Immunefi

CRYPTO LOSSES IN Q1 2024

PREPARED BY IMMUNEFI

Crypto Losses in Q1 2024

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 2024.

OVERVIEW

There is nearly **$100 billion** in capital locked across web3 protocols as of March 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 Q1 2024. We have located 61 such instances, including both successful and semi-successful hacking attempts, as well as alleged fraud.

In total, we have seen a loss of **$336,311,217** across the web3 ecosystem in Q1 2024. **$321,645,400** was lost to hacks across 46 specific incidents and **$14,665,817** was lost to fraud in across 15 specific incidents. Most of that sum was lost by two specific projects: Orbit Bridge, the bridging service of the cross-chain protocol Orbit Chain, suffered an attack that resulted in $81,680,000 lost and Munchables, a Web3 project on the Blast blockchain, which incurred a loss of $62,800,000.

This number represents a **23.1%** decrease compared to Q1 2023, when hackers and fraudsters stole **$437,483,543.**

Crypto Losses in Q1 2024

KEY TAKEAWAYS IN Q1 2024

- The 2 major exploits of the quarter totaled **$144,480,000** alone, accounting for **43%** of all losses in Q1 2024.
- In Q1 2024, hacks continued to be the predominant cause of losses at **95.6%** in comparison to fraud, which accounted to only **4.4%** of the total losses.
- DeFi remained the primary target of successful exploits in Q1 2024, comprising **100%** of cases, while CeFi experienced no incidents.
- The two most targeted chains in Q1 2024 were **Ethereum** and **BNB Chain**. Ethereum suffered the most individual attacks with 33 incidents, followed by BNB Chain with 14 incidents, and Arbitrum with 6 incidents.
- In total, **$73,885,000** has been recovered from stolen funds in **7** specific situations. This number makes up **22%** of the total losses in Q1 2024.

KEY INSIGHTS IN Q1 2024

- Q1 2024 is marked by a considerable decrease in the total number of losses, down by **23.12%** compared to Q1 2023, amounting to $437,483,543.
- Overall, January witnessed the highest loss in Q1 2024.
- The number of attacks decreased by **17.57%** from 74 in Q1 2023 to 61 in Q1 2024.
- In Q1 2024, Ethereum once again surpassed BNB Chain and became the most targeted chain compared to the previous period.
- In Q1 2024, funds recovery has proven less effective than in the previous period. To date, **22%** of stolen funds have been recovered, compared to the 40.5% recovered in Q1 2023.

Top 10 Losses in Q1 2024 *

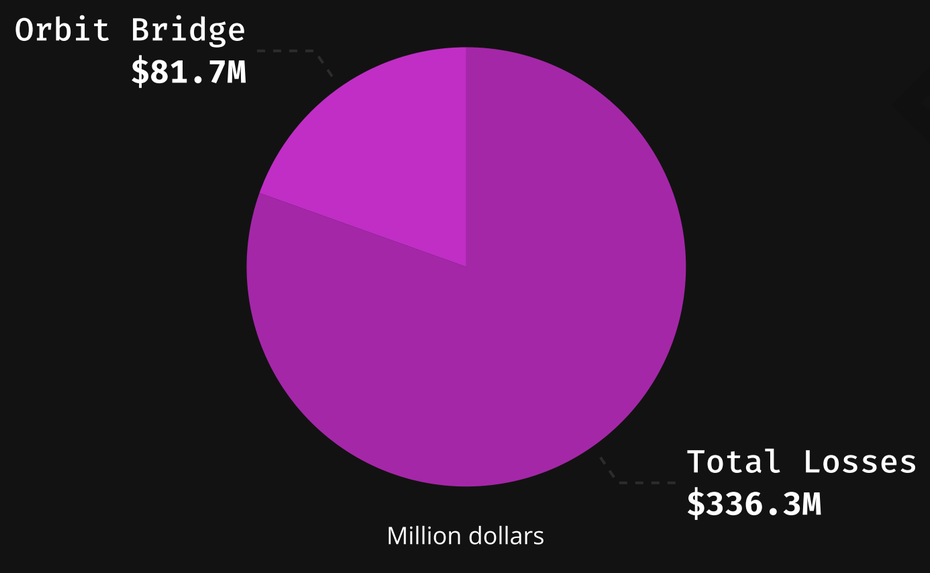
Orbit Bridge	$81,680,000
Munchables	$62,800,000
PlayDapp	$32,350,000
FixedFloat	$26,100,000
GMEE	$15,000,000
WOOFi	$8,750,000
Coinspaid	$7,500,000
Abracadabra Money	$6,500,000
Seneca	$6,500,000
Gamma Strategies	$6,200,000

