Immunefi

CRYPTO LOSSES IN 2024

PREPARED BY IMMUNEFI

Crypto Losses in 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 2024.

OVERVIEW

The global crypto market cap surpassed **$3 trillion** in 2024, with over **$137 billion** in Total Value Locked (TVL) in Decentralized Finance (DeFi). This 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 2024. We have located 232 such instances, including both successful and semi-successful hacking attempts, as well as alleged fraud.

In total, we have seen a loss of **$1,495,487,055** across the web3 ecosystem in 2024. **$1,467,448,336** was lost to hacks in 2024 across 192 specific incidents and **$28,038,719** was lost to fraud in across 40 specific incidents. The year was marked by two major attacks: DMM Bitcoin, a Japanese crypto exchange**,** and WazirX, India's leading domestic crypto exchange.

This number represents a 17% decrease compared to total losses in 2023, when hackers and fraudsters stole **$1,803,290,600.**

Crypto Losses in 2024

KEY TAKEAWAYS IN 2024

- The two major exploits of the year, DMM Bitcoin and WazirX, alone accounted for **$540,000,000**, representing 36% of all losses in 2024.
- In 2024, hacks continued to be the predominant cause of losses at **98.1%** in comparison to frauds, scams, and rug pulls, which amounted to only **1.9%** of the total losses.
- In 2024, DeFi continued to be the main target of successful exploits at **51.4%** as compared to CeFi at **48.6%** of the total losses. While most of the hackers' interest is directed toward DeFi, CeFi is experienced higher losses, most likely due to their outsized returns.
- The two most targeted chains in 2024 were Ethereum and BNB Chain. Ethereum witnessed 104 incidents representing 44% of the total losses across targeted chains. BNB Chain suffered 71 incidents, representing 39% respectively. Arbitrum came in third with 16 incidents, representing 6.8% of total losses across chains. Solana, Optimism, Blast, and Base followed with 6 incidents each.
- North Korean hackers have allegedly been responsible for two notable attacks, WazirX and Radiant Capital, profiting a combined total of $285 million and representing 16% of total crypto losses in 2024.
- In total, **$115,577,966** has been recovered from stolen funds in **14** specific situations. This number makes up **7.7%** of the total losses in 2024.
- The number of successful attacks decreased: single incidents decreased **27.5%** YoY from 320 in 2023 to 232 in 2024, along with the total number of losses.

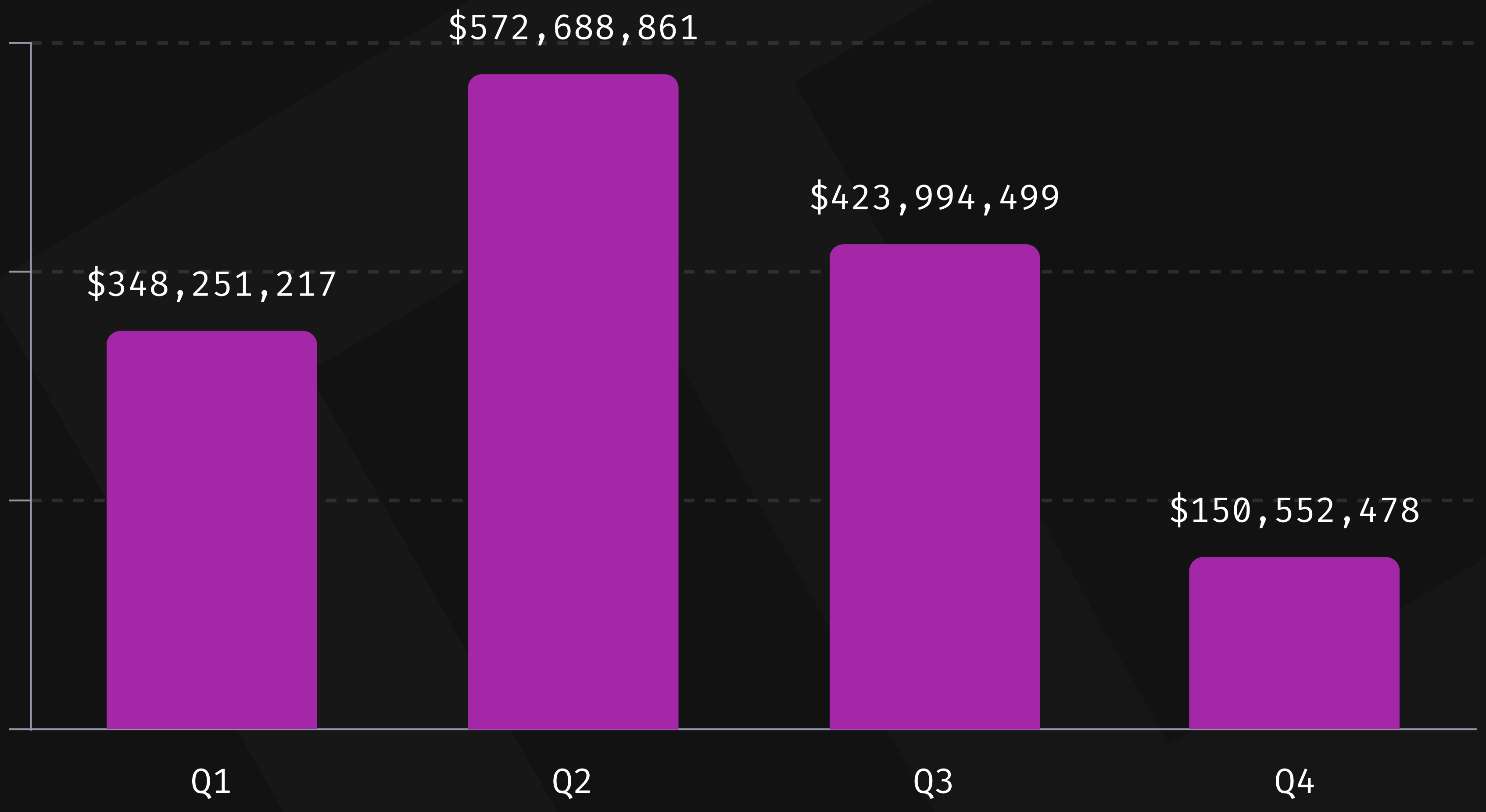
Top 10 Losses in 2024*

DMM Bitcoin	$305,000,000
WazirX	$235,000,000
Orbit Bridge	$81,680,000
Munchables	$62,800,000
BtcTurk	$55,000,000
BingX	$52,000,000
Radiant Capital	$50,000,000
Hedgey	$44,600,000
PlayDapp	$32,350,000
Penpie	$27,000,000

Losses by quarter in 2024

OVERVIEW

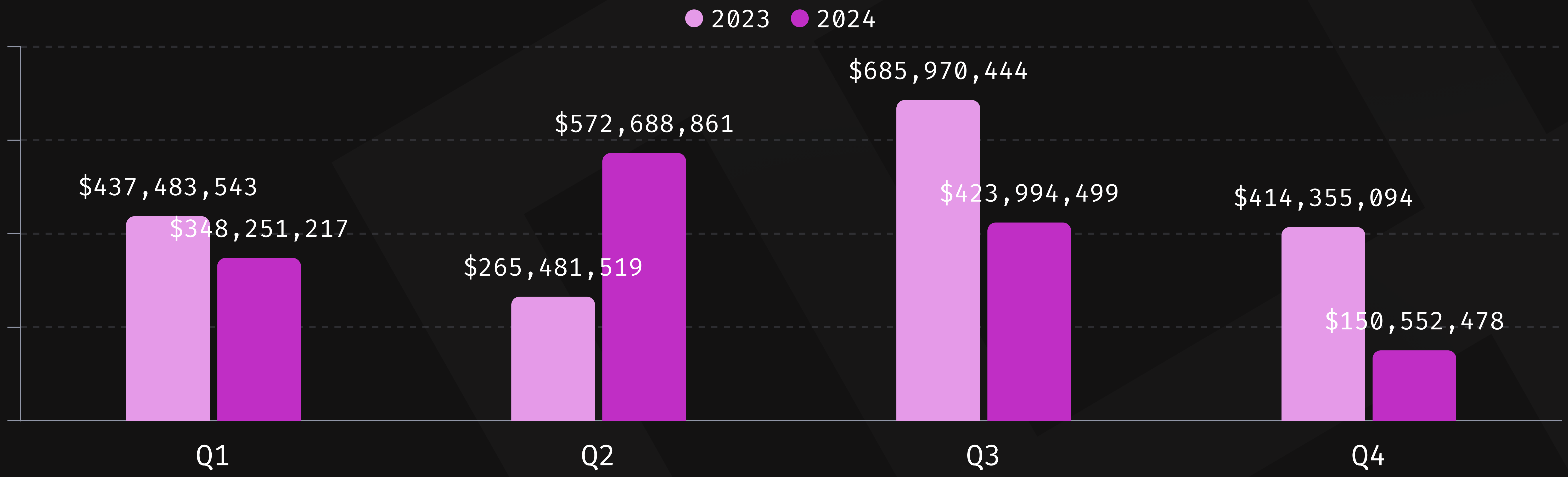
In 2024, Q2 took the lead with **$572,688,861** in total losses across 72 incidents, representing 38% of the total losses.



Losses by quarter in 2024

2023 VS 2024

In 2023, Q3 took the lead with $685,970,444 in total losses across 75 incidents, representing 38% of the total losses.
In 2024, Q2 took the lead with $572,688,861 in total losses across 72 incidents, representing 38% of the total losses.



Losses by quarter in 2024

OVERVIEW

Q1 2024

The total losses in Q1 2024 were $348,251,217. This number represents a 20.4% decrease compared to Q1 2023, when hackers and fraudsters stole $437,483,543. Most of that sum was lost by two specific projects: Orbit Bridge and Munchables. These projects together amounted to a total loss of $144,480,000.

Q2 2024

The total losses in Q2 2024 were $572,688,861. This number represents a 115.7% increase compared to Q2 2023, when hackers and fraudsters stole $265,481,519. Most of that sum was lost by two specific projects: DMM Bitcoin and BtcTurk. These projects together amounted to a total loss of $360,000,000.

Q3 2024

The total losses in Q3 2024 were $423,994,499. This number represents a 38% decrease compared to Q3 2023 when hackers and fraudsters stole $685,970,444. Most of that sum was lost by two specific projects: WazirX and the BingX. These projects together amounted to a total loss of $287,000,000.

Q4 2024

The total losses in Q4 2023 were $150,552,478. This number represents 63.6% decrease compared to Q4 2023, when hackers and fraudsters stole $414,355,094. Most of that sum was lost by two specific projects: Radiant Capital and Thala. These projects together amounted to a total loss of $75,500,000.

Top losses by quarter in 2024

Q1

Orbit Bridge	$81,680,000
Munchables	$62,800,000
PlayDapp	$32,350,000
FixedFloat	$26,100,000
Curio Ecosystem	$16,000,000
GMEE	$15,000,000
Prisma Finance	$11,600,000
NFPrompt	$10,400,000
WOOFi	$8,750,000
Coinspaid	$7,500,000

Q2

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

Q3

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

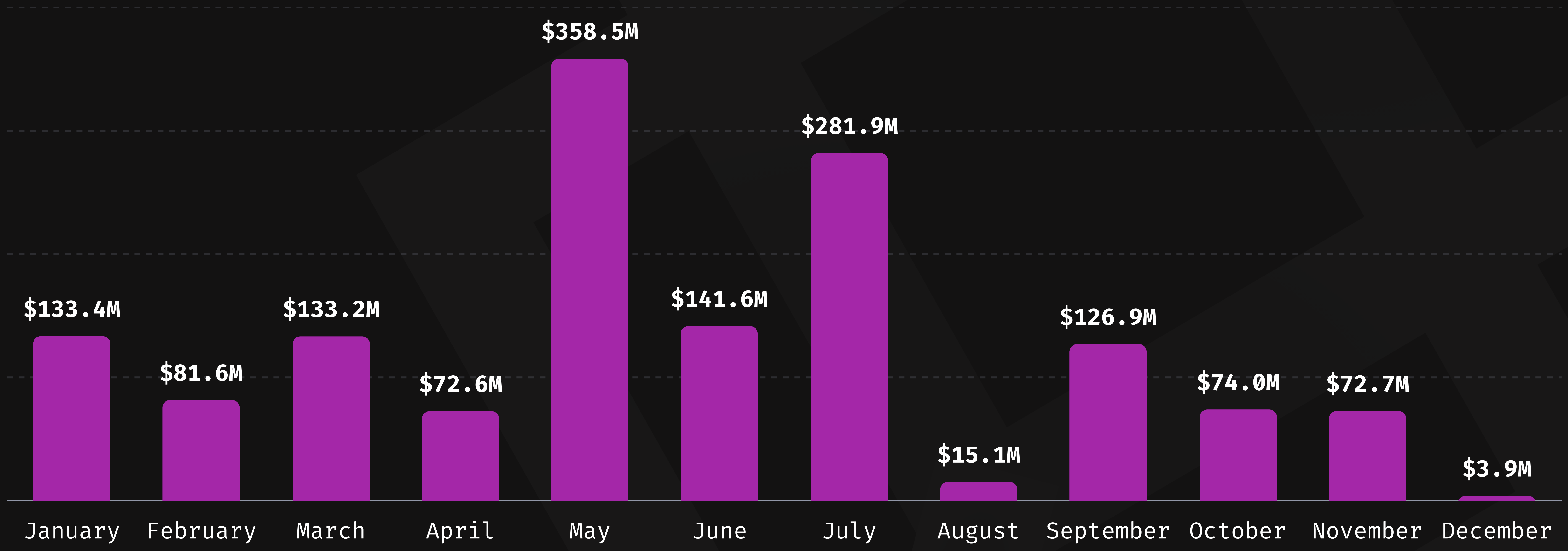
Q4

Radiant Capital	$50,000,000
Thala	$25,500,000
DEXX	$21,000,000
M2	$13,700,000
PolterFinance	$12,000,000
DeltaPrime	$4,750,000
Tapioca DAO	$4,405,600
MetaWin	$4,000,000
Sunray Finance	$2,700,000
CoinPoker	$2,000,000

Monthly Losses in 2024

OVERVIEW

In total, the ecosystem has witnessed **$1,495,487,055** in losses year-to-date (YTD) across 232 specific incidents. Overall, Q2 in 2024 recorded the highest losses, primarily driven by more than $358.5 million in May, followed by Q3, with over $281.9 million in July losses.

