Immunefi

CRYPTO LOSSES IN Q1 2025

PREPARED BY IMMUNEFI

Crypto Losses in Q1 2025

PREPARED BY IMMUNEFI

The team at Immunefi, the leading onchain crowdsourced security platform which protects over $190 billion in user funds, has assessed the volume of crypto funds lost by the community due to hacks and scams in Q1 2025.

OVERVIEW

As of March 2025, nearly **$100 billion** in capital was locked across Web3 protocols. That capital represents an unparalleled and attractive opportunity for blackhat hackers.

We have reviewed all instances in Q1 2025 where blackhat hackers exploited various crypto protocols. We have located 40 such instances, including successful and semi-successful hacking attempts and alleged fraud*.

Q1 2025 marks the worst quarter for hacks in the history of the crypto ecosystem. In total, we have seen a loss of **$1,635,933,800** across the ecosystem in Q1 2025. The majority of the funds were lost to hacks. Most of that sum was lost by two specific CeFi crypto exchanges: **Bybit** suffered an attack that resulted in **$1.46 billion** in losses, and **Phemex** incurred a loss of **$69.1 million**.

The total number of losses in Q1 2025 represents an **4.7x increase** compared to Q1 2024, when hackers and fraudsters stole **$348,251,217.**

Crypto Losses in Q1 2025

KEY TAKEAWAYS IN Q1 2025

- The 2 major exploits of the quarter totaled **$1.52 billion** alone, accounting for **94%** of all losses in Q1 2025.
- In Q1 2025, hacks continued to be the main cause of losses.
- CeFi became the primary target of successful exploits, comprising **94%** of cases, while DeFi accounts for **6%** of total losses.
- The two most targeted chains in Q1 2025 were **BNB Chain and Ethereum**. BNB Chain suffered the most individual attacks with 19 incidents, followed by Ethereum with 15 incidents, and Base with 3 incidents.
- In total, **$6,500,000** has been recovered from stolen funds in **2** specific situations. This number makes up **0.4%** of the total losses in Q1 2025.

KEY INSIGHTS IN Q1 2025

- Q1 2025 is marked by a considerable increase in the total number of losses, up by 4.7x compared to Q1 2024, amounting to **$348,251,217.**
- Overall, **February** witnessed the highest loss in Q1 2025, primarily due to the Bybit hack.
- The number of attacks decreased by **36%** from 63 in Q1 2024 to 40 in Q1 2025.
- In Q1 2025, BNB Chain surpassed Ethereum and became the most targeted chain compared to the previous period.
- In Q1 2025, funds recovery has proven less effective than in the previous period. To date, only **0.4%** of stolen funds have been recovered, compared to the **21.2%** recovered in Q1 2024.

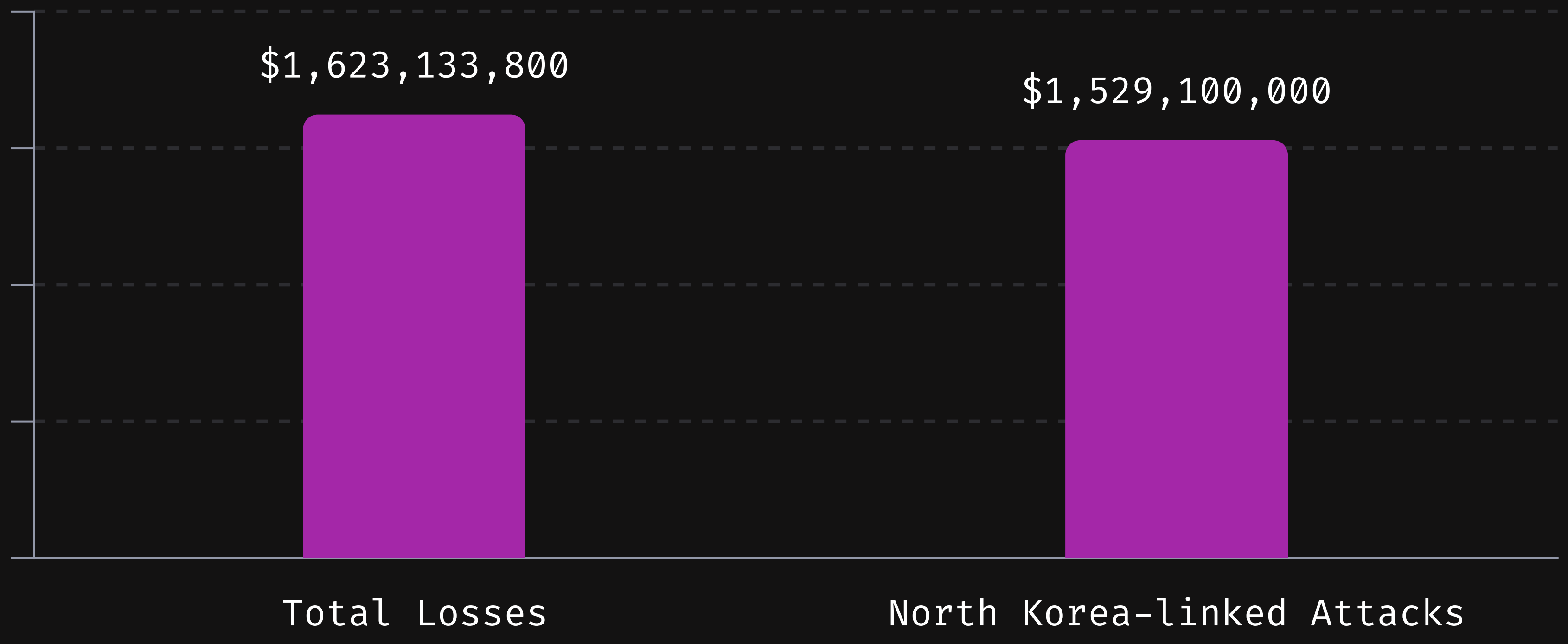
Top 10 Losses in Q1 2025 *

Bybit	$1,460,000,000
Phemex	$69,100,000
Infini	$49,500,000
MIM Spell	$12,800,000
zkLend	$9,500,000
Zoth	$8,850,000
Ionic Money	$8,600,000
Wemix	$6,000,000
1inch	$5,000,000
Moby Trade	$2,500,000

North Korean Hackers

IN FOCUS

- In Q1 2025, the North Korean Lazarus Group is suspected to be behind two major crypto attacks, causing **94% of total losses**. They hacked Bybit and Phemex, stealing a total of **$1.52 billion**. Industry investigations found a direct link between the two attacks by analyzing test transactions, connected wallets, and the subsequent movement of funds.
- These incidents highlight once again the growing trend of state-backed hackers targeting centralized exchanges and project infrastructure to carry out massive exploits. Such compromises are among the most devastating in crypto, as a leaked private key can give attackers full control over all associated funds. Since exchanges manage large sums of capital, even a small breach can result in hundreds of millions in losses, making them prime targets for malicious actors. In contrast, vulnerabilities in smart contracts may only allow partial or conditional access to funds.



