Immunefi

CRYPTO LOSSES IN Q1 2023

PREPARED BY IMMUNEFI

Crypto Losses in Q1 2023

PREPARED BY IMMUNEFI

The team at Immunefi, the leading bug bounty and security services platform for web3 which protects over $60 billion in user funds, has assessed the volume of crypto funds lost by the community due to hacks and scams in Q1 2023.

OVERVIEW

The global web3 space was valued at over **$934 billion** in 2022. That capital represents an unparalleled and attractive opportunity for blackhat hackers.

We have reviewed all instances where blackhat hackers have exploited various crypto protocols, as well as cases of protocols that have allegedly performed a rug pull in Q1 2023. We have located 73 such instances, including both successful and semi-successful hacking attempts, as well as alleged fraud.

In total, we have seen a loss of **$437,483,543** across the web3 ecosystem in Q1 2023. **$418,589,089** was lost to hacks in Q1 2023 across 59 specific incidents and **$18,894,454** was lost to fraud in across 15 specific incidents. Most of that sum was lost by two specific projects: Euler Finance*, a DeFi lending platform**,** and BonqDAO, a self-sovereign finance solution.

This number represents a 64.4% decrease compared to Q1 2022, when hackers and fraudsters stole $1,229,500,867.

***Euler Finance** later recovered $177 million of the stolen fund. The project exposure is counted as a part of the total losses.

Crypto Losses in Q1 2023

KEY TAKEAWAYS IN Q1 2023

- The 2 major exploits of the quarter totaled $317,000,000 alone, accounting for 72.5% of all losses in Q1 2023.
- In Q1 2023, hacks continued to be the predominant cause of losses at 95.7% in comparison to frauds, scams, and rug pulls, which amounted to only 4.3% of the total losses.
- In Q1 2023, DeFi continued to be the main target of successful exploits at 99.6% as compared to CeFi at 0.4% of the total losses.
- The two most targeted chains in Q1 2023 were BNB Chain and Ethereum. BNB Chain surpassed Ethereum and became the most targeted chain in Q1 2023, with 33 incidents, while Ethereum witnessed 22 incidents. Arbitrum, which had no incidents in Q1 2022, witnessed 8 incidents, followed by Polygon with 5 incidents and Optimism with 3 incidents.
- In total, $177,250,000 of stolen funds have been recovered across 2 specific instances, Euler Finance and SperaxUSD. This number represents just 40.5% of the total losses in Q1 2023.

KEY INSIGHTS IN Q1 2023

- The rise in targeted attacks and scams on Arbitrum-based projects moving into 2023 becomes relevant, as the protocol recently released its token — a recent report by Immunefi shows that token prices drop on average by 20% after hacks, and the majority never recover.
- While the number of total losses is down 64.4% from Q1 2022, likely due to market conditions affecting the Total Value Locked (TVL) in the ecosystem, attacks and activity spiked: the number of single incidents increased 192% YoY from 25 to 73 in Q1 2023 — the highest activity the sector has witnessed in the past 2 years.
- BNB Chain continues to be the prime target for exploits and scams — in fact, 73.3% of total rug pulls in Q1 2023 happened on BNB Chain.

Top 10 Losses in Q1 2023*

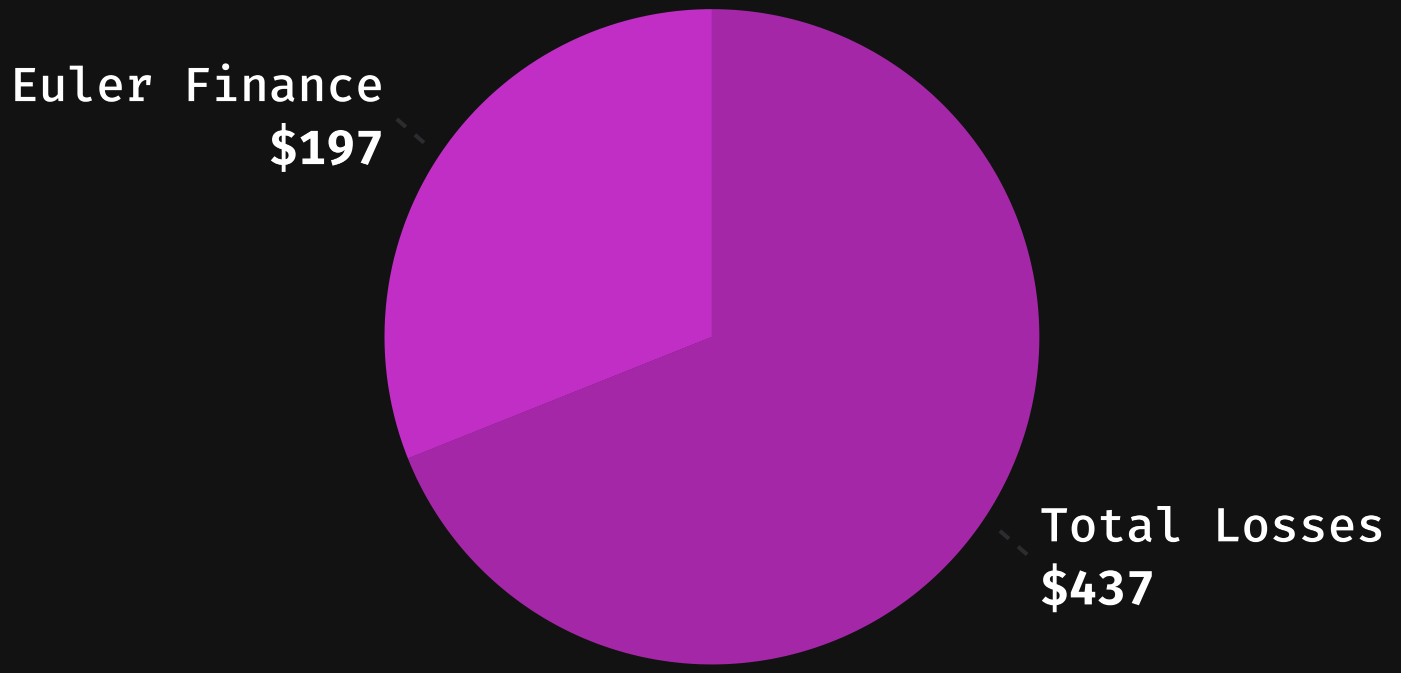
Euler Finance	$197,000,000
BonqDAO	$120,000,000
Angle Protocol	$17,000,000
Balancer	$11,900,000
MyAlgo	$9,200,000
Platypus	$8,500,000
Safemoon	$8,500,000
LendHub	$6,000,000
Idle Finance	$5,900,000
Shata Capital	$5,140,000

