- 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

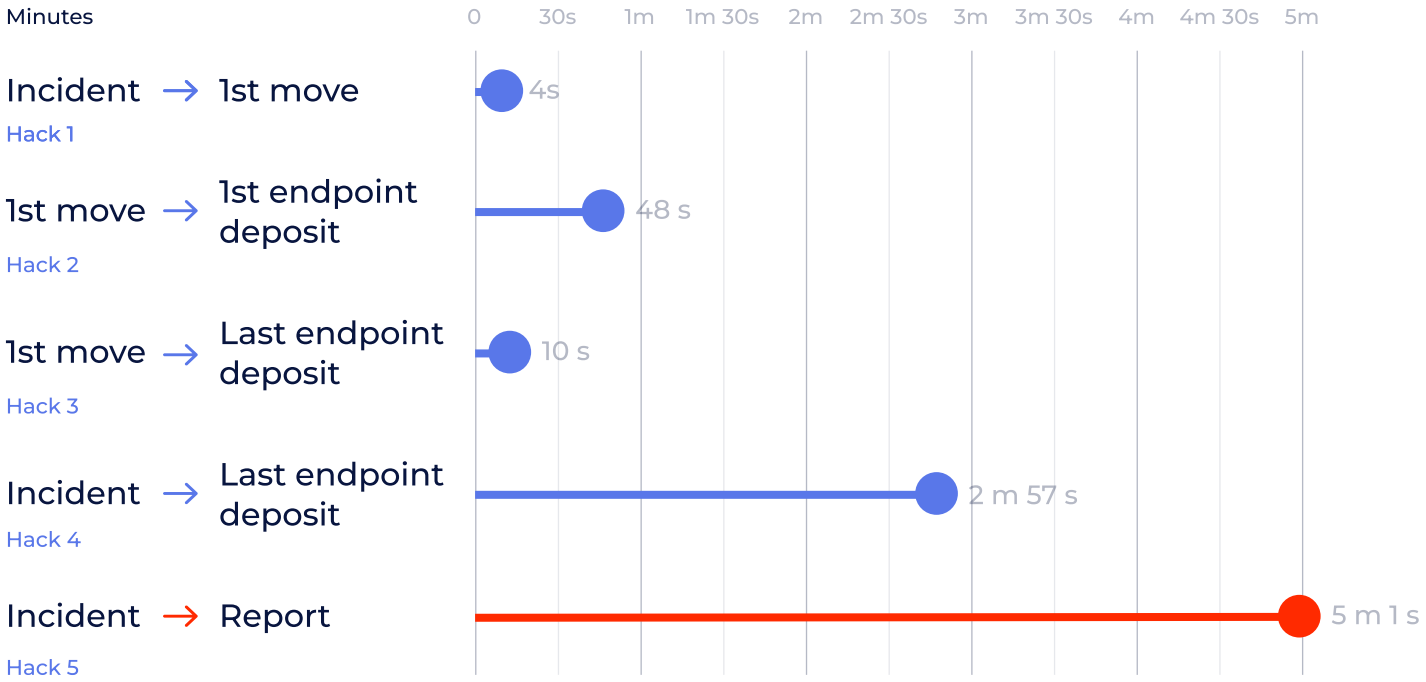
Problem

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[2] (from first movement[3] to last endpoint deposit): 10 seconds **(30× faster).**
- 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**).

AML Lag Leaves 75x Head Start for Fastest Hackers



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

3 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.

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

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.

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.

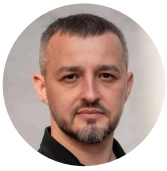
What is at stake?

1 You've got just 10–15 minutes to respond before recovery chances vanish

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

2 You may unknowingly become part of a laundering chain

Manual post-incident checks have become ineffective. By the time the check started, the funds have already been scattered across multiple addresses, funnelled through various entities, and cashed out. As a result, there is nothing left to freeze.

> 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

Prevent risks with Global Ledger

Enhanced due diligence (EDD)

Anonymous sources like non-KYC exchanges, cross-chain bridges, and mixers make it easier for illicit funds to slip through unnoticed. In many cases, flagged funds can be held during the EDD review, and by the time press releases go out, you're already a step ahead.

