GLOBAL LEDGER

2025 Q1 Crypto Hacks Report

Executive summary

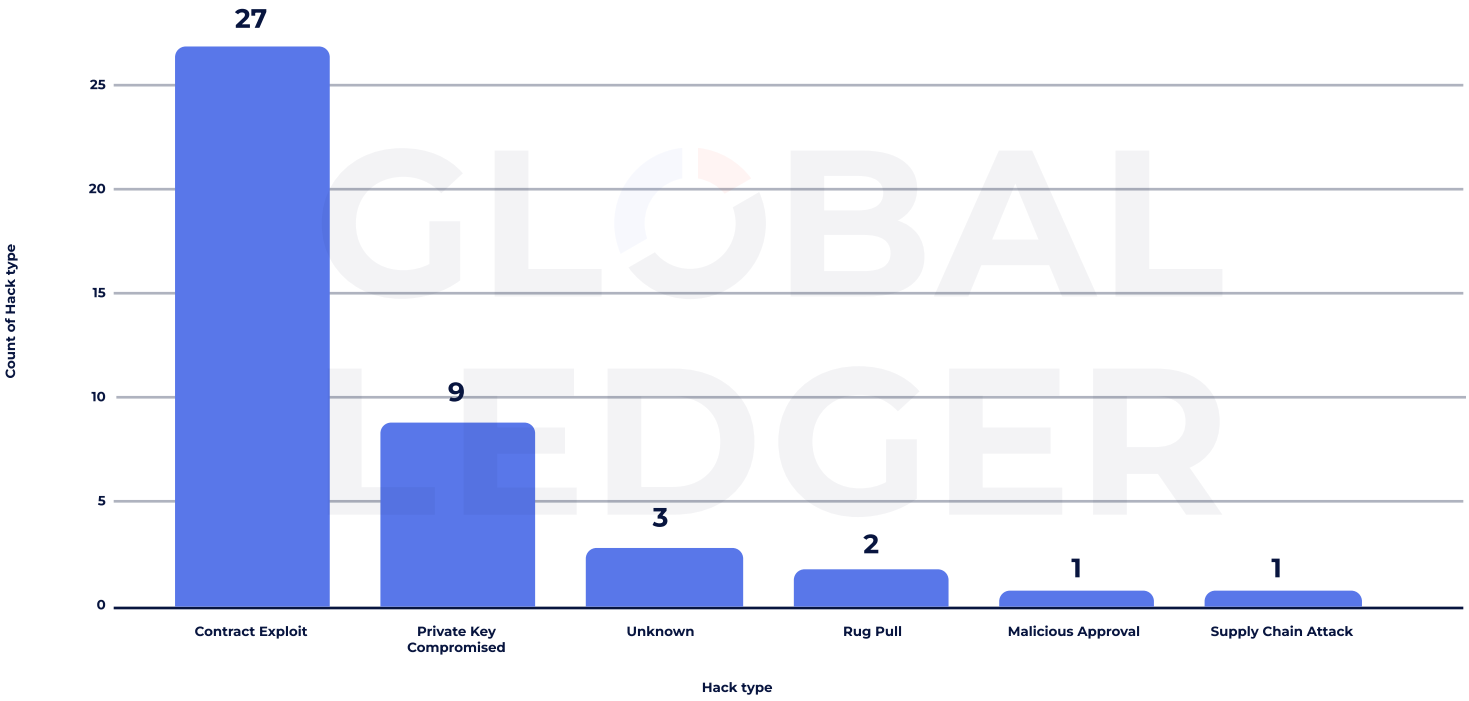
Q1 2025 marked one of the most devastating quarters in the history of crypto-related hacks, with stolen funds totalling over $1.84 billion across 43 separate incidents. While a single event — the Bybit exploit — accounted for the majority of the losses, the data reveals broader shifts in attacker behaviour, laundering patterns, and institutional vulnerabilities.

This report from Global Ledger dissects each breach by type, timing, laundering method, and target profile, offering a rare level of granularity into how crypto hacks unfold in real-time and where the industry remains most exposed.