Major Exploits in Q1 Analysis

Most of the Q1 loss sum was lost by 2 specific projects, Euler Finance and BonqDAO, totaling $317,000,000. Together, these two projects represent 72.5% of Q1 losses alone.

EULER FINANCE, $197 MILLION

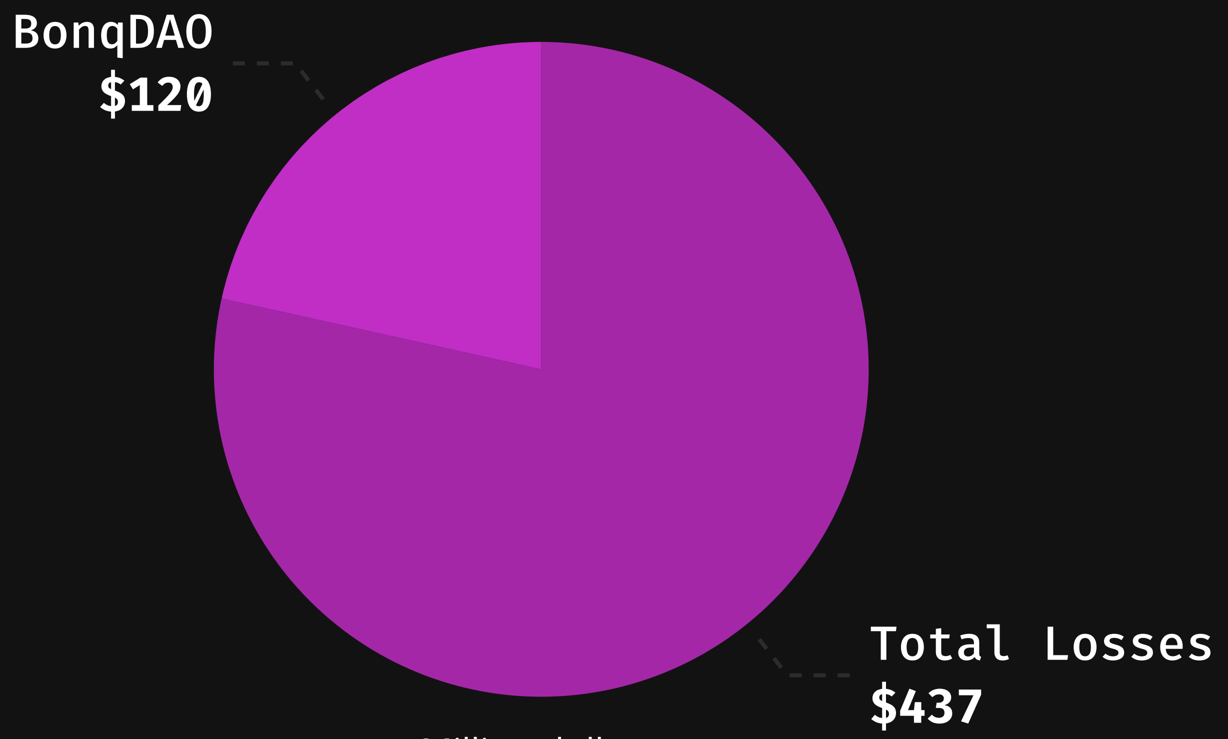
- On March 13th, 2023, Euler Finance, a DeFi lending protocol, suffered a flash-loan attack that resulted in a $197 million loss. The attacker drained several assets, including $136 million of stETH, $34 million of USDC, $19 million of WBTC, and $8.7 million of DAI.



Million dollars

BONQDAO, $120 MILLION

- On February 1st, 2023, BonqDAO, a self-sovereign finance solution, suffered an oracle attack that allowed a blackhat hacker to manipulate the price of the AllianceBlock (ALBT) token. This led to a $120 million loss.



