Immunefi

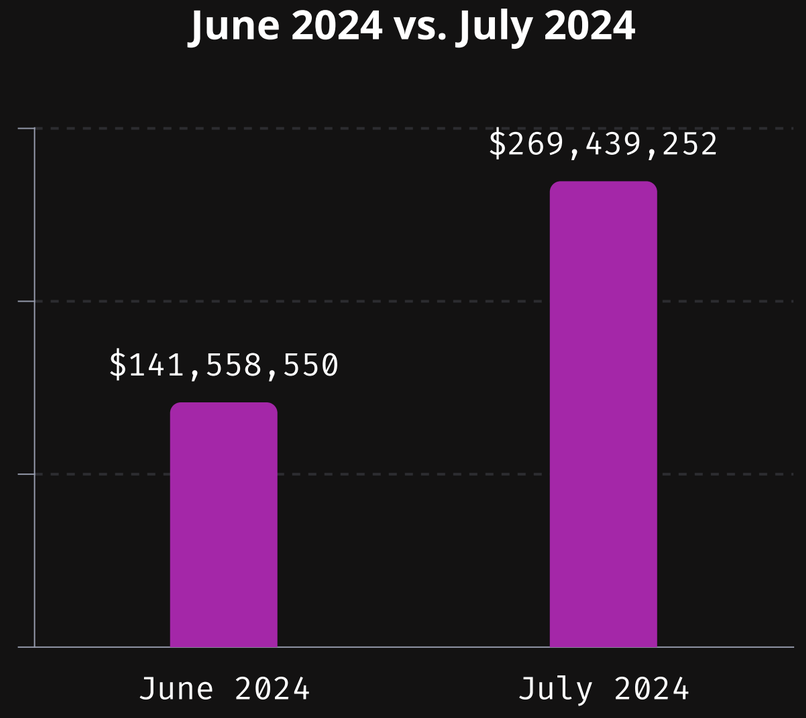
CRYPTO LOSSES IN JULY 2024

PREPARED BY IMMUNEFI

Crypto Losses: July 2024

ANALYSIS

- In total, we have seen a loss of **$1,190,379,330** to hacks and rug pulls in 2024 YTD across 149 specific incidents. This represents a **16.3% increase** when compared with the same period in 2023 at **$1,023,463,722.**
- In July 2024, **$269,439,252** was lost due to hacks and fraud across 14 specific incidents. This represents a **15.9% decrease** from July 2023, when registered losses were **$320,498,660**, and a **90% increase** month-over-month.
- Most of the sum was lost in two specific projects: WazirX, an Indian cryptocurrency exchange, with a loss of **$235 million**, and LI.FI protocol, a platform to swap and bridge across major blockchains and protocols, which incurred a loss of **$10 million**.
- In July 2024, CeFi surpassed DeFi with only one case occurring, representing **87%** of the total volume of funds lost.
- Hacks continued to be the predominant cause of losses as compared to fraud. A total of **$266,481,700** was lost due to hacks across 12 specific incidents. 2 fraud events happened in July, totaling **$2,957,552.**
- The most targeted chains in July 2024 were Ethereum and BNB Chain, representing 71.4% of the total losses across targeted chains.



PREPARED BY IMMUNEFI

Top 10 Losses in July 2024

WazirX (Safe Multisig wallet)	$235,000,000
LI.FI protocol	$10,000,000
Bittensor (Wallet)	$8,000,000
RHO Markets	$7,600,000
ETHTrustFund	$2,000,000
Dough Finance	$1,810,000
Minterest	$1,400,000
Monoswap	$1,300,000
TRUMP (MAGA)	$957,552
Spectra App	$529,700

