Immunefi

CRYPTO LOSSES IN 2022

Immunefi

CRYPTO LOSSES IN 2022

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 2022.

Overview

The global web3 space was valued at over $934 billion in 2022. 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 2022. We have located 168 such instances, including both successful and semi-successful hacking attempts, as well as alleged fraud.

In total, we have seen a loss of **$3,948,856,037** across the web3 ecosystem in 2022. **$3,773,906,837** was lost to hacks in 2022 across 134 specific incidents and **$174,949,200** was lost to fraud in 2022 across 34 specific incidents. Most of that sum was lost by four specific projects: Ronin Network, BNB Chain, Wormhole, and FTX.

This number represents a 51.2% decrease compared to 2021, when hackers and fraudsters stole **$8,088,338,239**.

Key Takeaways in 2022

- The 5 major exploits of the year totaled $2,361,000,000 alone, accounting for 59.8% of all losses in 2022.
- In 2022, hacks continued to be the predominant cause of losses at 95.6%, in comparison to frauds, scams, and rug pulls which comprised only 4.4% of the total losses.
- In 2022, DeFi continued to be the main target of successful exploits at 80.5% as compared to CeFi at 19.5% of the total losses.
- The two most targeted chains in 2022 were BNB Chain and Ethereum. BNB Chain surpassed Ethereum and became the most targeted chain in 2022, with 65 incidents, while Ethereum witnessed 49 incidents.
- In total, $204,157,000 of stolen funds have been recovered across 12 specific instances. This number represents just 5.2% of the total losses in 2022.

TOP 10 LOSSES IN 2022

FTX	$650,000,000
Ronin Network	$625,000,000
BNB Chain	$570,000,000
Wormhole	$326,000,000
Nomad Bridge	$190,000,000
Beanstalk	$182,000,000
Wintermute	$160,000,000
Harmony	$100,000,000
Mango Markets*	$100,000,000
Mirror Protocol	$90,000,000

Get the full dataset here

* Mango Markets later recovered $67 million of the stolen funds.

TOP 10 LOSSES IN 2022 BY QUARTER

Q1 2022

Ronin Bridge	$625,000,000
Wormhole	$326,000,000
Qubit	$80,000,000
Cashio	$50,000,000
IRA Financial	$36,000,000
crypto.com	$30,000,000
Lympo	$18,700,000
Superfluid	$13,000,000
Arbix Finance	$10,000,000
Dego Finance	$10,000,000

Q2 2022

Beanstalk	$182,000,000
Harmony	$100,000,000
Mirror Protocol	$90,000,000
TribeDAO	$80,340,000
Fantom Scream	$35,000,000
Optimism	$35,000,000
Akutars	$33,000,000
Deus Finance	$13,400,000
Elephant Money	$11,200,000
Venus Protocol	$11,200,00

Q3 2022

Nomad Bridge	$190,000,000
Wintermute	$160,000,000
Racoon Network and Freedom Protocol *	$20,000,000
Impermax Finance	$7,451,118
Audius	$6,000,000
The Bribe Protocol	$5,500,000
ZB	$4,800,000
Teddy Doge *	$4,500,000
Slope Mobile Wallet	$4,500,000
Nirvana	$3,500,000