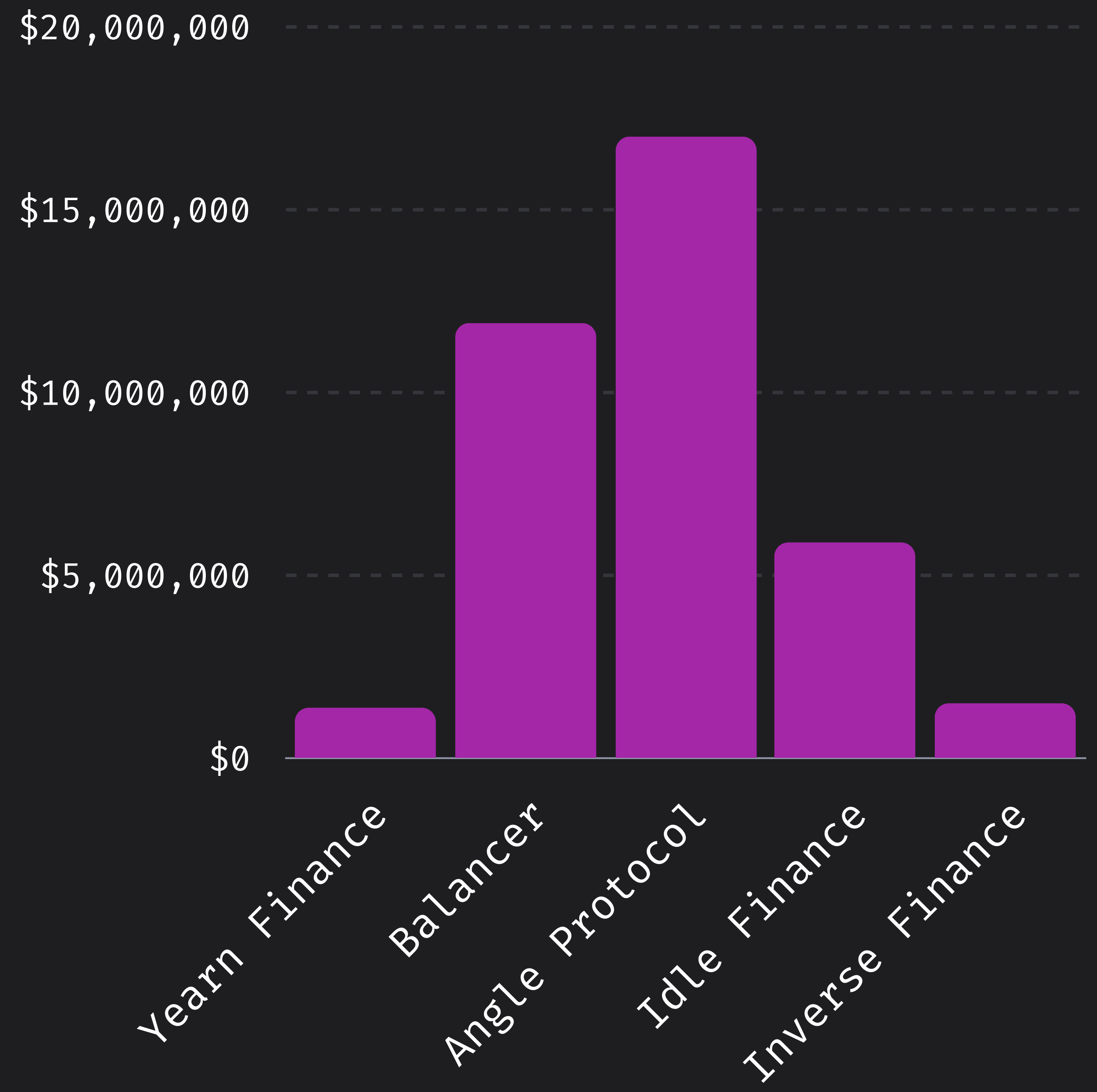
Million dollars

Major Exploits in Q1 Analysis

The Euler Finance hack sent shockwaves across the ecosystem. Several protocols have suffered exposure, ranging from $860,000 to as much as $17 million.

EULER FINANCE EXPOUSURE

- **Angle Protocol**
  At the time of the Euler's hack, over **$17 million USDC** had been routed by the Angle Protocol on Euler.
- **Balancer**
  $11.9 million was sent to Euler from the bbeUSD (Euler Boosted USD) pool at the time of the hack. This represented approximately 65% of the pool's TVL.
- **Idle Finance**
  Idle Finance had several strategies involved. The exposure amounted to over **$5.9 million** across eUSDC, eUSDC staking, eDAI, eUSDT, eUSDT staking, eWETH staking, and eagEUR pools.
- **Yearn Finance**
  Some of Yearn Finance's vaults had indirect exposure to Euler's hack. The exposure amounted to **$1.38 million** in total, across yvUSDT and yvUSDC via strategies using Idle and Angle.
- **Inverse Finance**
  The Euler hack affected Inverse Finance's DOLA-bb-e-USD pool on Balancer. The DOLA Fed for the pool suffered a loss of up to **$860,000.**

