Immunefi

CRYPTO LOSSES IN Q2 2024

PREPARED BY IMMUNEFI

Crypto Losses in Q2 2024

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 Q2 2024.

OVERVIEW

There is nearly **$100 billion** in capital locked across web3 protocols as of June 2024. 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 2024. We have located **72** such instances, including both successful and semi-successful hacking attempts, as well as alleged fraud.

In total, we have seen a loss of **$572,688,861** across the web3 ecosystem in Q2 2024. **$564,238,811** was lost to hacks across 53 specific incidents and **$8,450,050** was lost to fraud in across 19 specific incidents. Most of that sum was lost by two specific projects: DMM Bitcoin, a Japanese crypto exchange, suffered an attack that resulted in **$305,000,000** lost, and BtcTurk, Turkey's biggest cryptocurrency exchange, which incurred a loss of **$55,000,000.**

The total loss of Q2 2024 represents a **112% increase** compared to Q2 2023, when hackers and fraudsters stole **$265,481,519.**

Crypto Losses in Q2 2024

KEY TAKEAWAYS IN Q2 2024

- The 2 major exploits of the quarter totaled **$360,000,000** alone, accounting for **62.8%** of all losses in Q2 2024.
- In Q2 2024, hacks continued to be the predominant cause of losses at **98.5%** in comparison to fraud, which accounted for only **1.5%** of the total losses.
- CeFi was the main target of successful exploits at **70%** as compared to DeFi at **30%** of the total losses.
- The two most targeted chains in Q2 2024 were **Ethereum** and **BNB Chain**. Ethereum suffered the most individual attacks with 34 incidents, followed by BNB Chain with 18 incidents, and Arbitrum with **4** incidents.
- In total, **$26,736,000** has been recovered from stolen funds in **4** specific situations. This number makes up **5%** of the total losses in Q2 2024.

KEY INSIGHTS IN Q2 2024

- $920,940,078 was lost due to hacks and fraud year-to-date, up by **24%** compared with the previous period at $702,965,135.
- Q2 2024 was marked by a considerable increase in the total number of losses, up by **112%** compared to Q2 2023, amounting to $265,481,519.
- Overall, May and June witnessed the highest volume of losses in Q2 2024. May reached $358,523,484 in total losses, and June reached $141,558,550.
- The number of individual successful attacks decreased by **11%** from 81 in Q2 2023 to 72 in Q2 2024.
- In Q2 2024, Ethereum once again surpassed BNB Chain, becoming the most targeted chain compared to the previous period.
- In Q2 2024, funds recovery has proven slightly more effective than in the previous period. To date, **5%** of stolen funds have been recovered, compared to the **3.9%** recovered in Q2 2023.

Top 10 Losses in Q2 2024*

DMM Bitcoin	$305,000,000
BtcTurk	$55,000,000
Hedgey	$44,600,000
Lykke	$23,600,000
Gala Games*	$21,000,000
SonneFinance	$20,000,000
UwU Lend	$19,300,000
Rain	$14,800,000
Holograph	$14,400,000
Velocore	$6,800,000

Major Exploits in Q2 Analysis

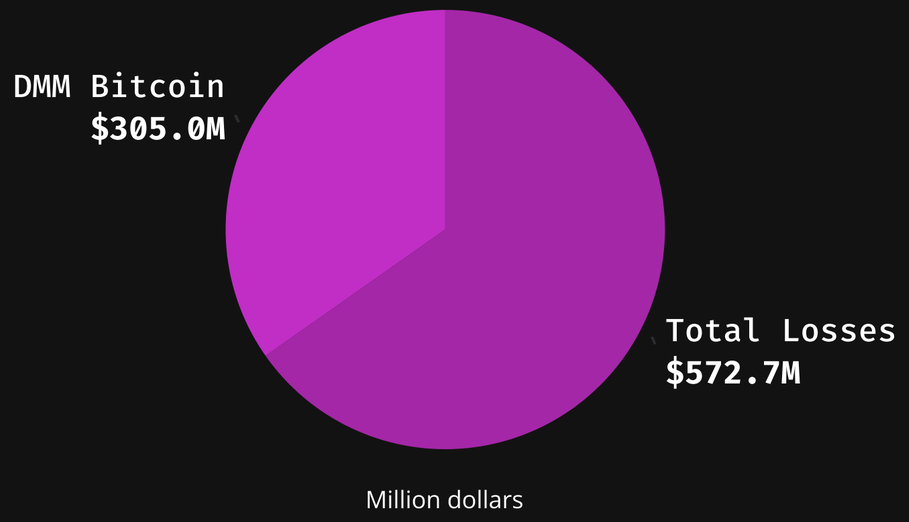
Most of that sum was lost by two specific projects: DMM Bitcoin and BtcTurk, totaling **$360,000,000**. Together, these two projects represent **62.8%** of Q2 losses alone.