Major Exploits in Q1 Analysis

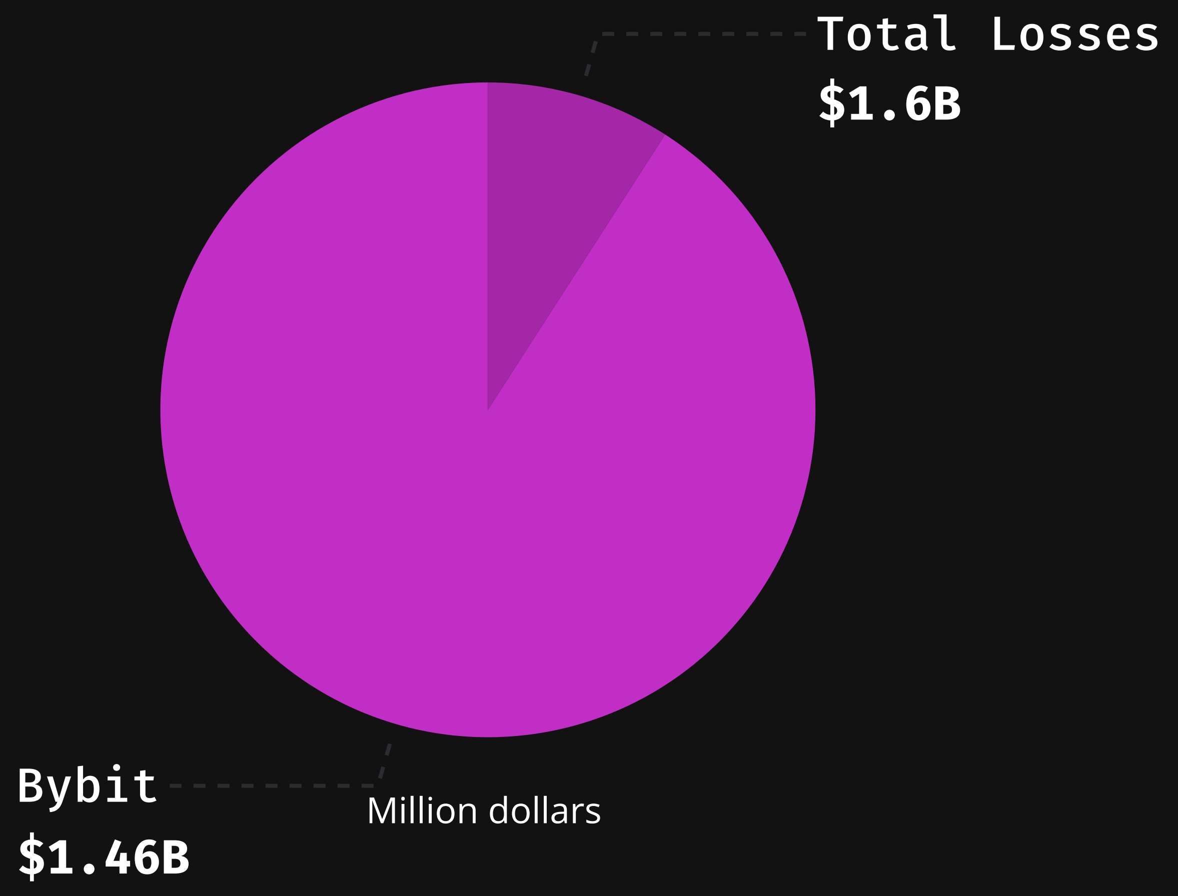
Most of that sum was lost by two specific centralized crypto exchanges: Bybit suffered an attack that resulted in $1.46 billion lost, and Phemex incurred a loss of $69.1 million.

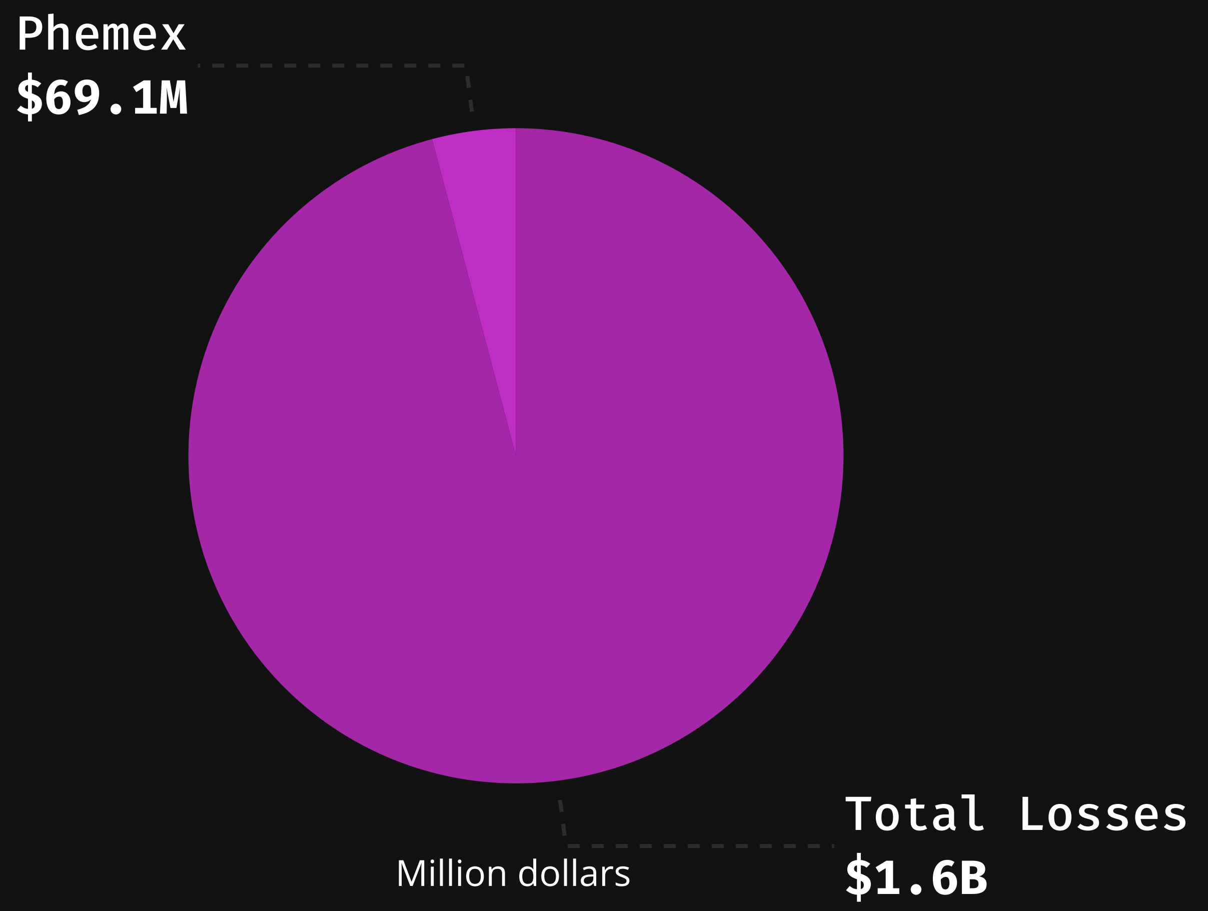
BYBIT, $1,46 BILLION

- On February 21, 2025, Bybit, the Singapore-based centralized crypto exchange, was hacked for $1.46 billion. In the largest crypto hack ever, the attackers gained control of an Ethereum cold wallet.