Key Takeaways

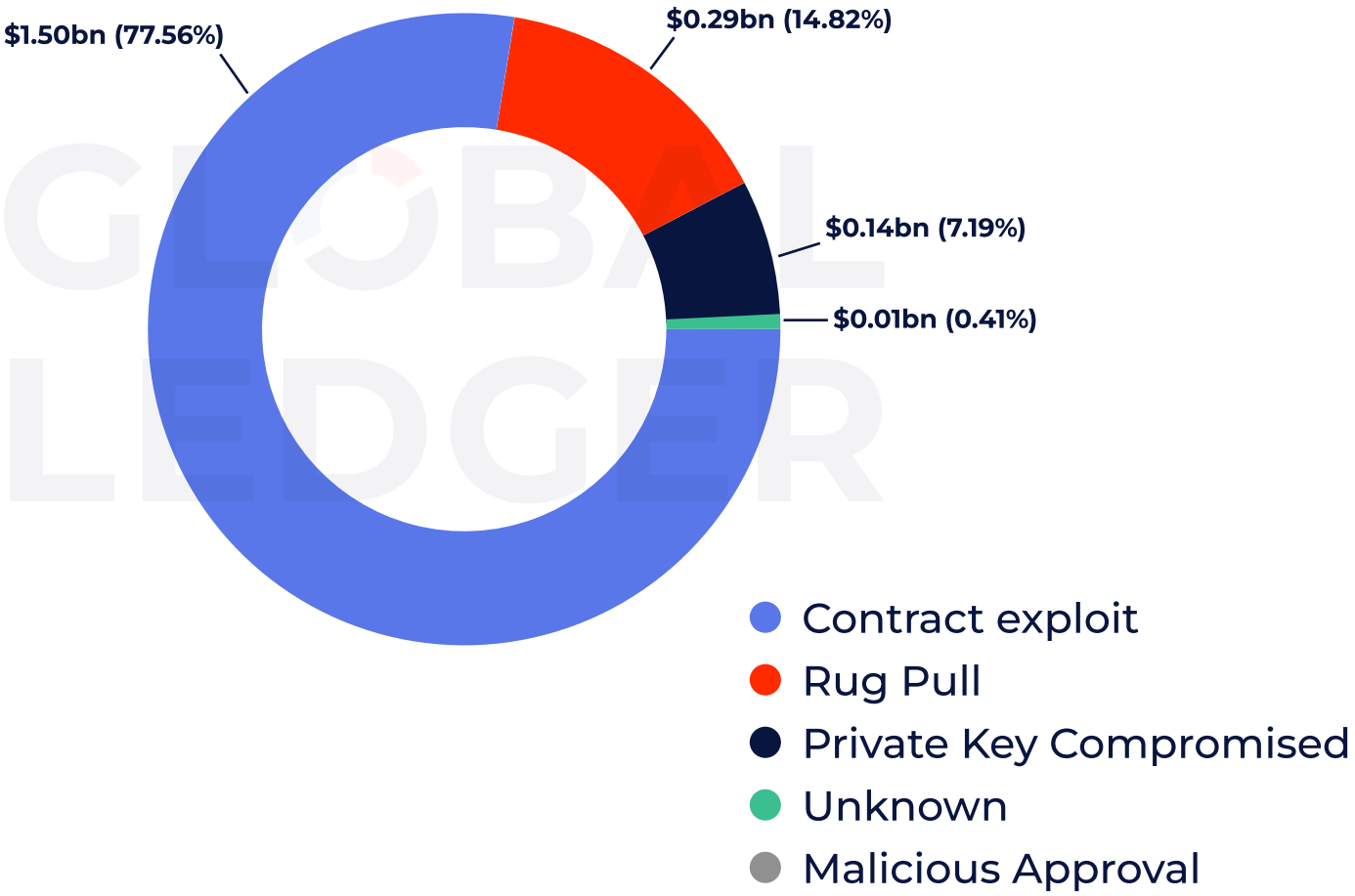
- $1.84B stolen across 43 hacks, making Q1 2025 one of the highest-loss quarters ever recorded.
- Contract Exploits remain the most common attack vector, accounting for 62.79% of all incidents (27 cases).
- Centralised exchanges were the hardest hit, responsible for 79.56% of all stolen funds (~$1.54B).
- North Korean-linked actors stole $1.44B, compared to just $0.45B by all other hacker groups combined.
- On average, 43.83 hours pass between an on-chain breach and public disclosure, while funds reach the target entity in under 68 hours.
- Unspent funds still total over $1.55B, underscoring ongoing recovery opportunities.
- Tornado Cash remains the top laundering method, used in over 53% of tracked laundering events, despite enforcement pressure.