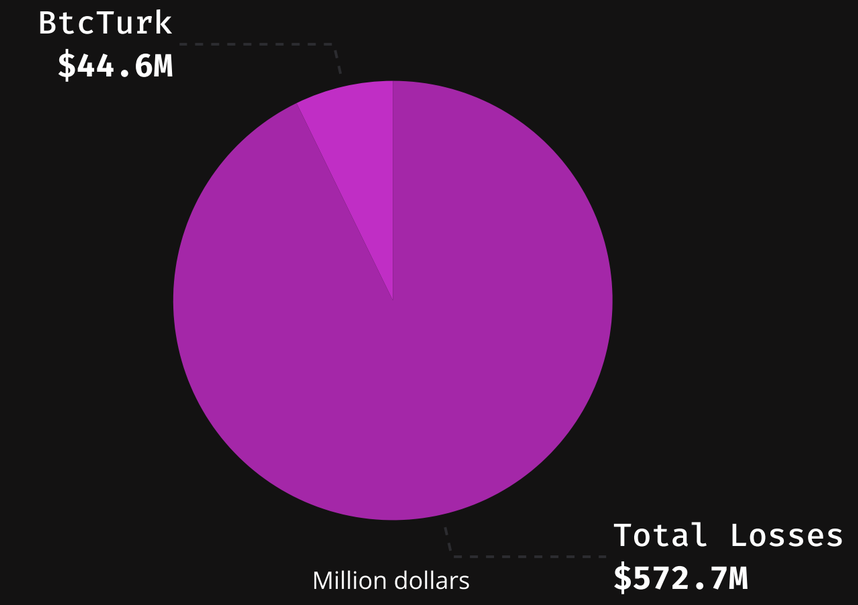
DMM BITCOIN, $305 MILLION

- On May 31 2024, DMM Bitcoin, a Japanese cryptocurrency trading platform, fell victim to a hack resulting in a massive loss of Bitcoin worth around $305 million.

BTCTURK, $55 MILLION

- On June 23, 2024, BtcTurk, a Turkish crypto exchange, suffered a cyberattack amounting to $55 million of lost funds.