PHEMEX, $69.1 MILLION

- On January 23, 2025, the Singapore-based cryptocurrency exchange Phemex suffered an exploit, resulting in over $69 million in losses drained from its hot wallets.



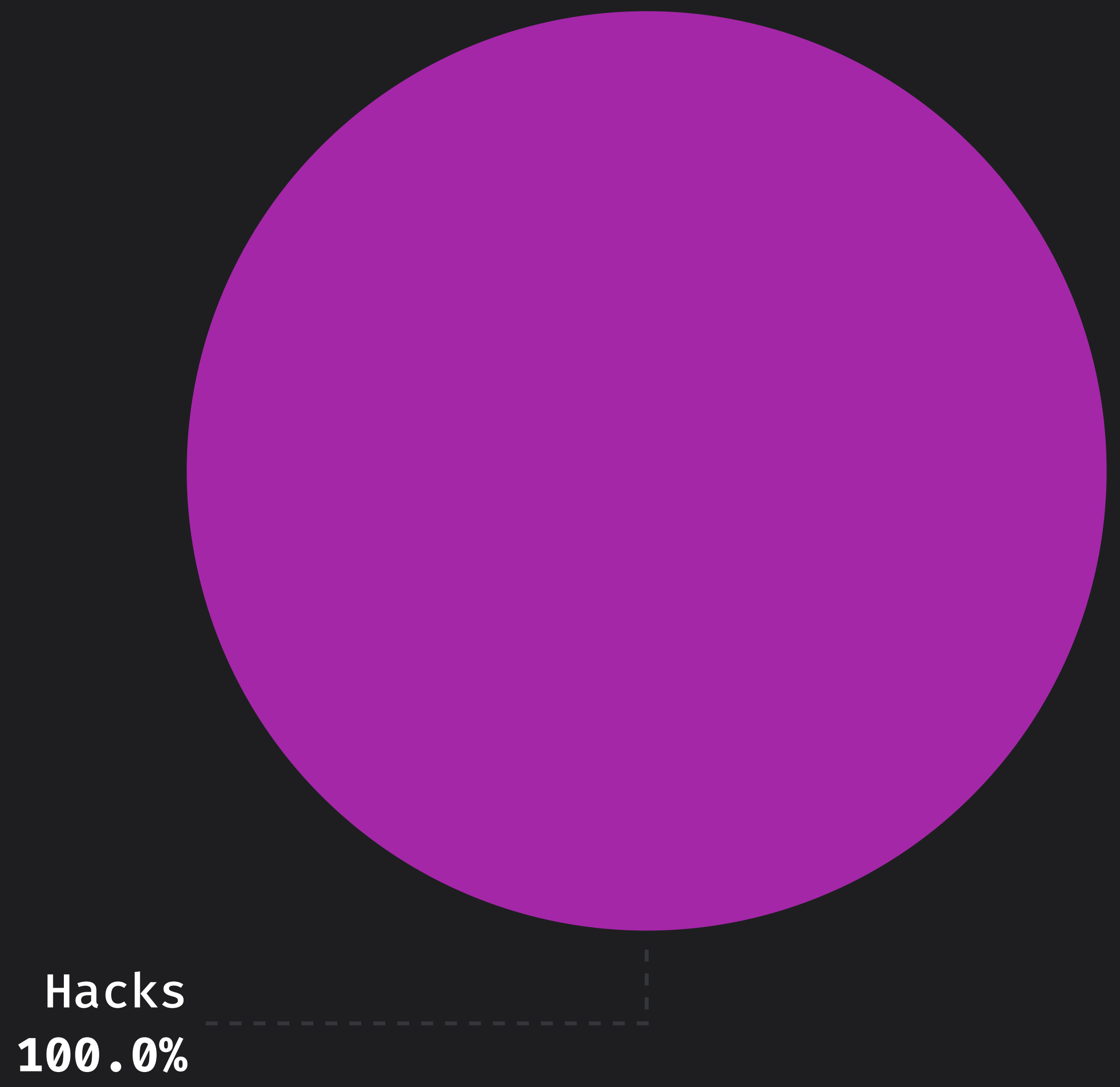


Hacks vs. Fraud Analysis

In Q1 2025, hacks continue to be the predominant cause of losses far surpassing fraud. An analysis reveals that hacks accounted for 100% of the total losses during this period, with no notable fraud incidents reported.

OVERVIEW

- **Hacks**
  In total, we saw a loss of **$1,635,933,800** due to hacks in Q1 2025 across 39 specific incidents. These numbers represent an 390% increase compared to Q1 2024, when losses caused by hacks totaled $333,585,400.
- **Fraud**
  The ecosystem hasn't seen specific fraud accidents in Q1 2025. This represents a significant decrease compared to Q1 2024, when losses caused by frauds, scams, and rug pulls totaled $14,665,817.