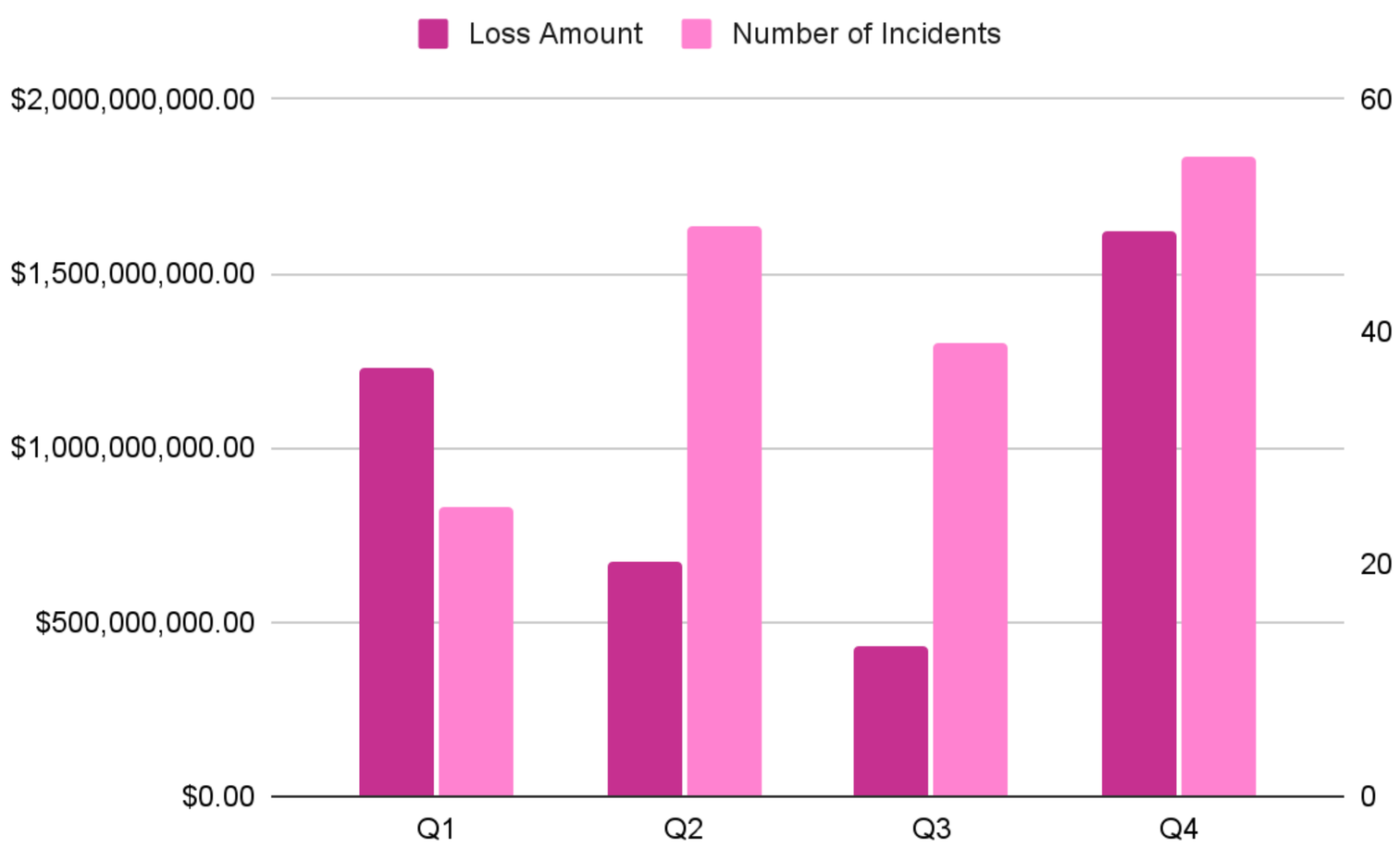
Q4 2022

FTX	$650,000,000
BNB Chain	$570,000,000
Mango Markets**	$100,000,000
mgnr*	$52,000,000
DeFiAI	$40,000,000
Transit Swap	$28,900,000
Deribit	$28,000,000
UXD Protocol**	$20,000,000
Flare	$18,500,000
Helio	$15,000,000

* The teams behind Raccoon Network and Freedom Protocol, Teddy Doge, and mgnr allegedly performed a rug pull.
** Mango Markets later recovered $67 million of the stolen funds. UXD Protocol later recovered over $19 million of the stolen funds.

Losses by quarter in 2022

In 2022, Q4 took the lead with **$1,620,138,807** in total losses across 55 incidents, representing 41% of the total losses.



Overview

Q1 2022

The total losses in Q1 2022 were **$1,229,500,867**. This number represents almost a 7.9x growth compared to Q1 2021, when hackers and fraudsters stole $154,609,199. Most of that sum was lost by two specific projects: Ronin Network, known for the Axie Infinity game, and the Wormhole bridge. These projects together amounted to a total loss of $951,000,000.