Major Exploits in Q1 Analysis

Most of that sum was lost by two specific projects: Orbit Bridge and Munchables, totaling **$144,480,000**. Together, these two projects represent **43%** of Q1 losses alone.

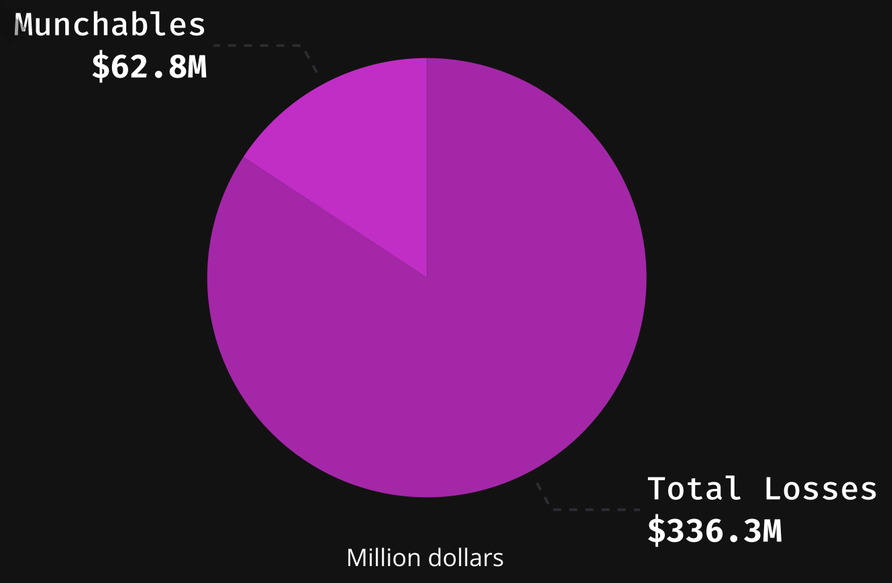
ORBIT BRIDGE, $81 MILLION

- On January 1, 2024, Orbit Bridge, the bridging service of the cross-chain protocol Orbit Chain, suffered an $81 million exploit. The attack was likely generated from compromised private keys, which the exploiter then leveraged to run unauthorized transactions.



MUNCHABLES, $62 MILLION

- On March 26, 2024, Munchables, an NFT game on the Ethereum layer 2 Blast, suffered an exploit resulting in over $62 million in losses*.