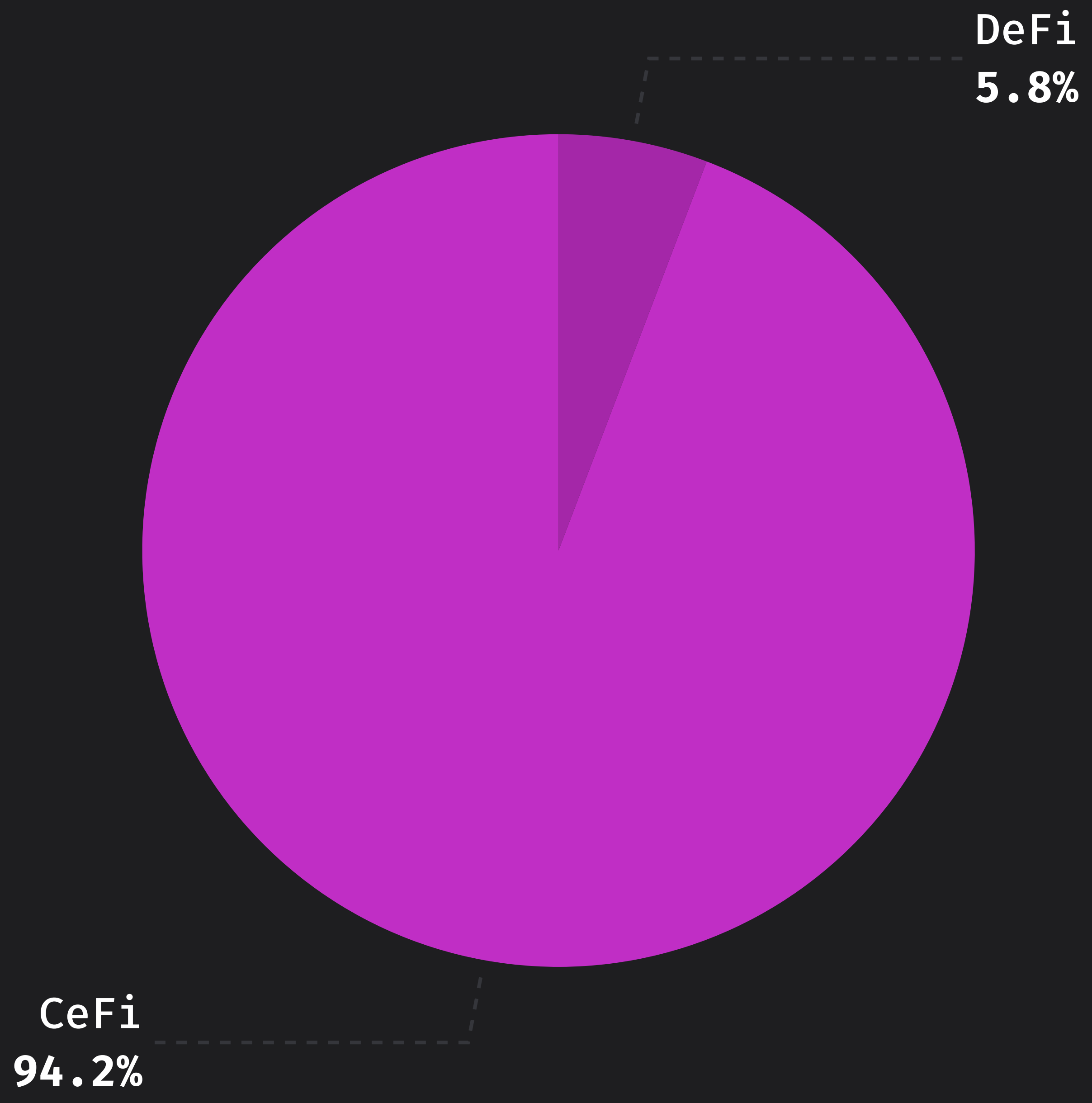


DeFi vs. CeFi Analysis

In Q1 2025, CeFi became the primary target for exploits, despite only two major attacks being recorded. This contrasts sharply with DeFi, which experienced a significantly higher incidence rate, with 38 documented attacks.

OVERVIEW

- **DeFi**
  DeFi has suffered **$106,833,800** in total losses in Q1 2025 across 38 incidents. These numbers represent a 69% decrease compared to Q1 2024, when DeFi losses totaled **$348,251,217.**
- **CeFi**
  CeFi has suffered from 2 major attacks in Q1 2025, totalling in **$1,529,100,000.** In Q1 2024, no incidents were recorded on CeFi projects.



Losses by Chain

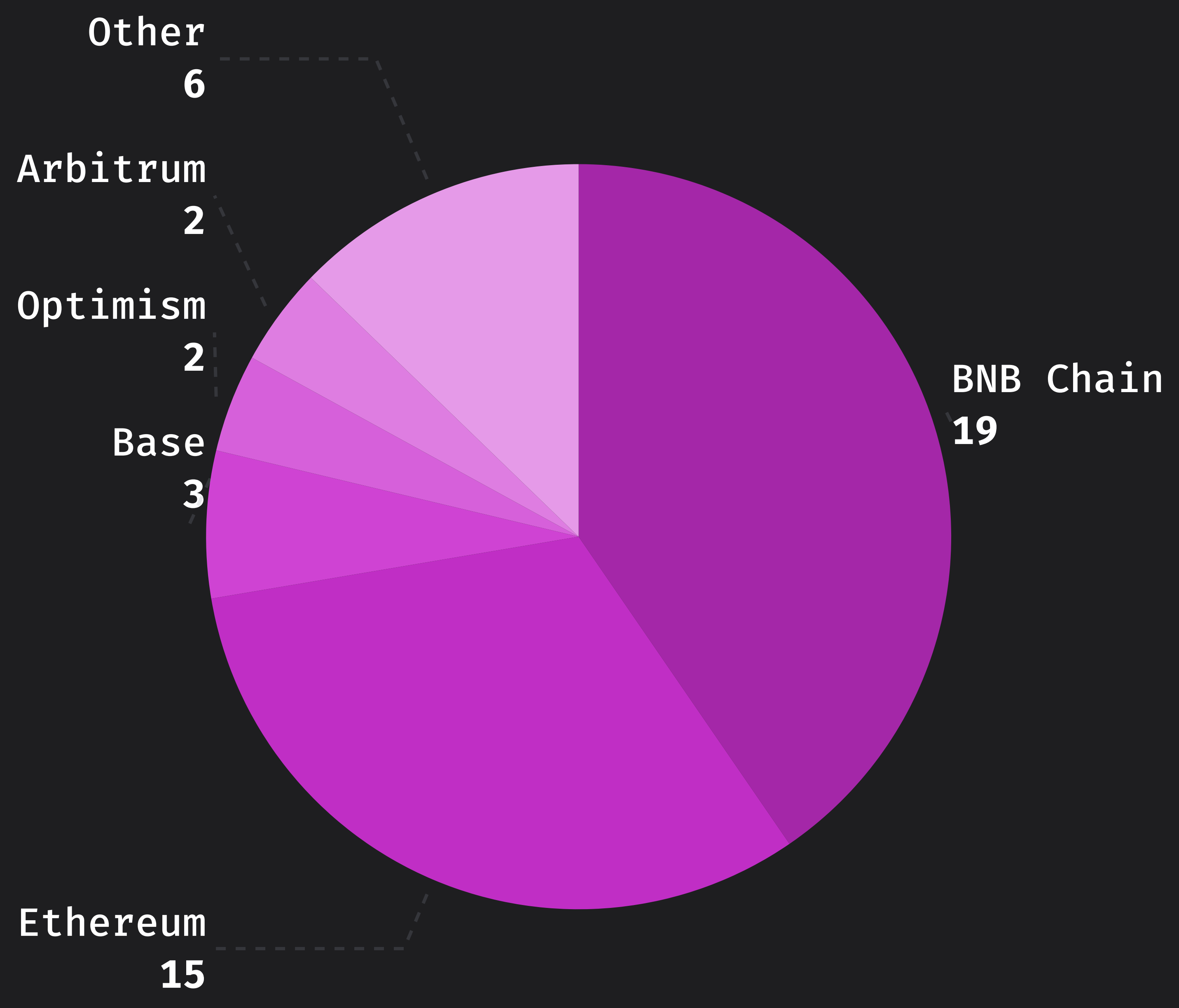
The two most targeted chains in Q1 2025 were Ethereum and BNB Chain. BNB Chain suffered the most individual attacks with 19 incidents, representing 44% of the total losses across targeted chains. Ethereum witnessed 15 incidents, representing 32% respectively.