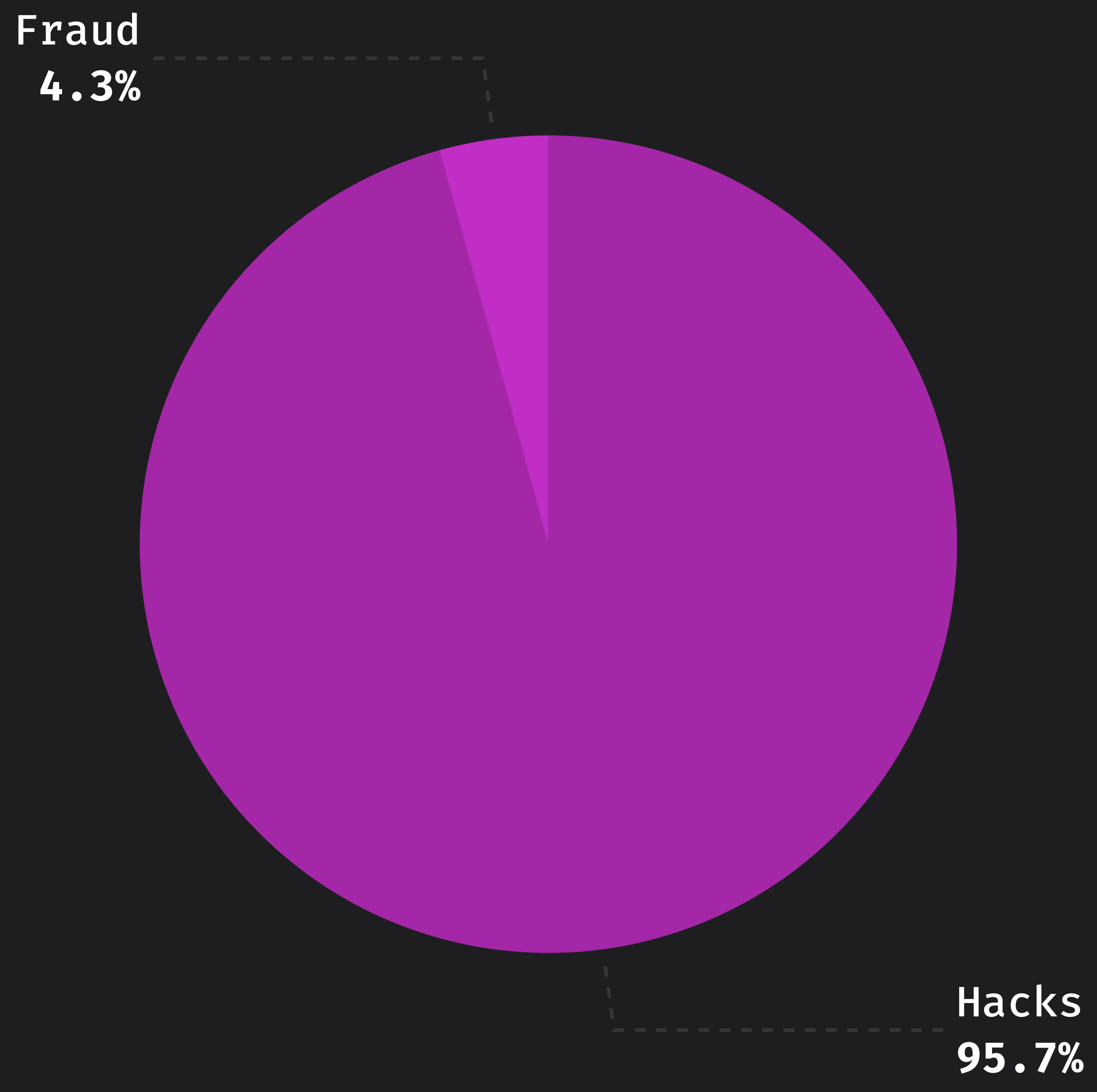


Hacks vs. Fraud Analysis

In Q1 2023, hacks continue to be the predominant cause of losses as compared to frauds, scams, and rug pulls. An analysis of the losses shows that fraud accounts for only 4.3% of the total losses in the Q1 2023, while hacks account for 95.7%.

OVERVIEW

- **Hacks**
  In total, we have seen a loss of **$418,589,089** to hacks in Q1 2023 across 59 specific incidents. These numbers represent a 65.6% decrease compared to Q1 2022, when losses caused by hacks totaled $1,218,500,867.
- **Fraud**
  In total, we have seen a loss of **$18,894,454** to fraud in Q1 2023 across 15 specific incidents. These numbers represent a 71.8% increase compared to Q1 2022, when losses caused by frauds, scams, and rug pulls totaled $11,000,000.

