# Immunefi

# CRYPTO LOSSES IN NOVEMBER 2023

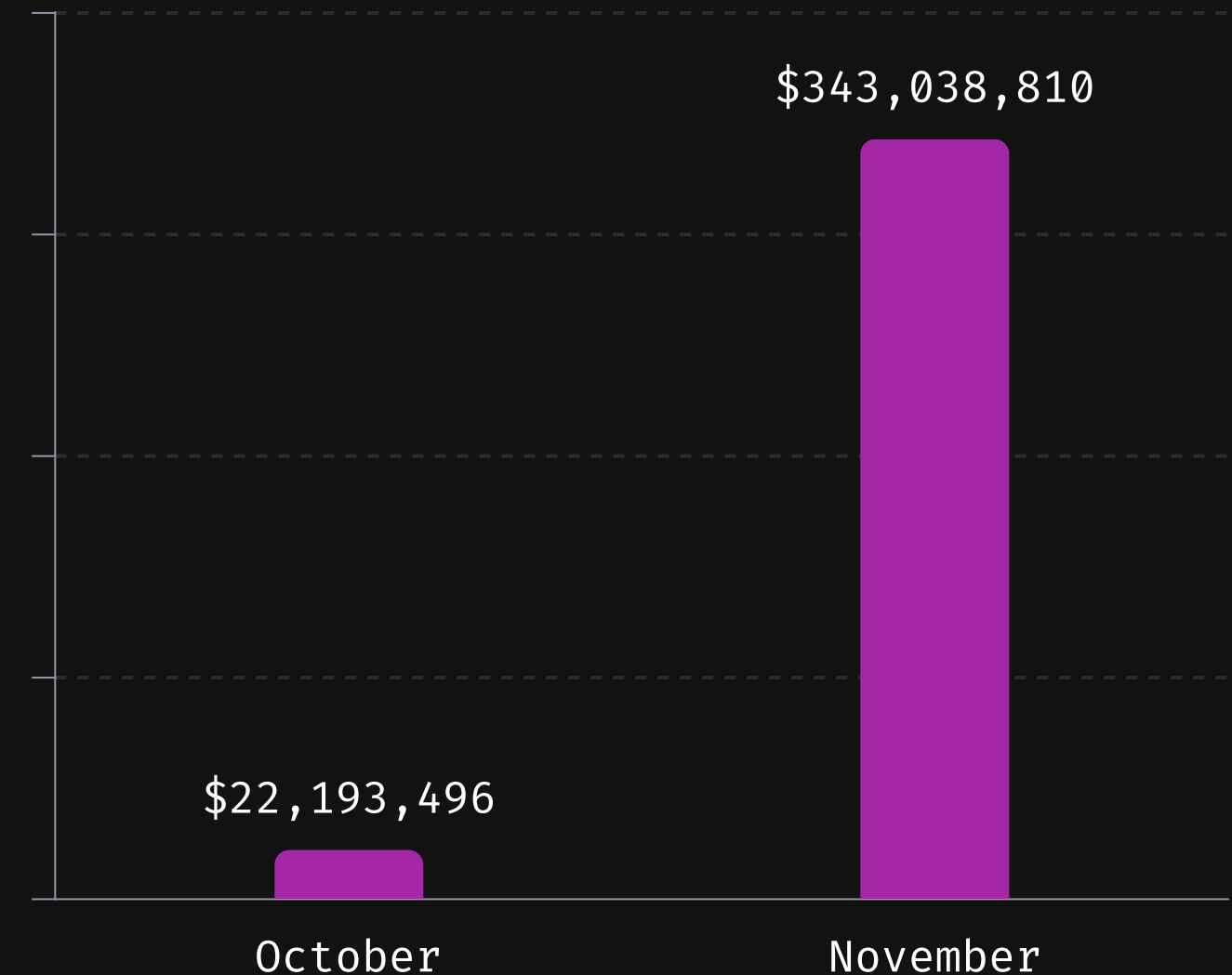PREPARED BY IMMUNEFI

# Crypto Losses: November 2023

**ANALYSIS**

- In total, we have seen a loss of **$1,753,707,812** to hacks and rug pulls in 2023 from January to November across 296 specific incidents.

