Immunefi

CRYPTO LOSSES IN Q3 2024

PREPARED BY IMMUNEFI

Crypto Losses in Q3 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 Q3 2024.

OVERVIEW

There is nearly **$90 billion** in capital locked across web3 protocols as of September 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 Q3 2024. We have located **34** such instances, including both successful and semi-successful hacking attempts, as well as alleged fraud.

In total, we saw a loss of **$412,994,499** across the Web3 ecosystem in Q3 2024. **$409,906,947** was lost to hacks across 31 specific incidents, and **$3,087,552** was lost to fraud across 3 specific incidents. Most of that sum was lost by two specific projects: WazirX, India's leading domestic crypto exchange, which suffered an attack that resulted in **$235,000,000** lost, and BingX, a Singapore-based cryptocurrency exchange, which incurred a loss of **$52,000,000.**

The total loss of Q3 2024 represents a **40% decrease** compared to Q3 2023 when hackers and fraudsters stole **$685,970,444.**

Crypto Losses in Q3 2024

KEY TAKEAWAYS IN Q3 2024

- The 2 major exploits of the quarter totaled **$287,000,000** alone, accounting for **69.5%** of all losses in Q3 2024.
- In Q3 2024, hacks continued to be the predominant cause of losses at **99.25%** in comparison to fraud, which accounted for only **0.75%** of the total losses.
- CeFi was the main target of successful exploits at **74.8%** as compared to DeFi at **25.2%** of the total losses.
- The two most targeted chains in Q3 2024 were **Ethereum** and **BNB Chain**. Ethereum suffered the most individual attacks with 15 incidents, followed by BNB Chain with 8 incidents, and Base with **2** incidents.
- In total, **$14,900,000** has been recovered from stolen funds in **2** specific situations. This number makes up **3.6%** of the total losses in Q2 2024.

KEY INSIGHTS IN Q3 2024

- **$1,333,934,577** was lost due to hacks and fraud year-to-date, down by **3.9%** compared with the previous period at **$1,388,935,506.**
- Q3 2024 was marked by a decrease in the total number of losses, down by **40%** compared to Q3 2023, when losses totaled **$685,970,444**.
- Overall, July and September witnessed the highest volume of losses in Q3 2024. July reached **$281,919,252** in total losses, and September reached **$115,940,247.**
- The number of individual successful attacks decreased by **54%** from 75 in Q3 2023 to 34 in Q3 2024.
- In Q3 2024, Ethereum once again surpassed BNB Chain, becoming the most targeted chain compared to the previous period.
- In Q3 2024, funds recovery has proven less effective than in the previous period. To date, **3.6%** of stolen funds have been recovered, compared to the **8.9%** recovered in Q3 2023.

Top 10 Losses in Q3 2024*

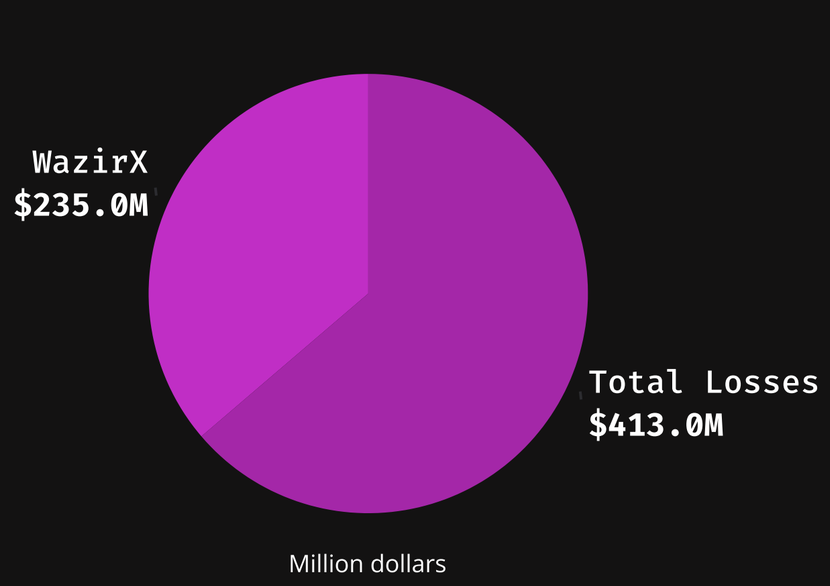
WazirX	$235,000,000
BingX	$52,000,000
Penpie	$27,000,000
Indodax	$22,000,000
Ronin	$12,000,000
LI.FI protocol	$10,000,000
Bittensor	$8,000,000
RHO Markets	$7,600,000
Casper Network	$6,700,000
Delta Prime	$6,000,000

Major Exploits in Q3 Analysis

Most of the sum was lost by two specific projects, WazirX and BingX, totaling **$287,000,000**. Together, these two CeFi projects represent **69.5%** of Q3 losses alone.

