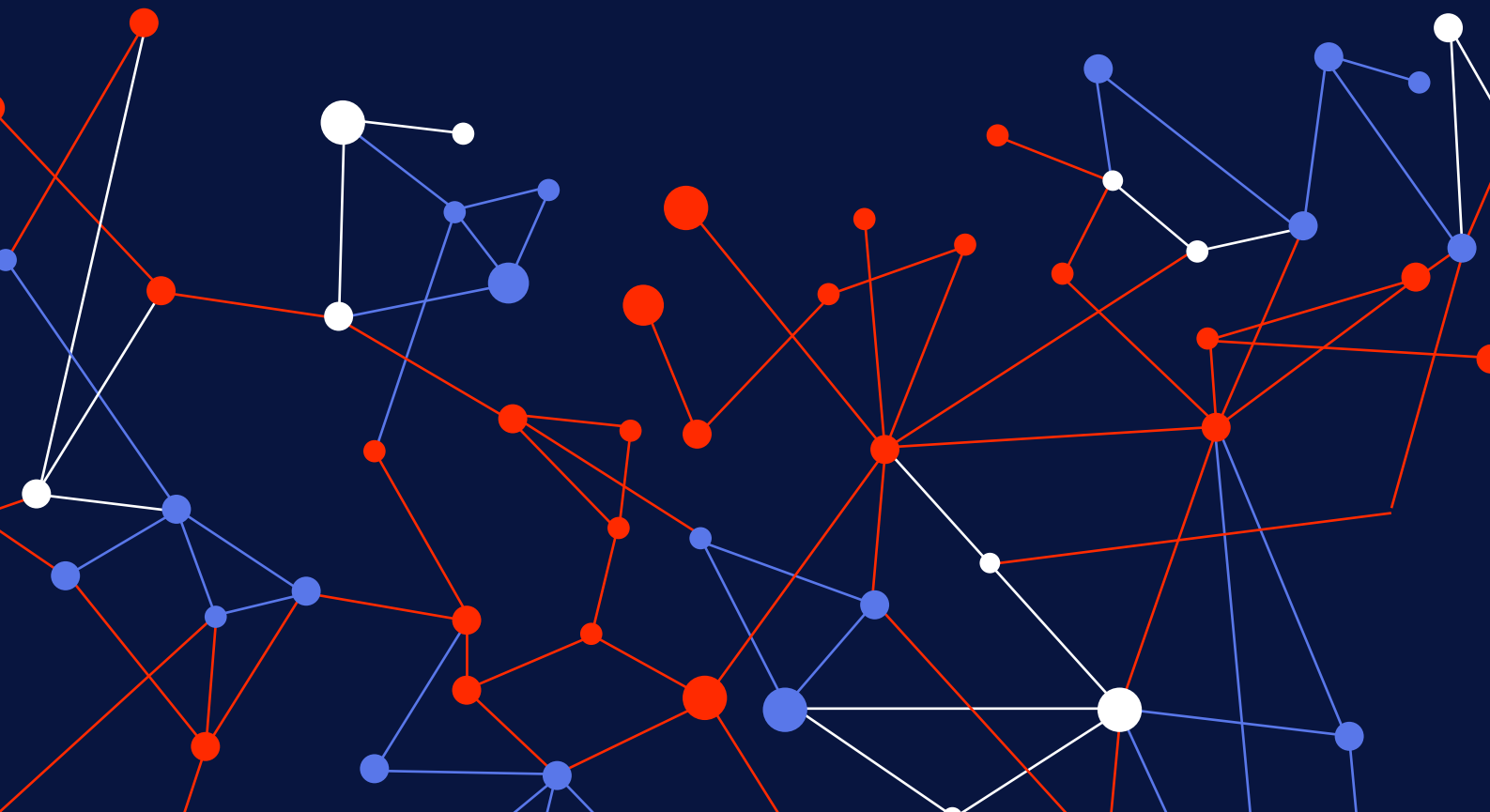
GLOBAL LEDGER

All Bridge Hacks, $2.9B Lost

Lessons from 2021–Q3 2025 Hacks



Key Takeaways

1

34

Cross-chain protocol hacks in 2021–Q3 2025

2

~$2.9B

Stolen in 4.5 years

3

85% of cases

Funds transferred before public disclosure

4

~33.5 min

The fastest laundering cycle

5

91% of incidents

Funds movement within the first 24 hours

6

~22 hrs

Average public reporting lag after a hack

7

87% of hacks

Involved mixers or other privacy services

8

~1.5% of funds

Recovered

Executive summary

Between 2021 and Q3 2025, 34 cross-chain bridge and interoperability protocol incidents accounted for **nearly $2.9 billion** in stolen assets. This analysis reveals how quickly funds were laundered, what tactics were used, how victims reacted, and the risks of the response lag.

In 85% of cases, funds were moved before the incident was publicly disclosed. First transfers occurred on average within **2 hours and 15 minutes**, while public reporting **lagged by ~22 hours**. In 91% of incidents, movement happened within the first 24 hours, and in one case, the full laundering cycle, from the incident to the last endpoint, took just **~33.5 minutes**.

The report also traces how stolen assets were routed through **mixers**, **bridges**, and **CEXs** and highlights the heavy reliance on **Tornado Cash**, involved in 96% of mixer-related cases. With recovery rates of ~1.5%, and flows split across multiple endpoints, traditional post-incident strategies are proving ineffective.

Methodology

This report is based on a structured analysis of **34 confirmed cross-chain bridge and interoperability protocol hacks** that took place between 2021 and the first half of 2025. The research draws on multiple data sources to ensure both accuracy and breadth.