3 ways EDD helps protect your platform before others even react:

- 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 risky services quickly, you can use Entity Database, with over 51,000 of entities and information about ownership, status, services, jurisdiction limitations, privacy coin support and more.

Summary

ENTITY NAME
Binance

STATUS
Active

LEGAL NAME
Binance Holdings Limited

WEBSITE
https://www.binance.com

DOMICILED COUNTRY
Malta

Entity Details

KYC
Required

FIAT CURRENCY TRADING
Yes

PROVIDED SERVICES
API, Payments, Trading, Wallet, Staking, NFT, Mining etc.

PRIMARY OPERATIONAL REGIONS
Argentina Turkey Ukraine India

RESTRICTED JURISDICTIONS
Canada Malaysia Netherlands United States

Regulatory Compliance

COUNTRY	LOCAL AUTHORITY
France	Binance France SAS
Italy	Binance Italy S.R.L.
Poland	Polish Tax Administration Chamber of Poland in Katowice
Sweden	Swedish Financial Supervisory Authority
Kazakhstan	Astana International Financial Centre (AIFC)

Before it becomes a problem, EDD can raise the signal.

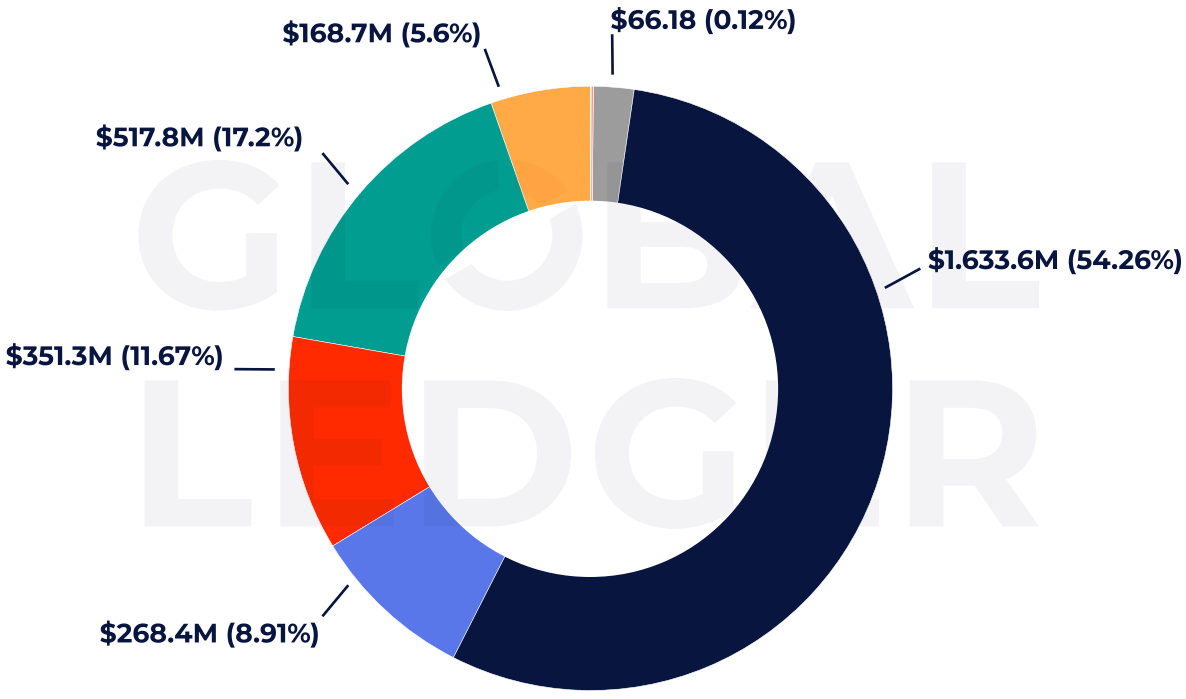
Schedule a demo

Problem

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.

What is at stake?

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

Centralised exchanges remain the main off-ramp for stolen funds. Many platforms have implemented manual review processes for high-risk cases, and that's a valuable step. But if alerts arrive too late or cases are processed only by ticket, this creates a critical delay.