OVERVIEW

- In Q1 2025, Ethereum and BNB Chain accounted for over half of the chain losses, totaling 76%.
- Base followed with 3 incidents, comprising 7%. Optimism and Arbitrum had 2 incidents, each representing 4.7%. Other chains, including Abstract, Wemix and Mode, suffered 1 attack each, representing 2.3% each.

INSIGHTS

- In Q1 2025, BNB Chain surpassed Ethereum and became the most targeted chain compared to the previous period.



Funds Recovery

OVERVIEW

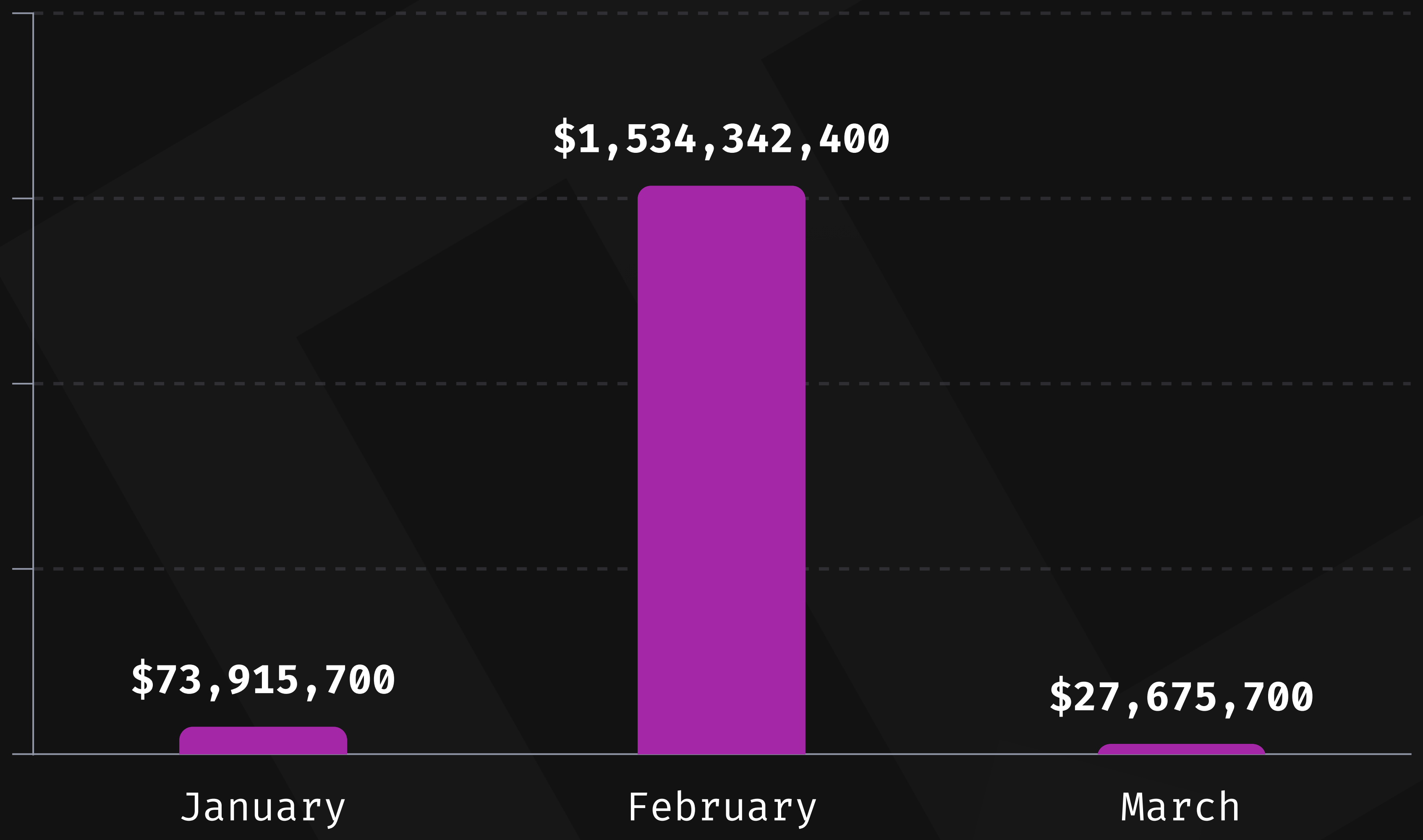
In total, **$6.5 million** was recovered from stolen funds in **2** specific situations. This number makes up **0.4%** of the total losses in Q1 2025.

