Immunefi

CRYPTO LOSSES IN Q2 2023

PREPARED BY IMMUNEFI

Crypto Losses in Q2 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 Q2 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 Q2 2023. We have located 81 such instances, including both successful and semi-successful hacking attempts, as well as alleged fraud.

In total, we have seen a loss of **$265,481,519** across the web3 ecosystem in Q2 2023. **$220,522,129** was lost to hacks in Q2 2023 across 63 specific incidents and **$44,959,390** was lost to fraud in across 18 specific incidents. Most of that sum was lost by two specific projects: Atomic Wallet*, a non-custodial decentralized wallet**,** and Fintoch, a defunct blockchain financial platform.

This number represents a 60.4% decrease compared to Q2 2022, when hackers and fraudsters stole $670,498,280.

***$1 million** in stolen funds were later recovered from the Atomic Wallet hacker.

Crypto Losses in Q2 2023

KEY TAKEAWAYS IN Q2 2023

- The 2 major exploits of the quarter totaled $131,600,000 alone, accounting for 49.6% of all losses in Q2 2023.
- In Q2 2023, hacks continued to be the predominant cause of losses at 83.1% in comparison to frauds, scams, and rug pulls, which amounted to only 16.9% of the total losses.
- In Q2 2023, DeFi continued to be the main target of successful exploits at 86.1% as compared to CeFi at 13.9% of the total losses.
- The two most targeted chains in Q2 2023 were BNB Chain and Ethereum. BNB Chain suffered the most individual attacks with 36 incidents, while Ethereum witnessed 26 incidents. Arbitrum, which had no incidents in Q2 2022, witnessed 10 incidents, followed by Polygon and ZKSync with 2 incidents each.
- In total, **$10,451,189** has been recovered from stolen funds in **8** specific situations. This number represents just **3.9%** of the total losses in Q2 2023.

KEY INSIGHTS IN Q2 2023

- The rise in targeted attacks and scams on Arbitrum-based projects continues as we move into 2023. For two consecutive quarters this year, Arbitrum has remained the third most targeted blockchain, reaching a total of 18 significant incidents reported YTD.
- While the number of total losses is down 60.4% from Q2 2022, mostly likely due to market conditions affecting the Total Value Locked (TVL) in the ecosystem, attacks spiked: the number of single incidents increased 65.3% YoY from 49 to 81 in Q2 2023, and rose 11% quarter over quarter.
- Atomic Wallet's hack has been linked to the North Korean state-backed Lazarus Group, which has allegedly been responsible for some of the largest-scale exploits in the ecosystem, including the $100 million Harmony Bridge hack in June 2022.