2 Becoming part of a laundering chain can put your licence, partners, and brand at risk

In 2025, minutes matter. Hackers often launder funds within minutes, scattering them across wallets, exchanges, or off-ramps before a review even begins. That leaves little chance to freeze assets, and your platform may unknowingly **become part of a laundering chain.**

Meanwhile, regulators increasingly expect reasonable efforts: active monitoring, automated alerts, clear escalation paths, and a working risk model. Without these, you may be **exposed to AML risk despite your best efforts**, which will put 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

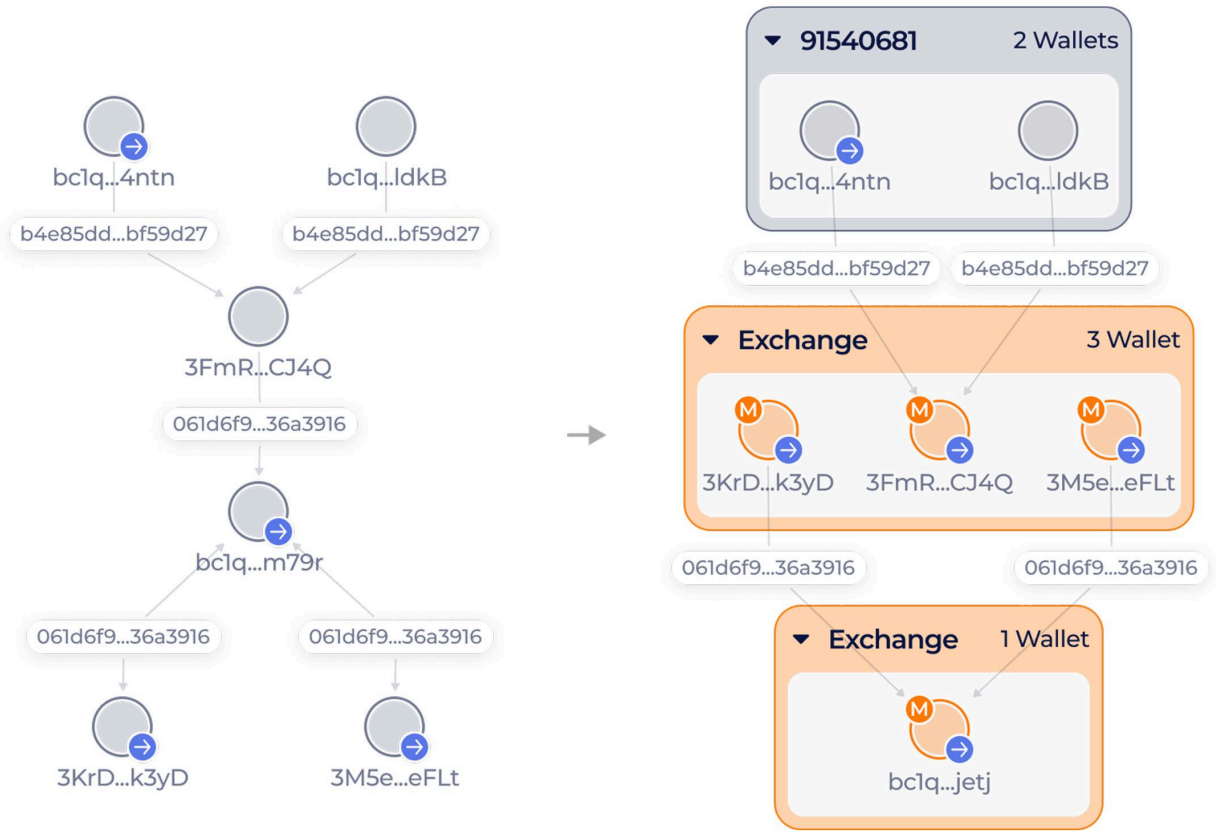
Prevent risks with Global Ledger

Time-based triggers and cluster analytics

To respond in time, you’ll need more than a case queue:

- Set up automatic triggers based on behavioural and time-based metrics, not just static rules.
- Aim for a 15-minute internal SLA for reviewing suspicious flows — just like incident response in cybersecurity. To support that, set up an alerting system that integrates with your team’s real channels like Slack, Jira, Telegram so that high-risk events are delivered instantly and can trigger action without delay.
- Consider using risk bursts: clusters of similar incidents in short timeframes that may point to coordinated laundering attempts.
- Use cluster-level analytics to identify behavioural patterns, transaction paths, and timing anomalies.