- In November 2023 alone, **$343,038,810** was lost due to hacks and fraud, marking the highest monthly loss witnessed this year to date. This represents a 15.4x increase from October when registered losses were $22,193,496.

- In November 2023, CeFi became the main target for exploits in terms of funds lost, compared to DeFi. CeFi represents 53.8% of the total losses, while DeFi represents 46.2%. An increase primarily led by the high-profile attacks on Poloniex, HTX Exchange, and Kronos Research.

- Hacks continue to be the predominant cause of losses as compared to frauds. In November 2023, a total of **$335,574,150** was lost due to hacks.

- The most targeted chains in November 2023 were BNB Chain and Ethereum, representing more than half of the total losses across targeted chains at 83%.

## October vs. November
### 2023

$343,038,810

$22,193,496

October          November

# Hacks vs. Fraud Analysis

In November 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 2.2% of the total losses in November 2023, while hacks account for 97.8%.
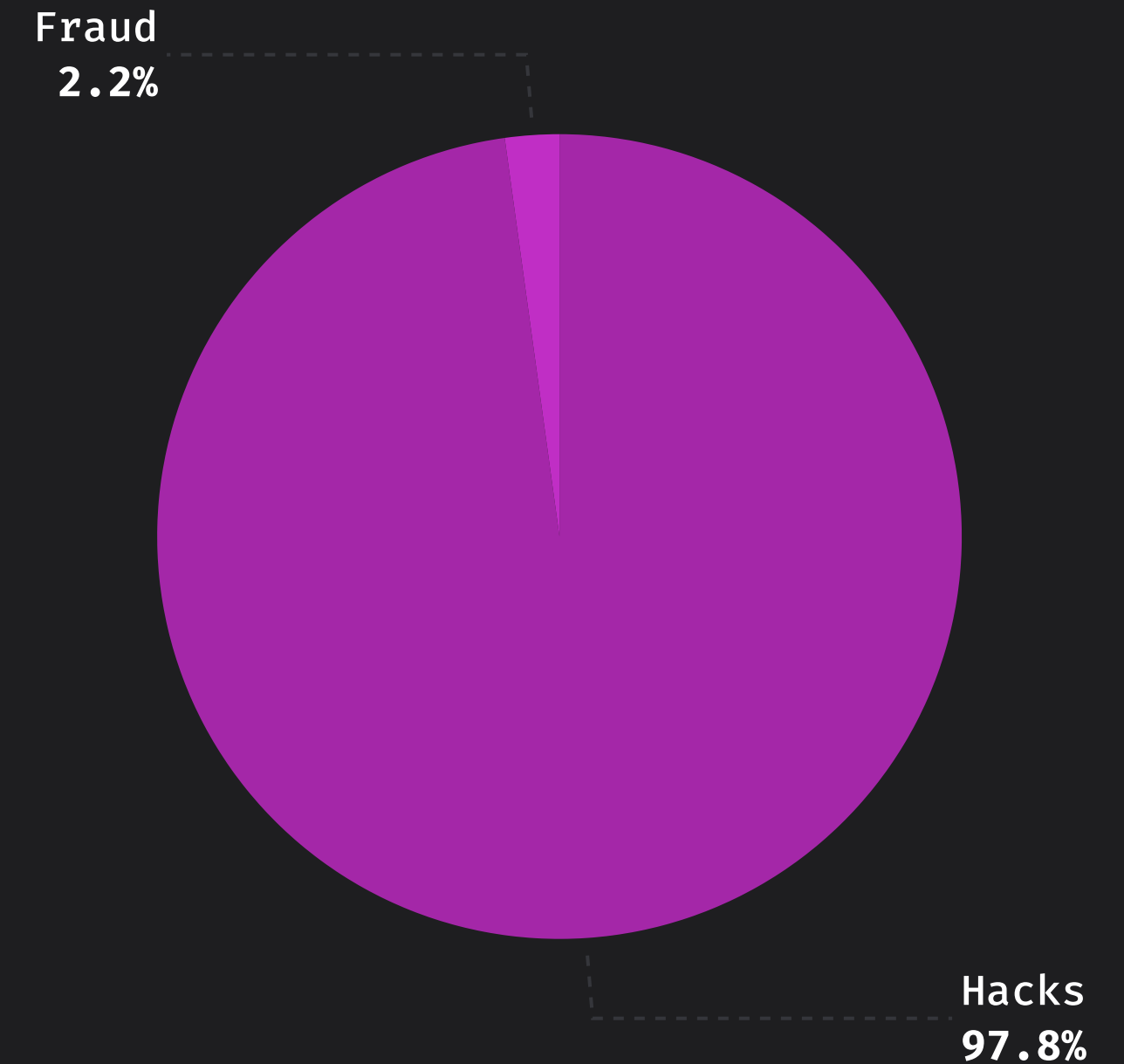
### OVERVIEW