Top 10 Losses in Q2 2023*

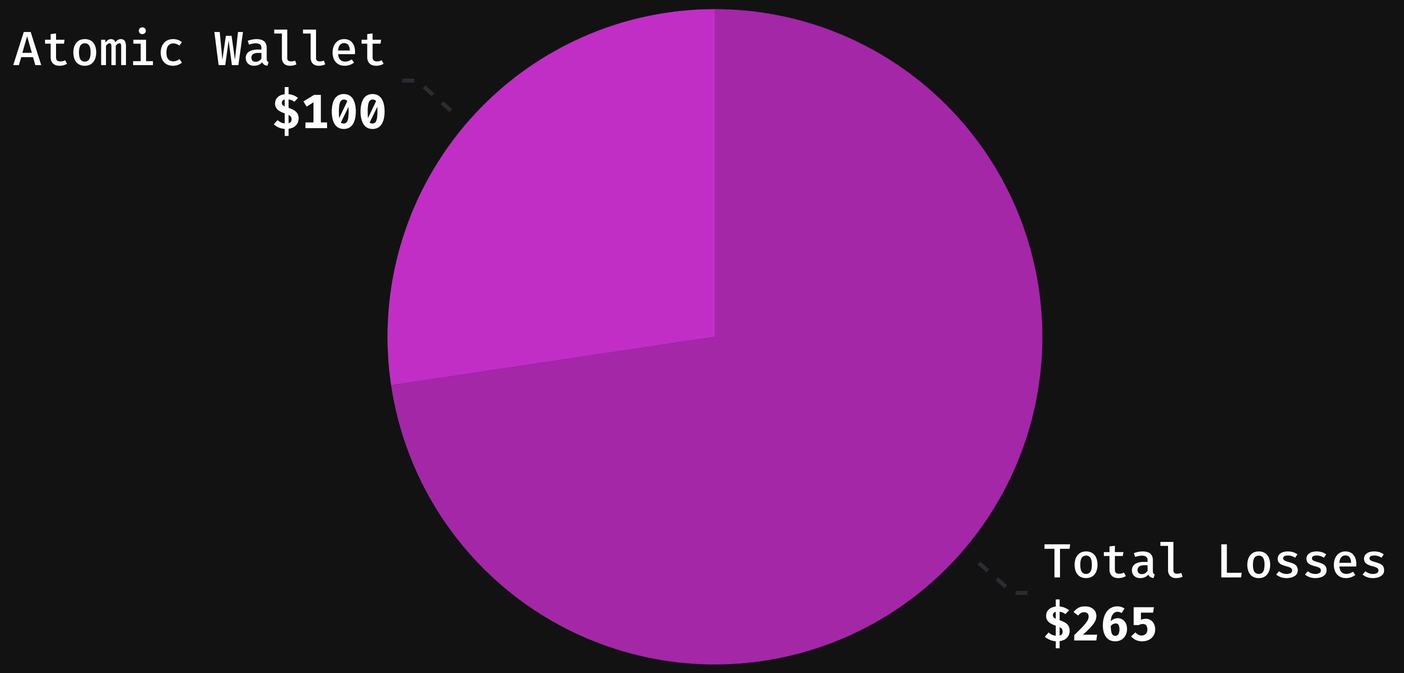
Atomic Wallet	$100,000,000
Fintoch	$31,600,000
Ethereum MEV bots	$25,000,000
Bitrue	$23,000,000
GDAC	$14,000,000
Yearn Finance	$11,600,000
Jimbos Protocol	$7,500,000
Hundred Finance	$7,400,000
Deus Finance	$6,380,000
Terraport Finance	$4,000,000

Major Exploits in Q2 Analysis

Most of the Q2 loss sum was lost by 2 specific projects, Atomic Wallet and