Number of Incidents by Hack Type



Contract Exploits were by far the most common, making up **62.79%** of all attacks. **Private Key Compromises** followed with 9 incidents, while Rug Pulls and others were rare.

Total Value Stolen by Hack Type



Contract Exploits caused the greatest monetary damage, totalling **$1.50B (77.56%)**.
Rug Pulls, though infrequent, resulted in a high **$290M loss (14.82%)**.
Other vectors had a limited financial impact.

Takeaways:

In Q1 2025, Contract Exploits dominated both in frequency and total value stolen, reinforcing their position as the most persistent and lucrative attack vector in the crypto crime ecosystem:

- Contract Exploits accounted for 27 out of 43 total incidents (62.79%) and were responsible for a staggering $1.50 billion in stolen funds, 77.56% of the total value lost.
- Rug Pulls, while less frequent (2 incidents), resulted in $290 million stolen (14.82%), underscoring how damaging even a small number of trust-based schemes can be.
- Private Key Compromises were the second most common vector (9 incidents), but represented only $140 million in total losses (7.19%), indicating a lower average haul per attack.
- Attacks with Unknown methods, Malicious Approvals, and Supply Chain Attacks were rare and accounted for minor losses by comparison.

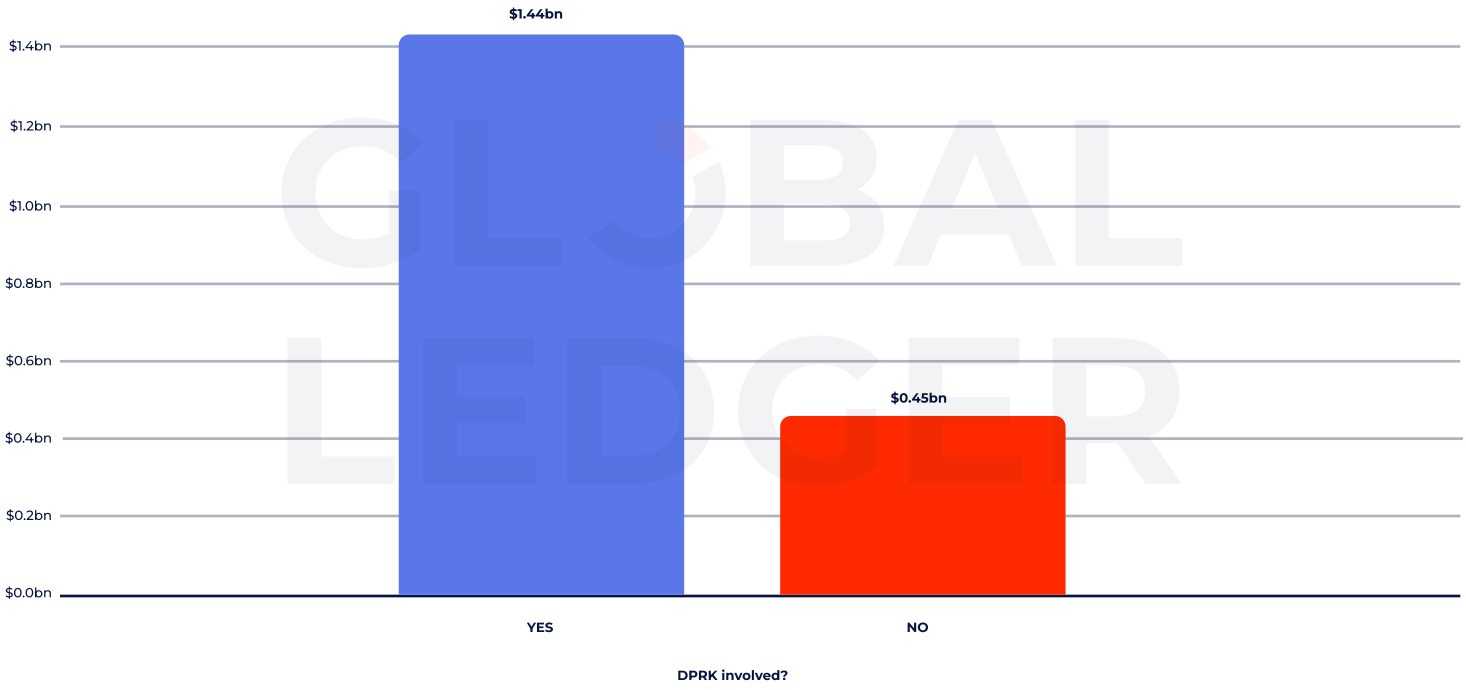
Insight:

This asymmetric relationship between incident count and financial impact shows that not all hacks are created equal. Smart contract vulnerabilities remain the highest-value risk, while insider-driven or social engineering attacks (like private key leaks) are more frequent but typically lower in yield.

Takeaways from the Breakdown of Hacked Entities by Total Value:

- Centralised Exchanges suffered the most severe financial damage, with $1.54 billion stolen, accounting for 79.56% of all losses in Q1 2025. This highlights how attractive CEXs remain as high-value, single-point-of-failure targets for sophisticated attackers.
- Tokens were the second-most affected by value, with $290 million stolen (14.86%) – likely driven by meme-token and low-liquidity project exploits.
- Payment platforms, DeFi platforms, and Lending protocols accounted for only a combined ~5% of total stolen funds, suggesting a lower concentration of value or better fragmentation/security across these verticals.
- Gaming/Metaverse, Personal Wallets, and NFT projects saw negligible losses in dollar terms, though they remain symbolically and reputationally sensitive targets, especially among retail users.

DPRK Involvement: Still the Most Dominant Threat Actor



- DPRK-linked hacks: $1.44B stolen
- Other actors: $0.45B stolen
- DPRK responsible for ~76% of all losses
- Fewer attacks, bigger targets

Key Takeaways:

- $1.44B in stolen funds were attributed to North Korean-linked attackers in Q1 2025 — nearly 76% of the total.
- By contrast, all other hacker groups combined were responsible for just $0.45B, despite representing a larger number of individual incidents.
- This highlights DPRK's outsized impact: fewer attacks, but on far higher-value targets, such as centralised exchanges and token infrastructure.
- The pattern reflects North Korea's state-sponsored precision in exploiting infrastructure weaknesses for large-scale financial gain.

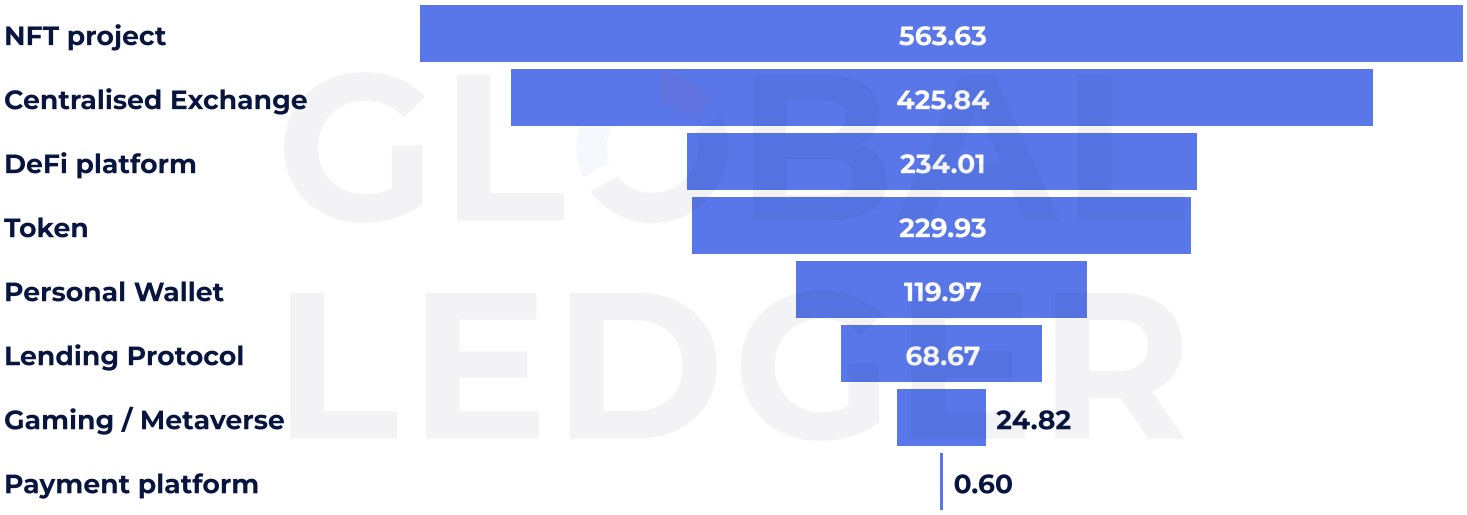
Mind the Gap: How Timing Shapes Hack Outcomes