Data sources

The study's primary foundation is **on-chain tracing** of addresses associated with bridge exploits. These were cross-referenced with **open-source reporting**, including official disclosures by affected projects, media coverage, and blockchain security research. External datasets from industry analytics providers were also consulted to verify transaction flows, laundering patterns, and attribution claims.

Scope

For the purposes of this research, we define Virtual Asset Service Providers (VASPs) and mixers/privacy services as **endpoints** — the points at which illicit funds are first introduced into services that significantly reduce traceability. When the last funds from a hacking incident reach a VASP or mixer/privacy service, it is considered the final endpoint, beyond which on-chain tracing and wallet attribution become increasingly unreliable or, in some cases, practically impossible due to obfuscation techniques, jurisdictional opacity, or custodial aggregation.

This classification helps establish a consistent benchmark for evaluating laundering speed and behaviour across cases. While technically further tracing may still occur, attribution beyond these endpoints carries a high risk of error or misinterpretation and is excluded from the scope of this analysis.

Limitations

As with all crypto crime research, several limitations apply. Not all hacks are publicly reported, and some remain undisclosed by affected projects. Attribution of attacks to specific actors, such as state-sponsored groups, is based on the best available evidence but cannot always be independently verified. Laundering flows may extend beyond the endpoints included here, but attribution beyond those points carries significant uncertainty.