Fintoch, totaling $131,600,000. Together, these two projects represent 49.6% of Q2 losses alone.

ATOMIC WALLET, $100 MILLION

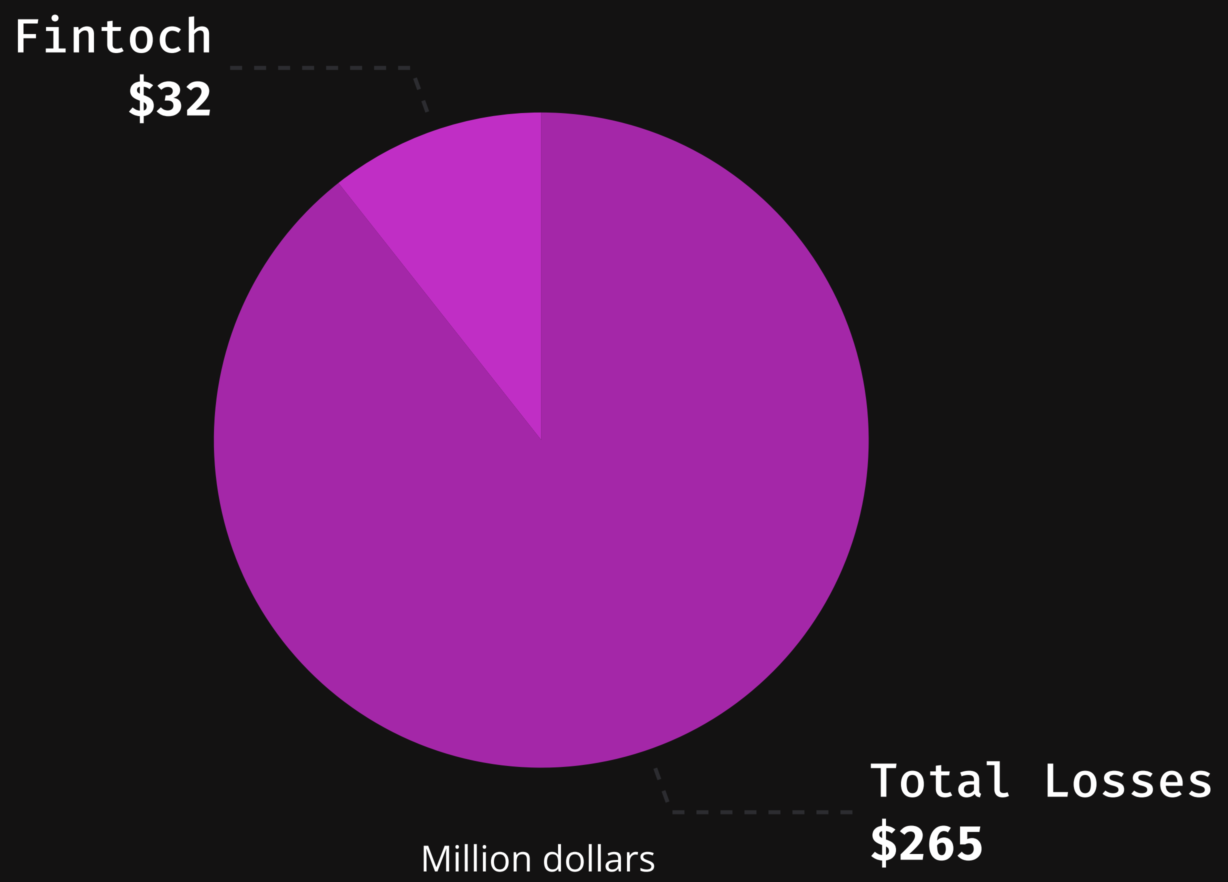
- On June 3rd, 2023, cybercriminals hacked the non-custodial, decentralized Atomic Wallet taking at the time $35 million-worth of digital tokens. The attack was later linked to the Lazarus Group, and the total loss amount calculation reached $100 million.