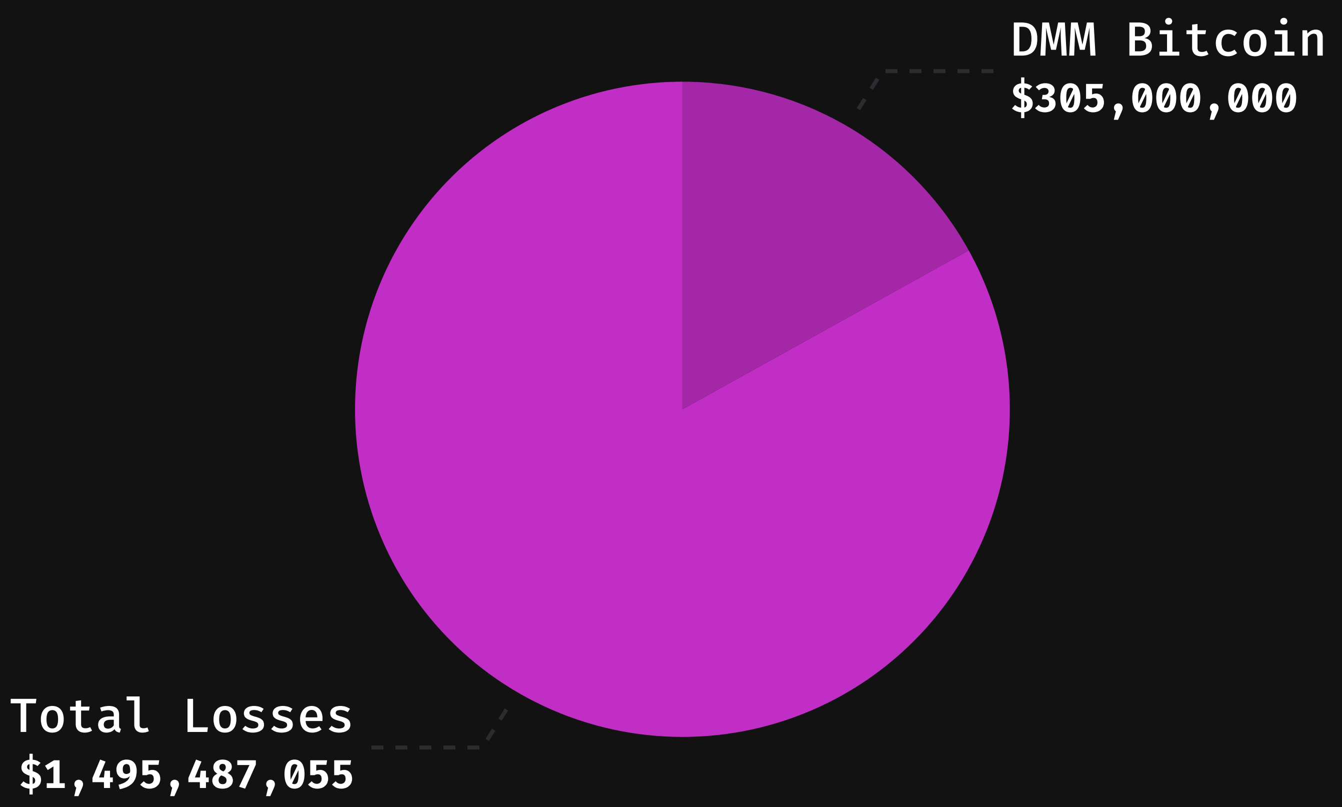


Major Exploits in 2024 Analysis

The year was marked by two major attacks on DMM Bitcoin and WazirX, totalling $540,000,000. Together, these two projects represent 36% of 2024 losses alone.

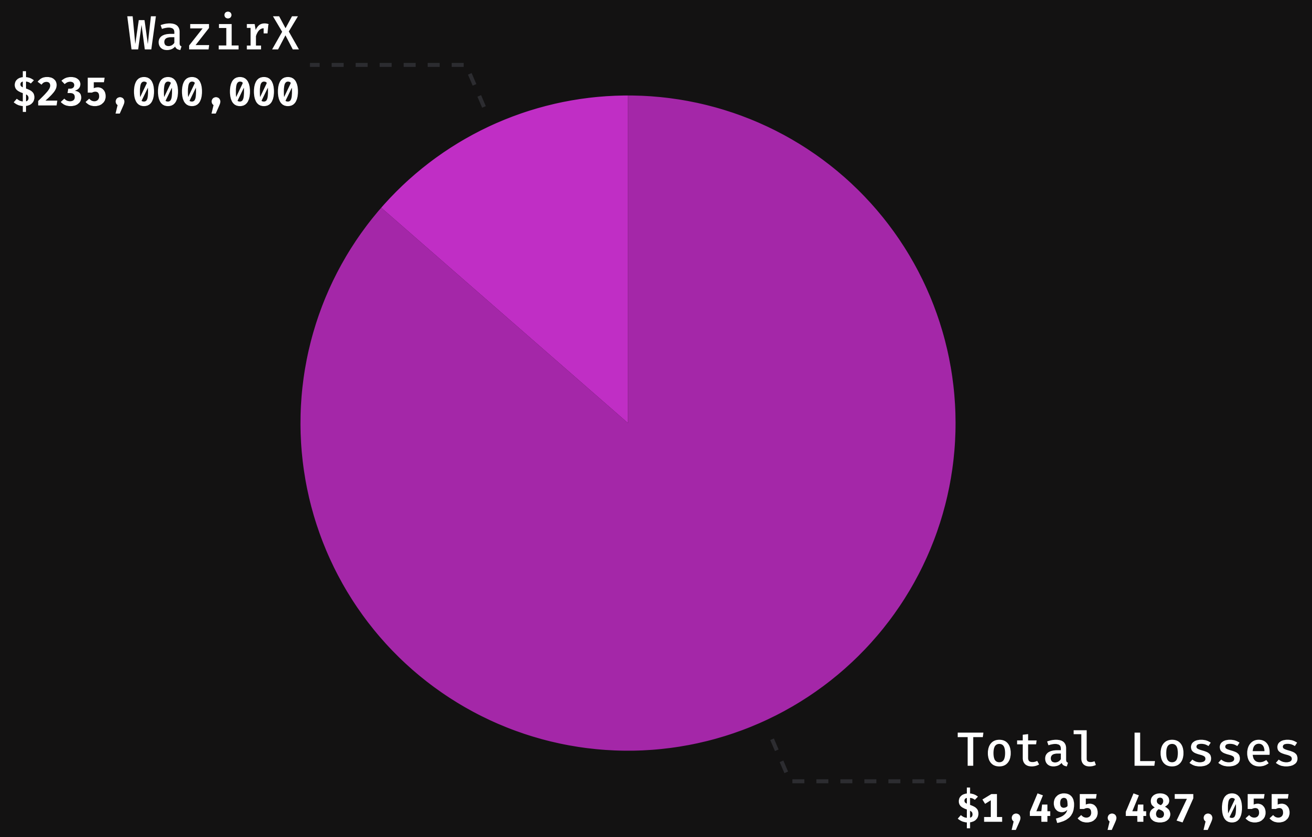
DMM BITCOIN, $305 MILLION

- On May 31st, 2024, the Japanese centralised cryptocurrency exchange suffered a private key hack that caused a loss of $305 million.



WAZIRX, $235 MILLION

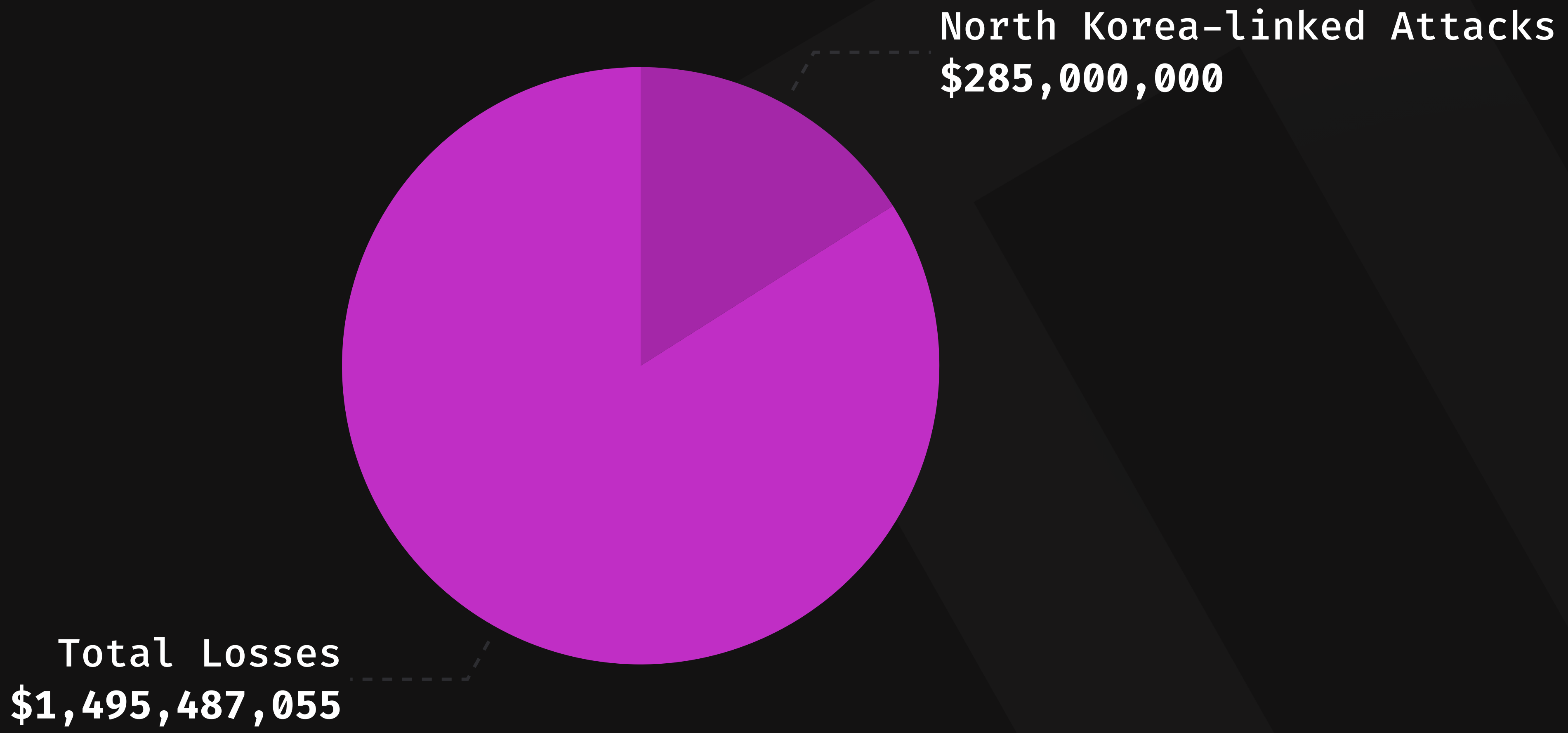
- On July 18th, 2024, WazirX, India's leading domestic crypto exchange, suffered an attack that resulted in a $325 million loss. WazirX's Safe Multisig wallet on Ethereum was compromised. The attack has since been linked to North Korean hackers.