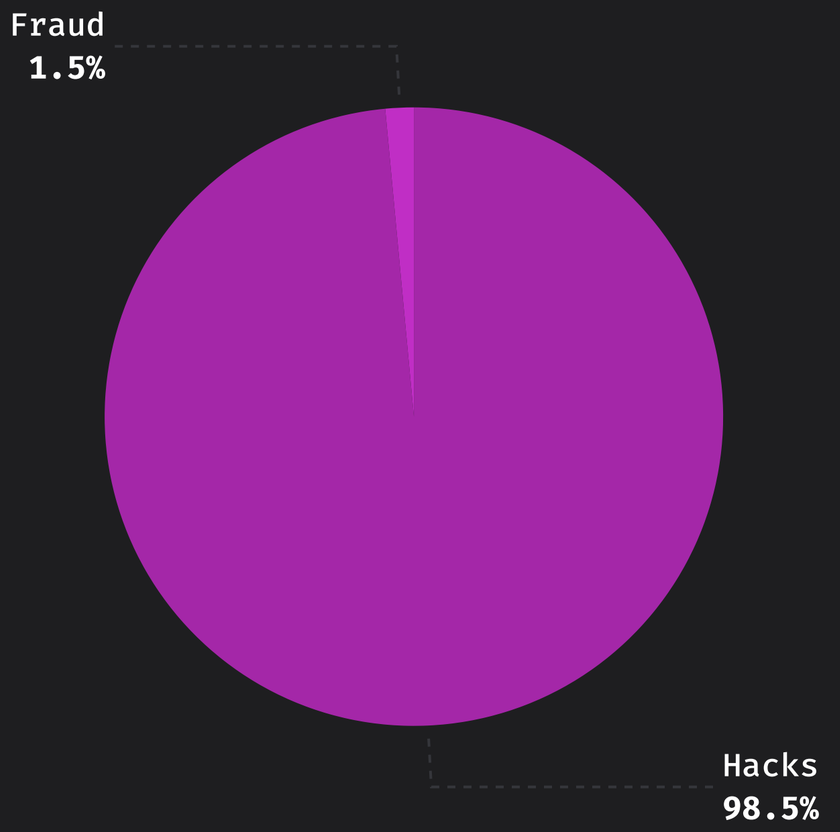


Hacks vs. Fraud Analysis

In Q2 2024, hacks continue to be the predominant cause of losses as compared to fraud. An analysis of the losses shows that fraud accounts for only 1.5% of the total losses in Q2 2024 while hacks account for 98.5%.

OVERVIEW

- **Hacks**
  In total, we have seen a loss of **$564,238,811** to hacks in Q2 2024 across 53 specific incidents. These numbers represent a 155% increase compared to Q2 2023, when losses caused by hacks totaled **$220,522,129.**
- **Fraud**
  In total, we have seen a loss of **$8,450,050** to fraud in Q2 2024 across 19 specific incidents. These numbers represent a 81% decrease compared to Q2 2023, when losses caused by frauds, scams, and rug pulls **totaled $44,959,390.**

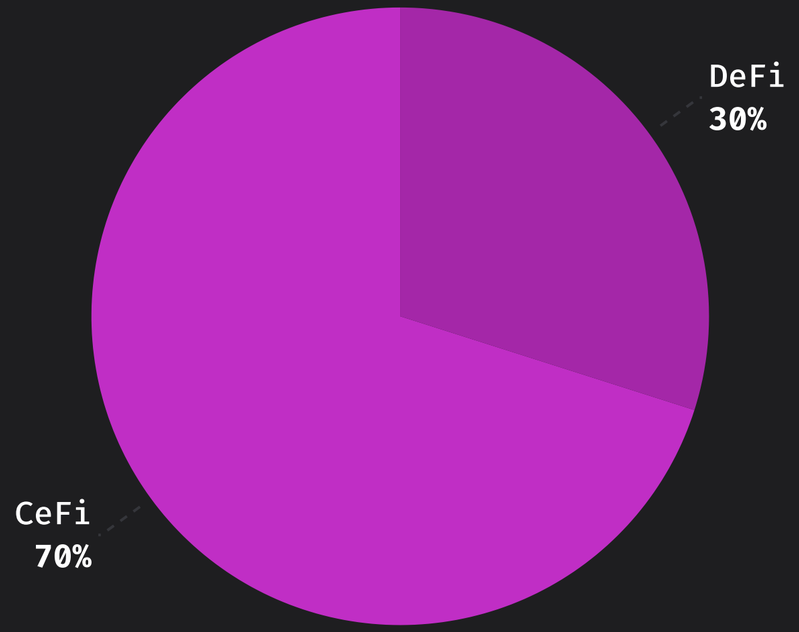


DeFi vs. CeFi Analysis

In Q2 2024, CeFi was the main target for exploits, representing 70% of total losses, while DeFi represented 30%.

OVERVIEW

- **DeFi**
  DeFi has suffered **$171,288,861** in total losses in Q2 2024 across 62 incidents. These numbers represent a 25% decrease compared to Q2 2023, when DeFi losses totaled **$228,481,519.**
- **CeFi**
  CeFi has suffered **$401,400,000** in total losses in Q2 2024 across 5 incidents. These numbers represent a 984% increase compared to Q2 2023, when CeFi losses totaled **$37,000,000.**