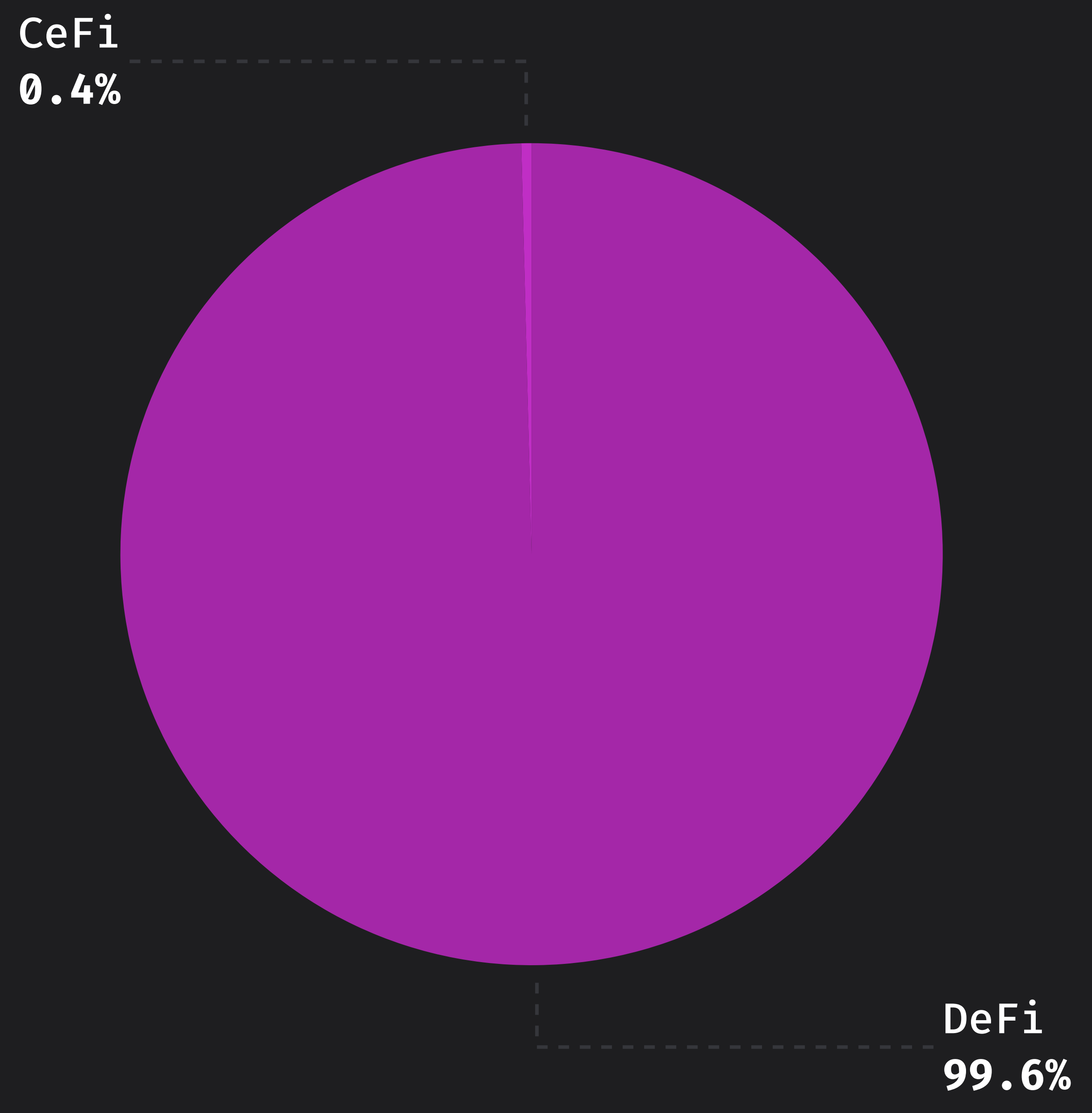


DeFi vs. CeFi Analysis

In Q1 2023, DeFi continues to be the key target for exploits as compared to CeFi. DeFi represents 99.6% of the total losses, while CeFi represents 0.4% of the total losses.

OVERVIEW

- **DeFi**
  DeFi has suffered **$435,675,543** in total losses in Q1 2023 across 72 incidents. These numbers represent a 62.2% decrease compared to Q1 2022, when DeFi losses totaled $1,153,060,867.
- **CeFi**
  CeFi has suffered **$1,808,000** in total losses in Q1 2023 across 2 incidents. These numbers represent a 97.6% decrease compared to Q1 2022, when CeFi losses totaled $76,440,000.