- **Hacks**
  In total, we have seen a loss of **$335,574,150** to hacks in November 2023 across 18 specific incidents.

- **Fraud**
  In total, we have seen a loss of **$7,464,660** to fraud in November 2023 across 23 specific incidents.

**Hacks vs. Fraud**
November 2023

Fraud
**2.2%**

Hacks
**97.8%**

# DeFi vs. CeFi Analysis

In November 2023, CeFi became the main target for exploits in terms of funds lost, compared to DeFi. CeFi represents 53.8% of the total losses, while DeFi represents 46.2%. This increase was primarily led by the high-profile attacks on Poloniex, HTX Exchange, and Kronos Research.

**OVERVIEW**

- **DeFi**
  DeFi has suffered **$158,638,810** in total losses in November 2023 across 37 incidents.
- **CeFi**
  CeFi has suffered **$184,400,000** in total losses in November 2023 across 4 incidents.

**DeFi vs. CeFi**

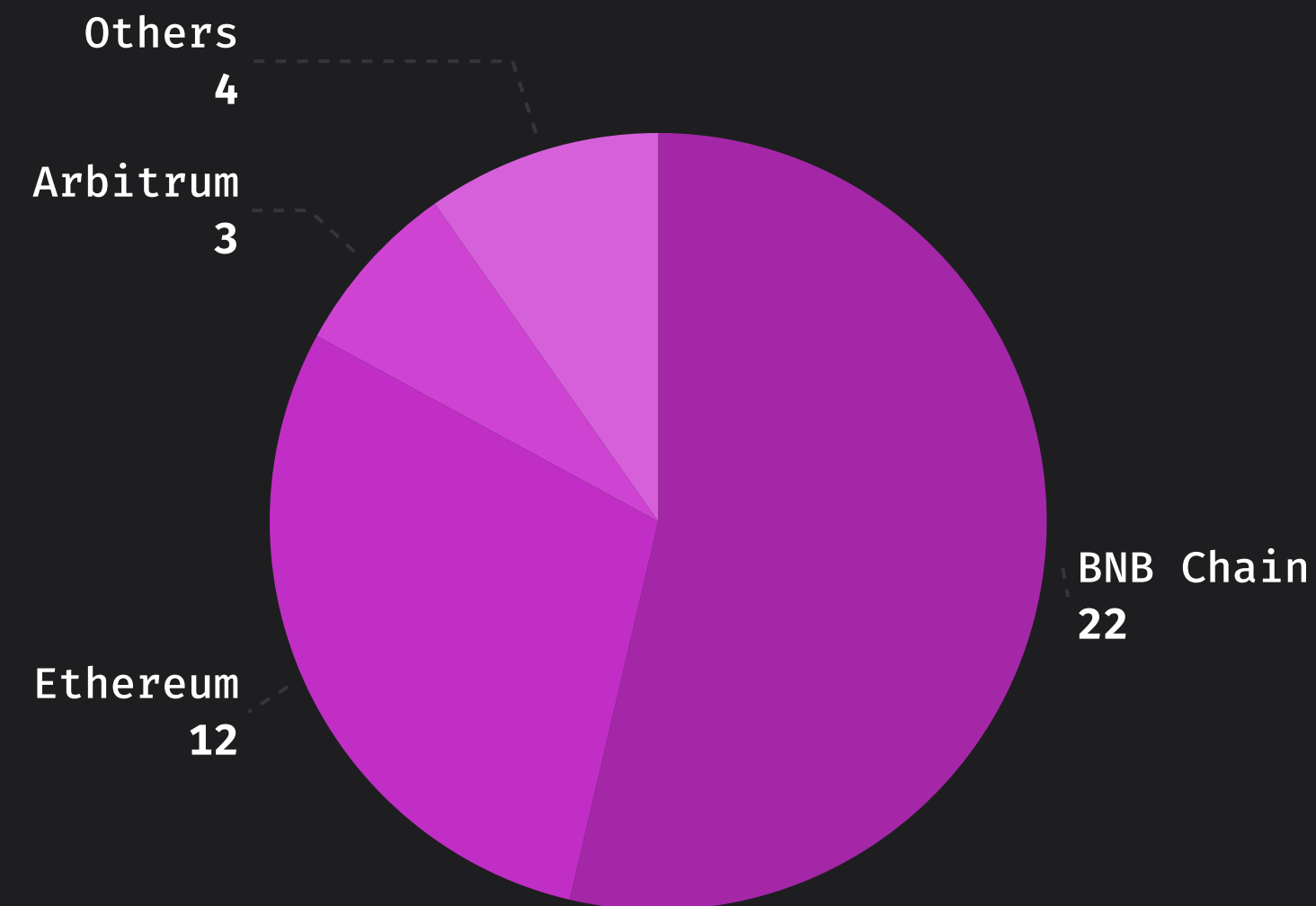November 2023



DeFi
46.2%

CeFi
53.8%
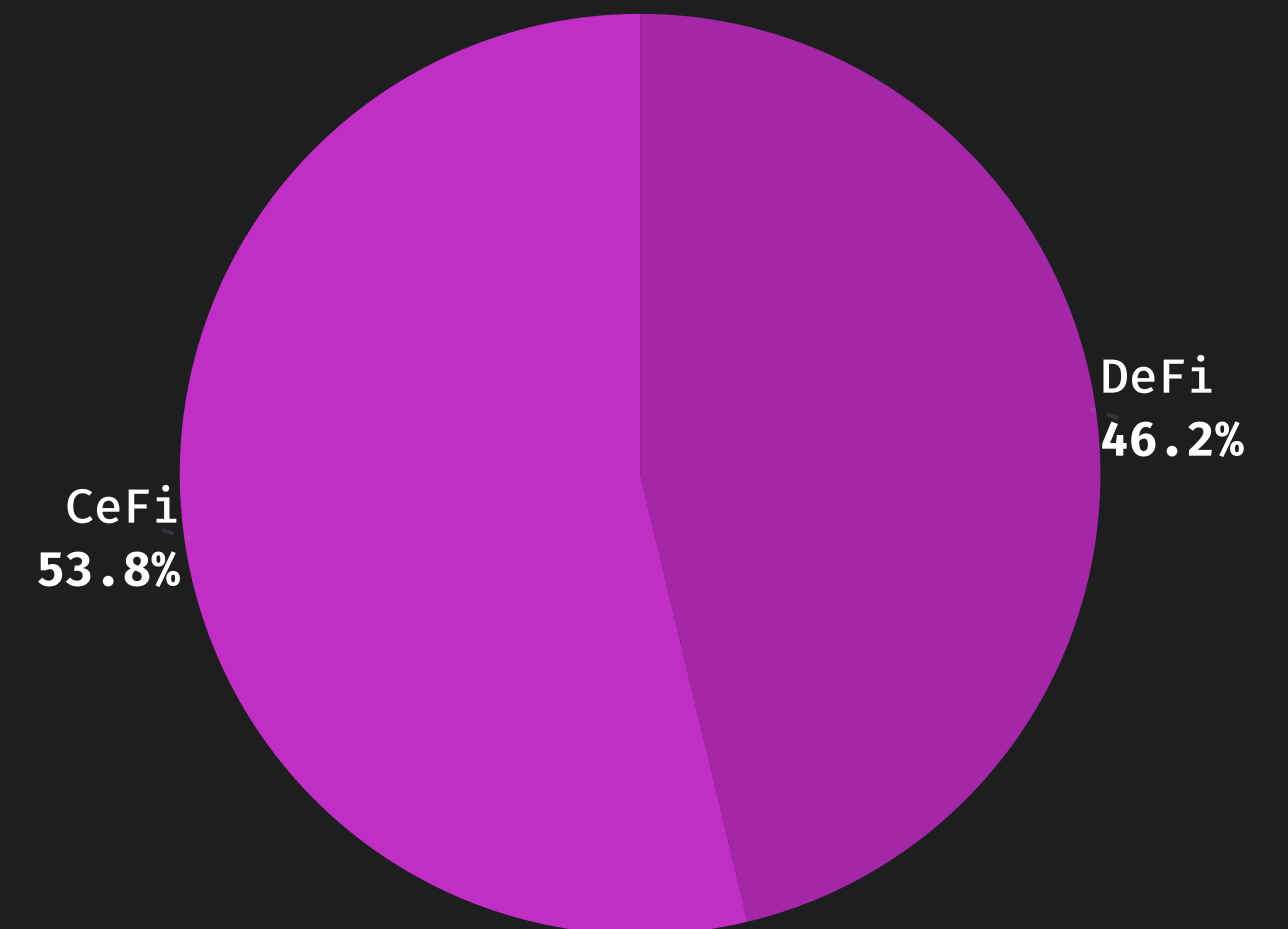
# Losses by Chain

The most targeted chains in November 2023 were BNB Chain and Ethereum. BNB Chain