Losses by Chain

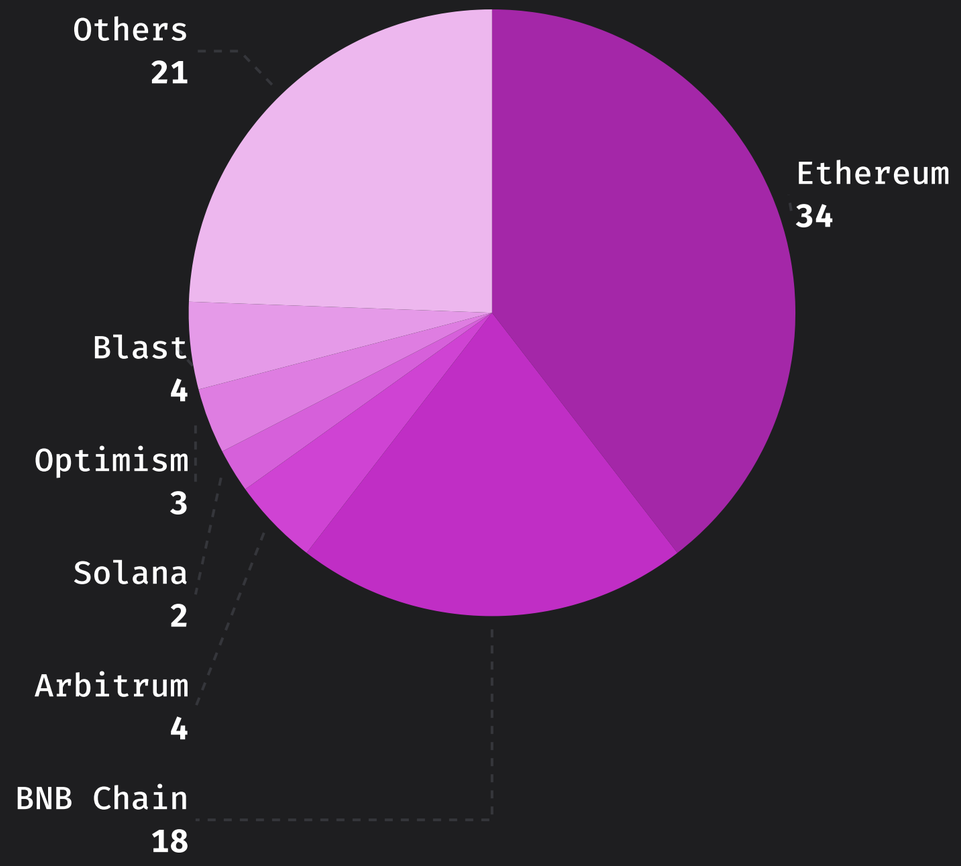
The two most targeted chains in Q2 2024 were Ethereum and BNB Chain. Ethereum suffered the most individual attacks with 34 incidents, representing 46.6% of the total losses across targeted chains. BNB Chain witnessed 18 incidents, representing 24.7% respectively.

OVERVIEW

- In Q2 2024, Ethereum and BNB Chain accounted for over half of the chain losses, totaling 71%.
- Arbitrum comes in third with 4 incidents, representing 5.5% of total losses across chains. Blast and Optimism follow with 3 incidents each. Remaining chains like Polygon, Solana, Fantom, Linea, Mantle, TON, and others together represent 15% of the total chain incidents, all with single incidents.

INSIGHTS

- In Q2 2024, Ethereum once again surpassed BNB Chain, becoming the most targeted chain compared to the previous period.