Losses by Chain

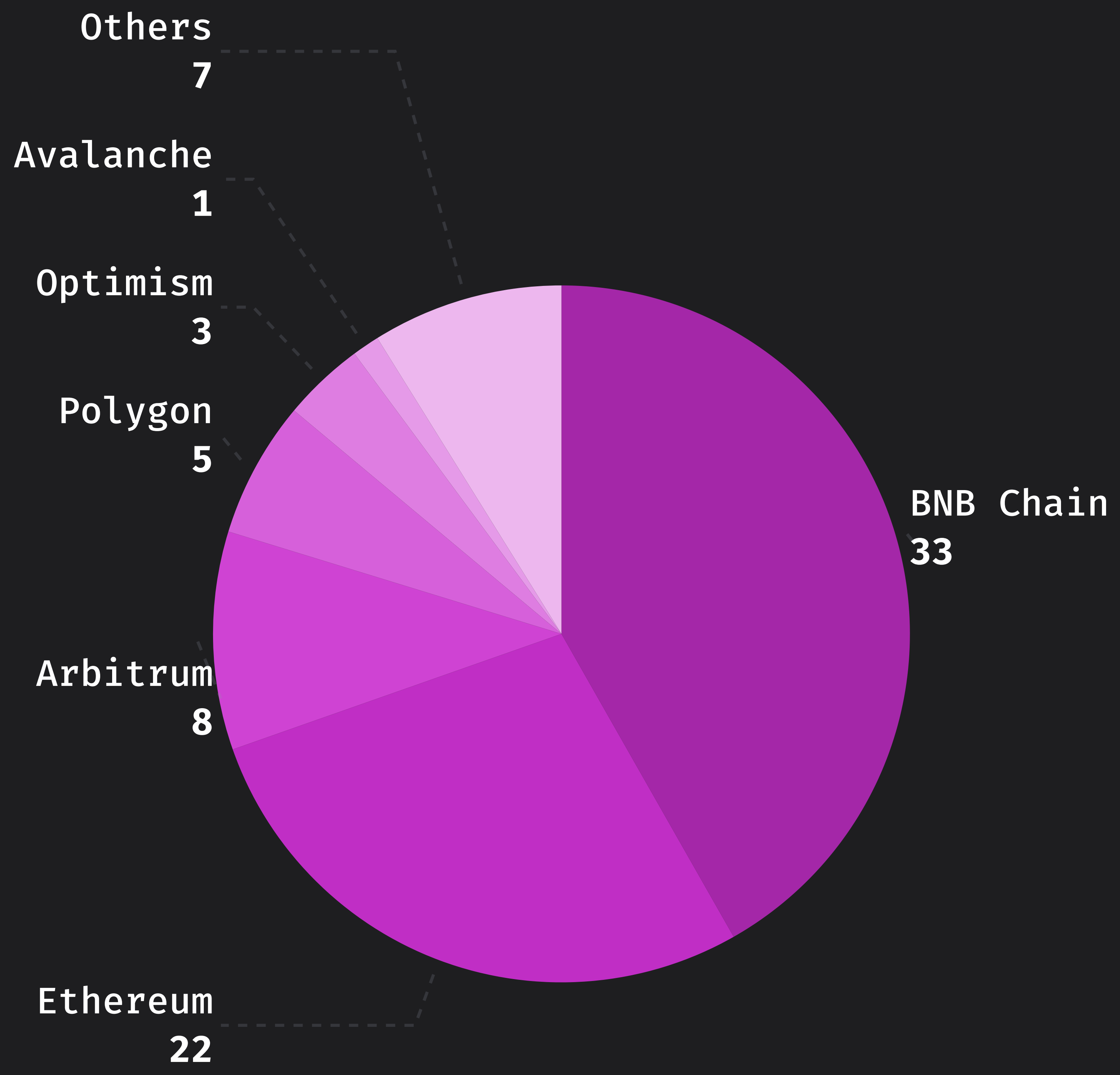
The two most targeted chains in Q1 2023 were BNB Chain and Ethereum. BNB Chain suffered the most individual attacks with 33 incidents, representing 41.3% of the total losses across targeted chains. Ethereum witnessed 22 incidents, representing 27.5% respectively.

OVERVIEW

- BNB Chain and Ethereum represent more than half of the chain losses in Q1 2023 at 68.8%. Arbitrum comes in third with 8 incidents, representing 10.1% of total losses across chains. Polygon follows with 5 incidents, Optimism with 3 incidents, and Avalanche with 1 incident. Remaining chains like Dogechain, Cardano, Cosmos, HECO, and others together represent 8.9% of the total chain incidents, all with single incidents.

INSIGHTS

- BNB Chain continues to be the prime target for exploits and scams — in fact, 73.3% of total rug pulls in Q1 2023 happened on BNB Chain.



“

BNB Chain still has a serious issue with developers using forked code. Its community lacks a security-first approach and attracts many users looking for a quick way to earn money. That's why we continue to see the biggest number of exploits and rug pulls in this ecosystem.

Adrian Hetman

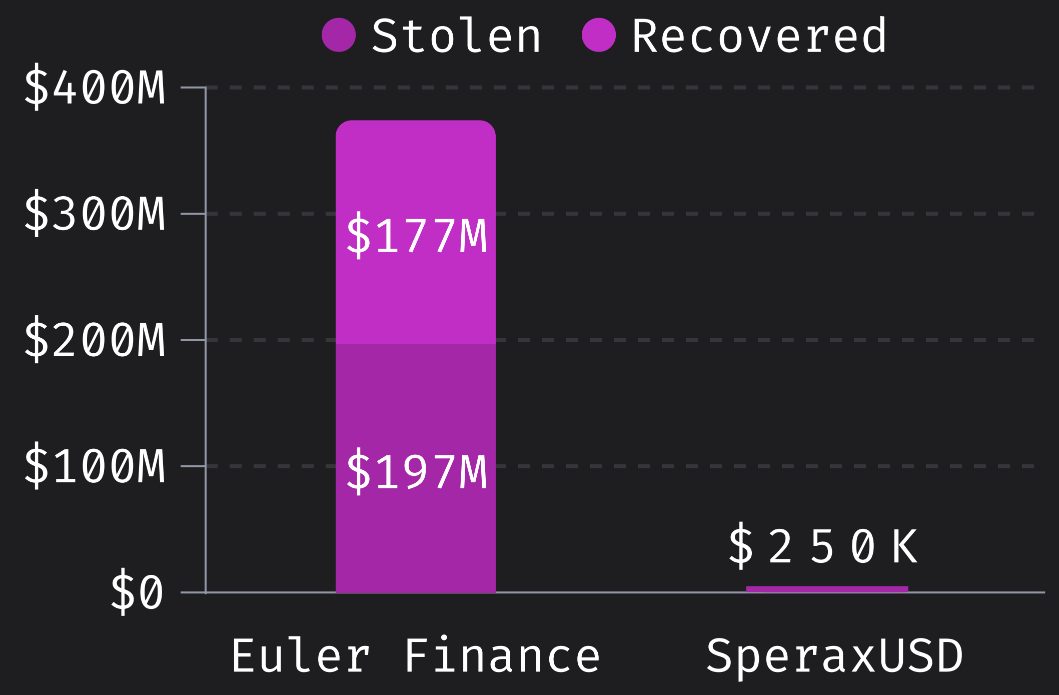
Tech Lead of the Triaging Team at Immunefi