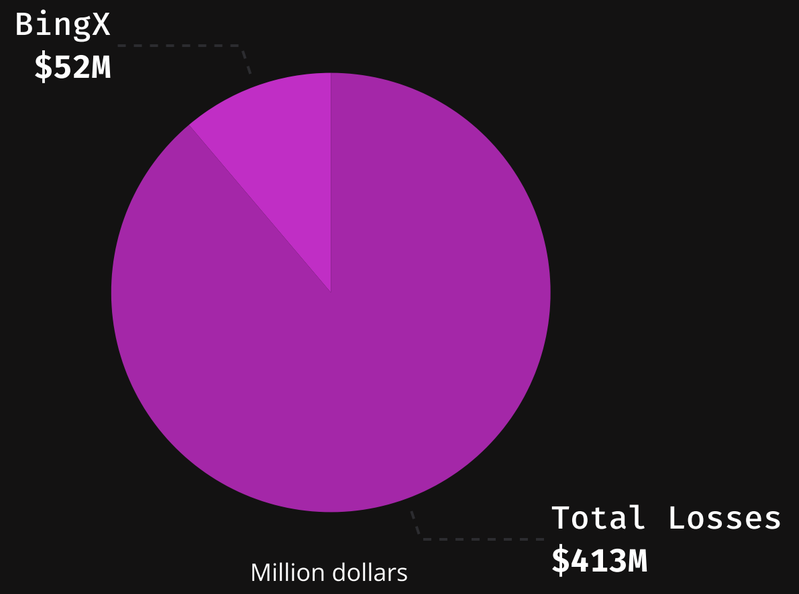
WAZIRX, $235 MILLION

- On July 18, 2024, WazirX, an Indian crypto exchange, was hacked, resulting in a massive loss of $235 million.



BINGX, $52 MILLION

- On September 20, 2024, BingX, a Singapore-based crypto exchange, suffered an attack that resulted in $52 million in lost funds.

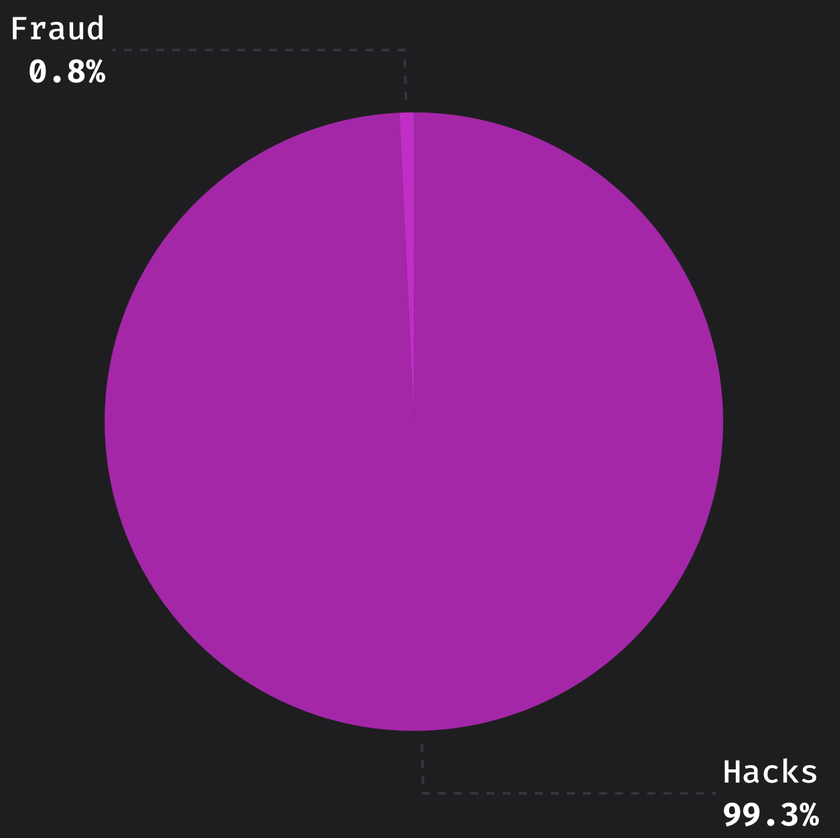


Hacks vs. Fraud Analysis

In Q3 2024, hacks continued to be the predominant cause of losses compared to fraud. An analysis of the losses shows that fraud accounts for only 0.8% of the total losses in Q3 2024, while hacks account for 99.3%.