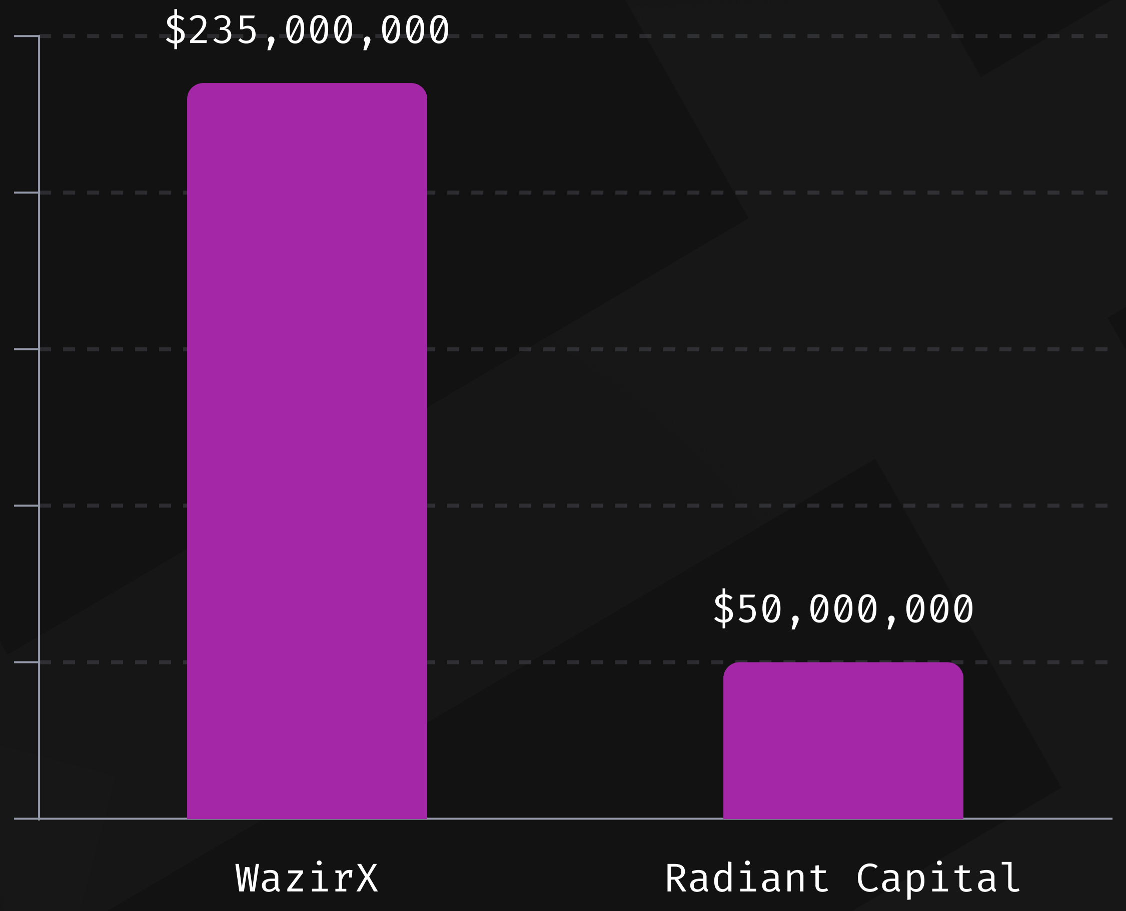


North Korean Hackers

NORTH KOREAN HACKERS IN FOCUS

- North Korean hackers have allegedly been responsible for two notable attacks, representing 16% of total crypto losses in 2024. They have been linked to breaches of WazirX and Radiant Capital, profiting a combined total of $285 million.
- In the WazirX attack, hackers compromised the platform's Safe Multisig wallet on Ethereum. Meanwhile, Radiant's exploit involved sending a malware-laced PDF to company engineers, allowing attackers to compromise multiple developer devices. Both attacks highlight how North Korean hackers continue to often target project infrastructure and leverage sophisticated social engineering operations to compromise systems.





Hacks vs. Fraud Analysis

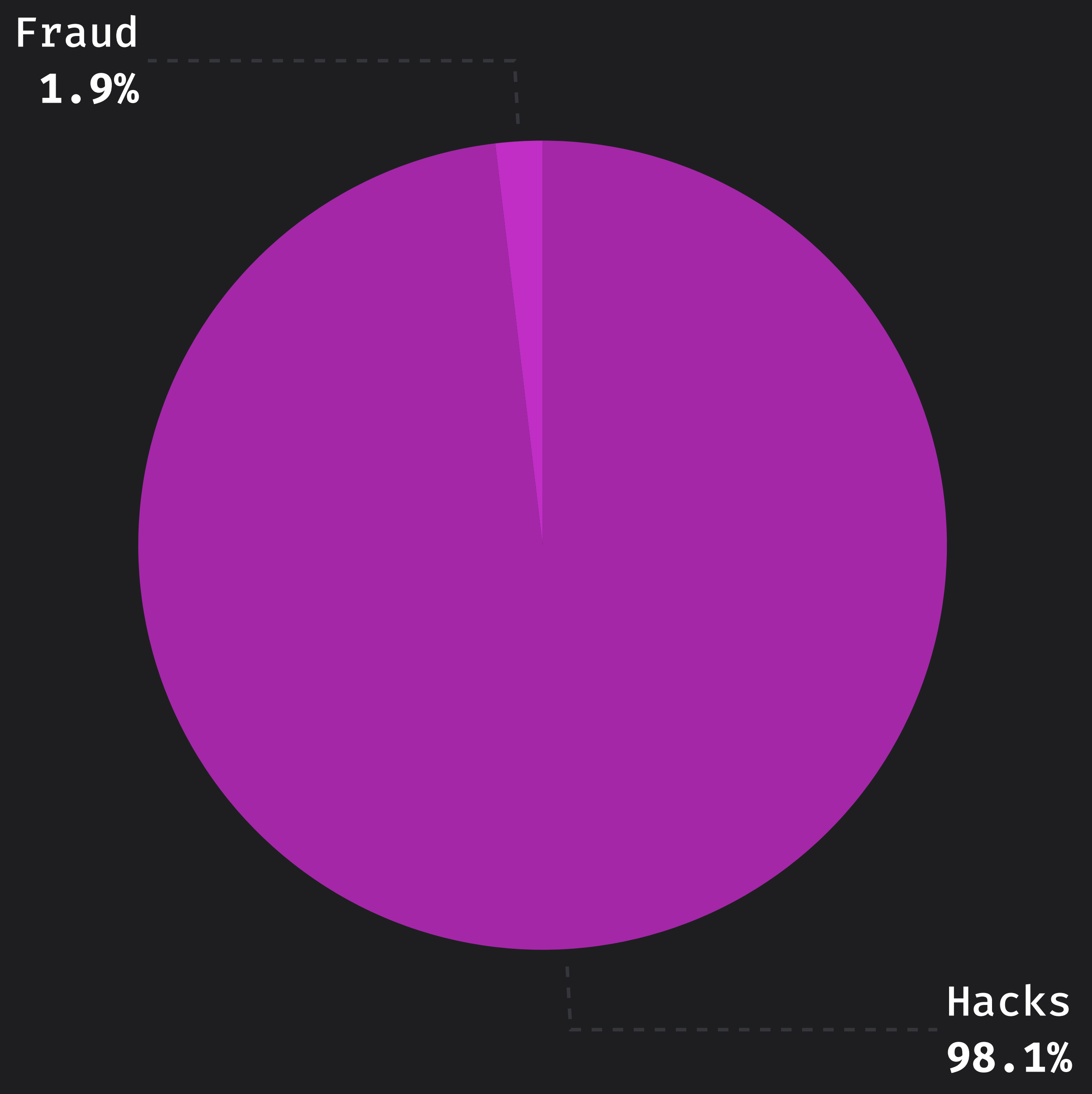
In 2024, hacks continue to be the predominant cause of losses as compared to frauds, scams, and rug pulls. An analysis of the losses shows that fraud accounts for 1.9% of the total losses in the 2024, while hacks account for 98.1%.

OVERVIEW

- **Hacks**
  In total, we have seen a loss of **$1,467,448,336** to hacks in 2024 across 192 specific incidents. These numbers represent a 13.6% decrease compared to 2023, when losses caused by hacks totalled $1,699,872,321.

- **Fraud**
  In total, we have seen a loss of **$28,038,719** to fraud in 2024 across 40 specific incidents. These numbers represent a 72% increase compared to 2023 when losses caused by frauds, scams, and rug pulls totalled $103,418,279.

Hacks vs. Fraud in 2024



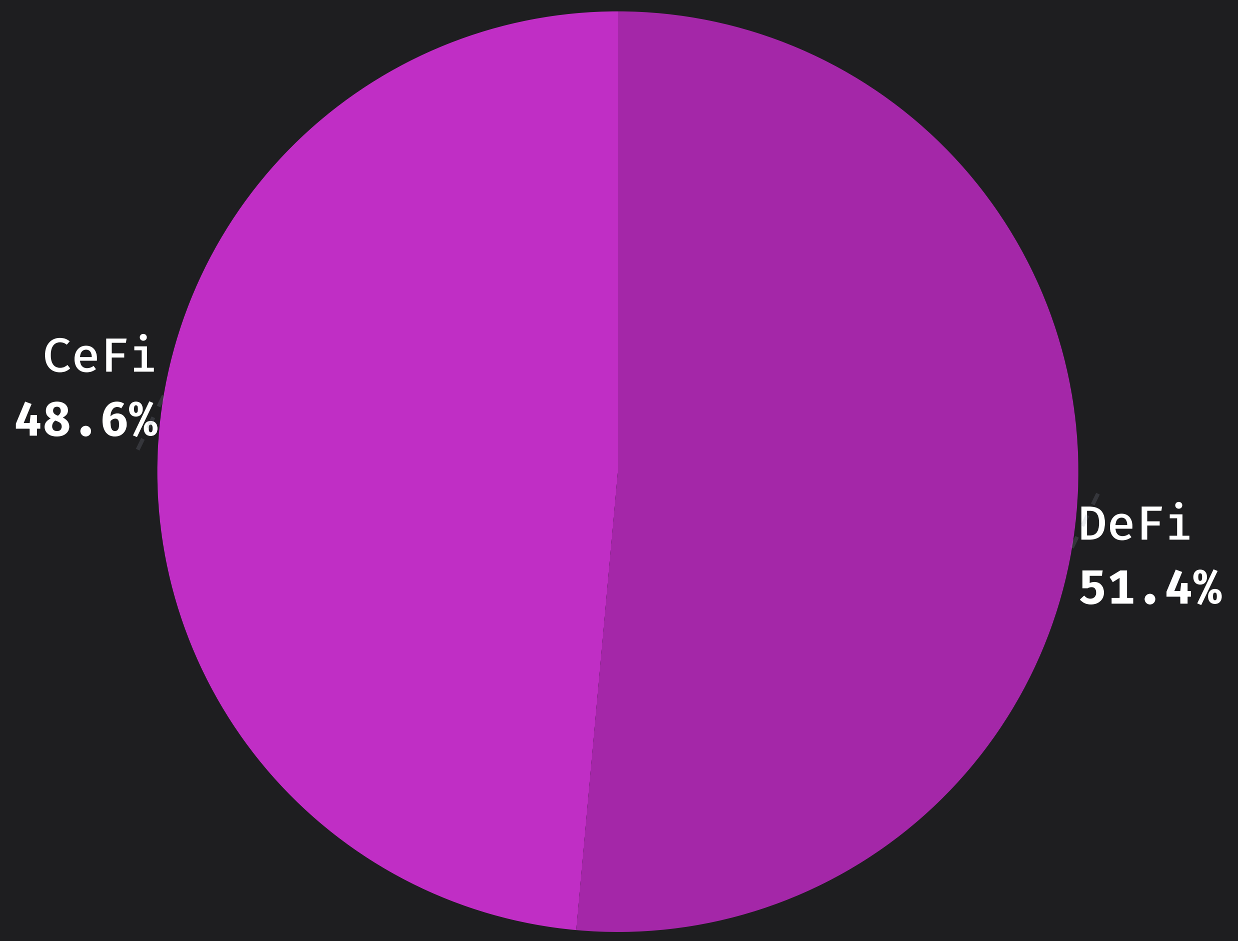
DeFi vs. CeFi Analysis

In 2024, DeFi continues to be the main target for exploits, compared to CeFi. DeFi represents 51.4% of the total losses, while CeFi represents 48.6% of the total losses.