suffered the most individual attacks, with 22 incidents representing 53.7% of the total losses across targeted chains. Ethereum witnessed 12 incidents, representing 29.3% respectively.

### OVERVIEW

- BNB Chain and Ethereum represent more than half of the chain losses in November 2023 at 83%, followed by Arbitrum with 3 incidents, representing 7.3%. Optimism, Avalanche, Fantom, and Heco Chain witnessed 1 incident each, representing 2.4% respectively.
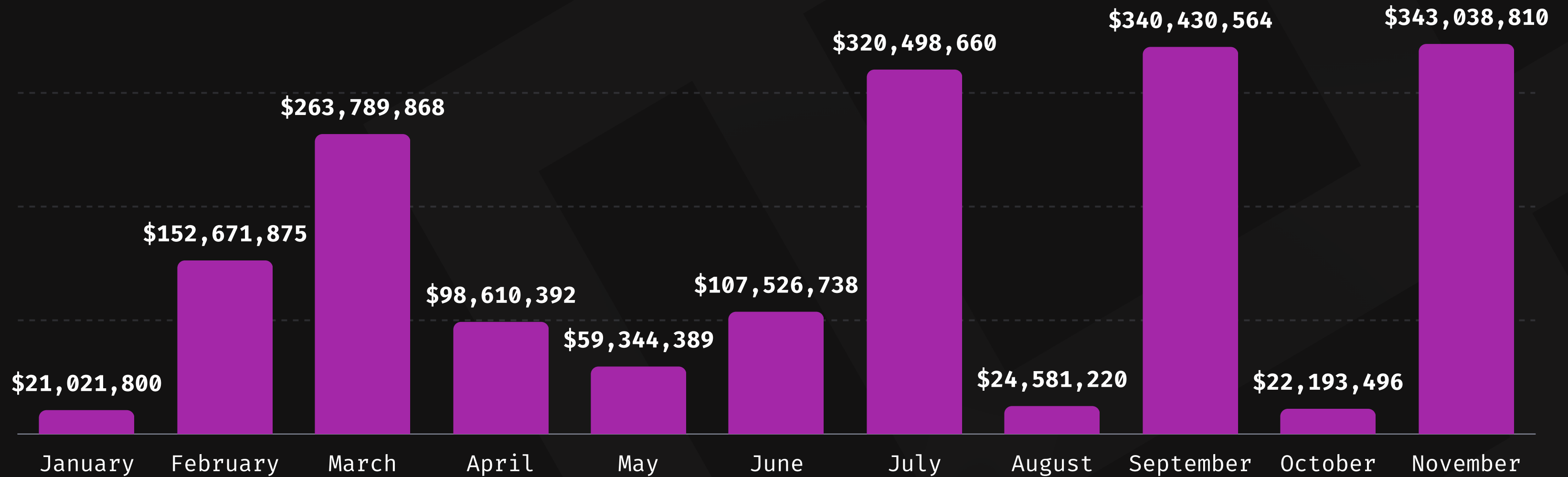
**Losses by Chain**
November 2023