OVERVIEW

- **Hacks**
  In total, we have seen a loss of **$409,906,947** to hacks in Q3 2024 across 31 specific incidents. These numbers represent a 38.2% decrease compared to Q3 2023, when losses caused by hacks totaled **$663,310,580**
- **Fraud**
  In total, we have seen a loss of **$3,087,552** to fraud in Q3 2024 across 3 specific incidents. These numbers represent a 86.4% decrease compared to Q3 2023, when losses caused by frauds, scams, and rug pulls totaled **$22,659,864**

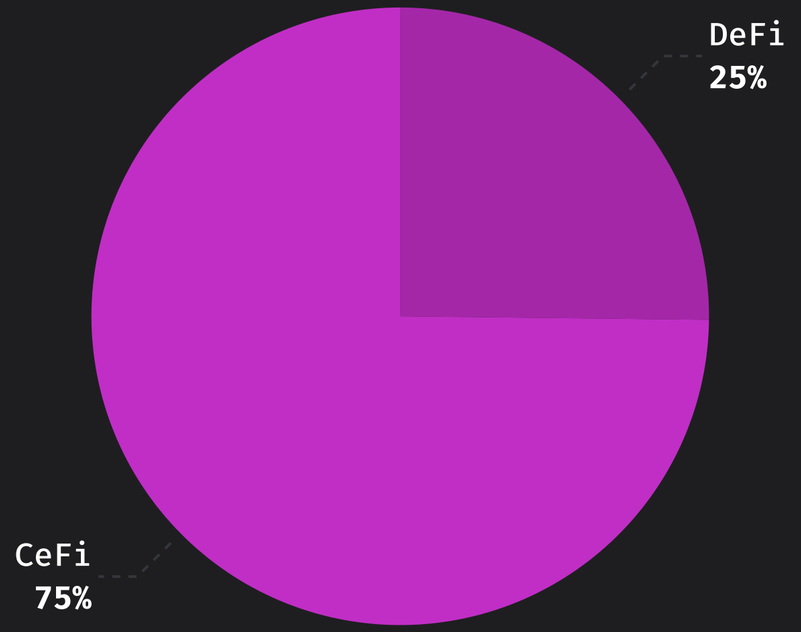


DeFi vs. CeFi Analysis

In Q3 2024, CeFi was the main target for exploits, representing 75% of total losses, while DeFi represented 25%.

OVERVIEW

- **DeFi**
  DeFi suffered **$103,994,499** in total losses across 31 incidents in Q3 2024. These numbers represent a 79.2% decrease compared to Q3 2023 when DeFi losses totaled **$500,270,444.**
- **CeFi**
  CeFi suffered **$309,000,000** in total losses in Q3 2024 across 3 incidents. These numbers represent a 66.4% increase compared to Q3 2023, when CeFi losses totaled **$185,700,000.**