Million dollars

FINTOCH, $31.6 MILLION

- On May 23rd, 2023, the Fintoch team allegedly executed a major rug pull of its own project, amounting to $31.6 million in stolen funds. Users reported being unable to access their funds, as the team transferred the stolen assets to other blockchains, including Tron and Ethereum.



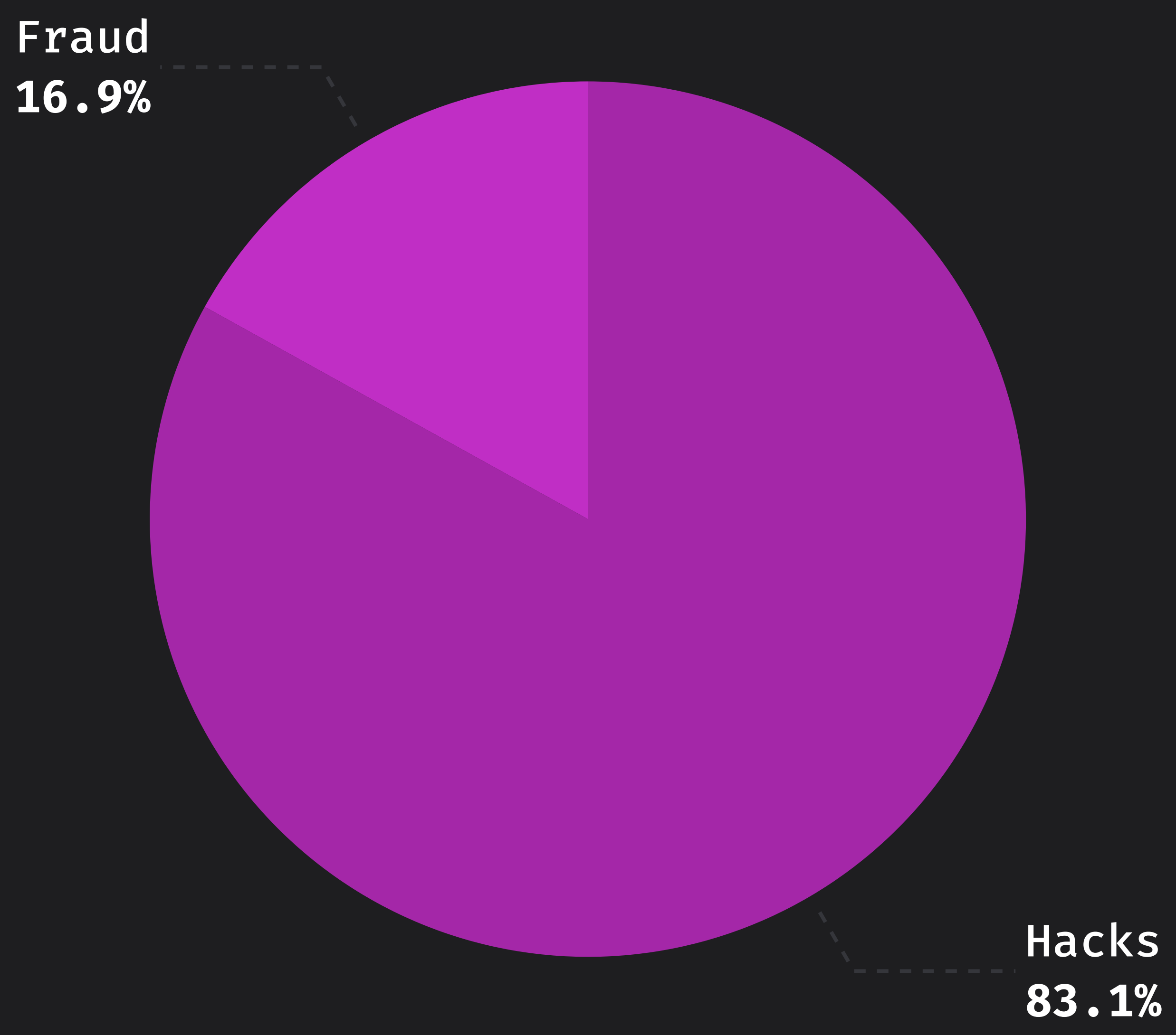
Million dollars

Hacks vs. Fraud Analysis

In Q2 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 16.9% of the total losses in the Q2 2023, while hacks account for 83.1%.

OVERVIEW

- **Hacks**
  In total, we have seen a loss of **$220,522,129** to hacks in Q2 2023 across 63 specific incidents. These numbers represent a 66.4% decrease compared to Q2 2022, when losses caused by hacks totaled $656,680,280.
- **Fraud**
  In total, we have seen a loss of **$44,959,390** to fraud in Q2 2023 across 18 specific incidents. These numbers represent a 225.4% increase compared to Q2 2022, when losses caused by frauds, scams, and rug pulls totaled $13,818,000.