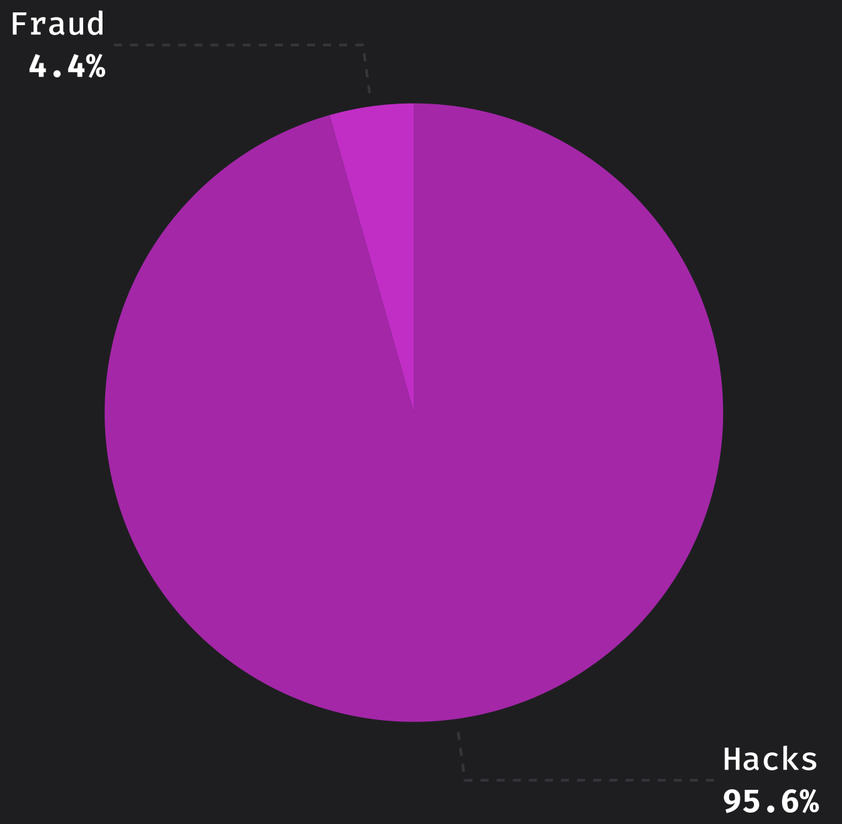


Hacks vs. Fraud Analysis

In Q1 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 4.4% of the total losses in the Q1 2024 while hacks account for 95.6%.

OVERVIEW

- **Hacks**
  In total, we have seen a loss of **$321,645,400** to hacks in Q1 2024 across 46 specific incidents. These numbers represent a 23.1% decrease compared to Q1 2023, when losses caused by hacks totaled $418,589,089.
- **Fraud**
  In total, we have seen a loss of **$14,665,817** to fraud in Q1 2024 across 15 specific incidents. These numbers represent a 22.4% decrease compared to Q1 2023, when losses caused by frauds, scams, and rug pulls totaled $18,894,454.

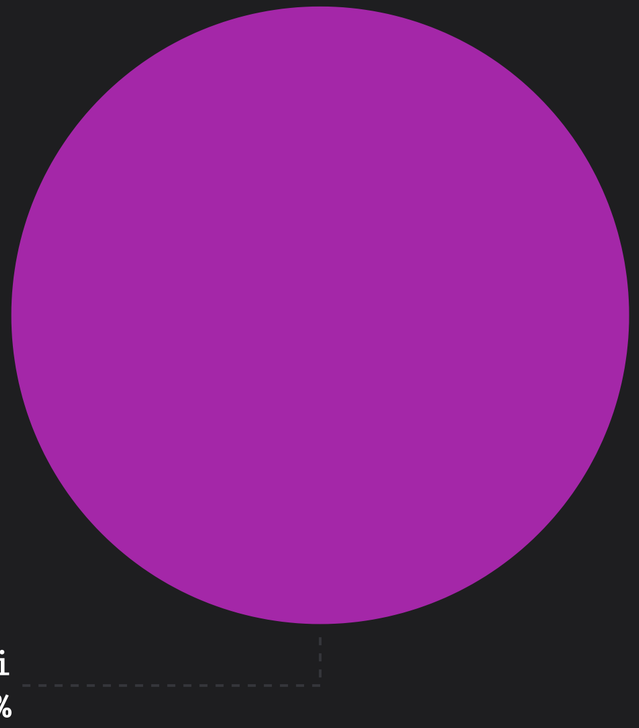


DeFi vs. CeFi Analysis

In Q1 2024, DeFi continues to be the main target for exploits, compared to CeFi. DeFi represented 100% of the total losses, while CeFi has not witnessed a single attack.

OVERVIEW

- **DeFi**
  DeFi has suffered **$336,311,217** in total losses in Q1 2024 across 61 incidents. These numbers represent a 22.8% decrease compared to Q1 2023, when DeFi losses totaled $435,675,543
- **CeFi**
  CeFi has not suffered from an attack in Q1 2024, compared to Q1 2023, when CeFi losses totaled $1,808,000.