Losses by Chain

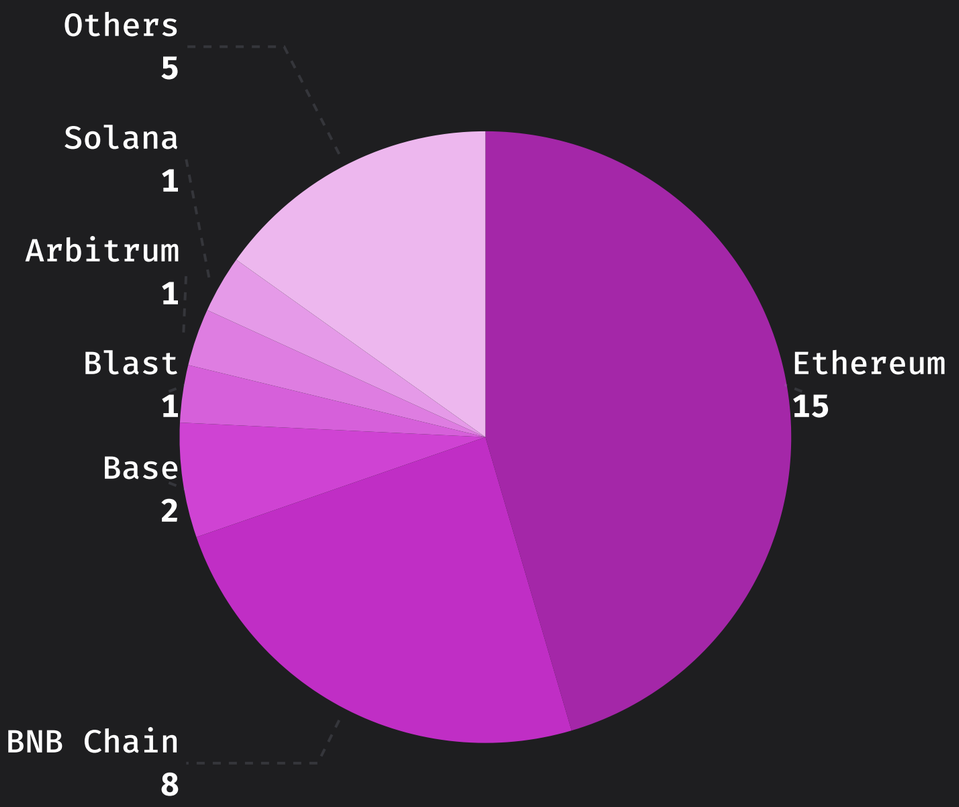
The two most targeted chains in Q3 2024 were Ethereum and BNB Chain. Ethereum suffered the most individual attacks, with 15 incidents representing 44.1% of the total losses across targeted chains. BNB Chain witnessed 8 incidents, representing 23.5% respectively.

OVERVIEW

- In Q3 2024, Ethereum and BNB Chain accounted for over half of the chain losses, totaling 67.6%.
- Base came in third with 2 incidents, representing 5.9% of total losses across chains. Blast, Solana, and Arbitrum follow with 1 incident each.

INSIGHTS

- In Q3 2024, Ethereum once again surpassed BNB Chain, becoming the most targeted chain compared to the previous period.



Funds Recovery

OVERVIEW

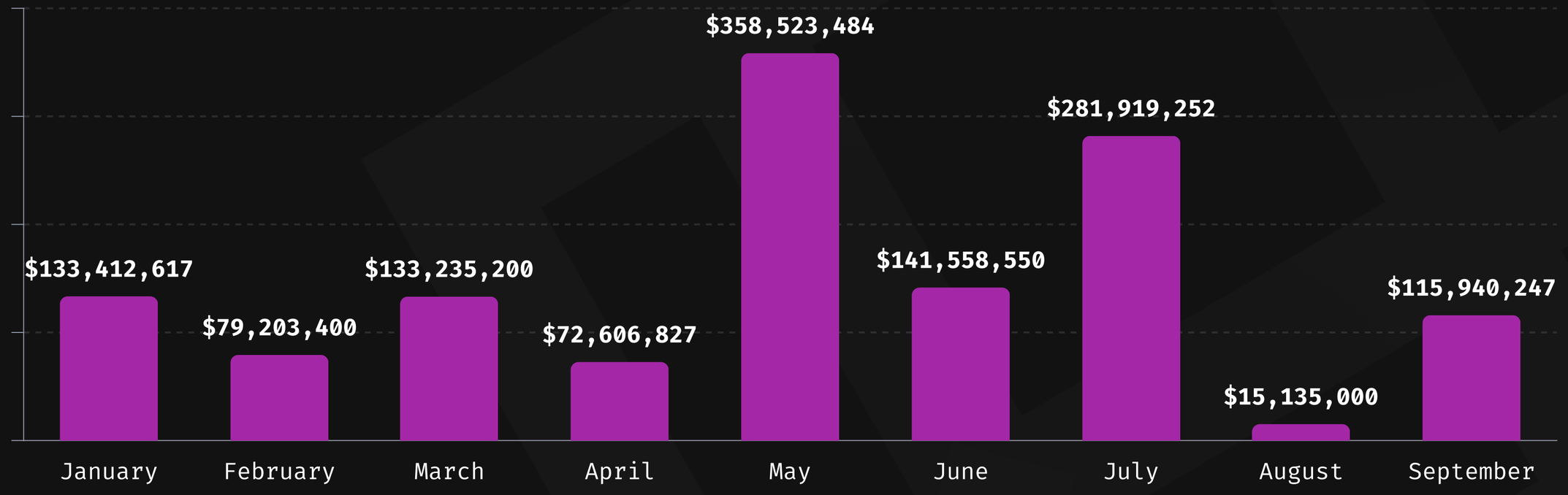
In total, **$14,900,000** has been recovered from stolen funds in **2** specific situations. This number makes up **3.6%** of the total losses in Q3 2024.