OVERVIEW

- **DeFi**
  DeFi has suffered **$769,287,055** in total losses in 2024 across 221 incidents. These numbers represent a 44.8% decrease compared to 2023 when DeFi losses totalled $1,394,382,600.
- **CeFi**
  CeFi has suffered **$726,200,000** in total losses in 2024 across 11 incidents. These numbers represent a 77.5% increase compared to 2023 when CeFi losses totalled $408,908,000.

DeFi vs. CeFi in 2024

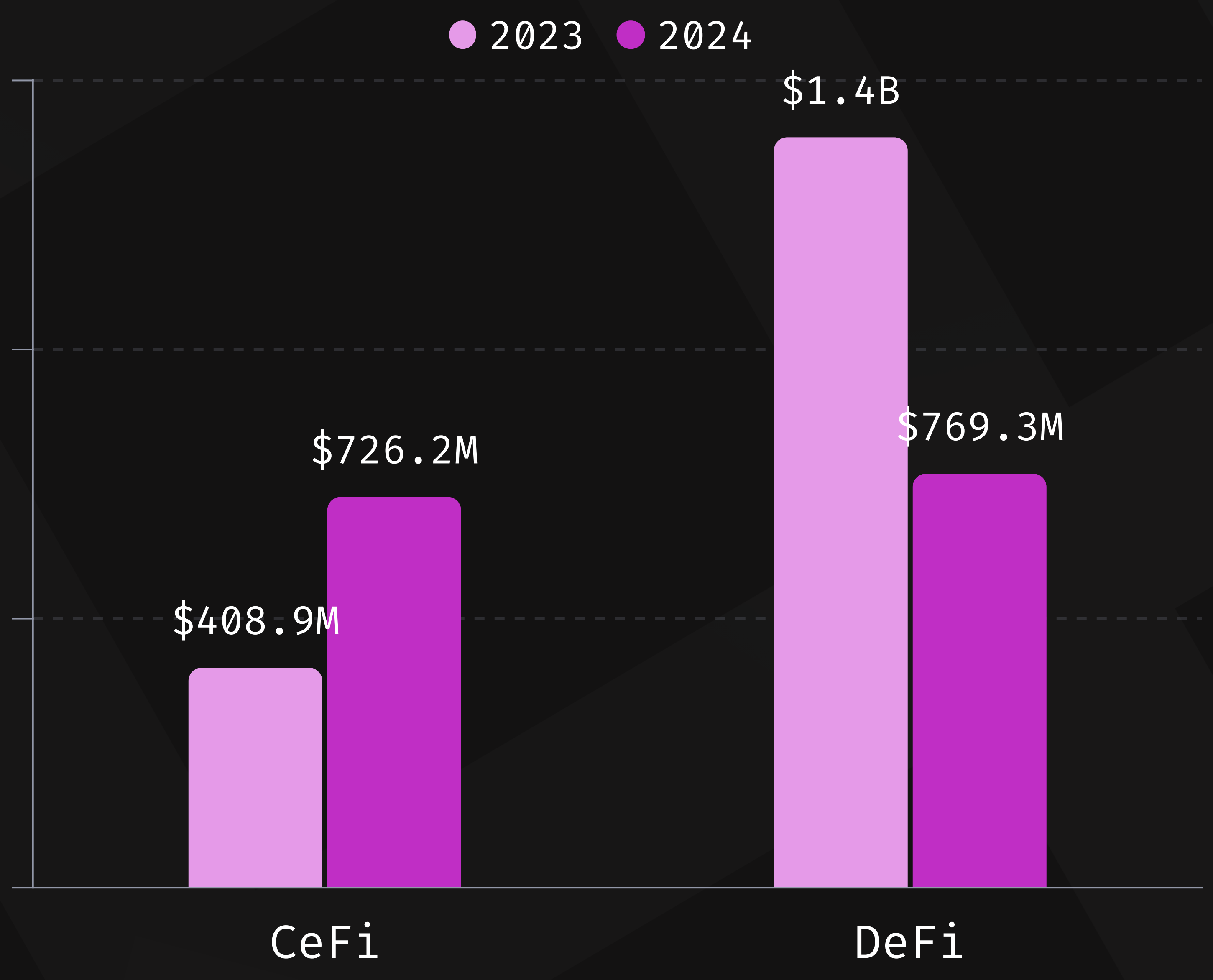


IN FOCUS

CeFi Regains Attackers' Attention

While Decentralized Finance (DeFi) remained the main focus of successful exploits, representing 51.4% of losses across 307 specific cases, attacks on CeFi saw a sharp increase. **CeFi accounted for nearly half of the total losses (48.6%)** despite only 11 significant cases. This hasn’t happened since 2021, as successful CeFi hacks have slowed considerably over the past two years.

DeFi vs. CeFi

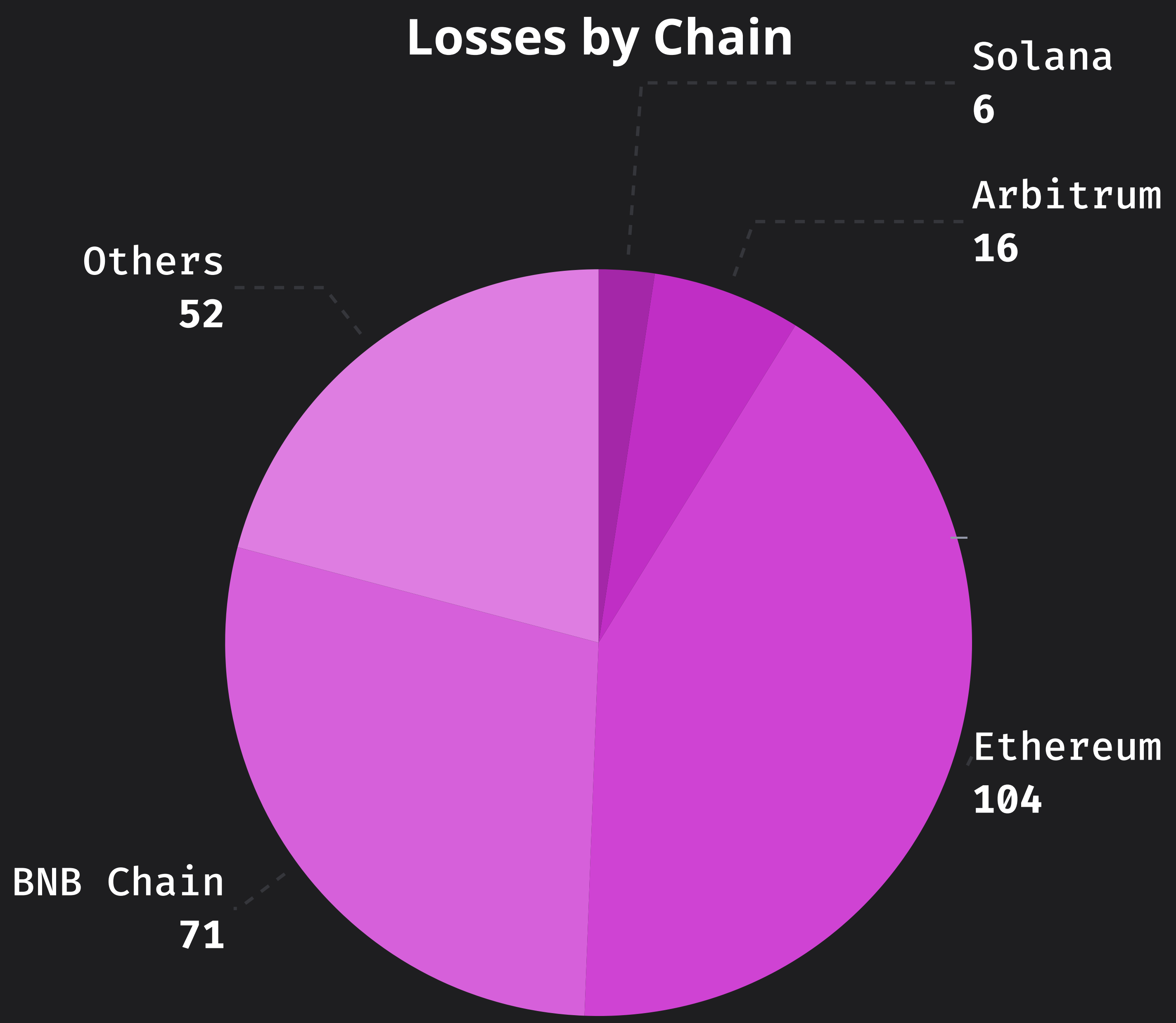


Losses by Chain

The two most targeted chains in 2024 were Ethereum and BNB Chain. Ethereum suffered the most individual attacks with 104 incidents representing 44% of the total losses across targeted chains. BNB Chain witnessed 71 incidents, representing 30% respectively.

OVERVIEW

- Ethereum and BNB Chain represent more than half of the chain losses in 2024.
- Arbitrum came in third with 16 incidents, representing 6.4% of total losses across chains. Solana, Optimism, Blast, and Base followed with 6 incidents each.



Funds Recovery

OVERVIEW

In total, **$115,577,966** has been recovered from stolen funds in **14** specific situations. This number makes up **7.7%** of the total losses in 2024.

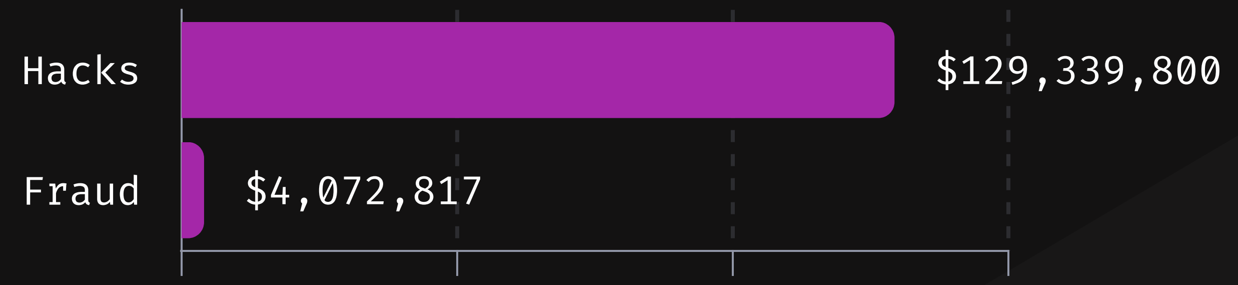
	Stolen	Recovered
Ronin Network	$12,000,000	$10,000,000
ShezmuTech	$4,900,000	$4,900,000
Bloom	$540,000	$486,000
ALEX Lab	$4,300,000	$3,900,000
Gala Games*	$21,000,000	$21,000,000
YOLO Games	$1,500,000	$1,350,000
Munchables	$62,800,000	$62,800,000
Seneca	$6,500,000	$5,300,000

	Stolen	Recovered
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
MAAT	$272,800	$56,966

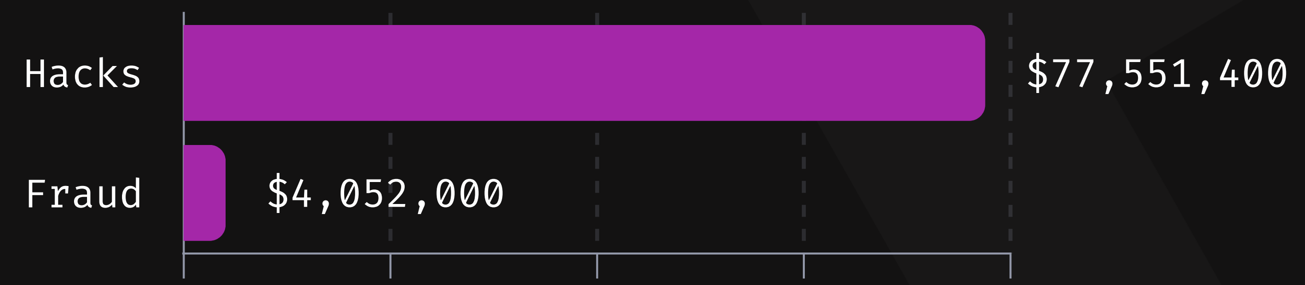
In Focus: Crypto Losses 2024 | Monthly Overview