Losses by Chain

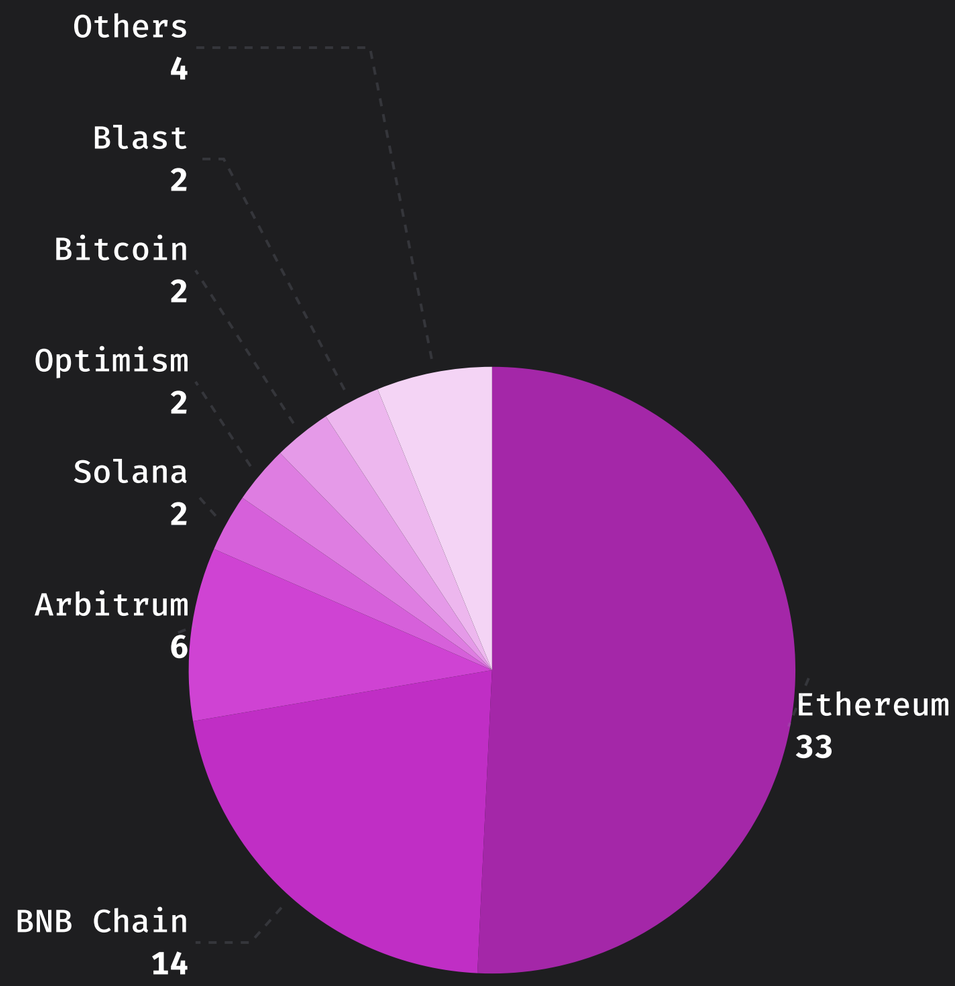
The two most targeted chains in Q1 2024 were Ethereum and BNB Chain. Ethereum suffered the most individual attacks with 33 incidents, representing 51% of the total losses across targeted chains. BNB Chain witnessed 14 incidents, representing 22% respectively.

OVERVIEW

- In Q1 2024, Ethereum and BNB Chain accounted for over half of the chain losses, totaling 73%.
- Arbitrum followed with 6 incidents, comprising 9.2%. Solana, Optimism, Bitcoin, and Blast had 2 incidents, each representing 3.1%. Other chains, including Polygon, Conflux Network, and Base, experienced 1 incident, each making up 1.5%.