Funds Recovery

OVERVIEW

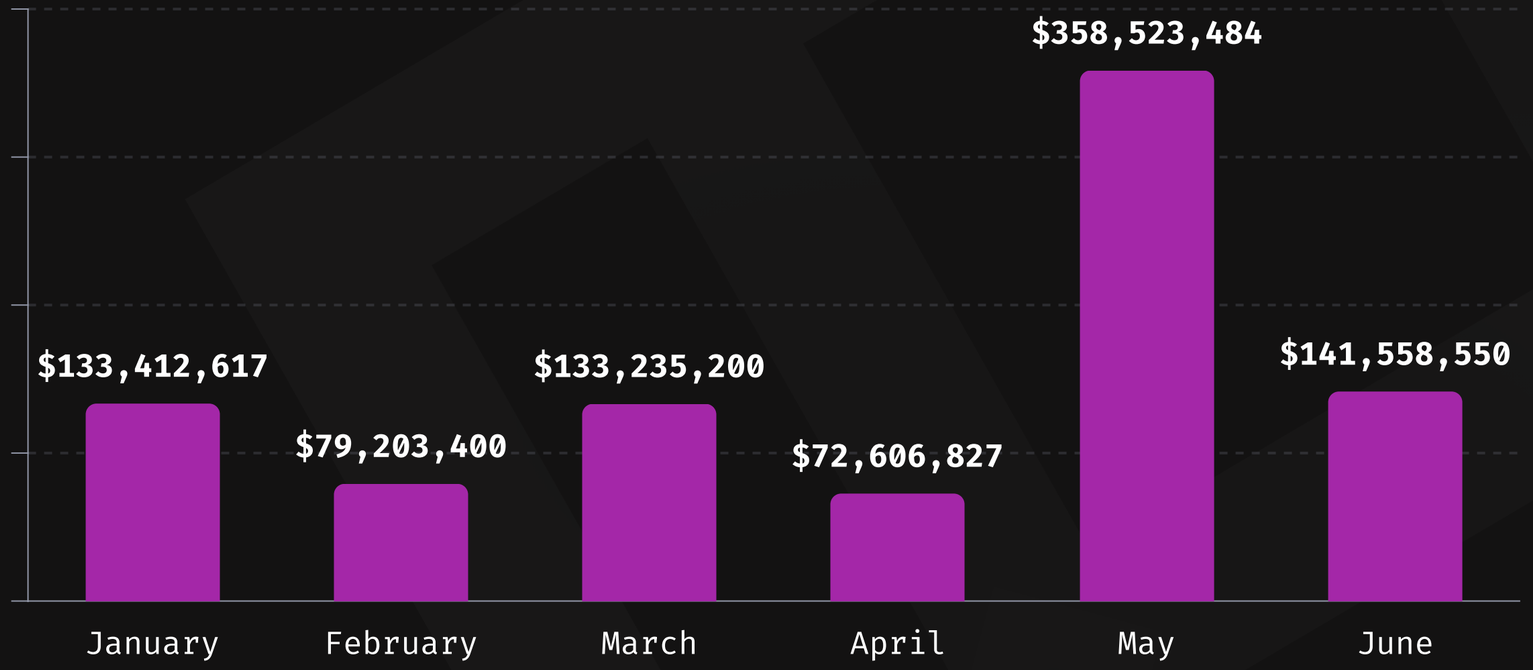
In total, **$26,736,000** has been recovered from stolen funds in **4** specific situations. This number makes up **5%** of the total losses in Q2 2024.

	Stolen	Recovered
Bloom	$540,000	$486,000
ALEX Lab	$4,300,000	$3,900,000
Gala Games*	$21,000,000	$21,000,000
YOLO Games	$1,500,000	$1,350,000