TOTAL LOSSES: HACKS VS. FRAUD

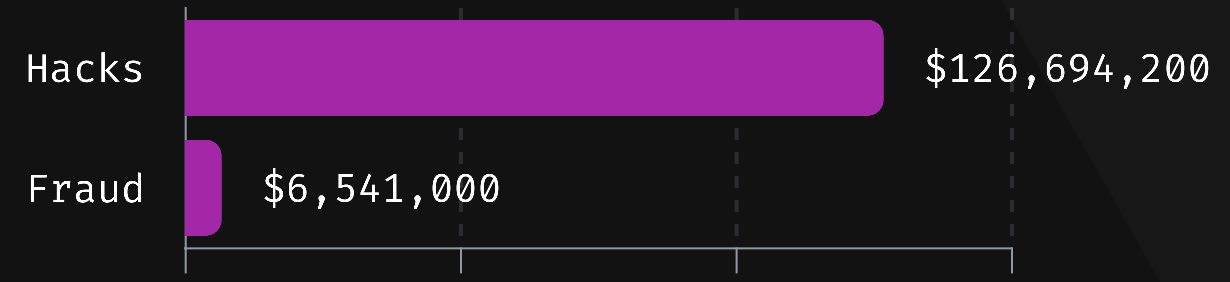
JANUARY



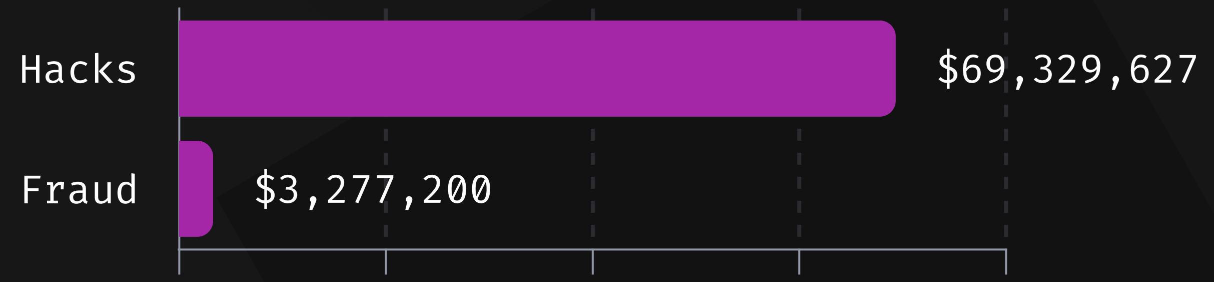
FEBRUARY



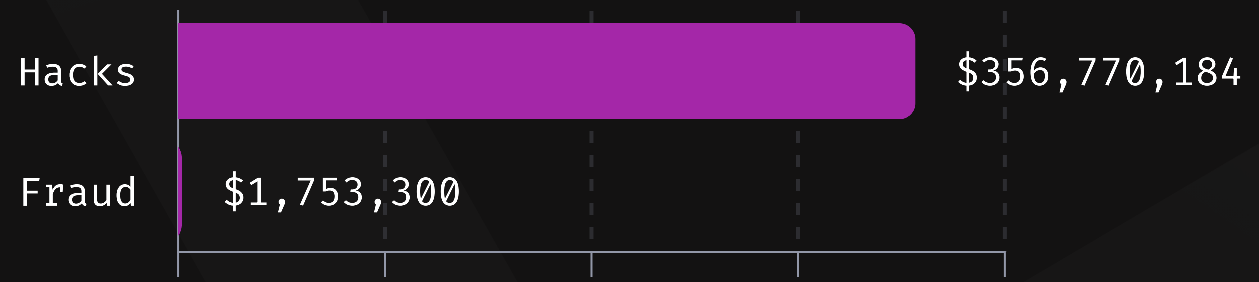
MARCH



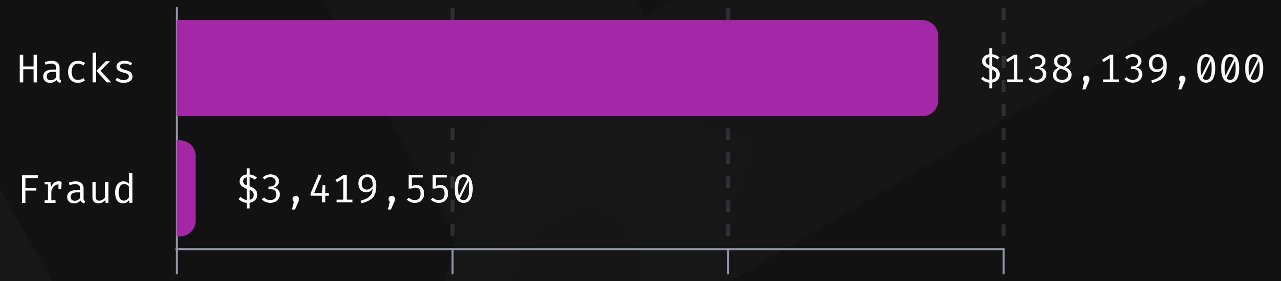
APRIL



MAY

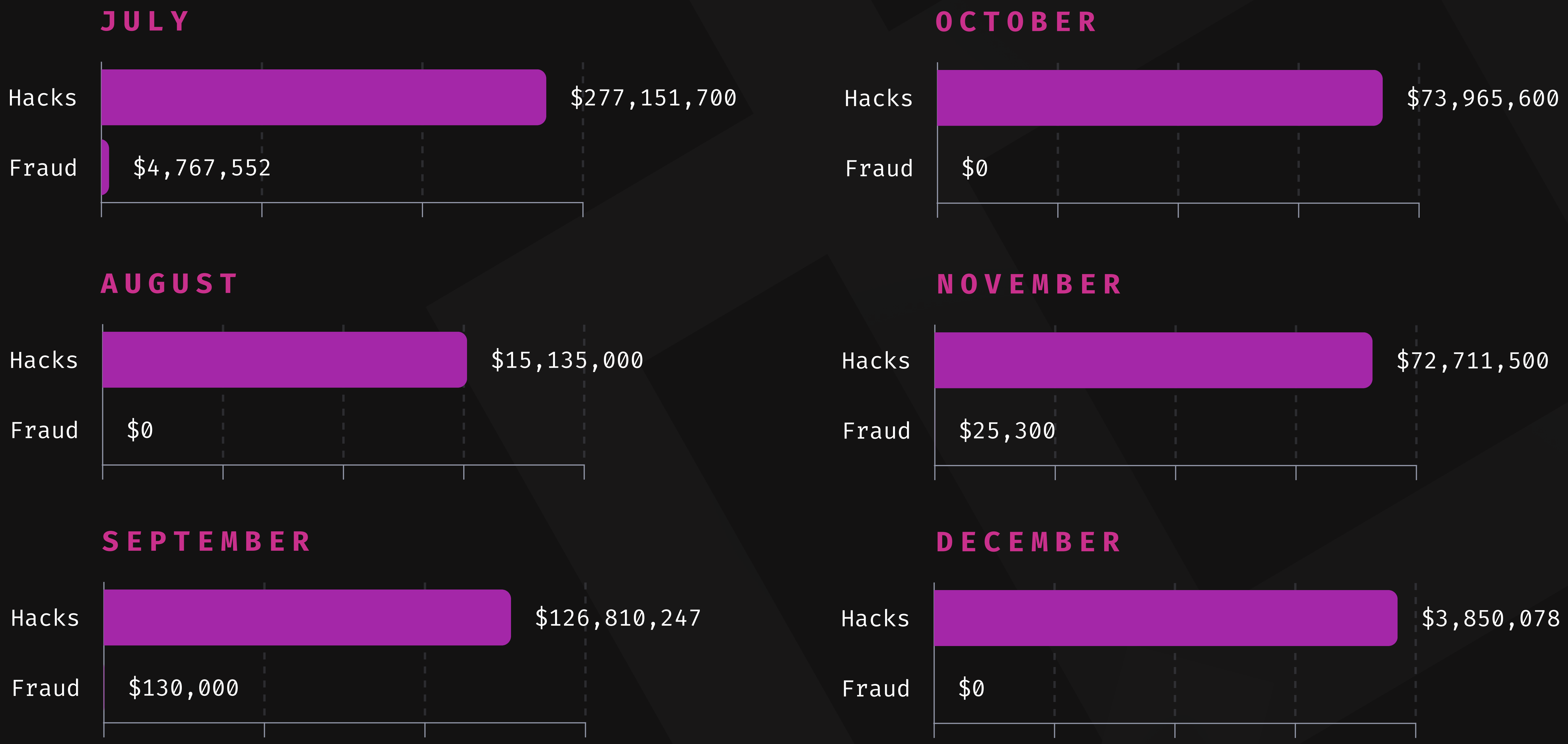


JUNE



In Focus: Crypto Losses 2024 | Monthly Overview

TOTAL LOSSES: HACKS VS. FRAUD



Web3 Security in 2025: Key Trends

HACKING

- Despite the slight improvement from last year's $1.7 billion in losses, threats persist. Hackers are evolving; they've infiltrated crypto projects, compromised hot wallets, and exploited vulnerabilities in the darkest corners of the ecosystem. What makes this even more pressing is the massive surge in the Total Value Locked (TVL) in DeFi, which has grown 163% this year from $51 billion to $134.17 billion. With so much at stake, the race between hackers and securing the technology for widespread adoption has never been more intense.
- Generally, losses have primarily been driven by larger-scale exploits, often resulting from private key compromises. Hackers will continue to target project infrastructure heavily, as the leakage of a key can lead to the theft of all funds controlled by it. Additionally, hackers will attempt to bypass the more mature and fortified DeFi projects, focusing more extensively on infrastructure and CeFi.

INDUSTRY

- Increasing use of automated tooling, especially Artificial Intelligence and Machine Learning (AI/ML) tooling. After years of being fairly inconsequential, AI/ML tooling are just beginning to show themselves to be effective. This trend is expected to accelerate rapidly.
- The rise of DeSec, or the decentralized security industry, complete with successful tokenized products. DeSec is likely to emerge over the next year as the first products get to maturity.

“

> Despite progress in making crypto safer, particularly in terms of hacks per dollar, the sector still faces significant challenges. As institutional money flows in and the Total Value Locked (TVL) in the ecosystem grows, security remains one of the major limiting factors for widespread adoption. The stakes are high, and we will also witness an unprecedented surge in security advancements, with AI-powered tools and decentralized security solutions becoming essential in the fight to safeguard the ecosystem.