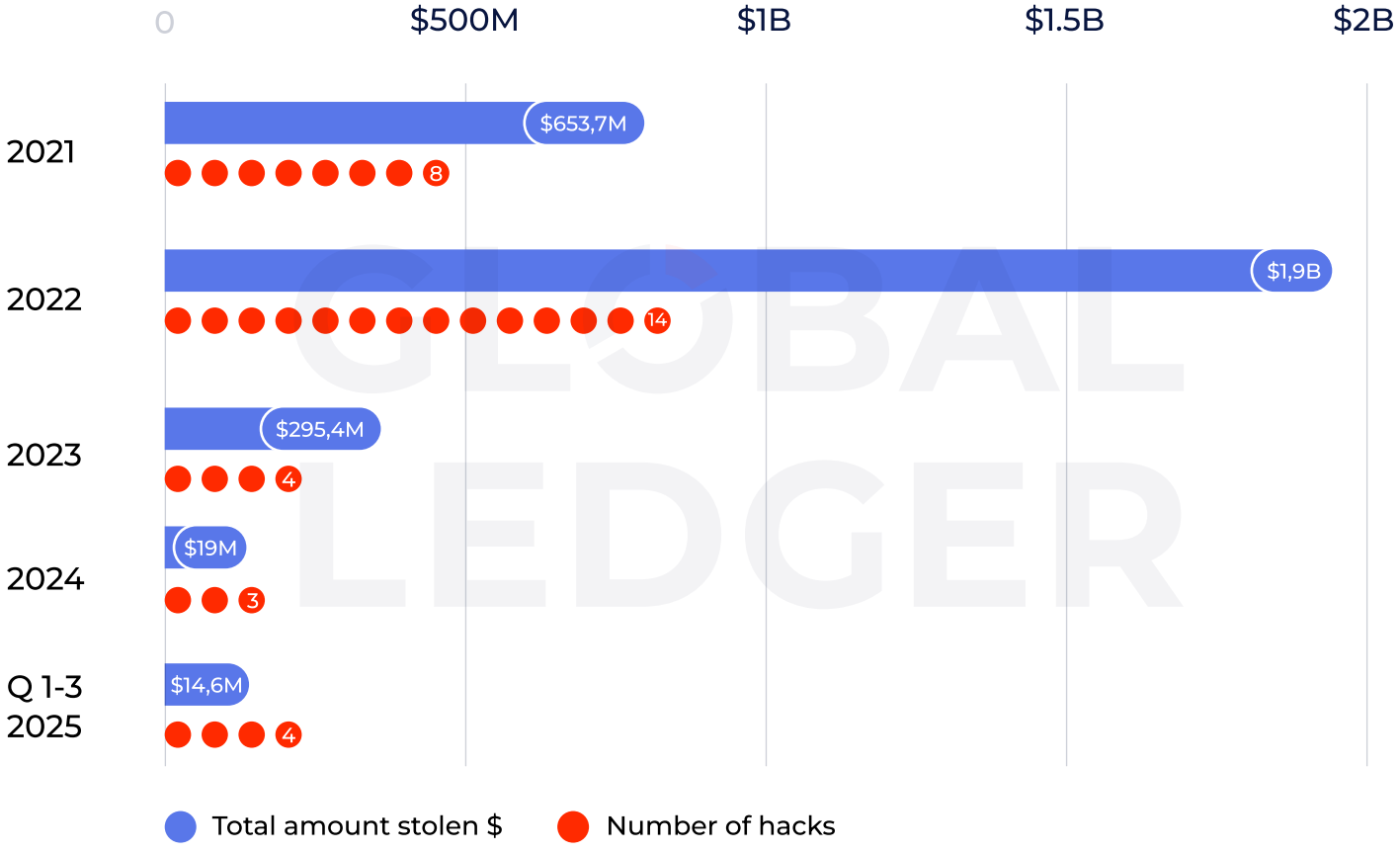
~2.9B stolen in bridge hacks in 2021–Q3 2025, with 2022 accounting for 66% of total losses

Between 2021 and Q3 2025, 34 cross-chain bridge and interoperability protocol incidents led to nearly **$2.9 billion** in stolen assets. Just ~ $42,8 million, or ~1.5% of total, was recovered (except the Poly Network case where hackers returned all stolen funds, except for the ~$33 million frozen by Tether.

The year **2022** alone accounted for 14 of those incidents and approximately **66% of the total losses** — around $1.9 billion. High-profile hacks like Ronin ($625 million), BNB Chain ($574.24 million), and Wormhole ($326 million) bridge hacks contributed significantly to the year's record-breaking losses.

This spike was driven by rapid DeFi and cross-chain growth, which concentrated liquidity in protocols that lacked rigorous audits and had complex architectures with multiple points of failure. Weaknesses in key management also contributed to losses, as in the case of the Ronin hack, where five out of nine multisig validators' private keys were compromised through a targeted social engineering attack.