In Focus: Crypto Losses YTD

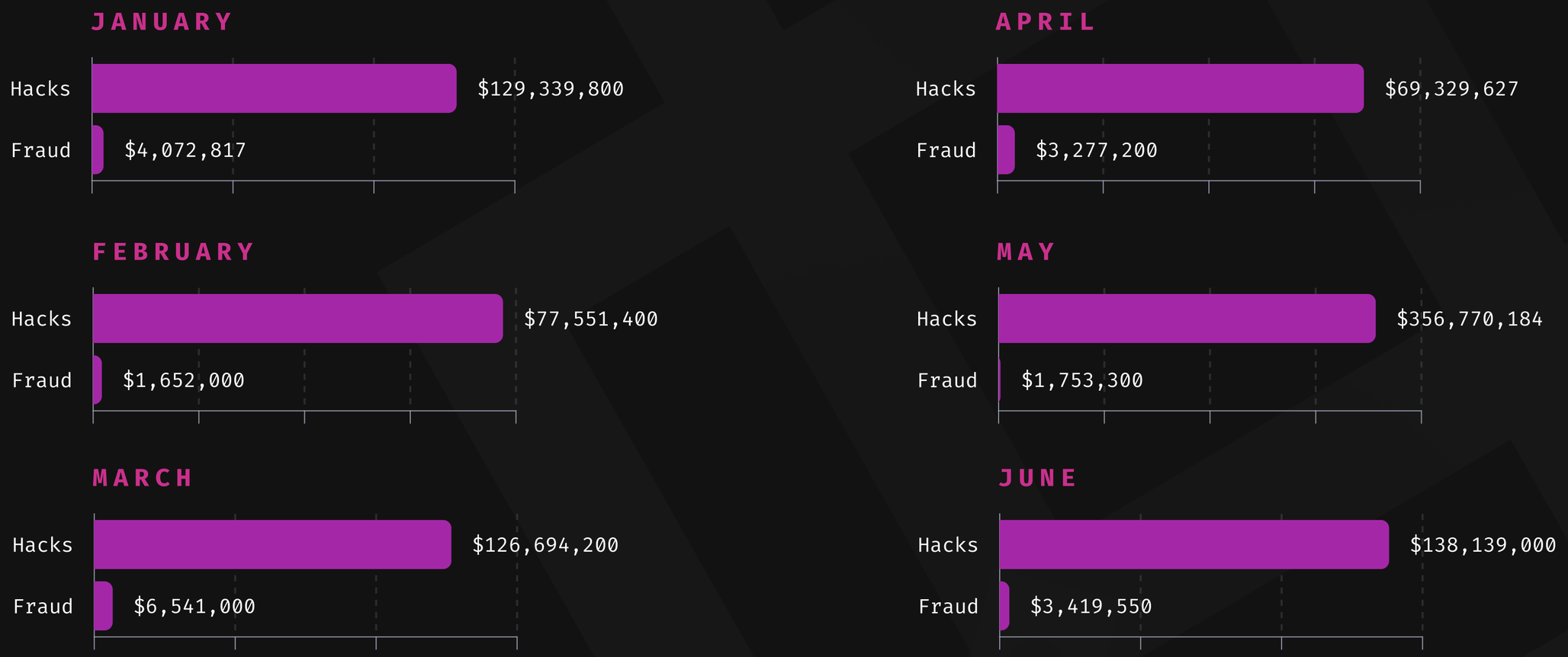
MONTHLY OVERVIEW

In total, the ecosystem has witnessed **$920,940,078** in losses year-to-date (YTD) across 135 specific incidents. Overall, the losses were primarily driven by over **$358 million** lost in May.