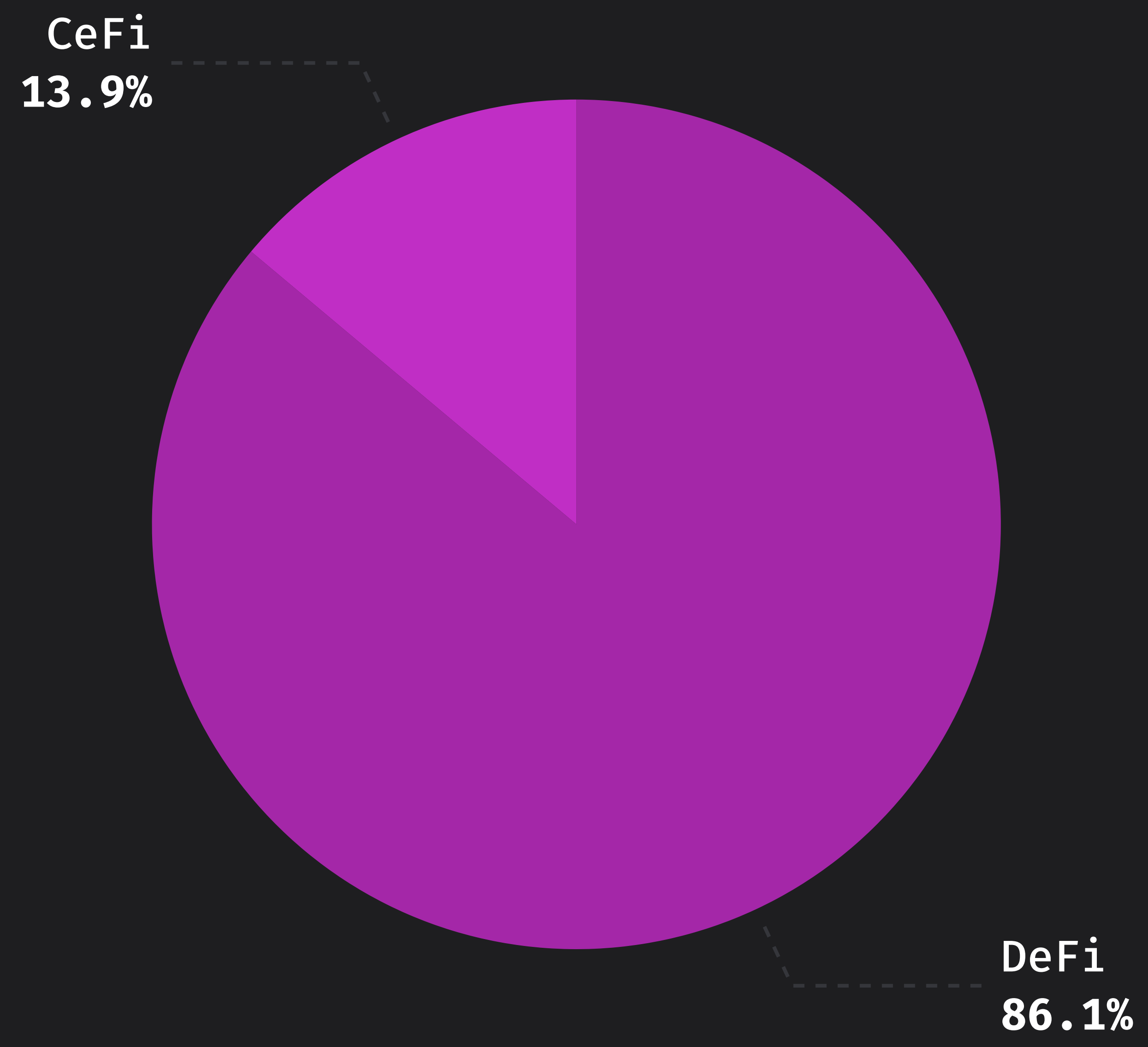


DeFi vs. CeFi Analysis

In Q2 2023, DeFi continues to be the main target for exploits, compared to CeFi. DeFi represents 86.1% of the total losses, while CeFi represents 13.9% of the total losses.

OVERVIEW

- **DeFi**
  DeFi has suffered **$228,481,519** in total losses in Q2 2023 across 79 incidents. These numbers represent a 65.9% decrease compared to Q2 2022, when DeFi losses totaled $670,498,280.
- **CeFi**
  CeFi has suffered **$37,000,000** in total losses in Q2 2023 across 2 incidents. In Q2 2022, no incidents were recorded on CeFi projects.