Mitchell Amador

Founder and CEO at Immunefi

Crypto Losses 2024

Immunefi

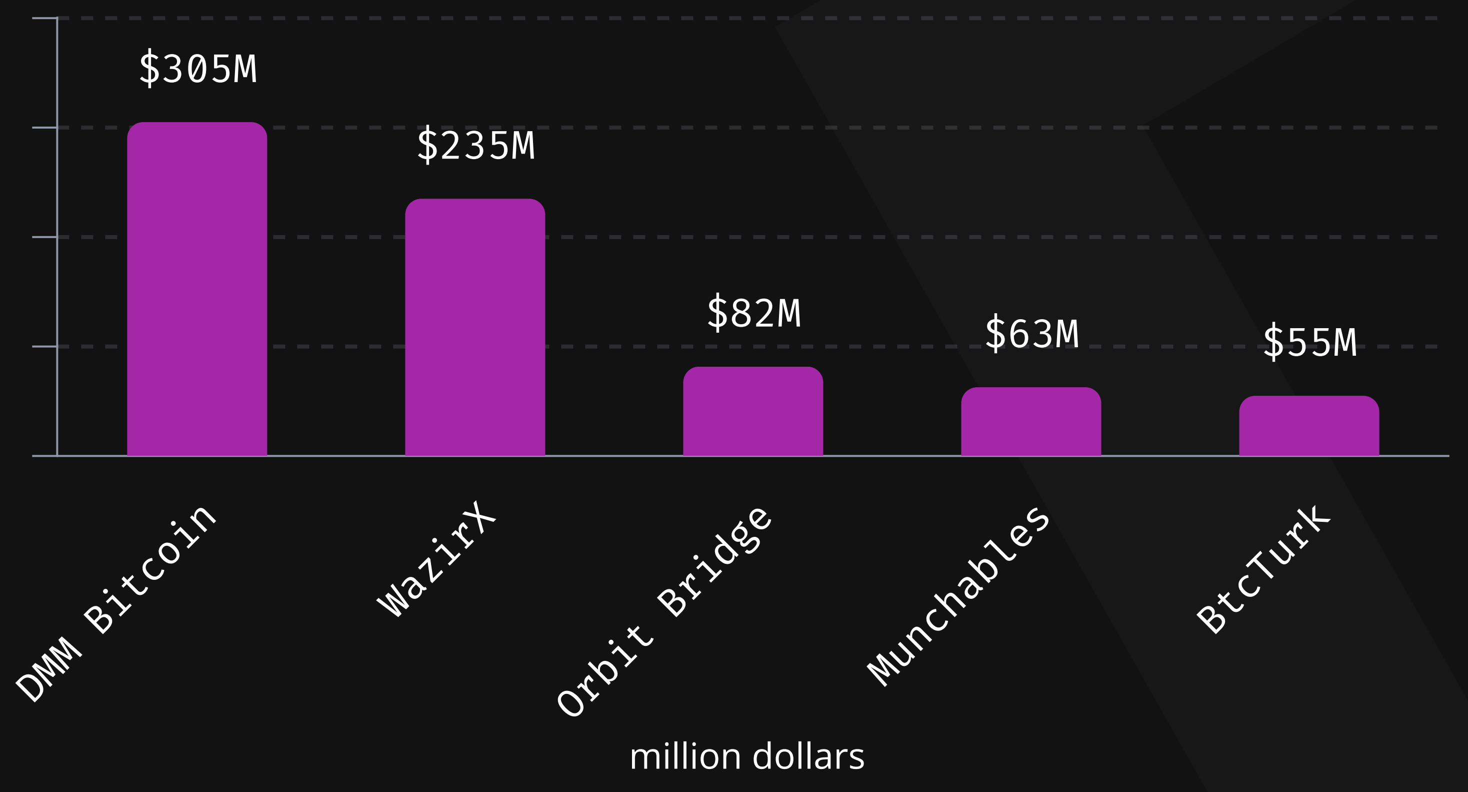
TOTAL LOSSES YTD

$1,495,487,055

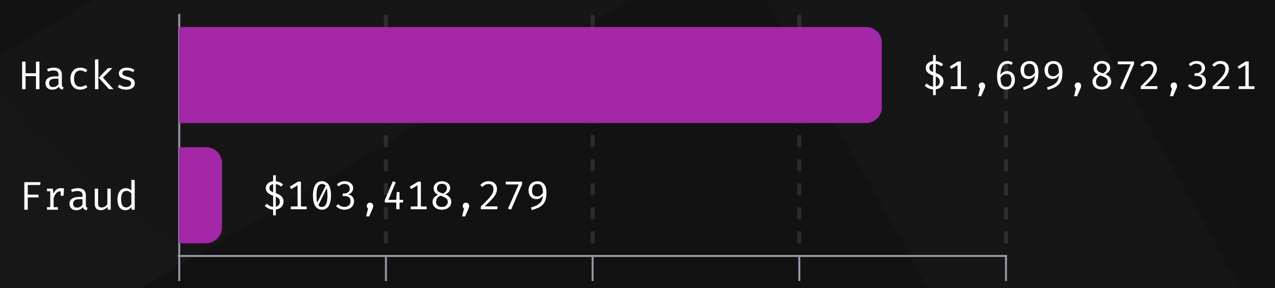
IN 2023

$1,803,290,600

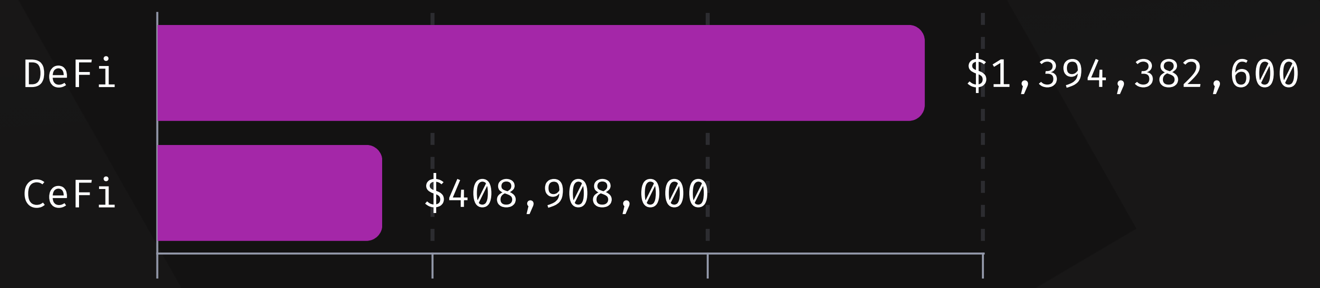
MAJOR LOSSES



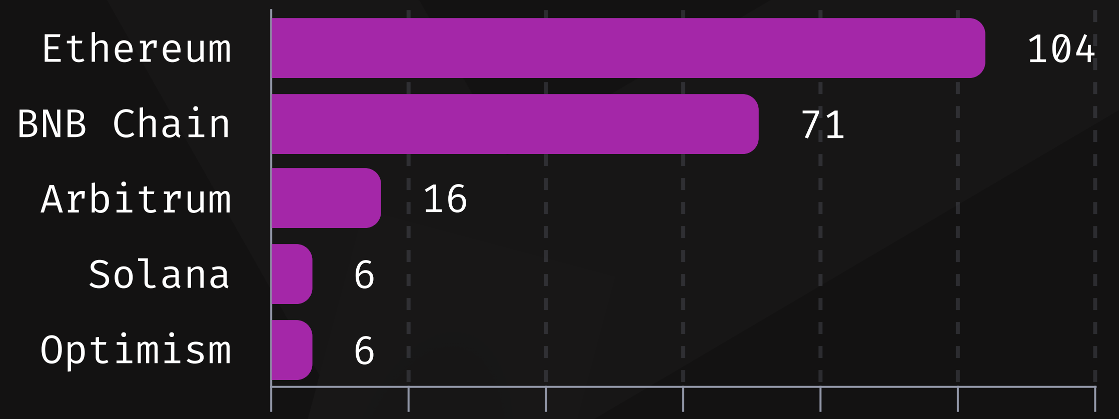
HACKS VS. FRAUD



DEFI VS. CEFI



TOP LOSSES BY CHAIN



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

IN FOCUS

CRYPTO LOSSES IN Q4 2024

Crypto Losses in Q4 2024

Overview of the volume of crypto funds lost by the community due to hacks and scams in Q4 2024, as assessed by Immunef.

OVERVIEW

In total, we have seen a loss of **$150,552,478** across the web3 ecosystem in Q4 2024. **$150,527,178** was lost to hacks in Q4 2024 across 58 specific incidents and **$25,300** was lost to fraud in across 2 specific incidents. This number represents a 64% decrease compared to Q4 2023, when hackers and fraudsters stole $414,355,094.

Most of the sum in Q4 was lost by two specific projects: Radiant Capital, the lending protocol**,** and Thala, a decentralized finance firm.

KEY TAKEAWAYS IN Q4 2024

- The two major exploits of the quarter totaled **$75,500,000** alone, accounting for **50.1%** of all losses in Q4 2024.
- In Q4 2024, hacks continued to be the predominant cause of losses at **99.9%** in comparison to frauds, scams, and rug pulls, which amounted to only **0.02%** of the total losses.
- In Q4 2024, DeFi continued to be the main target of successful exploits at **89.5%** as compared to CeFi at **10.5%** of the total losses.
- The two most targeted chains in Q4 2024 were BNB Chain and Ethereum. BNB Chain suffered the most individual attacks, with 31 incidents representing 49.2% of the total losses across targeted chains. Ethereum witnessed 18 incidents, representing 29% respectively. Avalanche followed with 3 incident.
- In total, **$25,556,966** has been recovered from stolen funds in **2** specific situations. This number makes up **17%** of the total losses in Q4 2024.

Top 10 Losses in Q4 2024*

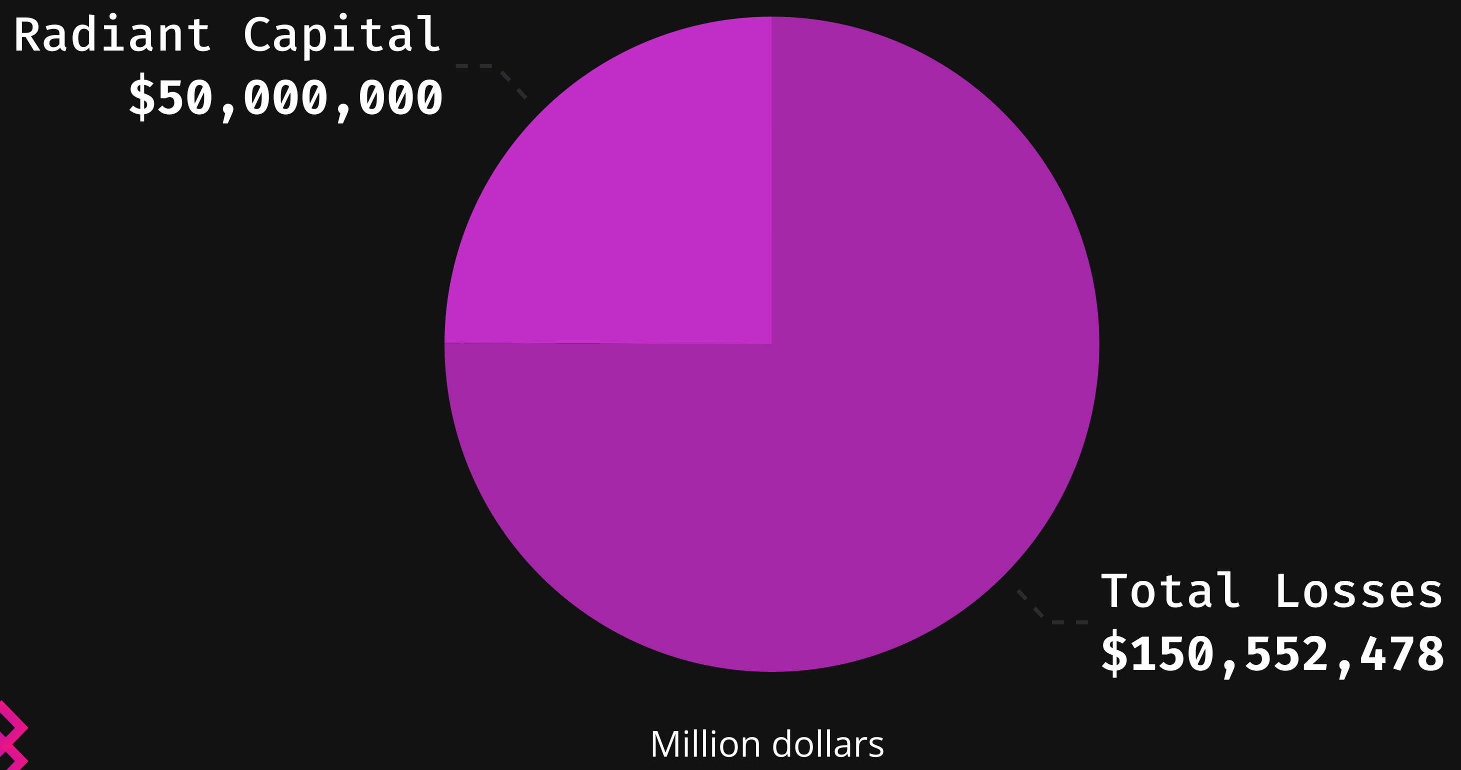
Radiant Capital	$50,000,000
Thala	$25,500,000
DEXX	$21,000,000
M2	$13,700,000
PolterFinance	$12,000,000
DeltaPrime	$4,750,000
Tapioca DAO	$4,405,600.00
MetaWin	$4,000,000
Sunray Finance	$2,700,000
CoinPoker	$2,000,000

Major Exploits in Q4 Analysis

Most of the Q4 loss sum was lost by two specific projects: Radiant Capital and Thala, totalling **$75,500,000**. Together, these two projects represent 50.1% of Q4 losses alone.