INSIGHTS

- In Q1 2024, Ethereum once again surpassed BNB Chain and became the most targeted chain compared to the previous period.



Funds Recovery

OVERVIEW

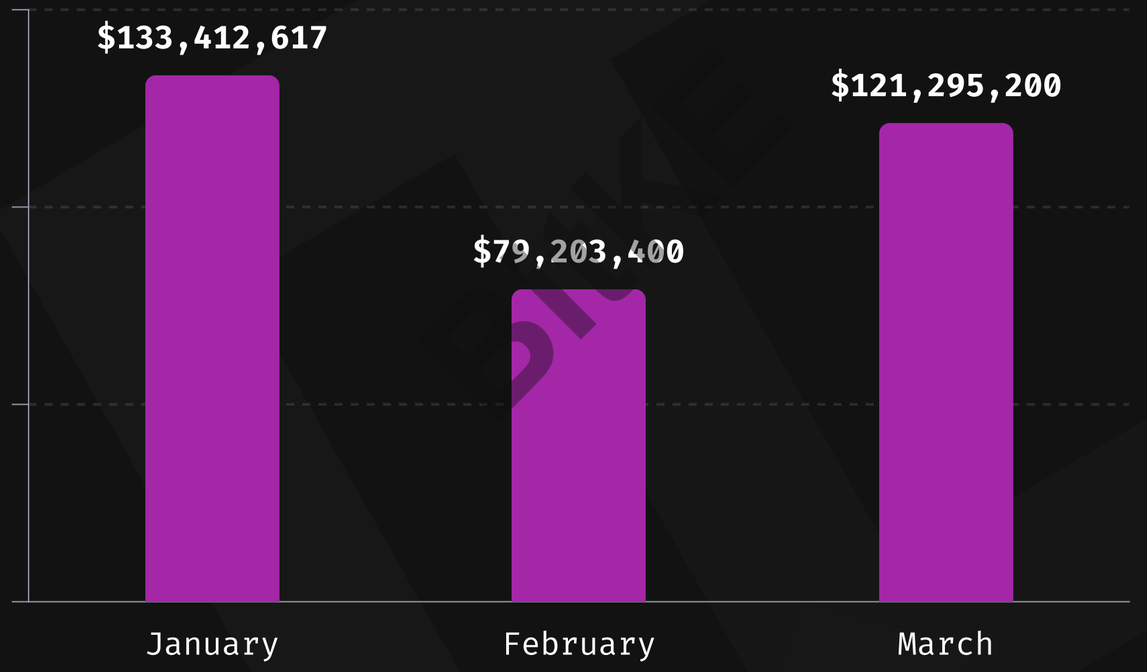
In total, **$73,885,000** has been recovered from stolen funds in **7** specific situations. This number makes up **22%** of the total losses in Q1 2024.

	Stolen	Recovered
Munchables	$62,800,000	$62,800,000
Seneca	$6,500,000	$5,300,000
Blueberry Protocol	$1,350,000	$1.080,000
Socket Bungee Bridge	$3,300,000	$2.300,000
Mozaic	$2,400,000	$2,160,000
Unizen	$2,100,000	$185,000
Saga DAO	$60,000	$60,000