Funds Recovery

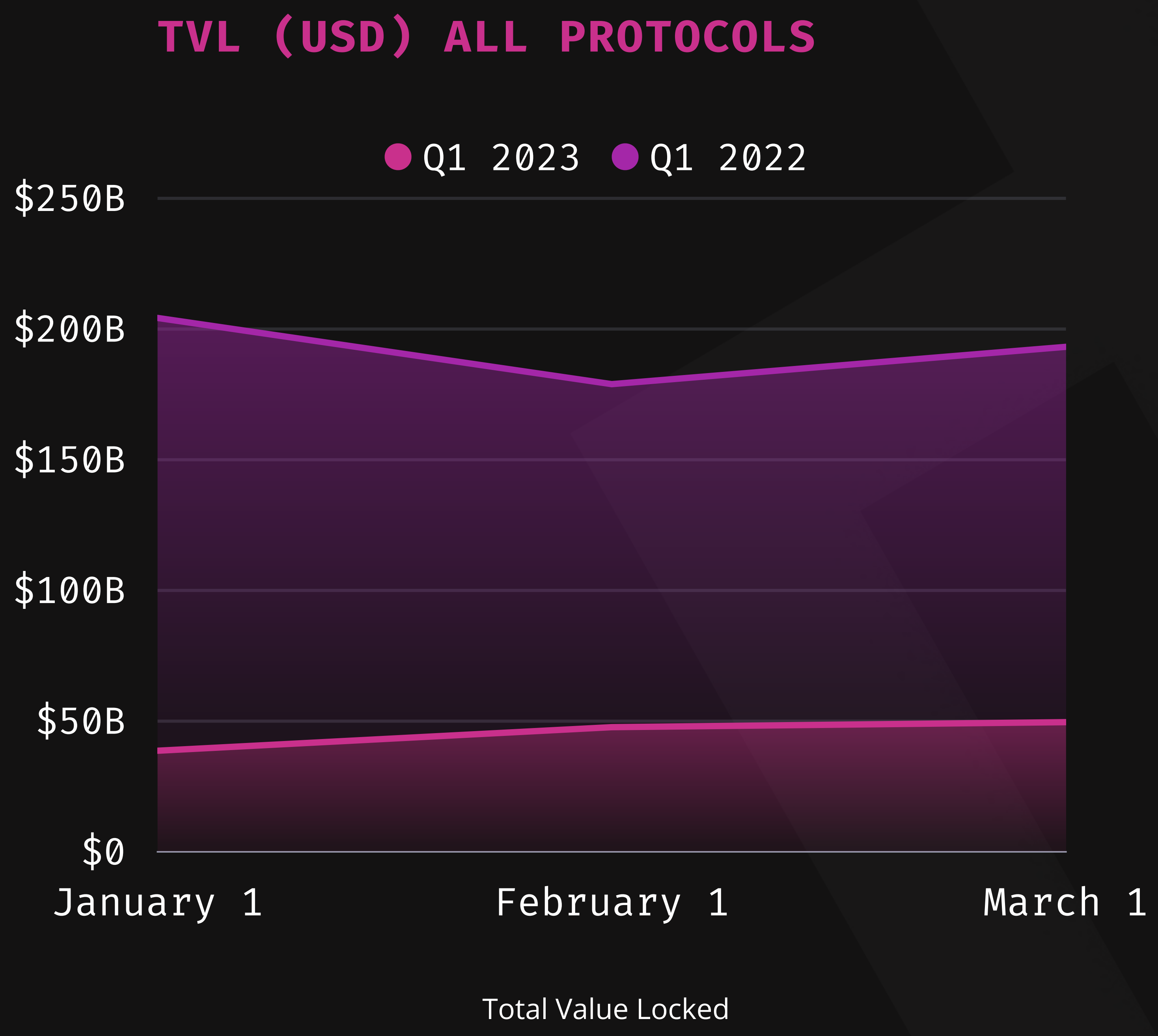
In total, **$177,250,000** has been recovered from stolen funds in **2** specific situations. This number makes up **40.5%** of the total losses in Q1 2023.