Others
4

Arbitrum
3

BNB Chain
22

Ethereum
12

# In Focus: Crypto Losses YTD

In total, the ecosystem has witnessed **$1,753,707,812** in losses year-to-date (YTD) across 296 specific incidents. In November 2023 alone, $343 million was lost due to hacks and fraud, marking the highest monthly loss witnessed this year to date. September follows with $340 million in losses, July with $320 million.



| Month | Loss |
|---|---|
| January | $21,021,800 |
| February | $152,671,875 |
| March | $263,789,868 |
| April | $98,610,392 |
| May | $59,344,389 |
| June | $107,526,738 |
| July | $320,498,660 |
| August | $24,581,220 |
| September | $340,430,564 |
| October | $22,193,496 |
| November | $343,038,810 |

# Crypto Losses November 2023

**Immunefi**

## TOTAL LOSSES YTD

# $1,753,707,812

### IN NOVEMBER

## $343,038,810

## MAJOR LOSSES



- PoLoniex — $126,000,000
- Heco Chain — $85,400,000
- KyberSwap — $48,300,000
- HTX Exchange — $30,000,000
- Kronos Research — $26,000,000

## HACKS VS. FRAUD



- Hacks — $335,574,150
- Fraud — $7,464,660

## DEFI VS. CEFI



- DeFi — $158,638,810
- CeFi — $184,400,000

## TOP LOSSES BY CHAIN



- BNB Chain — 53.7%
- Ethereum — 29.3%
- Arbitrum — 7.9%

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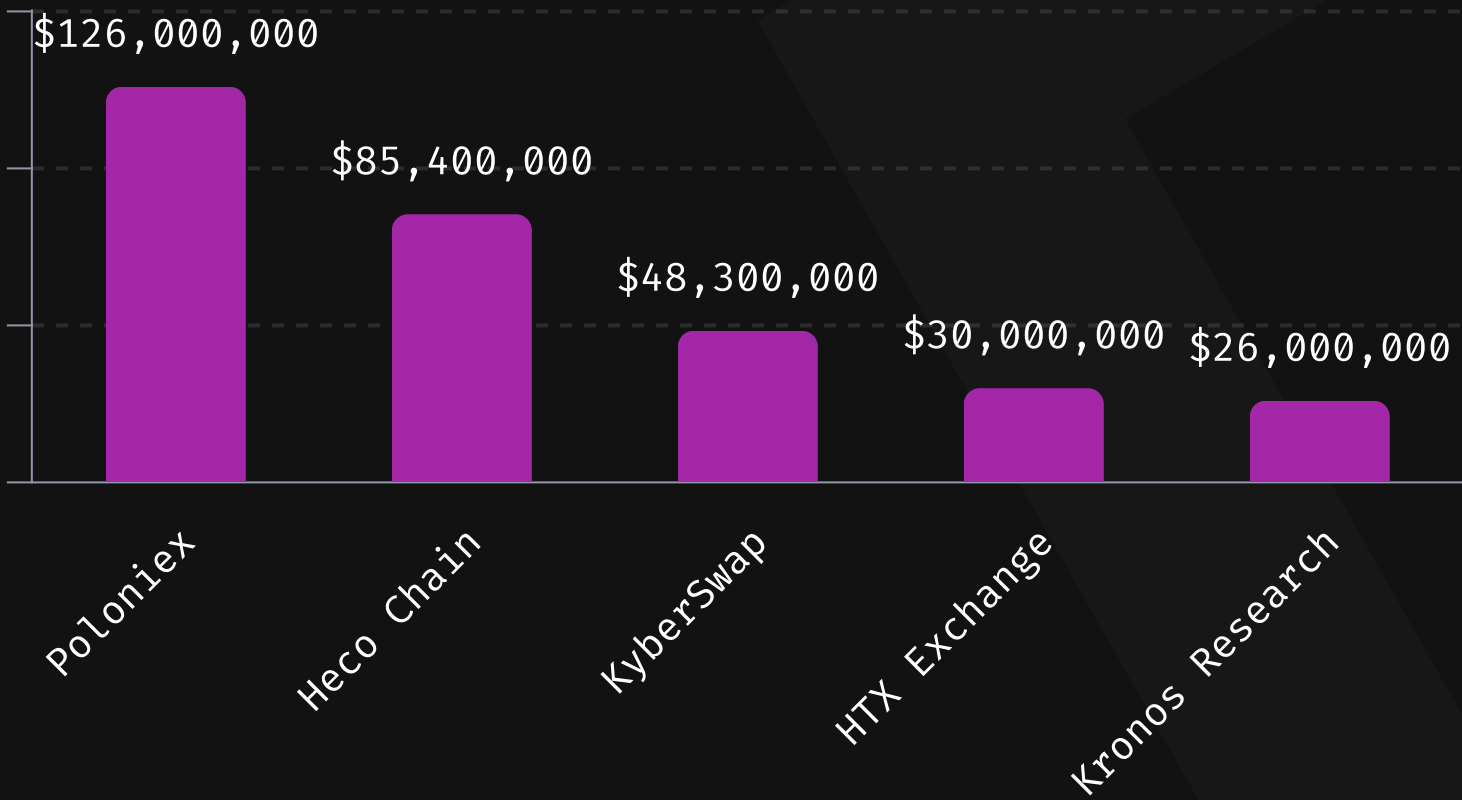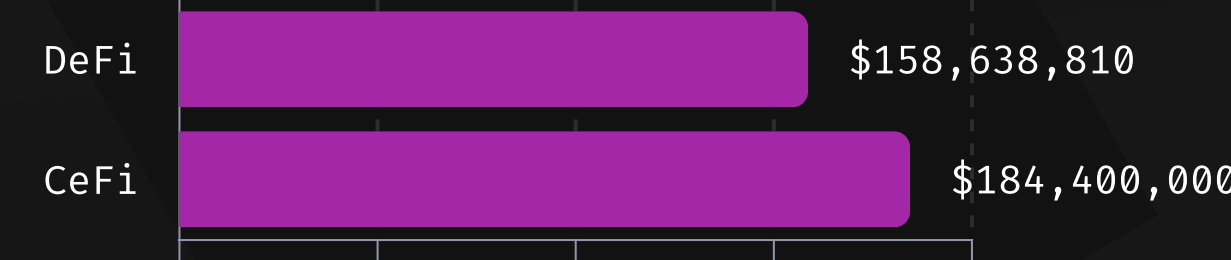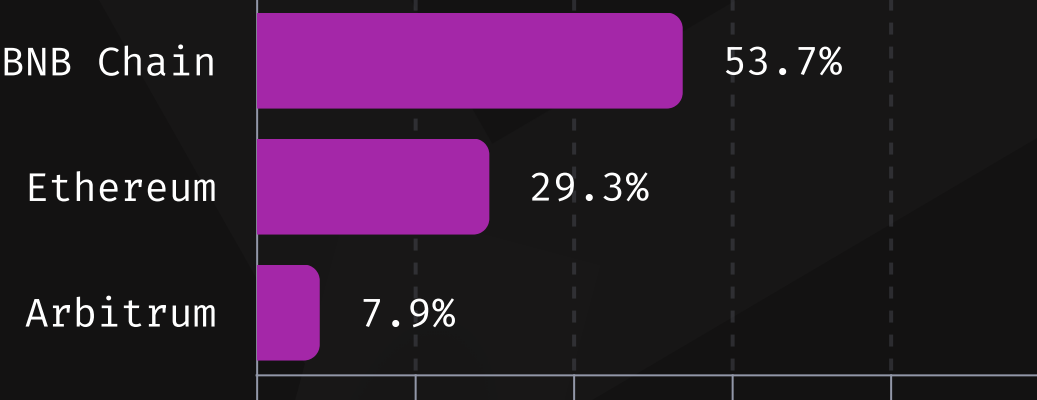
# Immunefi

Immunefi is the leading bug bounty and security services platform for web3 protecting over $50 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 **$85 million** in total bounties, while saving over **$25 billion** in user funds.

### TOTAL BOUNTIES AVAILABLE
Immunefi offers over **$150 million** in available bounty rewards.

### SUPPORTED PROJECTS
Trusted by established, multi-billion dollar projects like Synthetix, Chainlink, Polygon, LayerZero, MakerDAO, TheGraph, Wormhole, Optimism 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.

**Notes:**

- 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 $150M in rewards available on Immunefi — the leading bug bounty platform for web3.

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