~$2.9B Stolen in 34 Bridge Hacks in 2021–Q3 2025



1 minute 13 seconds — the record for funds movement after the exploit

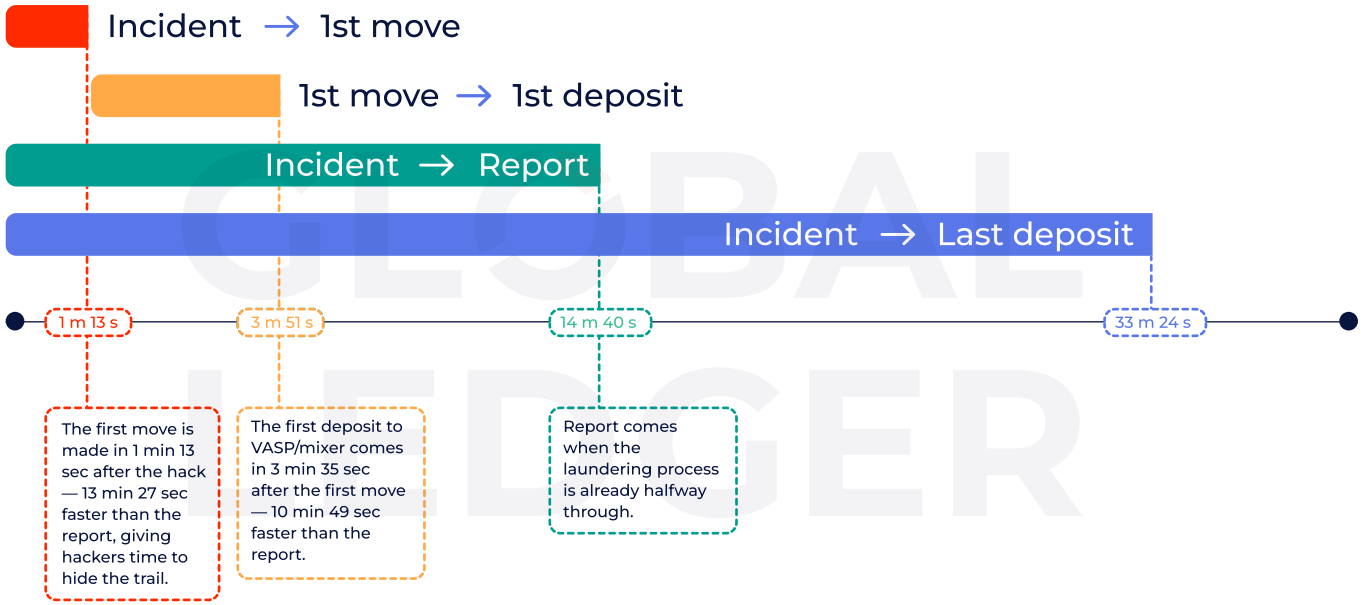
One of the defining characteristics of bridge hacks between 2021 and 2025 is the speed with which stolen funds are laundered. Hackers treat the post-exploit environment as a race to stay ahead of disclosure and move assets into endpoints before interventions can occur.

In 91.2% of incidents (31/34), funds began moving within the first 24 hours. The record for the immediate first movement[1] was just **1 minute 13 seconds** after the initial exploit transaction.[2]

Only two cases showed any delay longer than 24 hours, and in one instance (pNetwork pBTC-BSC Bridge), the funds were never moved: out of 277 BTC stolen, just 0.276 BTC — less than 0.01% of the total — was sent back to the victim shortly after the hack, likely by mistake.

Once laundering began, progression to endpoints was rapid. The fastest partial deposit into a mixer or VASP took just **3 minutes 51 seconds**, while the fastest cycle from hack to all funds at endpoints was finished in **33 minutes 24 seconds**. A separate benchmark, excluding the initial hack transaction, saw the full amount reach endpoints in 17 minutes 12 seconds.

In the fastest bridge hacks, funds moved 12x faster than incident was reported



1 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.

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

In 85.3% of incidents, assets moved before disclosure

There is a consistent gap between the fund movement and the timing of public disclosure. In 82.35% of incidents (28/34), projects publicly acknowledged the hack within 24 hours. For most attackers, this gap was more than enough. In **85.3%** of all incidents (29/34), stolen assets were on the **move before** the public knew what had happened. In **14.7% of hacks** (5/34), attackers managed to **move all stolen assets to endpoints before** the breach was **disclosed**.

On average, there is a ~22-hour lag between the initial fund movement and the public disclosure

The average time to first movement was **2 hours 15 minutes 10 seconds**, while it took, on average, **24 hours 44 minutes 32 seconds** for an incident to be disclosed.