PREPARED BY IMMUNEFI

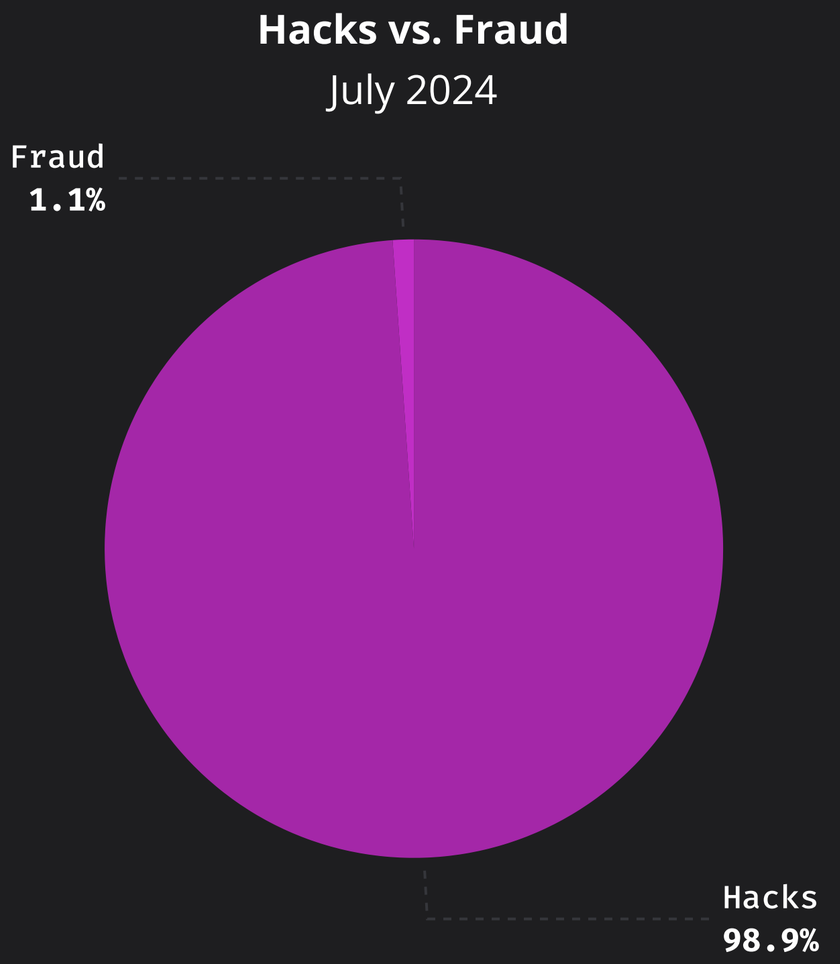
Hacks vs. Fraud Analysis

In July 2024, hacks continued to be the predominant cause of losses as compared to fraud. An analysis of the losses shows that fraud accounted for only 1.1% of the total losses in July 2024, while hacks accounted for 98.9%.

OVERVIEW

- **Hacks**
  In total, we have seen a loss of **$266,481,700** to hacks in July 2024 across 12 specific incidents.

- **Fraud**
  In total, we have seen a loss of **$2,957,552** to fraud in July 2024 across 2 specific incidents.



PREPARED BY IMMUNEFI

DeFi vs. CeFi Analysis

In July 2024, CeFi again surpassed DeFi, representing 87% of the total volume of funds lost.

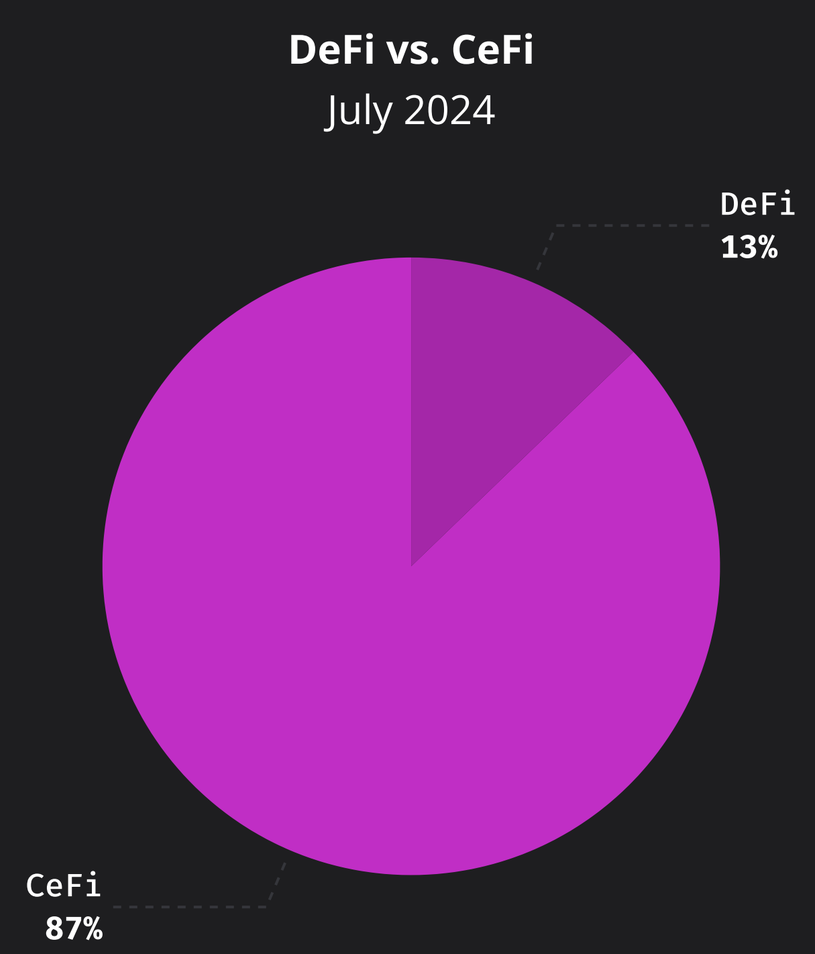
OVERVIEW

- **DeFi**
  DeFi suffered **$34,439,252** in total losses in July 2024 across 13 incidents.