Losses by Chain

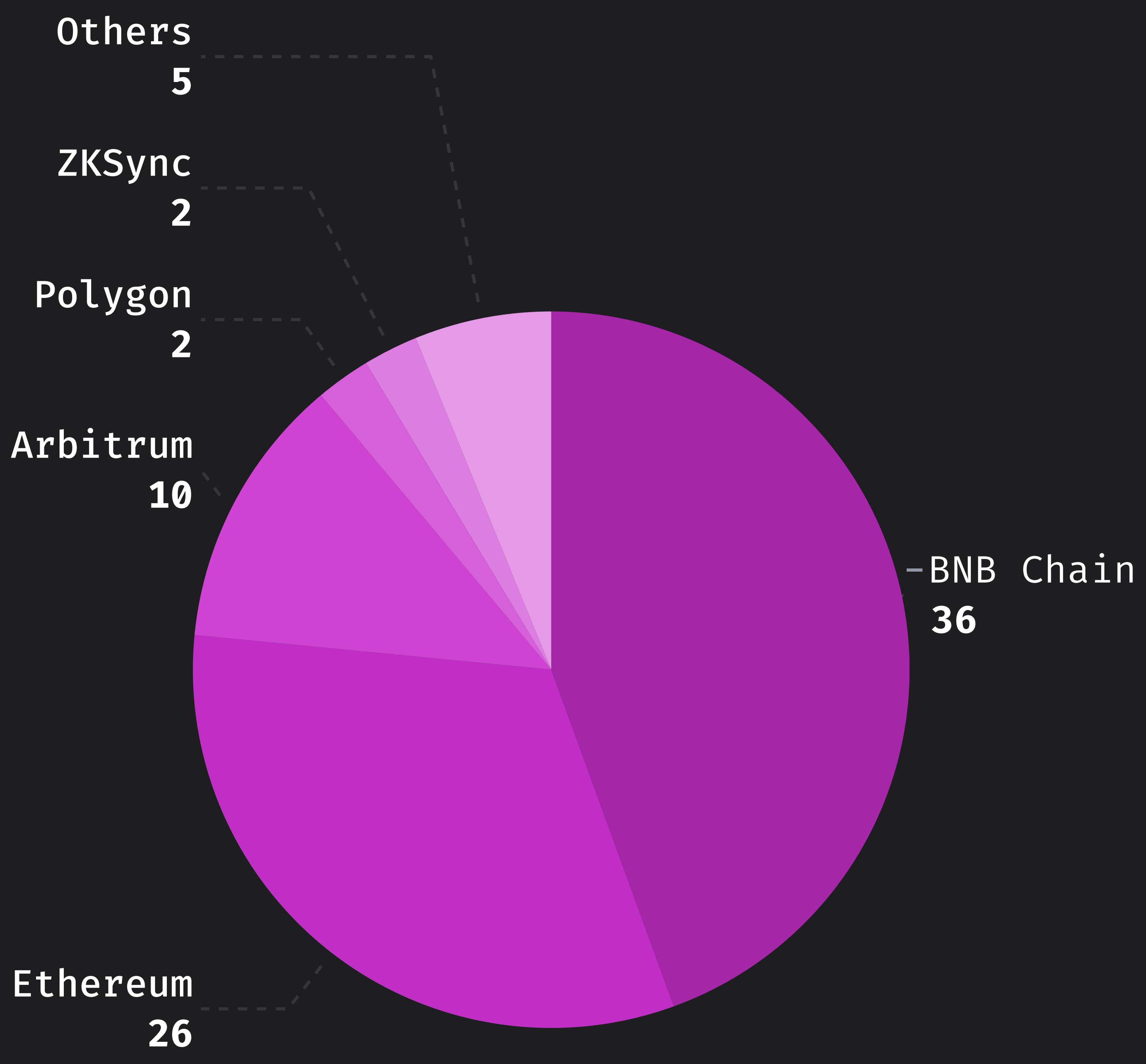
The two most targeted chains in Q2 2023 were BNB Chain and Ethereum. BNB Chain suffered the most individual attacks with 36 incidents, representing 44.4% of the total losses across targeted chains. Ethereum witnessed 26 incidents, representing 32.1% respectively.

OVERVIEW

- BNB Chain and Ethereum represent more than half of the chain losses in Q2 2023 at 76.5%. Arbitrum comes in third with 10 incidents, representing 12.1% of total losses across chains. Polygon and ZKSync follow with 2 incidents each. Remaining chains like Optimism, Terra, Sui Network, and others together represent 6.2% of the total chain incidents, all with single incidents.

INSIGHTS

- The rise in targeted attacks and scams on Arbitrum-based projects in 2023 continues when compared with the previous period. There was no recorded incident on Arbitrum in Q2 2022.