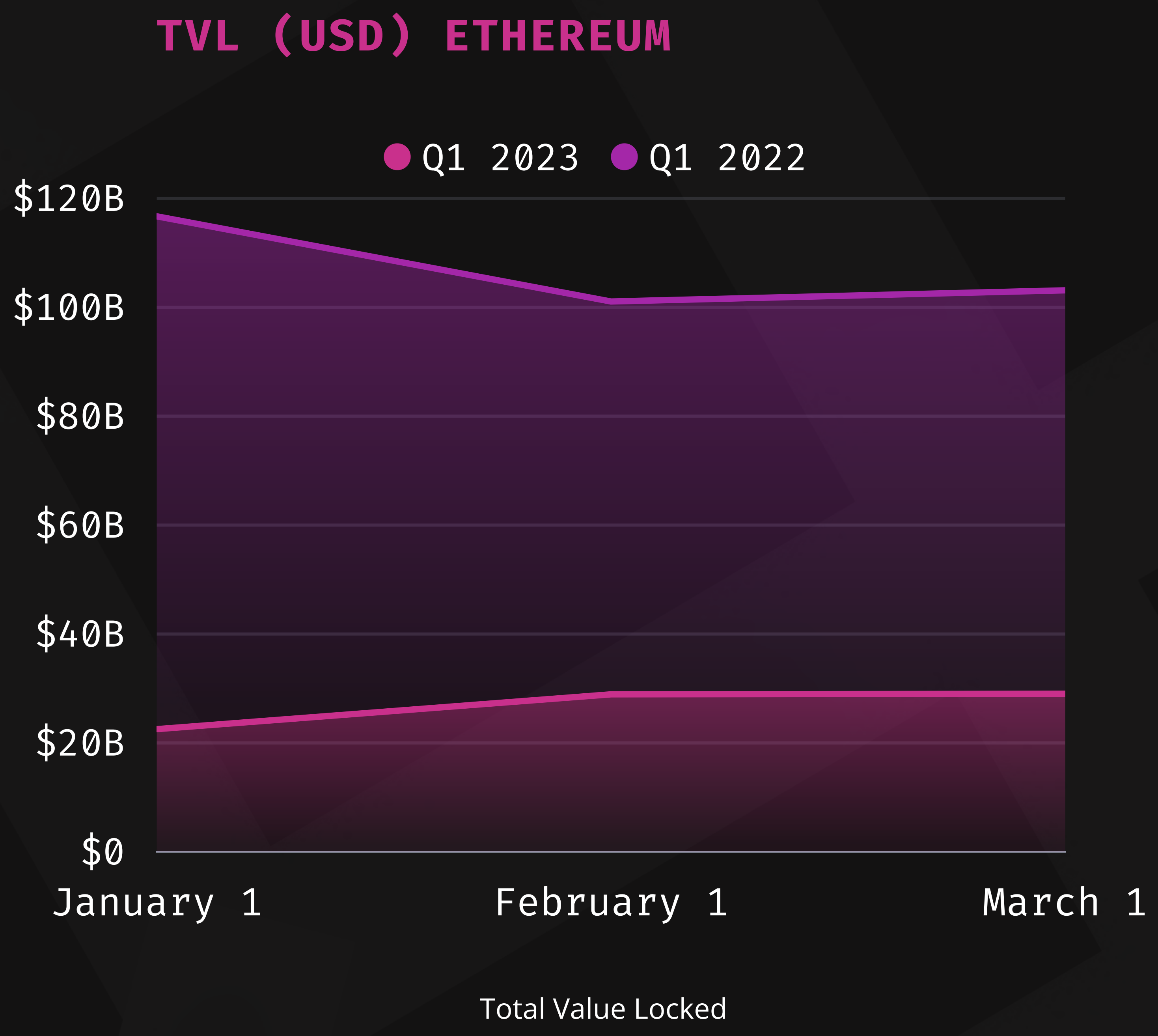
RECOVERIES

- Euler Finance has recovered **$177 million** from the $197 million stolen.
- SperaxUSD has recovered **$250,000**, **the full amount of stolen funds**.



In Focus: Q1 2022 vs. Q1 2023





In Focus: Q1 2022 vs. Q1 2023

HACKS VS. FRAUDS

65.5% ↓

Hacks

Losses are down 65.5% when compared to the previous period.

71.8% ↑

Fraud

Losses are up 71.8% when compared to the previous period.

In Focus: Q1 2022 vs. Q1 2023

DEFI VS. CEFI

62.2% ↓

DeFi

Losses are down 62.2% when compared to the previous period.

97.6% ↓

CeFi

Losses are down 97.6% when compared to the previous period.

“

> Projects have significantly increased their security measures through audits and bug bounties. But blackhats have kept pace. Losses are currently down, but mostly because the amount of funds in crypto has decreased, making hacks less devastating.

Mitchell Amador

Founder and CEO at Immunefi

Immunefi

Immunefi is the leading bug bounty and security services platform for web3 protecting over $60 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 **$70 million** in total bounties, while saving over **$25 billion** in user funds.

TOTAL BOUNTIES AVAILABLE

Immunefi offers over **$130 million** in available bounty rewards.

SUPPORTED PROJECTS

Trusted by established, multi-billion dollar projects like Chainlink, Wormhole, MakerDAO, TheGraph, Synthetix, 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:

- The Total Value Locked (USD) data has been extracted from DefiLlama.
- * Top 10 Losses in Q1 2023: **Euler Finance** later recovered $177 million of the stolen funds; **Angle Protocol**, **Balancer,** and **Idle Finance** have suffered exposure to Euler's hack, and this exposure is included in the dataset.

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 $130M in rewards available on Immunefi — the leading bug bounty platform for web3.

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