Response & Movement Timeline (Hours, avg.)

Takeaways: Movement & Response Timelines

- On average, it takes 43.83 hours from the on-chain incident until the hack is publicly reported, whether by the project itself or a third-party investigator.
- Funds are typically moved from the hacker's wallet to the first identified entity (e.g. exchange, mixer, DeFi protocol) in 46.74 hours.
- From the initial on-chain breach to the first interaction with any entity, the average time is 67.57 hours.
- The longest lag is from public disclosure to entity interaction, averaging 78.55 hours, meaning funds often land before the incident is even made public.

First vs Last Entity Arrival



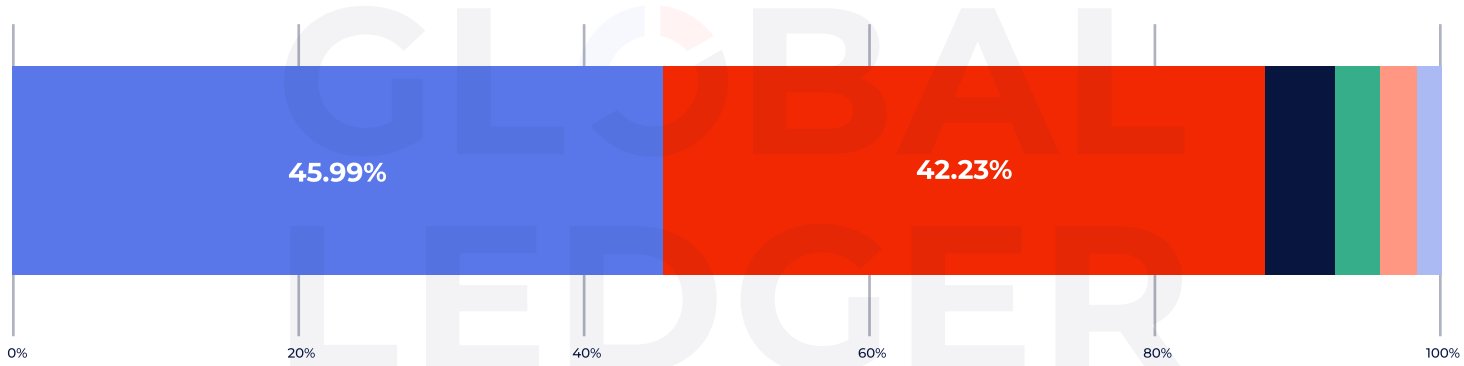
This metric reflects how attackers adjust laundering strategies depending on the nature of the hacked entity, with slower flows often indicating higher caution or obfuscation efforts.

Takeaways:

- NFT projects show the slowest fund movement, averaging 563.63 hours (~23.5 days) between the first and last known entities, possibly due to fragmented or delayed laundering routes.
- Centralised exchanges follow at 425.84 hours, suggesting prolonged transfer chains or attempts to delay detection.
- DeFi platforms and tokens land in the middle (~230 hours), often used as intermediate stops.
- Payment platforms saw the fastest movement, with funds reaching final destinations in just 0.6 hours, indicating either instant cashouts or direct swaps.
- Gaming/Metaverse projects also moved relatively quickly (24.82 hours), likely due to smaller sums and more straightforward laundering paths.