At Global Ledger, algorithms can surface hidden links between wallets and addresses by forming dynamic clusters, helping identify and associate them with specific entities, individuals, or events. Clustering methods are grounded in real data and enhanced through smart contract interactions and fund origin analysis that have proven effective in real-world investigations.



Review how your current setup handles cross-chain risk. We'll help fill the gaps.

Schedule a demo

Problem

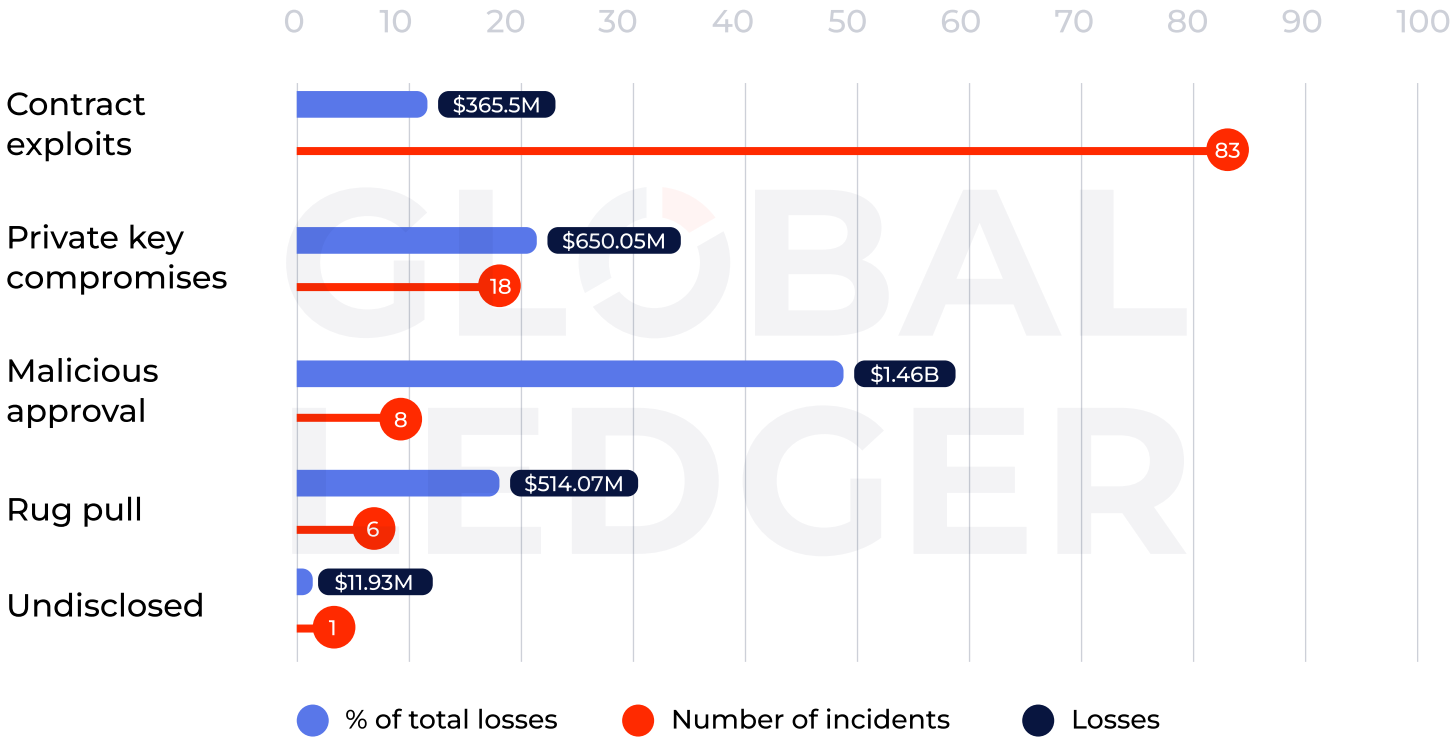
Malicious approvals caused just ~7% of cases but drove ~49% of total losses

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**[6] ($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).