- **CeFi**
  CeFi suffered **$235,000,000** in total losses across 1 incident.

CEFI AND NORTH KOREAN HACKING IN FOCUS

- Most of the losses in 2024 are attributed to attacks targeting CeFi infrastructure. Of the $1.19 billion stolen in 2024 YTD, over $636 million is attributed to CeFi.
- North Korean hackers are suspected to be behind the attack on WazirX, which occurred in July 2024. Recently, the DMM Bitcoin hack that happened in May 2024 has been linked to the Lazarus Group, a North Korean hacking group. The group began laundering the funds in July 2024.
- Lazarus consists of an unknown number of individuals and is affiliated with the government of North Korea. The group has been linked to some of the largest cyber attacks within the crypto ecosystem, including those on Atomic Wallet, CoinEx, Alphapo, Stake, and CoinsPaid.



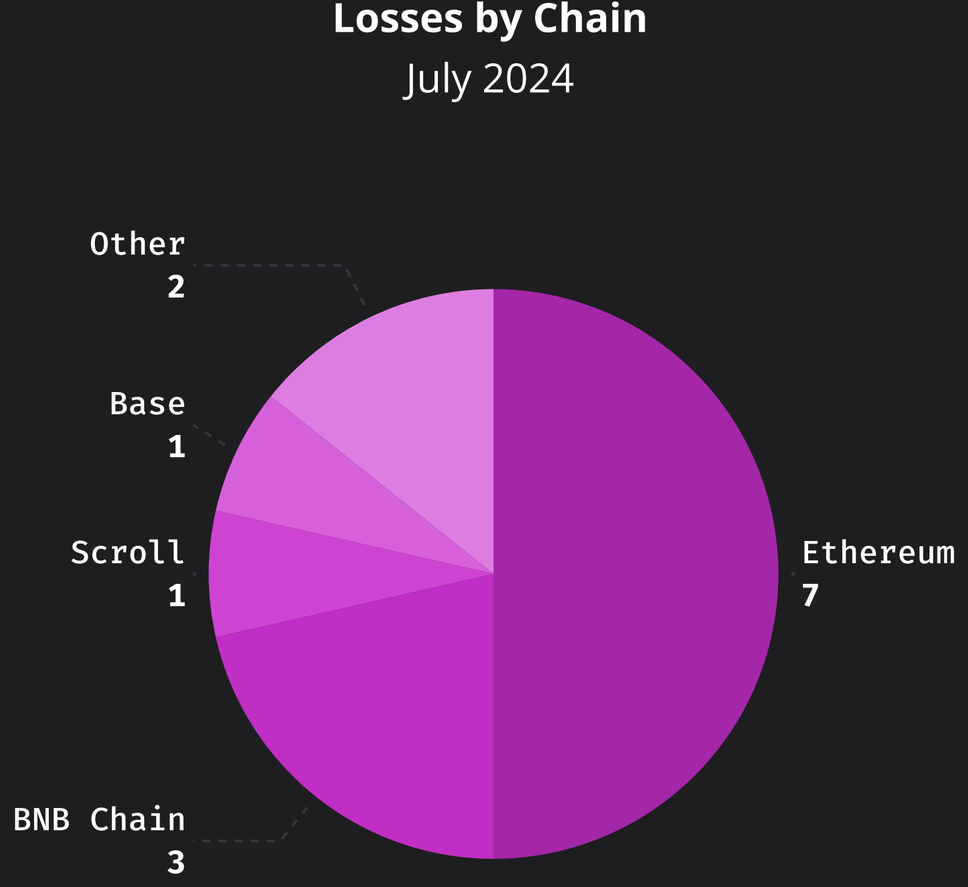
PREPARED BY IMMUNEFI

Losses by Chain

The most targeted chains in July 2024 were Ethereum and BNB Chain, representing 71.4% of the total losses across targeted chains.