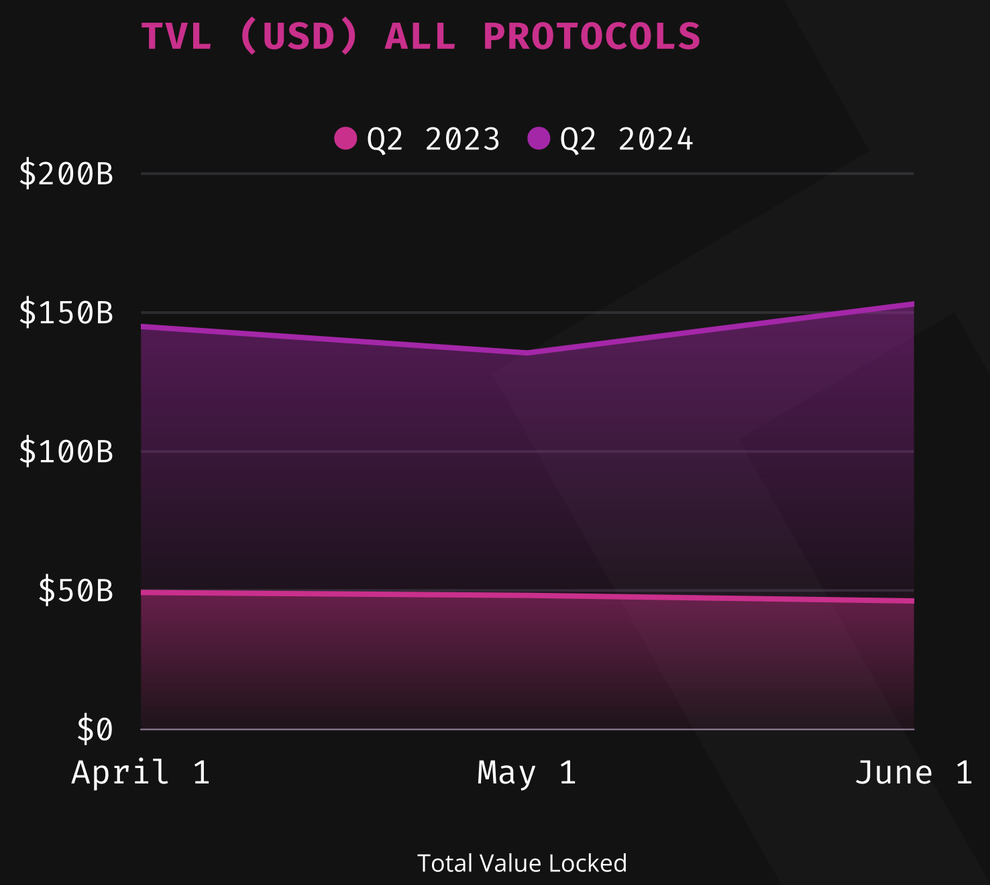


In Focus: Crypto Losses YTD

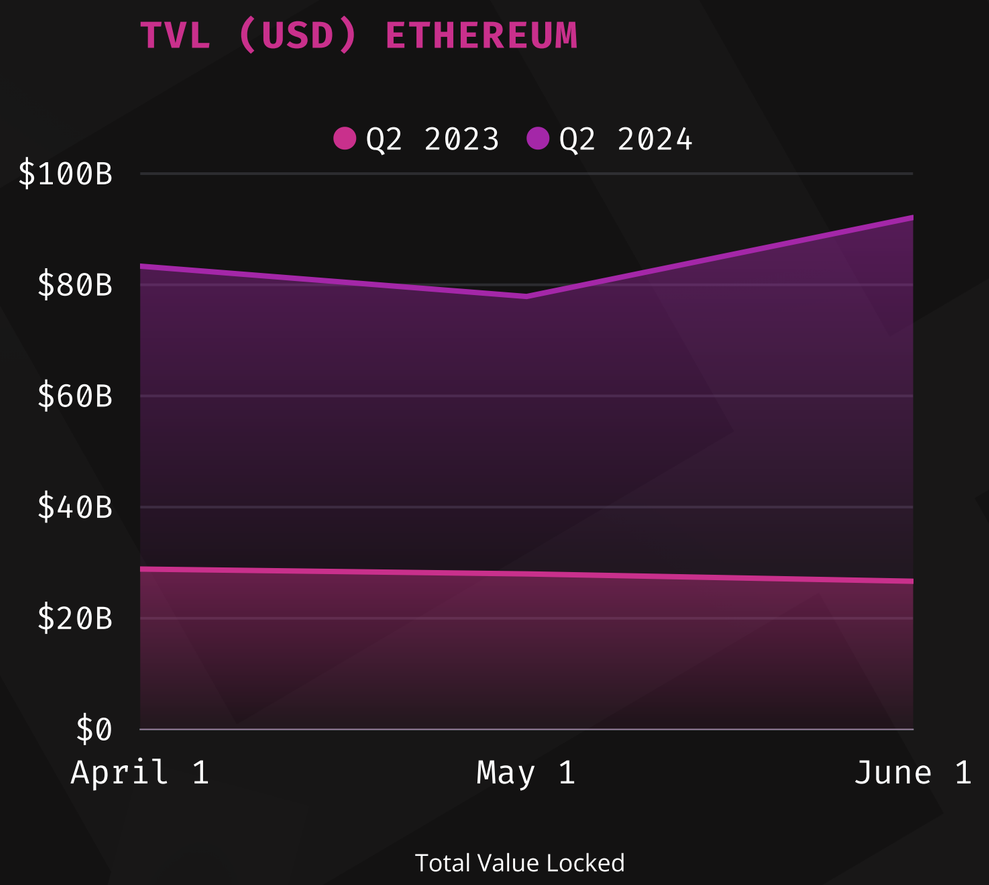
TOTAL LOSSES YTD: HACKS VS. FRAUD



In Focus: Q2 2023 vs. Q2 2024



Total Value Locked



Total Value Locked

In Focus: Q2 2023 vs. Q2 2024

HACKS VS. FRAUDS

155%

Hacks

Losses are up 155% when compared to the previous period.

81%

Fraud

Losses are down 81% when compared to the previous period.

In Focus: Q2 2023 vs. Q2 2024

DEFI VS. CEFI

25%

DeFi

Losses are down 25% when compared to the previous period.

984%

CeFi

Losses are up 984% when compared to the previous period.

“

This quarter highlights how infrastructure compromises can be the most devastating hacks in crypto, as a single compromise can lead to millions in damages. This was evident during this quarter, where losses surged primarily due to hacks targeting CeFi infrastructure, surpassing DeFi, despite a smaller number of hacks in that sector. Robust measures to safeguard the entirety of the ecosystem are crucial.