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



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

What is at stake?

Misplaced focus puts your funds at risk

The data reveals a 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

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. A second person must review and confirm it, reducing the risk of error and abuse.

- Also, make sure **client and corporate funds are properly segregated**, i.e., stored in separate wallets, with different permissions and clear reconciliation procedures. It's a simple but powerful way to limit damage if something goes wrong.

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

Schedule a demo

Problem

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.

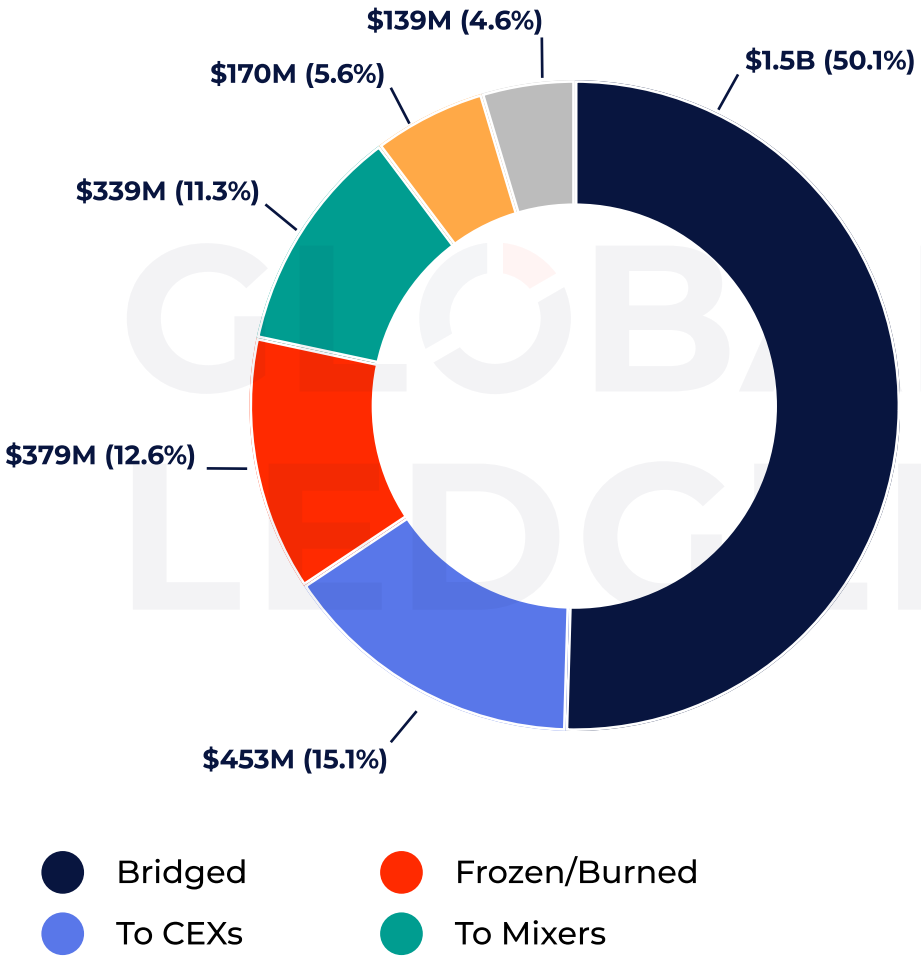
The functionality of cross-chain protocols (**bridges**) is heavily **leveraged** by illicit actors, making them a key tool for obfuscating stolen funds origin. In H1'25, **over $1.5 billion (50.1%)** of hacked assets were routed through them. This data shows a sharp difference compared to **$339M (11.3%)** 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.

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

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



What is at stake?

Attracting launderers = attracting oversight and risking reputation and trust

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 sophsticated 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.

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 a**ttractive tools for high-volume laundering,** leaving even well-intentioned protocols exposed to reputational and regulatory risks.