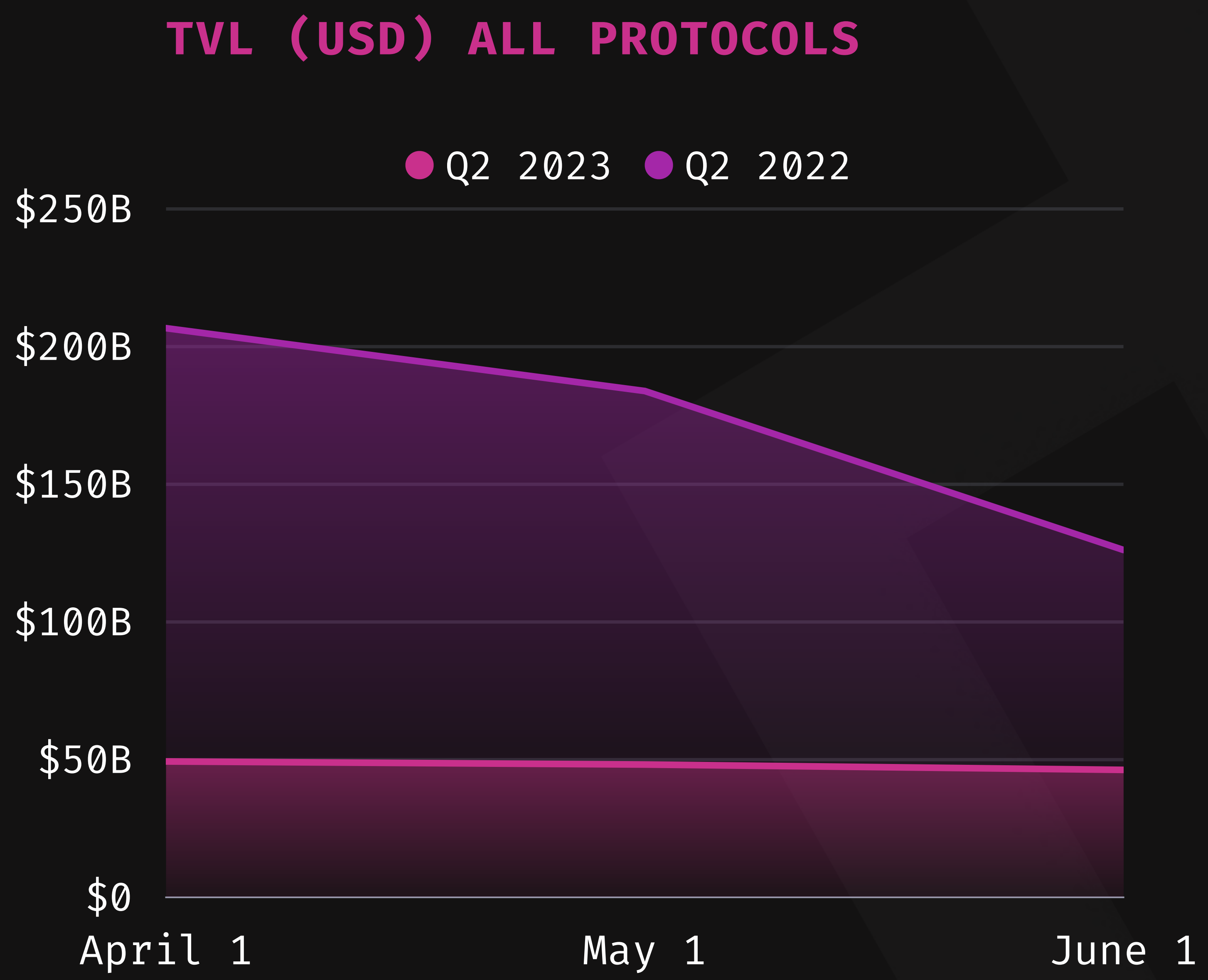
Funds Recovery

OVERVIEW

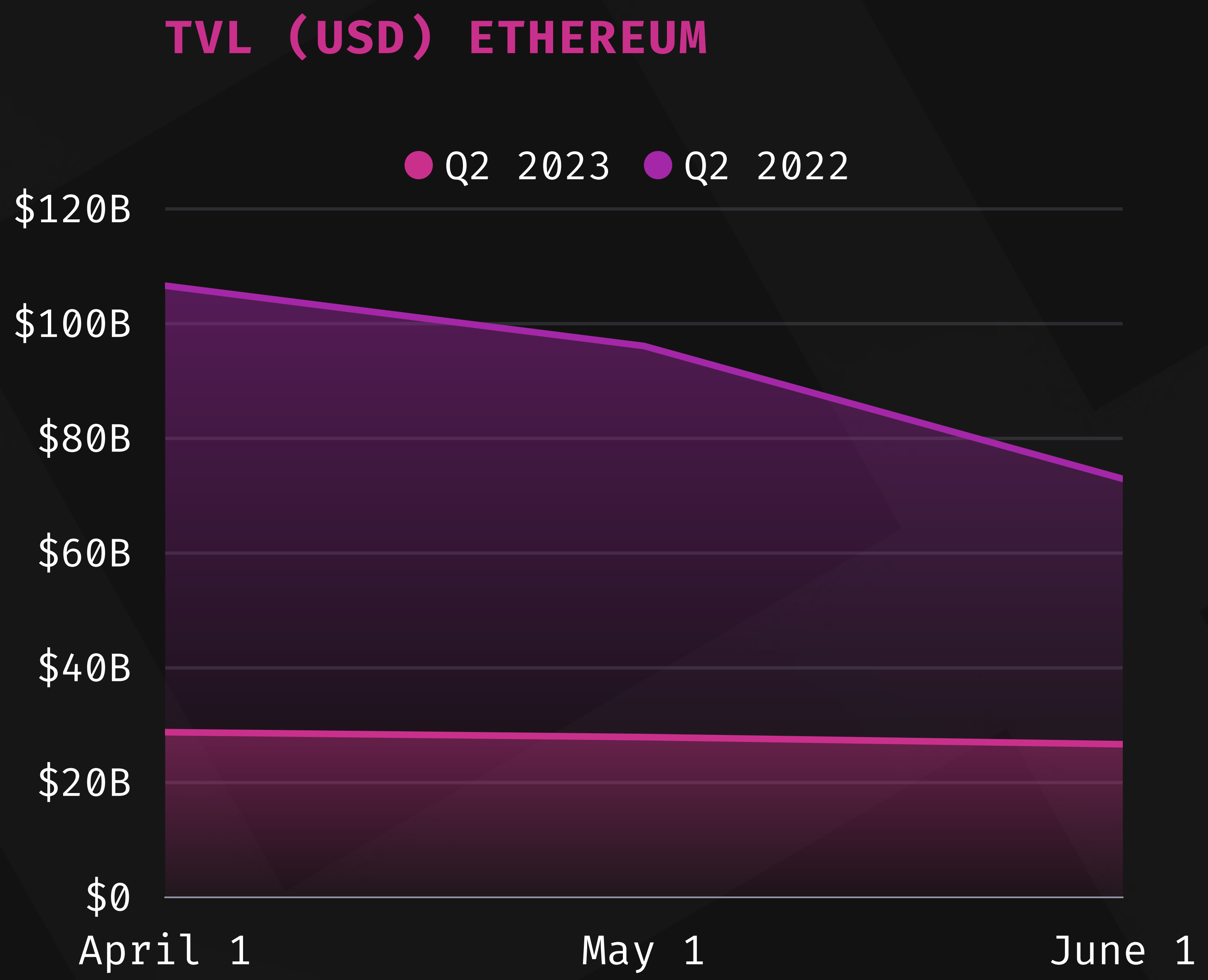
In total, **$10,451,189** has been recovered from stolen funds in **8** specific situations. This number makes up **3.9%** of the total losses in Q2 2023.

	Stolen	Recovered
Atomic Wallet	$100,000,000	$1,000,000
Deus Finance	$6,380,000	$5,500,000
SushiSwap	$3,340,000	$723,450
Sentiment	$969,000	$862,569
MetaPoint	$920,000	$63,000
FiLDA	$700,000	$560,000
EDE Finance	$580,000	$420,170
Allbridge	$570,000	$465,000

In Focus: Q2 2022 vs. Q2 2023



Total Value Locked



Total Value Locked

In Focus: Q2 2022 vs. Q2 2023

HACKS VS. FRAUDS

66.4% ↓

Hacks

Losses are down 66.4% when compared to the previous period.

225.4% ↑

Fraud

Losses are up 225.4% when compared to the previous period.

In Focus: Q2 2022 vs. Q2 2023

DEFI VS. CEFI

65.9% ↓

DeFi

Losses are down 65.9% when compared to the previous period.

* ↑

CeFi

Losses are up $37 million* when compared to the previous period.

*CeFi has suffered $37,000,000 in total losses in Q2 2023 across 2 incidents. In Q2 2022, there was no recorded incident on a CeFi project.

“

We have witnessed a considerable increase in rug pulls, both in terms of stolen funds and the number of incidents. As bad actors continue to expand their malicious activities and employ increasingly sophisticated scams, users must thoroughly assess projects.

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 **$80 million** in total bounties, while saving over **$25 billion** in user funds.

TOTAL BOUNTIES AVAILABLE

Immunefi offers over **$155 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:

- * Top 10 Losses in Q2 2023: ***$1 million*** in stolen funds were later recovered from the Atomic Wallet hacker; Deus Finance later recoved $5.5 million from the stolen funds.
- 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 rug pulls for its fraud category. A 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 $155M in rewards available on Immunefi — the leading bug bounty platform for web3.

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