(Except for the zkSwap incident who haven't reported the hack themselves as of the time of writing, and the only report was 15 days after the hack — the time is down to **14 hours 27 minutes 51 seconds**).

The average laundering cycle is 18.8 days

On average, stolen funds reached the endpoint in 45.4 days. However, this figure is skewed by two anomalies: pNetwork GALA Bridge, where funds lingered for 359.8 days, and Multichain v3, where laundering extended over 262.5 days. Excluding those, the **average cycle** fell to **18.8 days**. Once the first endpoint was reached, the rest of the funds typically followed quickly, on average, within four additional days.

In 27.3% (6/22) of incidents, funds reached endpoints within a day. For the rest of incidents, it took more time:

- 18.2% (4/22) — within a window of 1 to 7 days.
- 27.3% (6/22)[3] — between 1 week and 1 month.
- 27.3% (6/22) — more than a month.

On average, laundering begins ~22 hr before public disclosure

3 Considering only incidents where data is available and funds were moved to endpoints.

In ~87% of hacks, mixers or other privacy services were used

45.5% (15/33) of the hacks saw the first transfers go **directly into mixers or VASPs**, the first endpoints[4] where traceability sharply drops. This left virtually no opportunity for freezing or intervention.

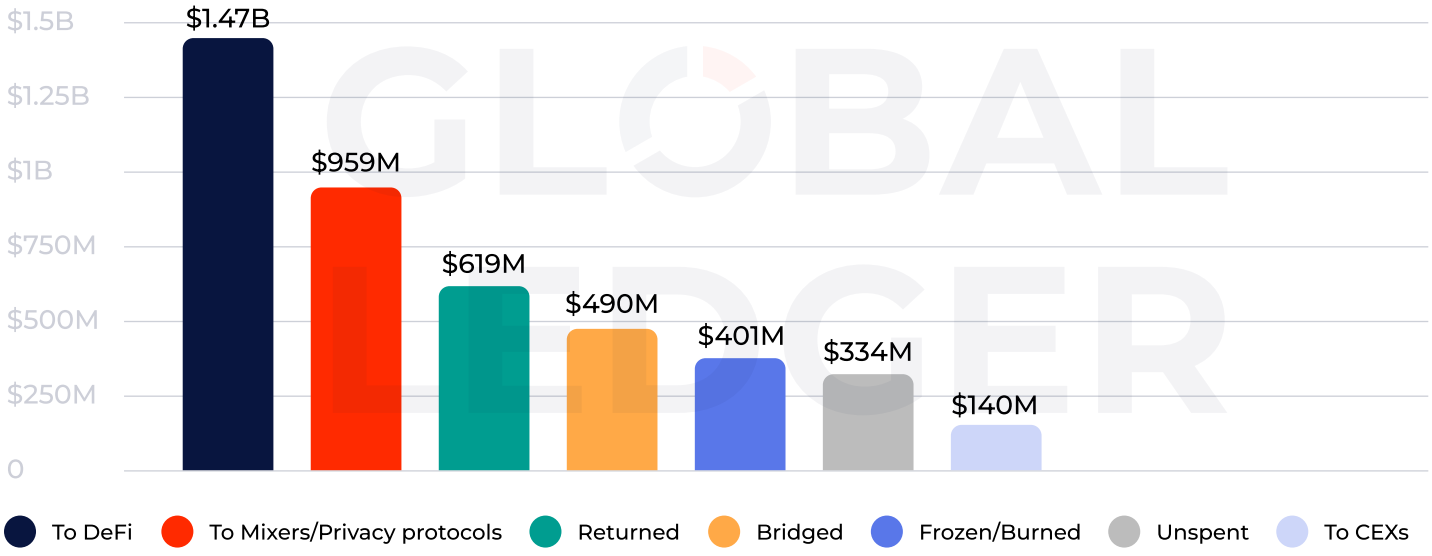
Overall, **87.1%** of incidents (27/33) involved the use of **mixers or other privacy services**. Of those, **96.3%** (26/27) relied on **Tornado Cash**, making it the dominant laundering infrastructure of the bridge hack era. Only a single case used an alternative: zkWrapper.io, a privacy dApp on the Tron blockchain.