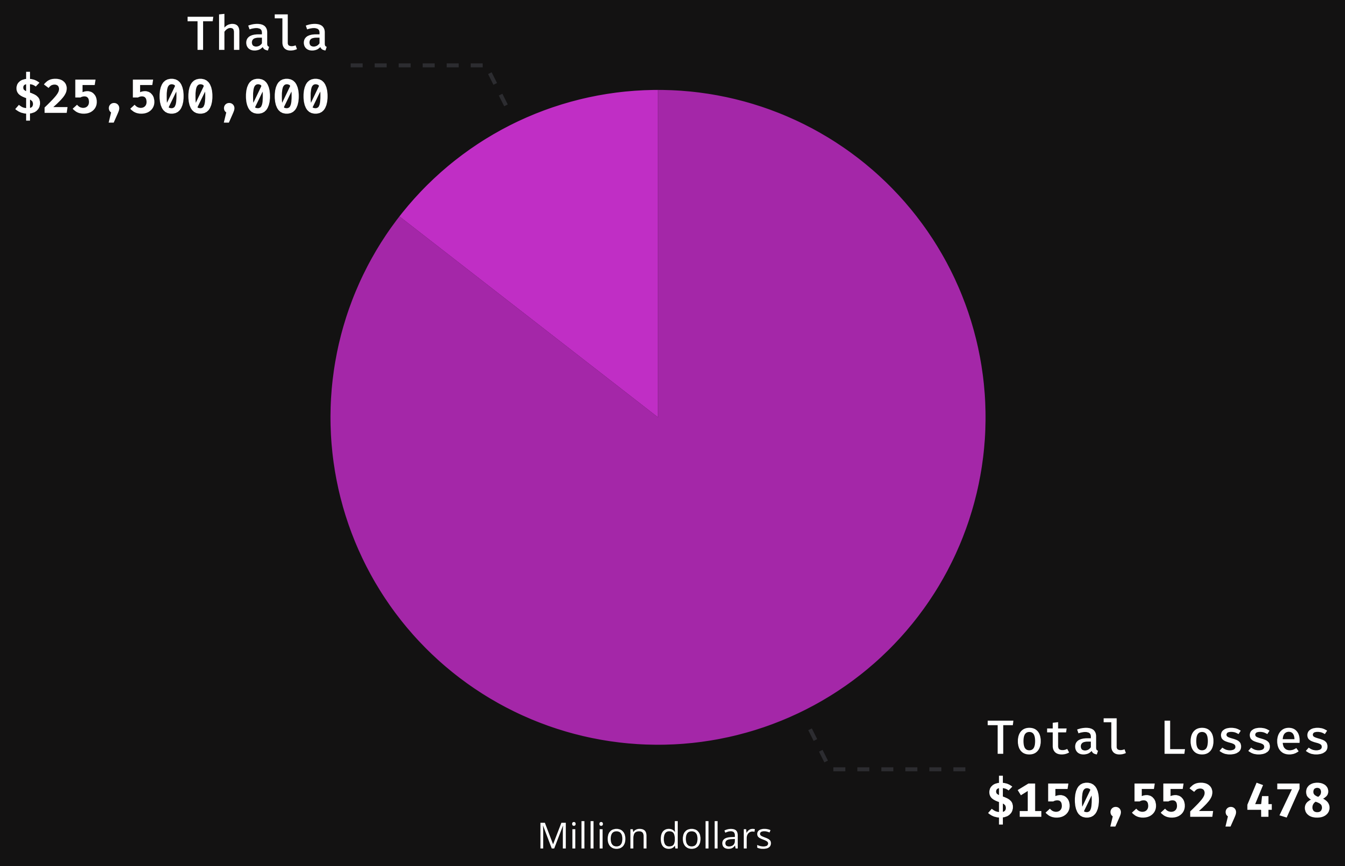
RADIANT CAPITAL, $50 MILLION

- On October 17, 2024, blockchain lending protocol Radiant Capital has suffered a private key compromise and lost more than $50 million.



THALA, $25,5 MILLION

- On November 15, 2024, decentralized finance firm Thala Labs suffered a security breach, allowing the exploiter to withdraw $25.5 million. Later, Thala recovered the whole sum, after the hacker was tracked down by law enforcement and crypto sleuths.

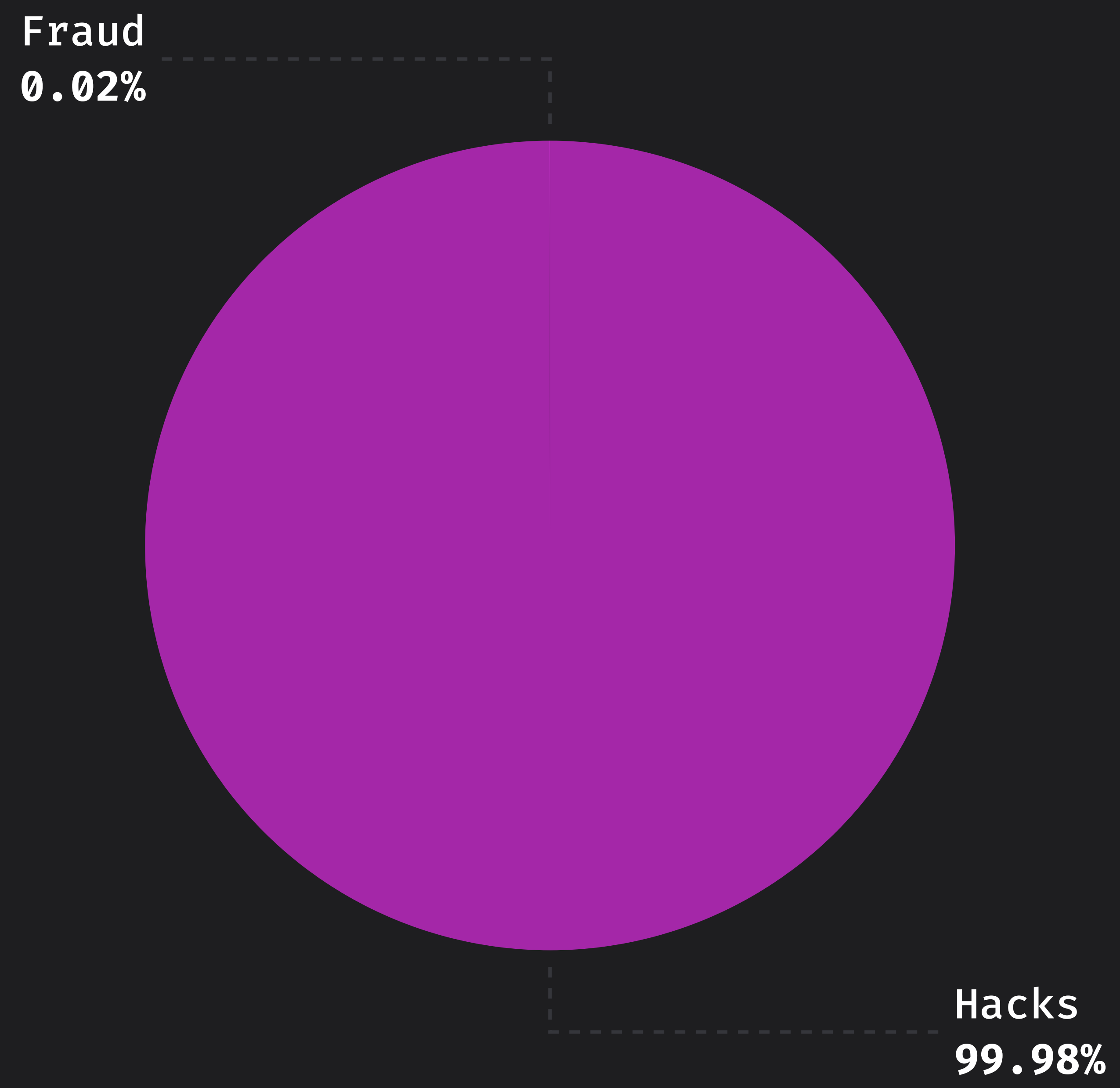


Hacks vs. Fraud Analysis

In Q4 2024, 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 0.02% of the total losses in the Q4 2024, while hacks account for 99.98%.

OVERVIEW

- **Hacks**
  In total, we have seen a loss of **$150,527,178** to hacks in Q4 2024 across 58 specific incidents. These numbers represent a 62% decrease compared to Q4 2023 when losses caused by hacks totalled $397,450,523.
- **Fraud**
  In total, we have seen a loss of **$0.02** to fraud in Q4 2024 across 2 specific incidents. These numbers represent a 99.8% decrease compared to Q4 2023, when losses caused by frauds, scams, and rug pulls totaled $16,904,571.

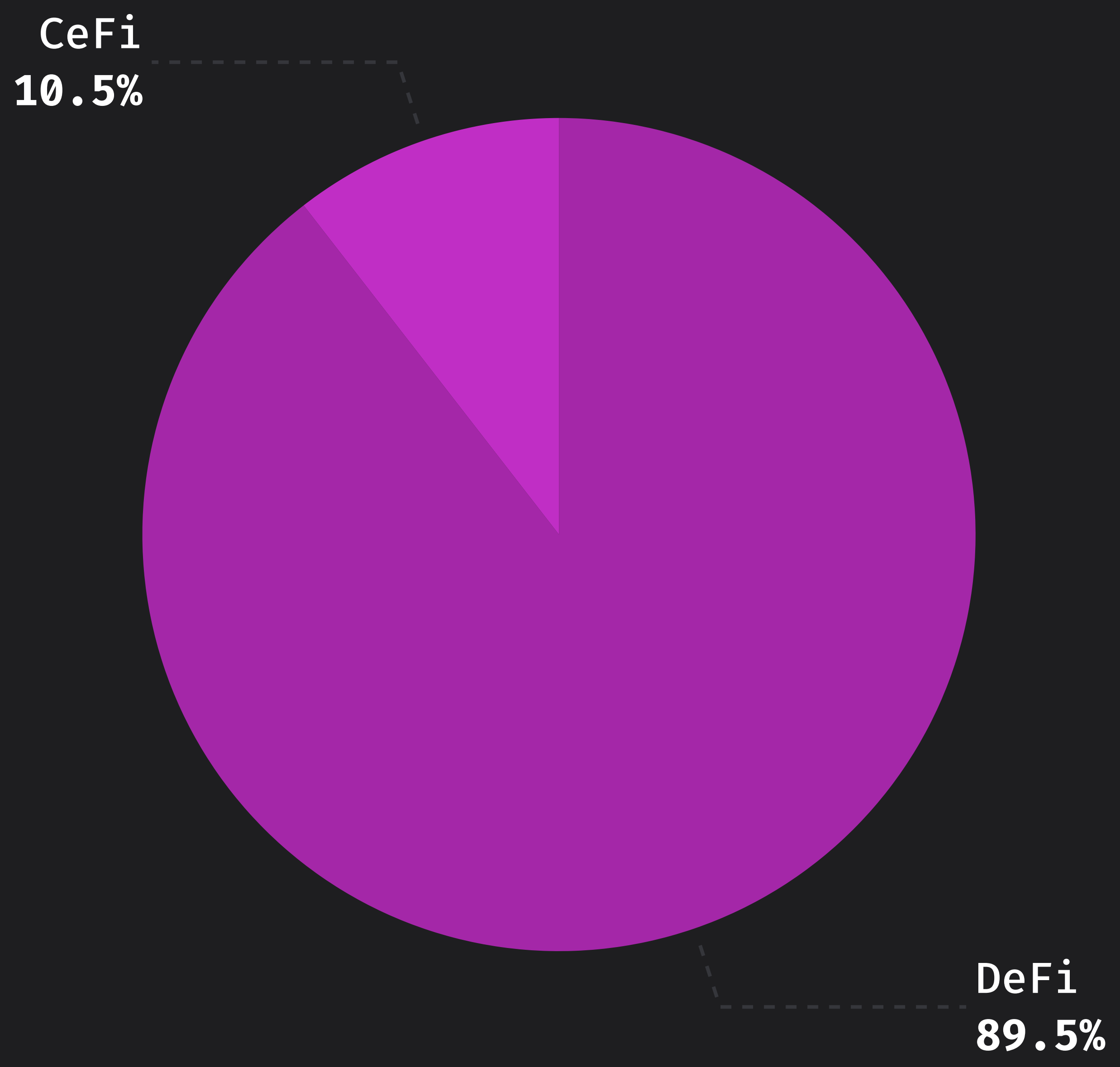


DeFi vs. CeFi Analysis

In Q4 2024, DeFi continues to be the main target for exploits, compared to CeFi. DeFi represents **89.5%** of the total losses, while CeFi represents **10.5%** of the total losses.

OVERVIEW

- **DeFi**
  DeFi has suffered **$134,752,478** in total losses in Q4 2024 across 57 incidents. These numbers represent a 41.4% decrease compared to Q4 2023, when DeFi losses totaled $229,955,094.
- **CeFi**
  CeFi has suffered **$15,800,000** in total losses in Q4 2024 across 3 incidents. These numbers represent a 91.4% decrease compared to Q4 2023, when DeFi losses totaled $184,400,000.