Where the Money Goes: Post-Hack Fund Flows

Distribution of Funds Post-Hack



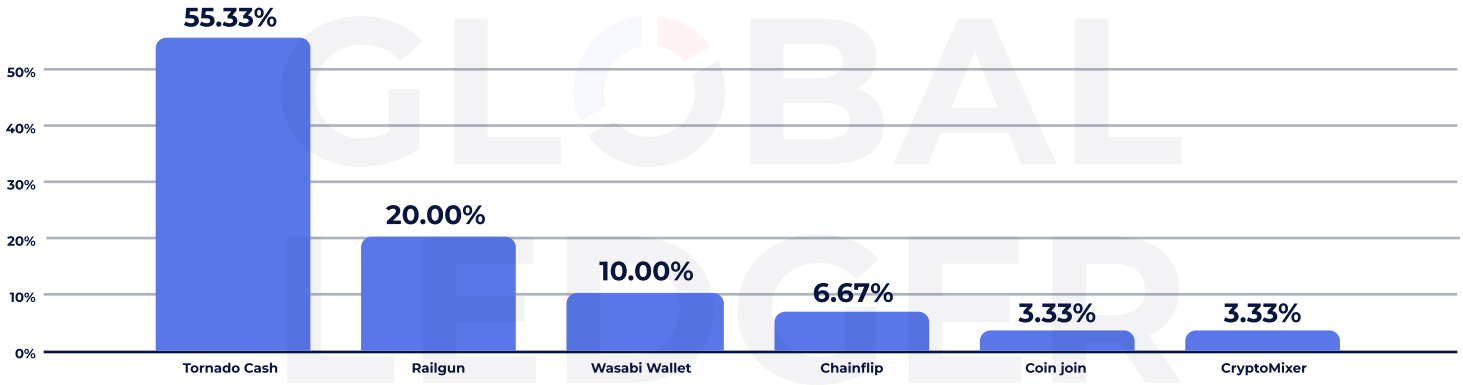
- **Unspent**
- **Cross-chained**
- **To exchanges**
- **To mixers/privacy protocols**
- **To DeFies**
- **Frozen**

Takeaways:

- Nearly 46% of stolen funds remain unspent, offering continued opportunities for tracking and recovery.
- 42.23% of funds were cross-chained, reflecting an ongoing shift toward using interoperability to avoid detection.
- Only a small share of funds flowed to centralised exchanges, DeFi protocols, or mixers, showing attackers are increasingly diversifying their laundering strategies.
- A tiny portion has been frozen, underscoring the challenge of real-time response despite growing compliance infrastructure.

The Preferred Escape Routes: Laundering Tools of Choice

Laundering Methods by Frequency of Use



Even under regulatory pressure and sanctions, privacy protocols remain key to post-hack laundering. The data reveals that **Tornado Cash** is still the most frequently used tool for obfuscating stolen crypto flows, despite being sanctioned in the U.S. and actively scrutinised globally.

Takeaways:

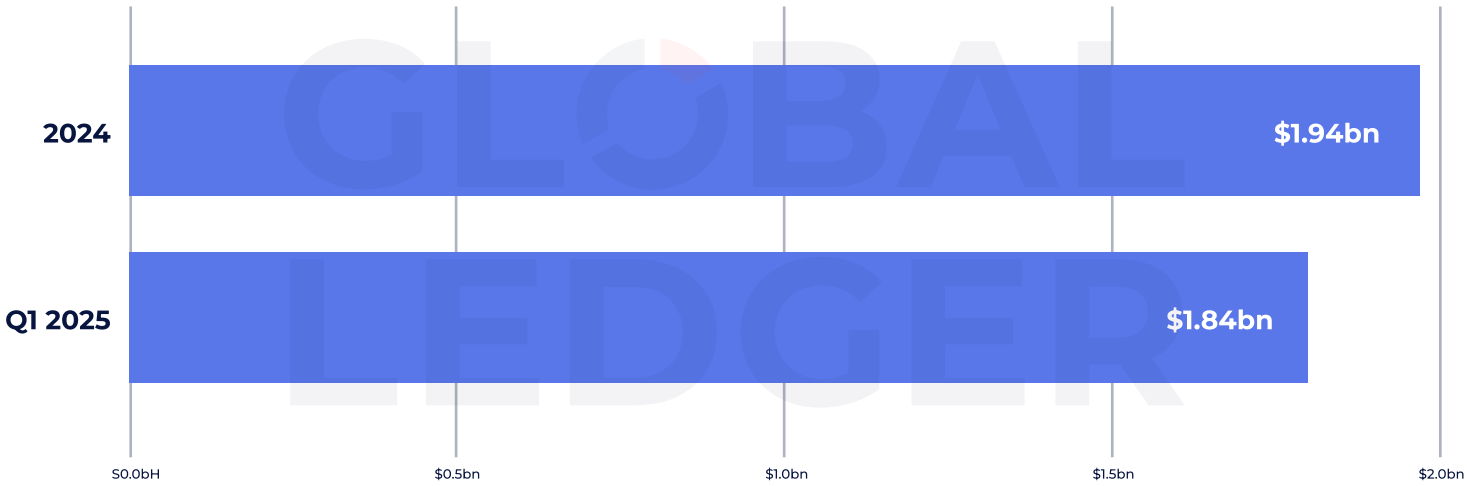
- **Tornado Cash** was used in **53.33%** of laundering cases, confirming it remains the **default solution** for attackers seeking anonymity. Its continued dominance suggests that **protocol-level censorship and regulatory sanctions** have n**ot meaningfully deterred** malicious use. Even after being sanctioned by OFAC in 2022, Tornado Cash remained in use. And following a **2024 U.S. court ruling** that overturned the sanctions on constitutional grounds, its usage has surged back, underscoring the challenges of regulating immutable smart contracts.

  Railgun (20%) and **Wasabi Wallet (10%)** are gaining traction — likely as fallback options or complementary obfuscation layers.
- **Chainflip, CoinJoin, and CryptoMixer**, while less commonly used (under 7% combined), still play a role in diversifying laundering flows.

Tornado Cash's sustained presence highlights the tension between decentralised infrastructure and traditional enforcement, making it one of the most important platforms to watch in ongoing AML strategy discussions.

A Year's Worth of Hacks in Just One Quarter

Value of Stolen Assets by Year: 2024 vs Q1 2025



2024: $1.94B lost over the year
Q1 2025: $1.84B lost in 3 months

Takeaways:

- Over $1.84 billion was stolen in Q1 2025 alone, almost equalling the $1.94 billion total for all of 2024.
- This means the crypto ecosystem lost almost 95% of 2024's total in just three months, signalling a sharp escalation in attack volume and sophistication.
- The near parity suggests a trend reversal, following slight declines observed throughout late 2023.
- High-profile breaches (e.g., Bybit, LIBRA, Infini) played a major role in driving Q1 numbers up.
- If this trajectory continues, 2025 could become the most financially damaging year for crypto hacks on record.

Final Conclusion: An Era of Precision and Pressure

The data from Q1 2025 signals a sobering shift: crypto hacks are no longer just frequent – they are faster, more targeted, and strategically laundered.

Attackers are exploiting not only smart contracts but also the timing gaps between breach, detection, and disclosure, moving assets across chains in under 48 hours – often before anyone sounds the alarm. The fact that nearly half of the stolen funds remain unspent suggests that while response infrastructure is improving, real-time threat mitigation is still lagging.

Meanwhile, decentralised laundering protocols like Tornado Cash continue to thrive, even amid sanctions and legal battles – underscoring the limitations of enforcement in a permissionless ecosystem.

Crucially, the data also shows that not all hacks are created equal. A small number of incidents (primarily targeting centralised exchanges and meme-token projects) are responsible for the majority of financial damage, while others, though more numerous, remain smaller in scope.

If Q1 is any indication, 2025 won't just be a high-loss year – it will be a stress test for how fast the crypto industry can adapt, react, and defend.