In Focus: Crypto Losses YTD

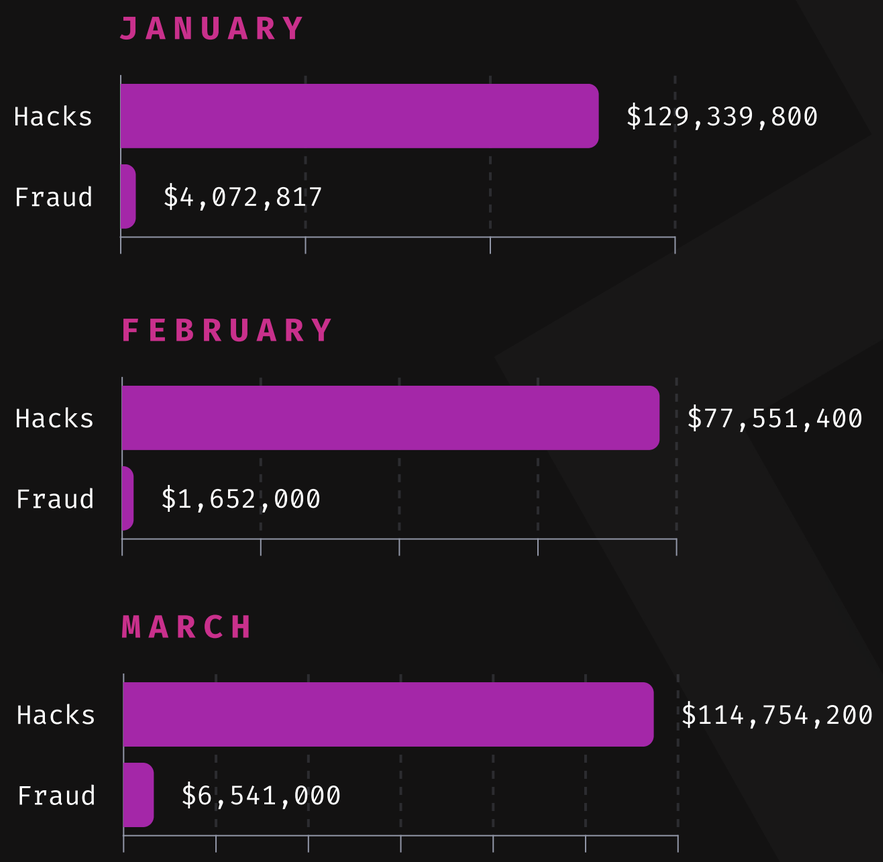
MONTHLY OVERVIEW

In total, the ecosystem has witnessed **$336,311,217** in losses year-to-date (YTD) across 61 specific incidents. Overall, the losses are primarily driven by over **$133 million** lost in January.