	Stolen	Recovered
Ronin Network	$12,000,000	$10,000,000
ShezmuTech	$4,900,000	$4,900,000

In Focus: Crypto Losses YTD

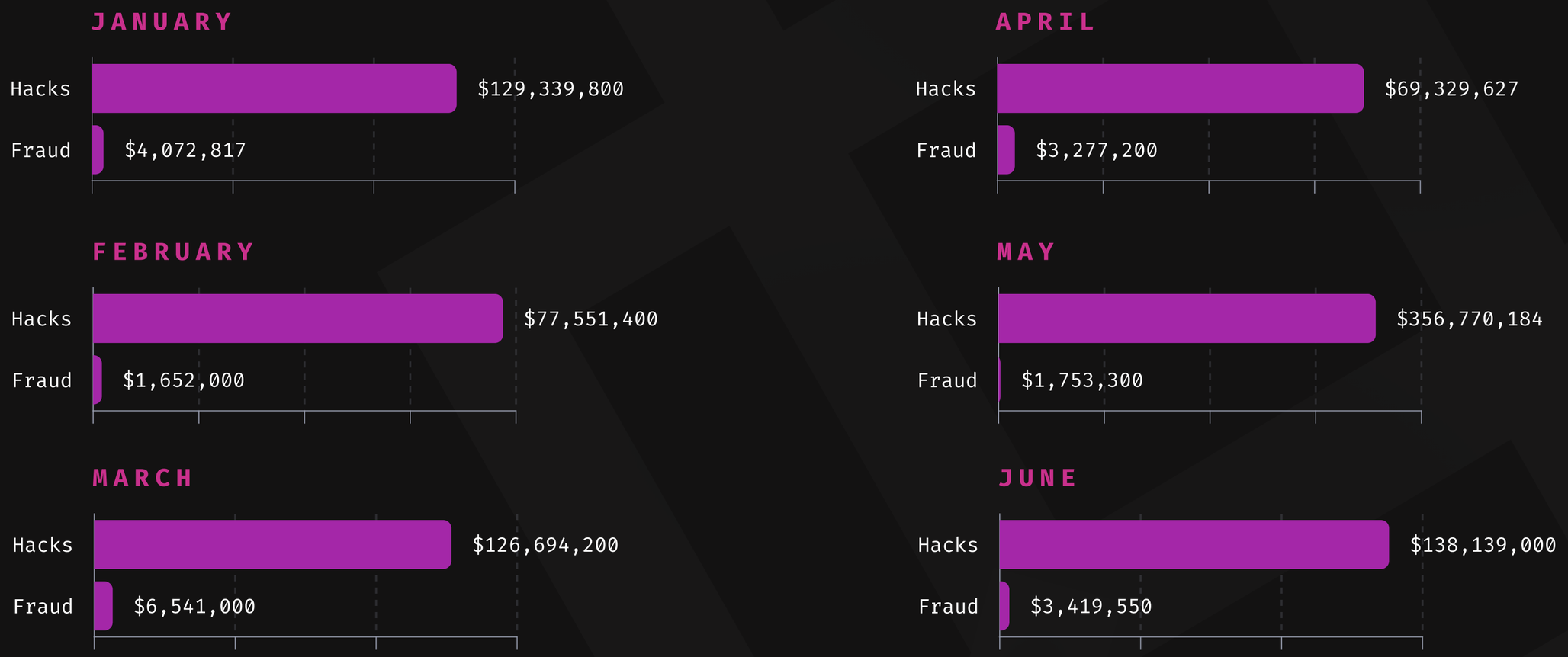
MONTHLY OVERVIEW

In total, the ecosystem has witnessed **$1,333,934,577** in losses year-to-date (YTD) across 169 specific incidents. Overall, the losses were primarily driven by over **$358 million** lost in May and over **$281 million** lost in July.