	Stolen	Recovered
1inch	$5,000,000	$5,000,000
Moby Trade	$2,500,000	$1,500,000

In Focus: Crypto Losses YTD

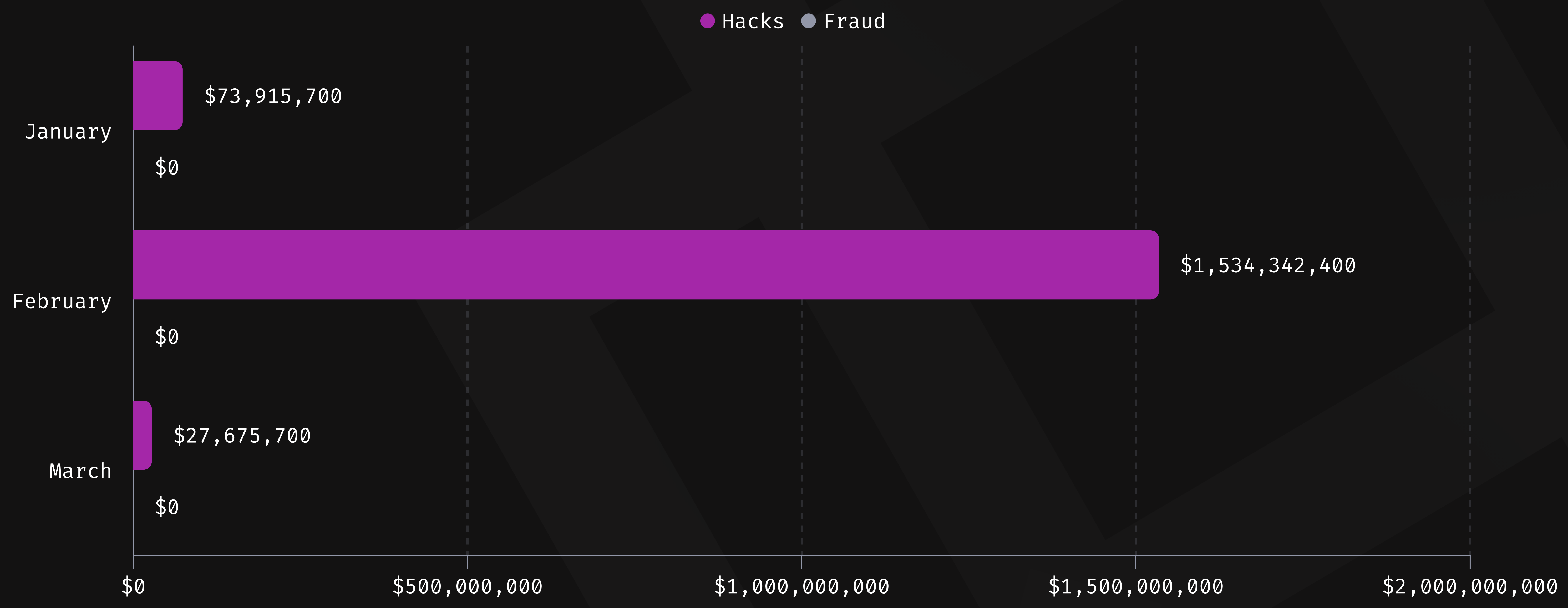
MONTHLY OVERVIEW

In total, the ecosystem has witnessed **$1.62** billion in losses year-to-date (YTD) across 40 specific incidents. The majority of these losses came from over $1.5 billion lost in February alone.