Over 51% of funds stolen in bridge hacks went to DeFi platforms

The largest share of stolen assets — about **$1.48 billion** — was funneled to DeFi platforms. Approximately **$959 million** was routed through mixers and other privacy-focused services, and **$490 million** was bridged. **$140 million** ended up on **CEXs**, likely as the final step before fiat conversion.

Roughly **$619 million** was returned. Around **$401 million** was frozen or burned, making it inaccessible. Over **$334 million** remains unspent, as of the time of writing, sitting in wallets linked to the attackers.

More than 50% of funds stolen in bridge hacks went to DeFi platforms



4 For this section, pNetwork pBTC-BSC Bridge exploit is excluded, as the hacker never moved funds since 19.09.2021 except for a single minor transaction just 42 minutes after the hack (0.276 BTC out of 277 BTC total stolen).

No hack funneled all its stolen funds to endpoints in a single move. Instead, attackers often **split flows across multiple wallets and time intervals**, sometimes rotating through DeFi protocols or cross-chain services to blur attribution before depositing into mixers or VASPs. This reflects an intentional strategy: rapid enough to stay ahead of disclosure, but staggered enough to complicate tracing.

Interestingly, laundering **duration showed almost no correlation with hack size**. Smaller incidents were sometimes drawn out for months, while billion-dollar exploits could be laundered within hours. This indicates that behavior depends less on absolute sums and more on available liquidity and the degree of public attention surrounding each case.

Contract exploits account for $1.84B (~64%) of losses

Most losses were caused by **contract exploits**, which accounted for **$1.84 billion** (63.72%), followed by **private-key compromises** with **$1.04 billion** (36.13%). Other vectors (malicious approvals, flash loans, access-control flaws, BPG hijacking) together made up only $4.2 million (0.15%).

These two attack vectors dominate across the broader ecosystem: In 2024, private key compromises became the top source of losses, with $930 million (48.03%), while contract exploits caused only $369.8 million (19.1%). In H1 2025, contract exploits were the most frequent (69.75% of cases) but accounted for just $365.5 million (12.15%) in losses. Meanwhile, malicious approvals, though less common (6.72%), caused the largest financial losses — $1.46 billion (48.51%). Private key compromises remained significant, contributing $650.05 million (21.61%).

~95% of incidents targeted EVM-compatible chains

Because the majority of value was concentrated in smart contracts, the attack surface tended to be the contract logic itself. This technical reality helps explain why **EVM-compatible chains dominated** the incident list: Ethereum (25 incidents), Binance Smart Chain (19), and Polygon (4) together account for 56[5] incidents (94.9%), while Bitcoin saw only one.

~95% of bridge hacks targeted EVM-compatible chains

5 These don't add up to 34 as there are multiple incidents where assets are drained from several chains simultaneously

Several factors plausibly drive a concentration of **94.9% of incidents** on EVM-compatible chains. They include the inherent complexity of smart contracts, which introduces more code and compatibility-related vulnerabilities compared to chains like Bitcoin, and the high number of cross-chain bridges, particularly those supporting L1–L2 transfers within the Ethereum ecosystem. These dynamics have resulted in large amounts of total value locked (TVL) within bridge protocols, creating attractive targets for exploitation. Additionally, the broader availability of hacker toolkits and a higher level of attacker expertise in Solidity may further contribute to this trend, though these factors are themselves likely influenced by the same underlying dynamics.

Conclusion: The cost of delayed response

Bridge hacks are defined by how quickly funds disappear. In 85% of incidents, assets were already moving before the breach was publicly disclosed. In the fastest case, the laundering cycle from exploit to endpoints took just **33 minutes**.

On average, attackers took only **2.25 hours** to begin moving stolen funds, while public disclosure lagged behind by more than **22 hours**. This timing gap remains a critical weakness: it gives laundering operations nearly a full-day head start, often enough to make freezing efforts ineffective.

With nearly 87% of cases involving mixers or privacy services, most notably **Tornado Cash**, and many flows split across wallets, chains, and protocols, tracing becomes increasingly complex the longer the delay.