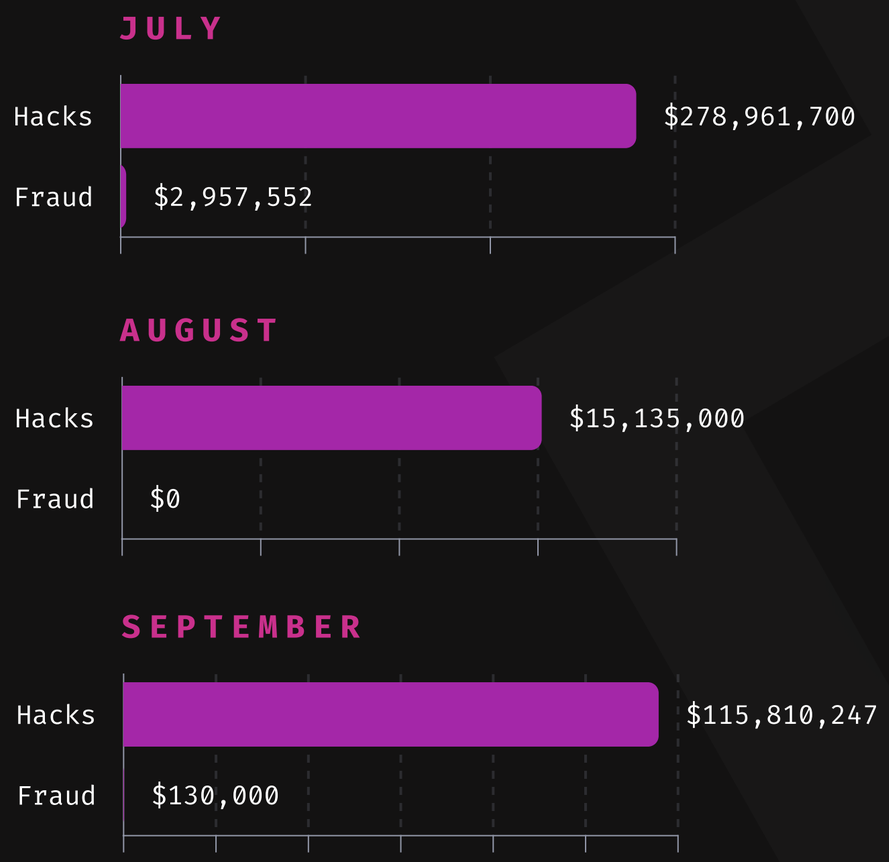
In Focus: Crypto Losses YTD

TOTAL LOSSES YTD: HACKS VS. FRAUD

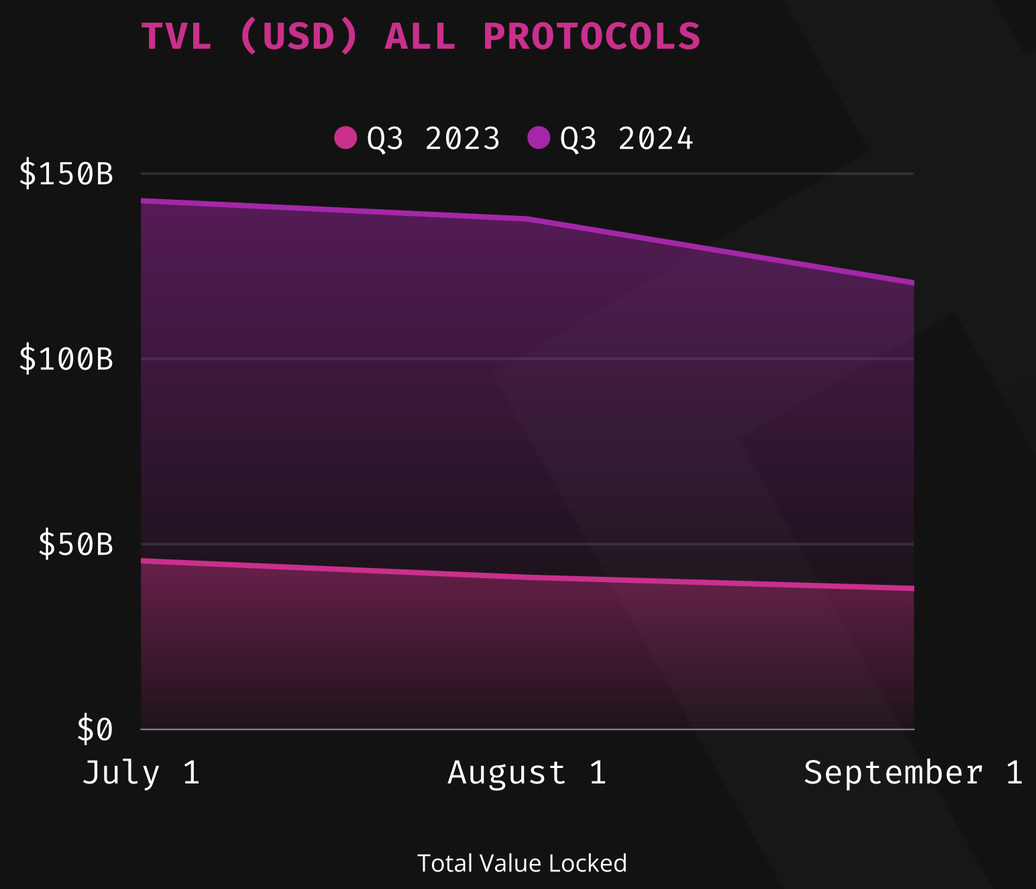


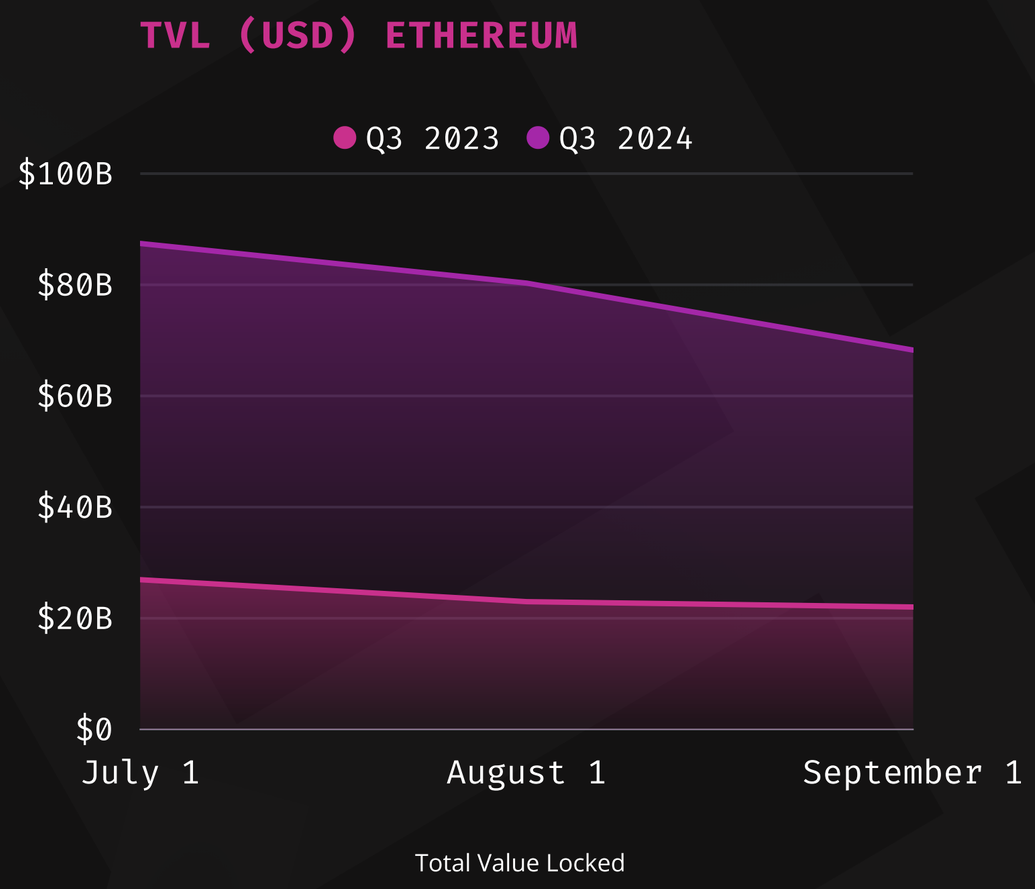
In Focus: Crypto Losses YTD

TOTAL LOSSES YTD: HACKS VS. FRAUD



In Focus: Q3 2023 vs. Q3 2024





In Focus: Q3 2023 vs. Q3 2024

HACKS VS. FRAUDS

38%

Hacks

Losses are down 38% when compared to the previous period.

86%

Fraud

Losses are down 86% when compared to the previous period.

In Focus: Q3 2023 vs. Q3 2024

DEFI VS. CEFI

79%

DeFi

Losses are down 79% when compared to the previous period.

66%

CeFi

Losses are up 66% when compared to the previous period.