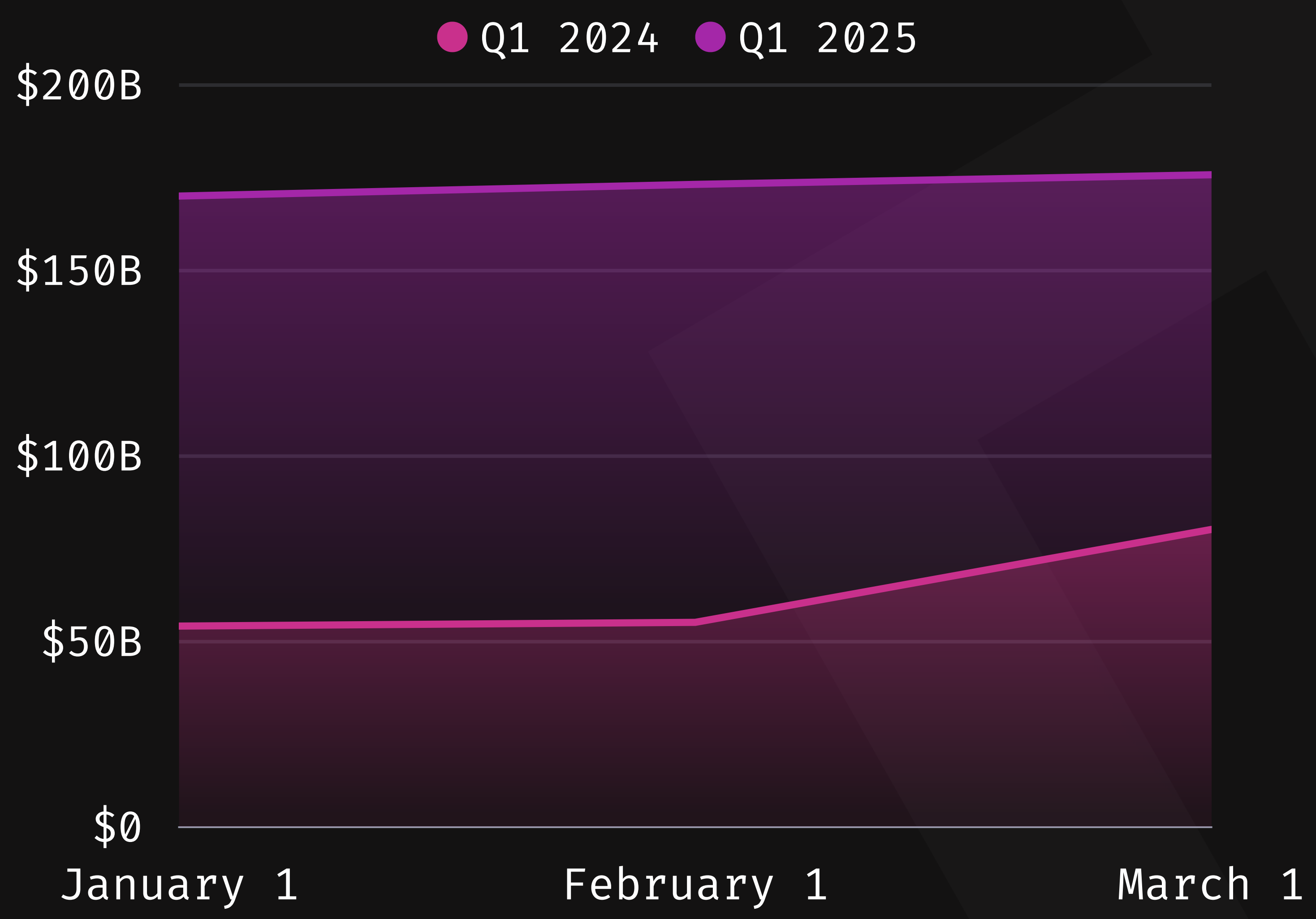
In Focus: Crypto Losses YTD

TOTAL LOSSES YTD: HACKS VS. FRAUD



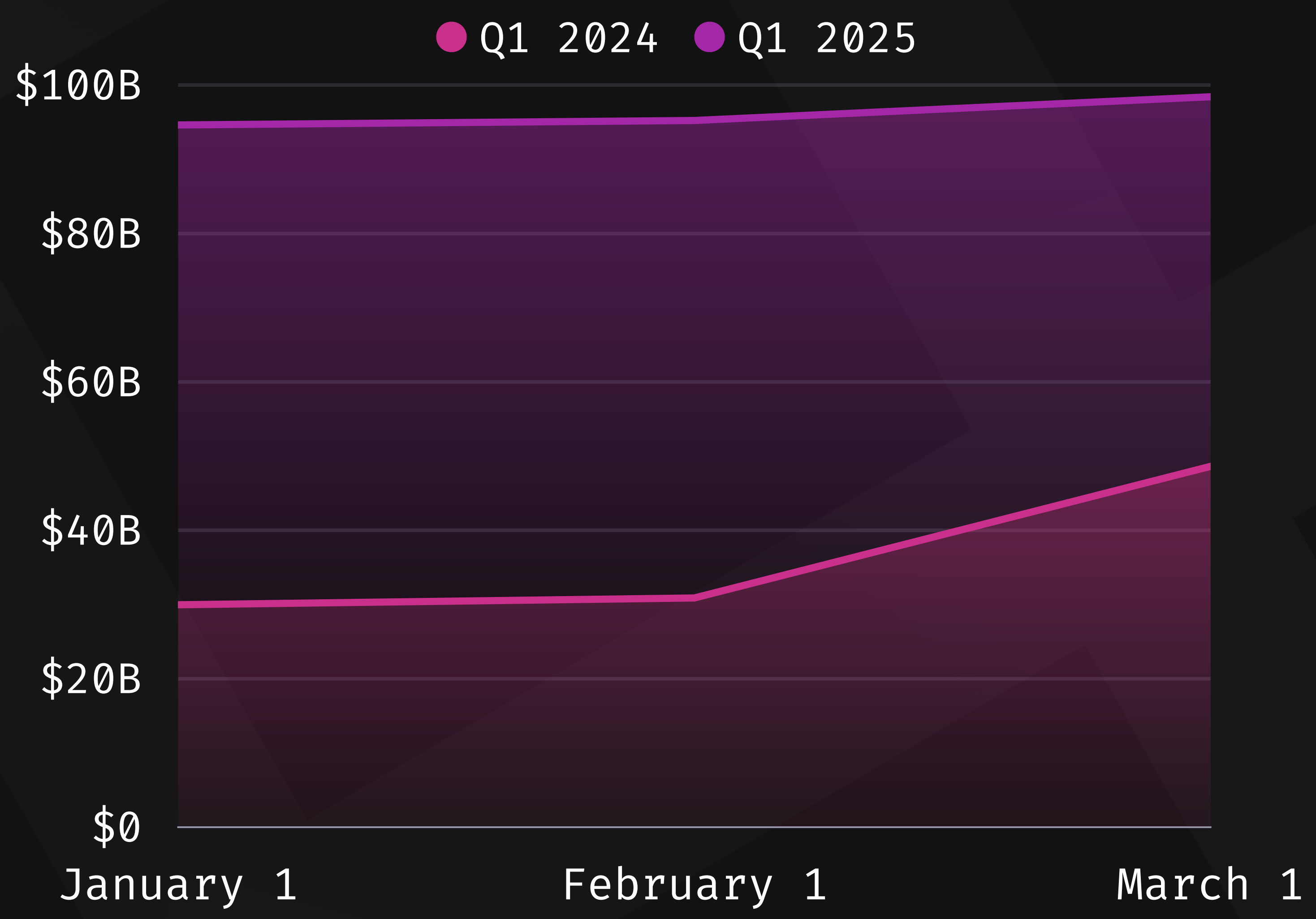
In Focus: Q1 2024 vs. Q1 2025

TVL (USD) ALL PROTOCOLS



Total Value Locked

TVL (USD) ETHEREUM



Total Value Locked

In Focus: Q1 2024 vs. Q1 2025

DEFI VS. CEFI

69% ↓

DeFi

Losses are down 69% when compared to the previous period.

* ↑

CeFi

Losses are up $1.5 billion when compared to the previous period.

*CeFi has suffered $1,529,100,000 in total losses in Q1 2025 across 2 incidents. In Q1 2024, there was no recorded incident on a CeFi project.

In Focus: Q1 2024 vs. Q1 2025

HACKS VS. FRAUD

390% ↑

Hacks

Losses are up 383% when compared to the previous period.

100% ↓

Fraud

Losses are down 100% when compared to the previous period.

“

The Q1 2025 breaches mark a historic moment in crypto security, with CeFi accounting for 94% of total losses, all caused by North Korean hackers. The sheer scale of the Bybit and Phemex attacks, totaling $1.5 billion, shows how state-backed actors are arguably the most pressing threat to our industry. Their success in breaching renowned, battle-tested platforms is a reminder of the need for security measures that protect the entire stack and help projects prevent catastrophic attacks before they happen.