Mitchell Amador
Founder and CEO at Immunefi

Crypto Losses Q2 2024

Immunefi

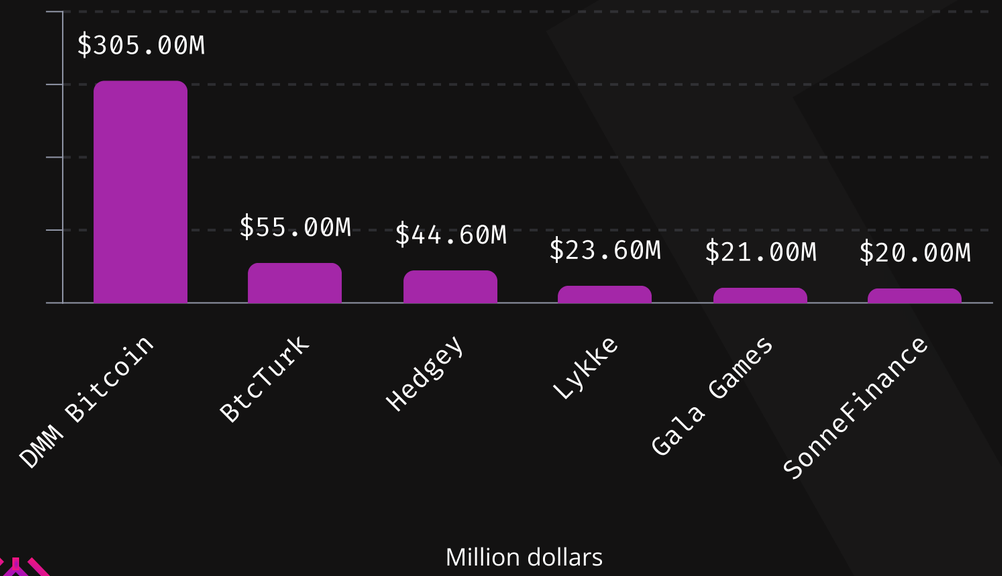
TOTAL LOSSES IN Q2

$572,688,861

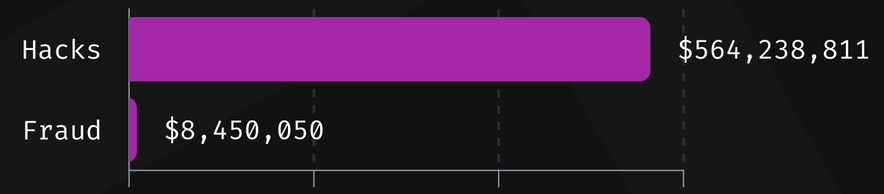
YTD

$920,940,078

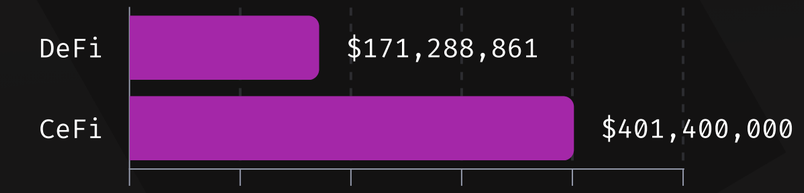
MAJOR LOSSES



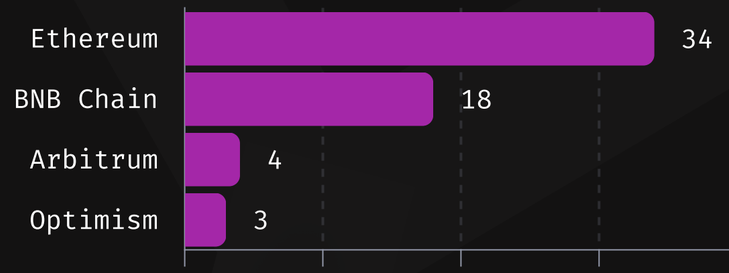
HACKS VS. FRAUD



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 **$100 million** in total bounties, while saving over **$25 billion** in user funds.

TOTAL BOUNTIES AVAILABLE

Immunefi offers over **$163 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 2024 & Funds Recovery: $21 million in stolen funds were later recovered from the Gala Games hack. The Gala Games hacker was able to trade 600 million GALA tokens for 5,913 Ethereum, amounting to about $21 million USD, and the effective burn of 4.4 billion GALA tokens. The hacker later returned the 5,913 Ethereum to Gala's wallet.
- 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 $157M in rewards available on Immunefi — the leading bug bounty platform for web3.

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