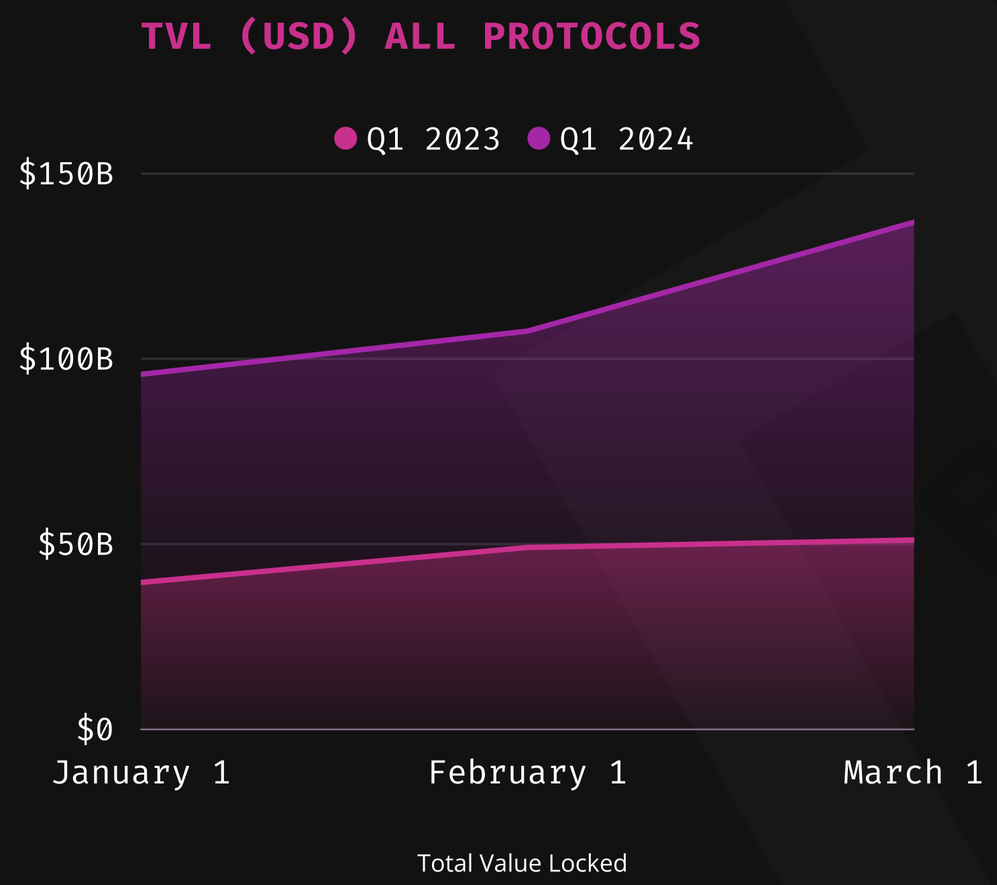


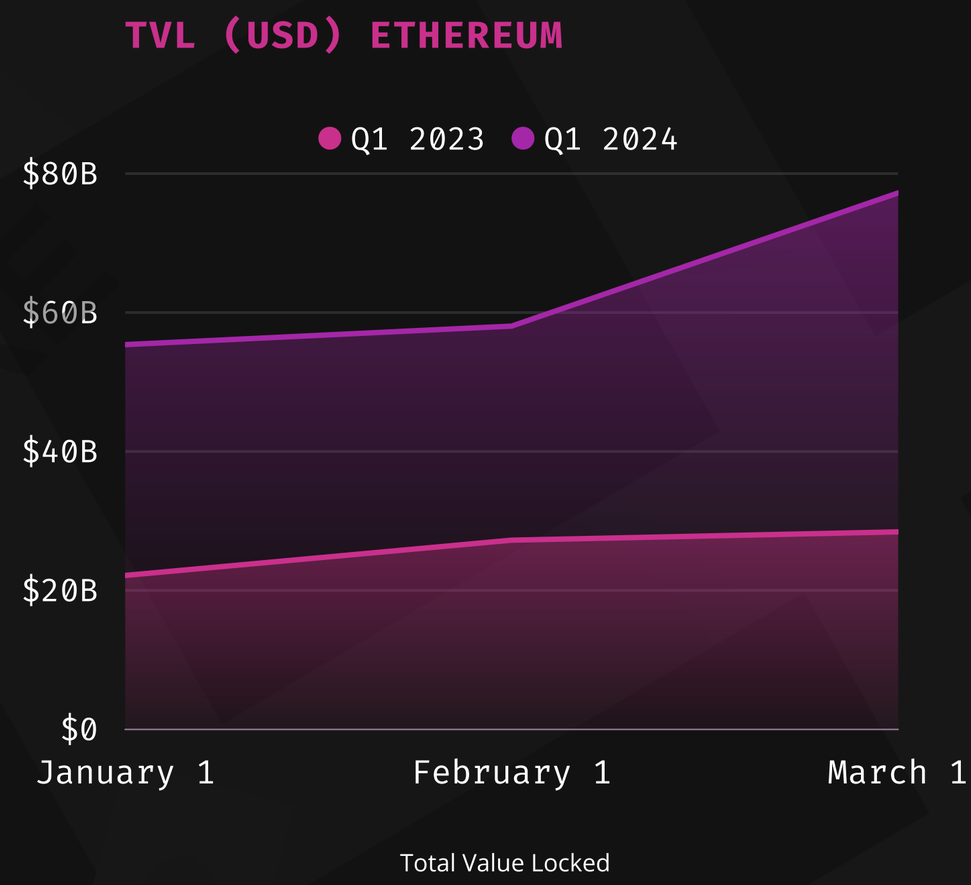
In Focus: Crypto Losses YTD

TOTAL LOSSES YTD: HACKS VS. FRAUD



In Focus: Q1 2023 vs. Q1 2024





In Focus: Q1 2023 vs. Q1 2024

HACKS VS. FRAUDS

23.1%

Hacks

Losses are down 23.1% when compared to the previous period.