Mitchell Amador

Founder and CEO at Immunefi

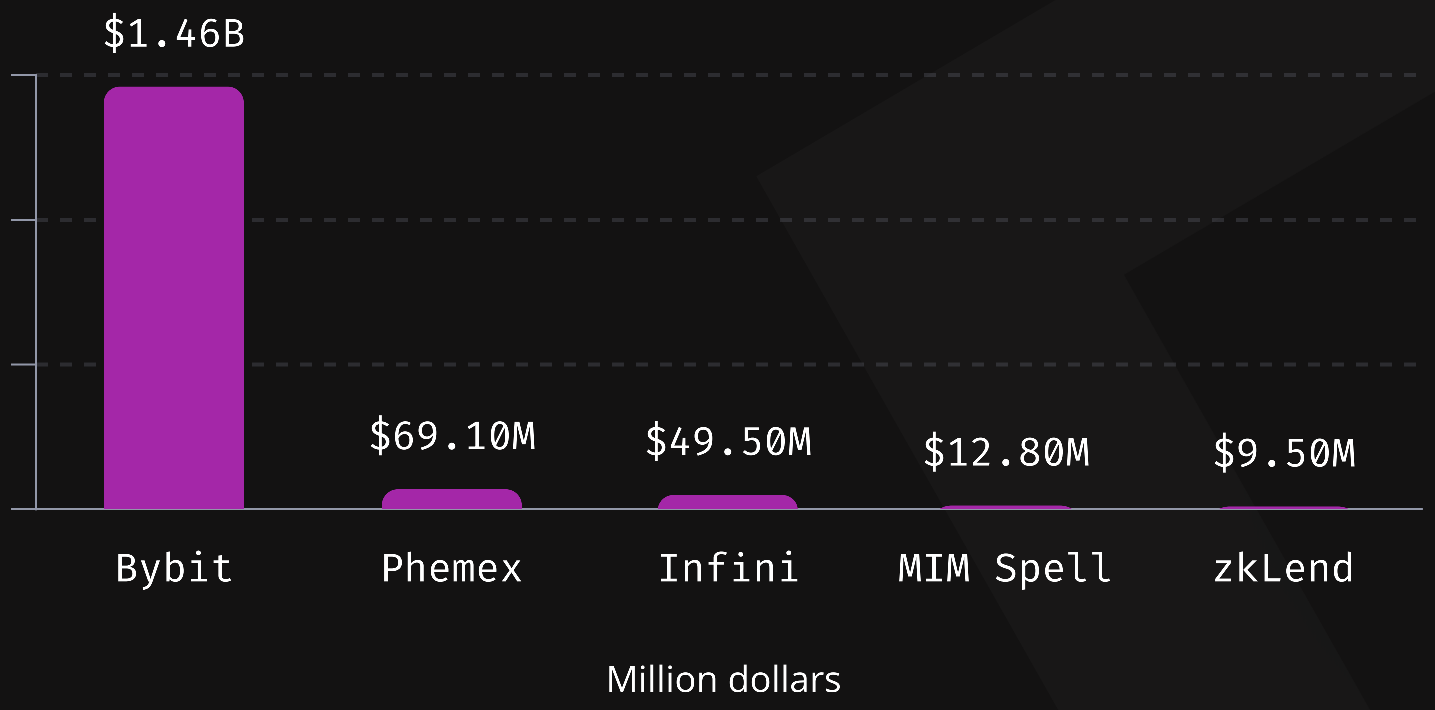
Crypto Losses Q1 2025

Immunefi

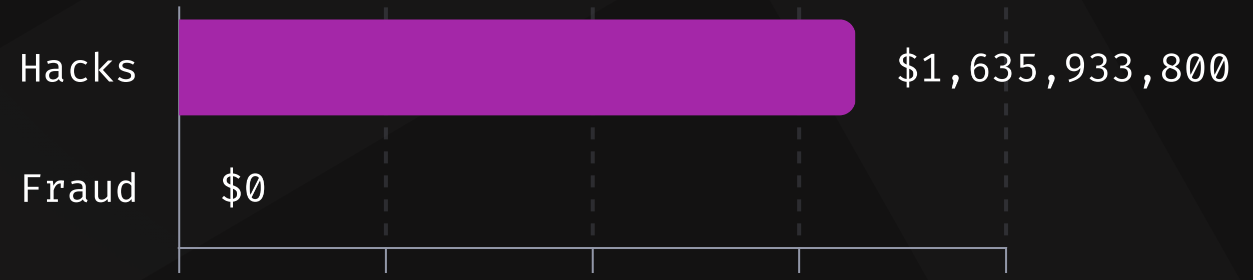
TOTAL LOSSES IN Q1

$1,635,933,800

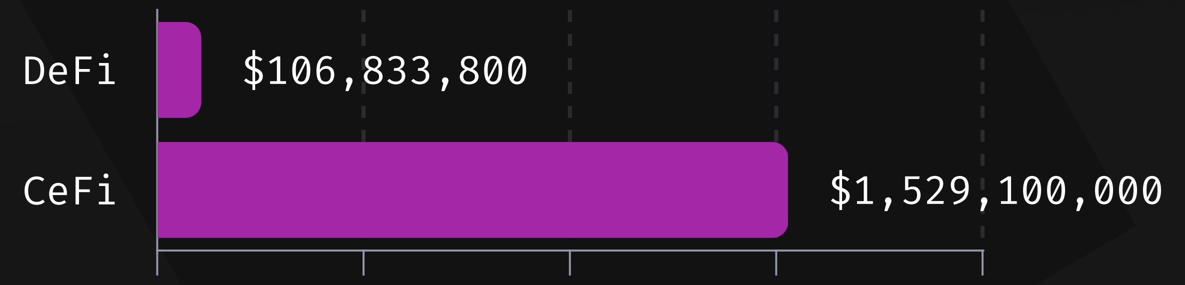
MAJOR LOSSES



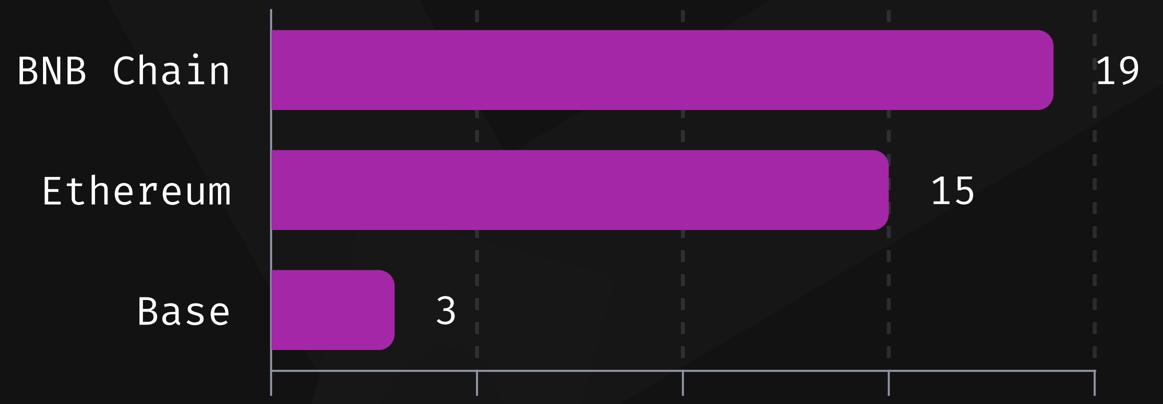
HACKS VS. FRAUD



DEFI VS. CEFI



TOP LOSSES BY CHAIN



For more information about the **Crypto Losses Report**, please visit immunefi.com/research.

Immunefi

Immunefi is the the leading onchain crowdsourced security platform protecting over $190 billion in user funds. Immunefi features a massive community of whitehat hackers who review projects' blockchain and smart contract code, find and responsibly disclose vulnerabilities, and get paid for making crypto safer. With Immunefi, whitehat hackers are rewarded based on the severity of the vulnerability that they discover, creating incentives for as many experts as possible to examine project code for vulnerabilities.

Immunefi has pioneered the scaling web3 bug bounties standard, meaning that rewards should be priced accordingly with the severity of an exploit and the volume of funds at risk, which resulted in the company building the largest community of security talent in the web3 space.

TOTAL BOUNTIES PAID

Immunefi has paid out over **$112 million** in total bounties, while saving over **$25 billion** in user funds.

TOTAL BOUNTIES AVAILABLE

Immunefi offers over **$180 million** in available bounty rewards.

SUPPORTED PROJECTS

Trusted by established, multi-billion dollar projects like Synthetix, Chainlink, Polygon, LayerZero, MakerDAO, TheGraph, Wormhole, Optimism and more, Immunefi now supports more than 300 projects across multiple crypto sectors.

LARGEST BUG BOUNTY PAYMENTS IN THE HISTORY OF SOFTWARE

Immunefi has facilitated the largest bug bounty payments in the history of software:

- **$10 million** for a vulnerability discovered in Wormhole, a generic cross-chain messaging protocol.
- **$6 million** for a vulnerability discovered in Aurora, a bridge, and a scaling solution for Ethereum.
- **$2.2 million** for a vulnerability discovered in Polygon, a decentralized Ethereum scaling platform that enables developers to build scalable, user-friendly dApps.

Disclaimer:

- Immunefi uses publicly available data and news reports in order to access and collect alleged frauds, scams, and rug pulls. Including such incidents in this report does not constitute a determination from Immunefi that a fraud, scam, or rug pull event did occur.
- The full dataset can be found **here**.

Notes:

- * Top 10 Losses in Q1 2025: **$5 million** in stolen funds were later recovered from the 1inch exploit and **$1.5 million** from the Moby Trade exploit.
- The Total Value Locked (USD) data has been extracted from DefiLlama.
- Immunefi assesses the volume of crypto funds lost by the community due to hacks and scams by reviewing, validating, and classifying publicly available data. In this report, Immunefi considered only hard rug pulls for its fraud category. A hard rug pull is a project that creates an image of credibility and attracts outside capital through token sales or other means with the sole purpose of stealing deposited user funds and disappearing.

More:

- If you're a developer thinking about a bug-hunting career in web3, we got you. Check out our **Web3 Security Library**, and start taking home some of the over $180M in rewards available on Immunefi — the leading bug bounty platform for web3.

For more information, please visit **https://immunefi.com/**