> 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

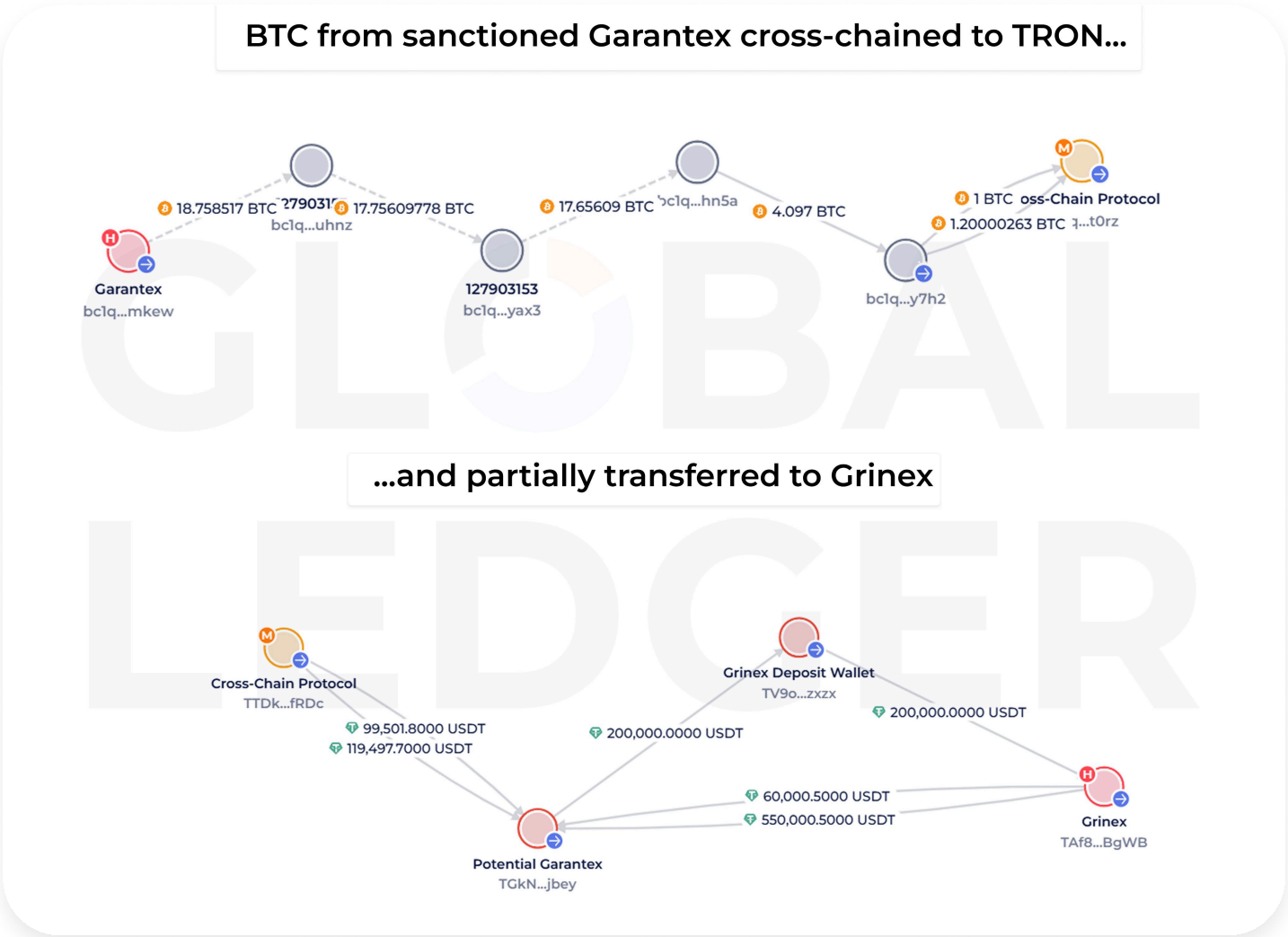
Prevent risks with Global Ledger

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.

- 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

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

Not knowing is no defence. When illicit exposure goes undetected, three things can follow:

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. Even the top CEX was disconnected from Clear Junction, Barclays, PaySafe. For smaller players, losing a single partner can mean losing the business.

Use our checklist to avoid costly blind spots.