OVERVIEW

- Ethereum suffered the most individual attacks, with 7 incidents, representing 50% of the total losses across targeted chains. BNB Chain experienced 3 incidents, representing 21.4% of the total. Scroll and Base each suffered 1 incident, respectively, representing 7.1% of the total losses.



PREPARED BY IMMUNEFI

Crypto Losses July 2024

Immunefi

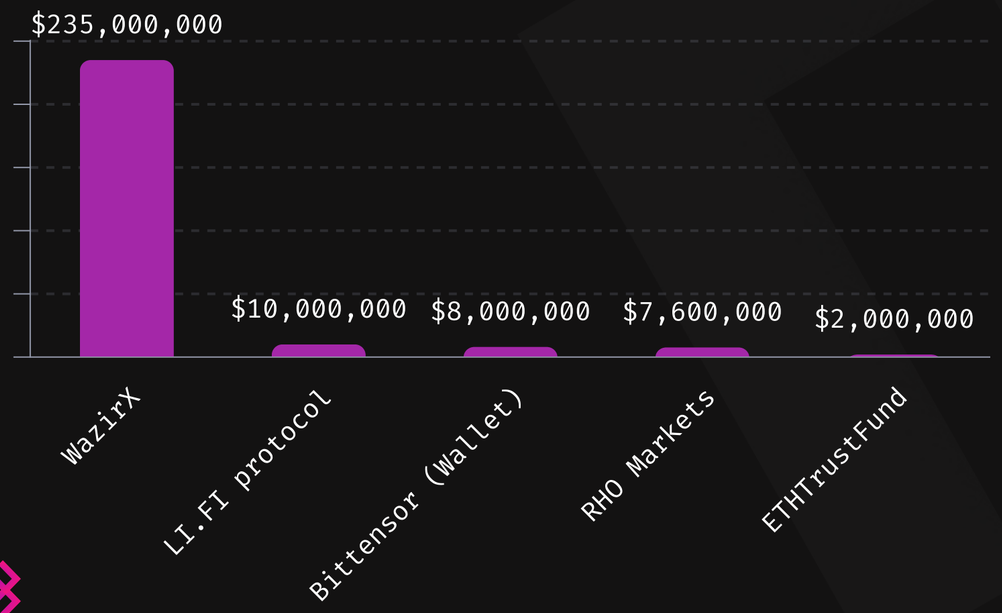
TOTAL LOSSES YTD

$1,190,379,330.

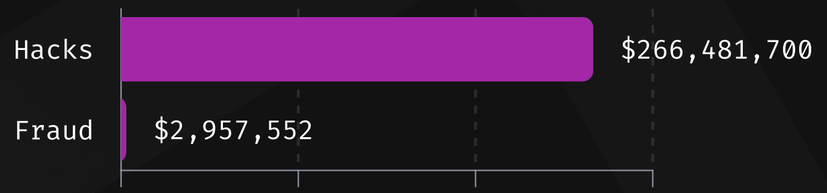
IN JULY

$269,439,252

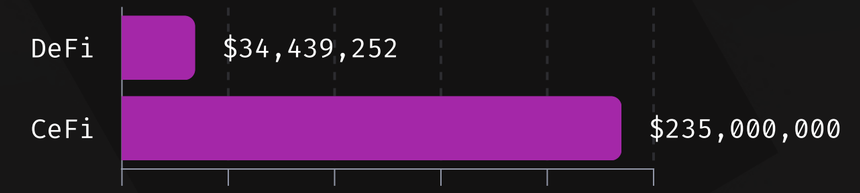
MAJOR LOSSES



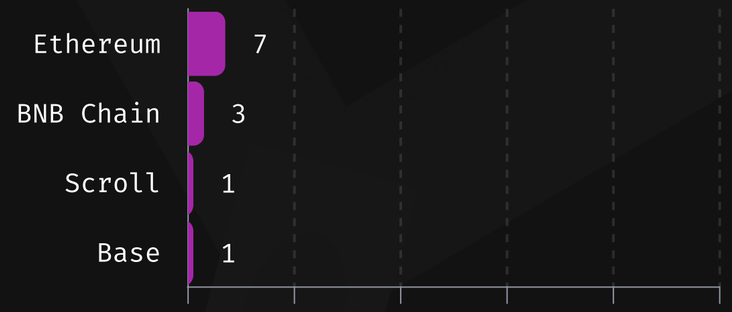
HACKS VS. FRAUD



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 **$157 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.

Disclaimer:

- Immunefi uses publicly available data and news reports in order to access and collect alleged fraud, 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.

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 $163M in rewards available on Immunefi — the leading bug bounty platform for web3.

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