“

We're seeing a higher number of incidents targeting DeFi, while CeFi experiences fewer incidents but often with more severe consequences, with hundreds of millions in stolen funds in a single exploit. In CeFi, the biggest infrastructural issue is private key management, which is essential to maintaining the self-custody of crypto assets but is not typically subject to security audits. It requires rigorous key management policies, practices, and emergency plans.

Mitchell Amador
Founder and CEO at Immunefi

Crypto Losses Q3 2024

Immunefi

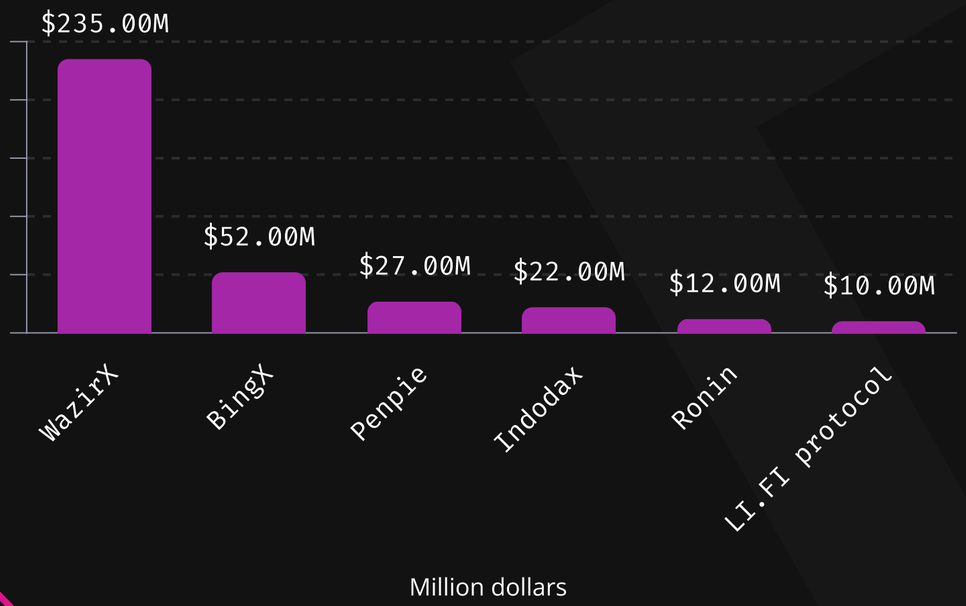
TOTAL LOSSES IN Q3

$412,994,499

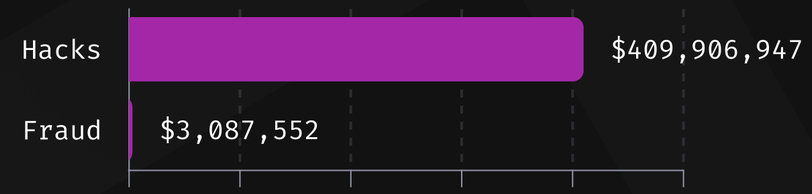
YTD

$1,333,934,577

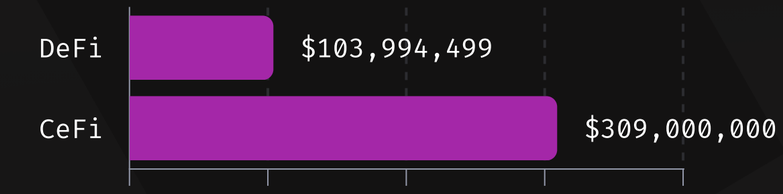
MAJOR LOSSES



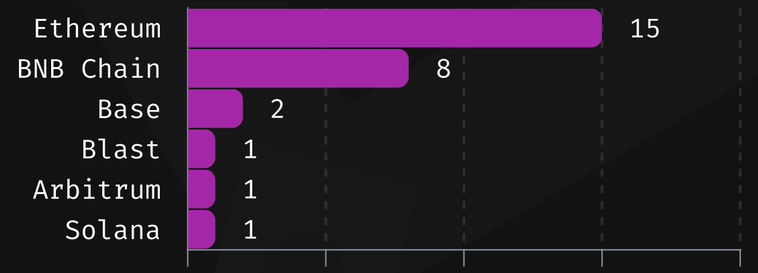
HACKS VS. FRAUD



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: Ronin later recovered $10 million in stolen funds. The hacker was able to drain $12 million in tokens from the platform. Later, the ETH (approximately $10 million) was returned.
- 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/**