Losses by Chain

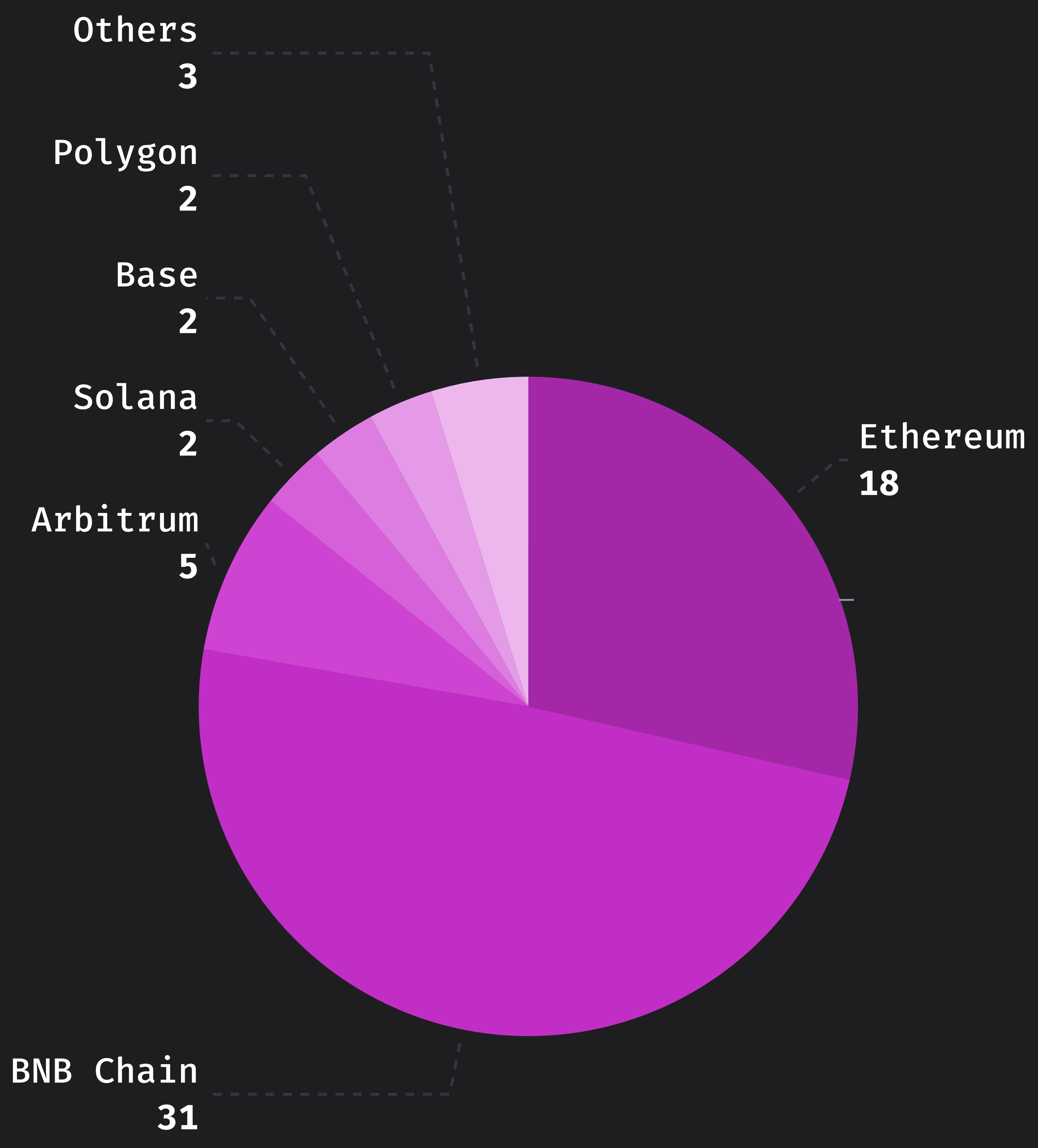
The two most targeted chains in Q4 2024 were BNB Chain and Ethereum. BNB Chain suffered the most individual attacks, with 31 incidents representing 49.2% of the total losses across targeted chains. Ethereum witnessed 18 incidents, representing 28.6% respectively.

OVERVIEW

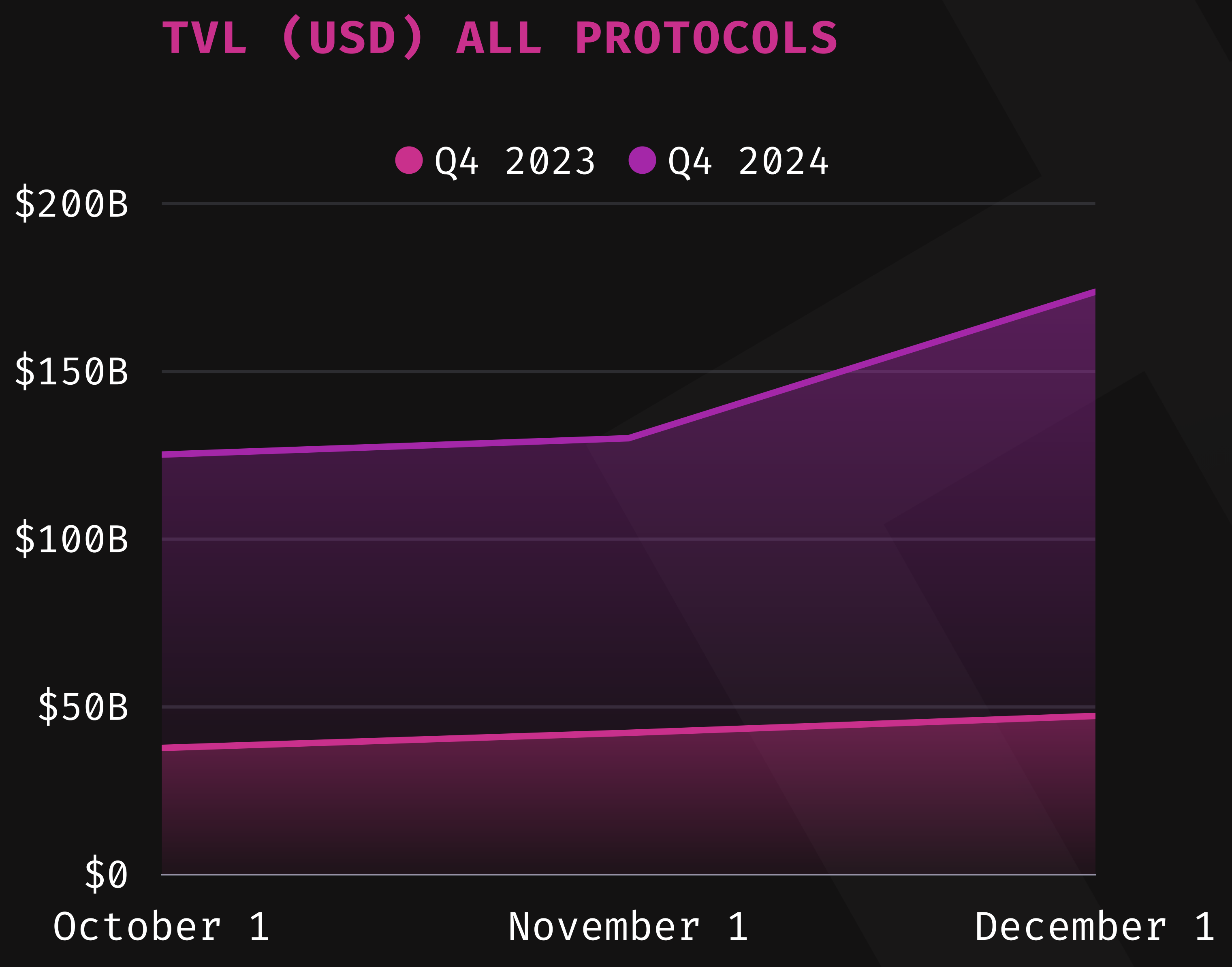
- BNB Chain and Ethereum represent more than half of the chain losses in Q4 2024. Arbitrum came in third with 5 incidents, representing 7.9% of total losses across chains.
- Solana, Base and Polygon followed with 2 incidents each.

INSIGHTS

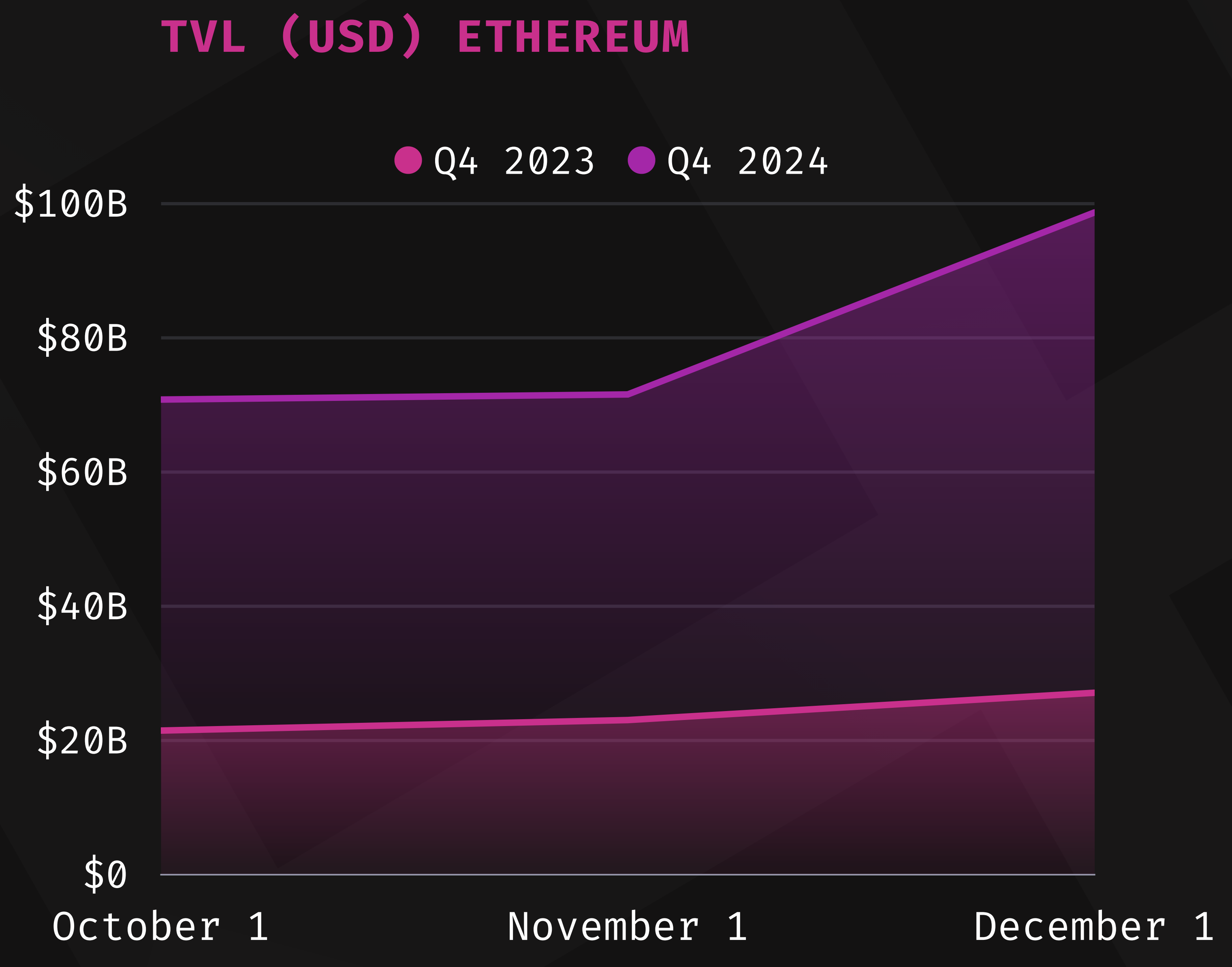
- In Q4 2024, BNB Chain once again surpassed Ethereum and became the most targeted chain compared to the previous period.



In Focus: Q4 2023 vs. Q4 2024



Total Value Locked



Total Value Locked

In Focus: Q4 2023 vs. Q4 2024

HACKS VS. FRAUDS

62% ↓

Hacks

Losses are down 62% when compared to the previous period.

99.8% ↓

Fraud

Losses are also down 99.8% when compared to the previous period.

In Focus: Q4 2022 vs. Q4 2023

DEFI VS. CEFI

41.4% ↓

DeFi

Losses are down 41.4% when compared to the previous period.

91.4% ↓

CeFi

Losses are down 91.4% when compared to the previous period.

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 **$110 million** in total bounties, while saving over **$25 billion** in user funds.

TOTAL BOUNTIES AVAILABLE

Immunefi offers over **$180 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:

- The Total Value Locked (USD) data has been extracted from DefiLlama.
- * Top 10 Losses in 2024: Munchables later recovered $62,8 million in stolen funds after the developer had shared all private keys.
- * Top 10 Losses in Q4 2024: Thala later recovered the whole sum ($25,5 million), after the hacker was tracked down by law enforcement and crypto sleuths.
- 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 $180M in rewards available on Immunefi — the leading bug bounty platform for web3.

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