Implication for the industry

Hackers are no longer waiting.
They exploit a vulnerability, move funds within hours, and obfuscate flows before most teams even issue a statement.

In Q1 2025:

- Funds reached an entity in under 68 hours, on average
- Movement from hacker wallets started within 47 hours
- Public reporting lagged behind at almost 79 hours

This time gap matters. It creates a window in which bad actors can operate with relative freedom – routing stolen assets through mixers, cross-chain protocols, or exchanges before anyone reacts.

That's why responsiveness in blockchain tracing and risk labelling is no longer a bonus – it's essential.
The faster we detect, the more effectively we disrupt laundering flows and protect downstream entities.

The list of all hacks that have been analysed

Hacked Entity	Entity Type	Total Loss, USD	Date
DMM Bitcoin	Centralised Exchange	$1 400 000 000,00	21.02.2025
LIBRA Meme Token	Token	$286 000 000,00	16.02.2025
Infini Exploit	Payment platform	$50 000 000,00	24.02.2025
Phemex Exploit	Centralised Exchange	$37 000 000,00	23.01.2025
FortuneWheel Exploit	Gaming / Metaverse	$21 000 000,00	10.01.2025
GMX_IO & MIM_Spell contracts hack	DeFi platform	$13 000 000,00	25.03.2025
Ionic Exploit	Lending Protocol	$12 300 000,00	04.02.2025
DogWifT	Software platform	$10 000 000,00	28.01.2025
zkLend Hack	DeFi platform	$9 500 000,00	12.02.2025
Zoth	DeFi platform	$8 290 000,00	21.03.2025
NoOnes	Centralised Exchange	$7 200 000,00	01.01.2025
Wemix	Gaming / Metaverse	$6 220 000,00	28.02.2025
1inch	DeFi platform	$5 000 000,00	05.03.2025
AdsPower	Browser extension	$4 700 000,00	24.01.2025
Suji Yan Phishing Exploit	Personal Wallet	$4 000 000,00	27.02.2025
Moby Trade Exploit	DeFi platform	$2 500 000,00	08.01.2025
TrumpDailyPosts	Twitter account	$1 250 000,00	21.01.2025
Orange Finance Hack	DeFi platform	$840 000,00	08.01.2025
IPC	Token	$590 000,00	07.01.2025
Fake LAYER Token	Token	$465 000,00	21.01.2025
Cardex	Gaming / Metaverse	$400 000,00	18.02.2025
chickengenius.eth phishing exploit	Personal Wallet	$394 000,00	29.01.2025

The list of all hacks that have been analysed

Hacked Entity	Entity Type	Total Loss, USD	Date
The Idols NFT exploit	NFT project	$340 000,00	14.01.2025
Voltage Finance	Crypto Wallet	$320 000,00	18.03.2025
Zoth	DeFi platform	$285 000,00	06.03.2025
UniLend Exploit	DeFi platform	$197 600,00	13.01.2025
Four.Meme exploit	DeFi platform	$183 000,00	11.02.2025
Cashverse	DeFi platform	$107 900,00	08.02.2025
ODOS	DeFi platform	$100 000,00	24.01.2025
Hegic(old contract)	DeFi platform	$94 000,00	01.03.2025
StepHeroNFTs Exploit	NFT project	$90 000,00	21.02.2025
Berally	DeFi platform	$90 000,00	14.03.2025
AST Token Hack	Token	$64 700,00	21.01.2025
LAURA token exploit	Token	$48 000,00	08.01.2025
Sorra	DeFi platform	$43 000,00	04.01.2025
BankX	DeFi platform	$43 000,00	07.02.2025
Alien Base	DeFi platform	$38 000,00	10.01.2025
OpenOcean exploit	DeFi platform	$22 000,00	11.02.2025
Mosca Hack	Token	$19 500,00	08.01.2025
BIGO token exploit	Token	$18 000,00	14.01.2025
HORS	Token	$10 300,00	08.01.2025
BUIDL	Token	$8 000,00	12.01.2025
Peapods Exploit	DeFi platform	$3 500,00	08.02.2025