22.4%

Fraud

Losses are down 22.4% when compared to the previous period.

In Focus: Q1 2023 vs. Q1 2024

DEFI VS. CEFI

22.8%

DeFi

Losses are down 22.8% when compared to the previous period.

100%

CeFi

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

“

While it's positive that overall losses have decreased, it's essential to note that DeFi faced significant challenges, accounting for 100% of total losses in Q1 2024. Particularly, the ecosystem witnessed a considerable volume of losses due to private key compromises, emphasizing the critical need to secure both code and protocol infrastructure.

Mitchell Amador
Founder and CEO at Immunefi

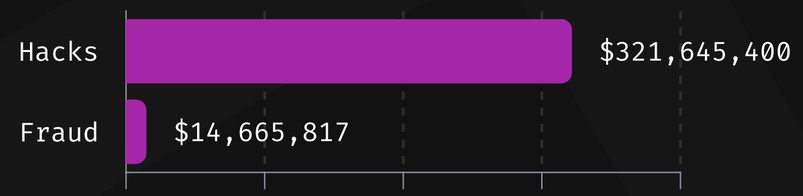
Crypto Losses Q1 2024

Immunefi

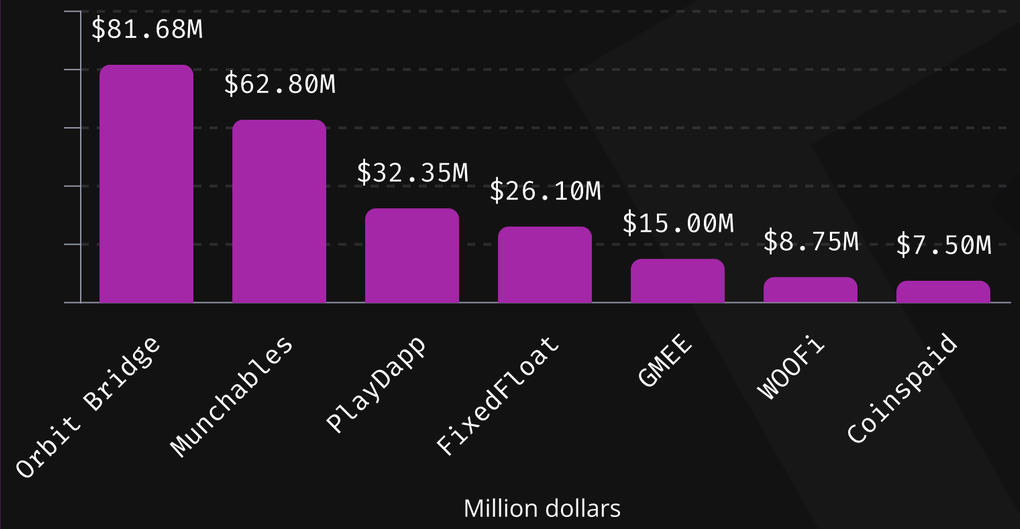
TOTAL LOSSES IN Q1

$336,311,217

HACKS VS. FRAUD

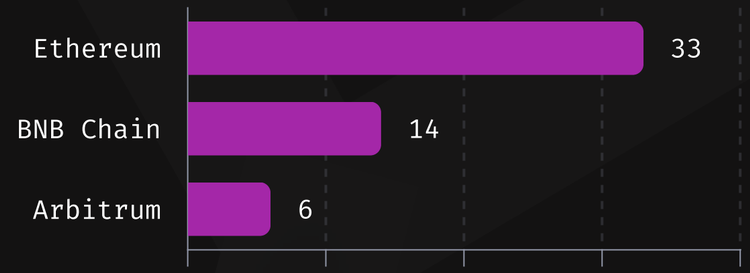


MAJOR LOSSES



DEFI VS. CEFI

TOP LOSSES BY CHAIN



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

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 **$95 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 Q1 2024: **$62million** in stolen funds were later recovered from the Munchables exploit and **$5.3 million** from the Seneca 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 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/**