Q2 2022

The total losses in Q2 2022 were **$670,698,280**. This number represents almost a 1.5x growth compared to Q2 2021, when hackers and fraudsters stole $440,021,559. Most of that sum was lost by two specific projects: Beanstalk and Harmony Horizon. These projects together amounted to a total loss of $282,000,000.

Losses by quarter in 2022

Q3 2022

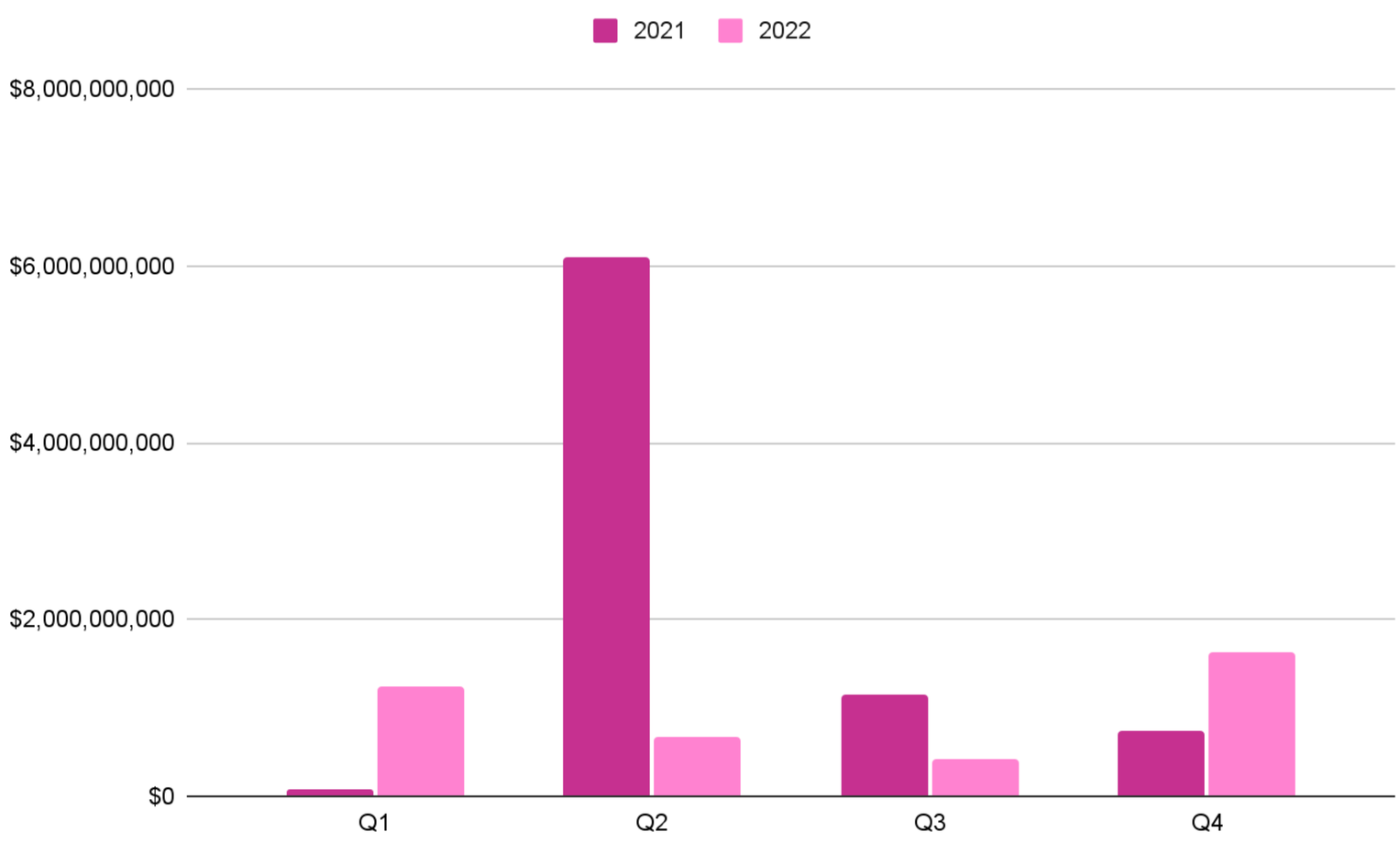
The total losses in Q3 2022 were **$438,324,902**. This number represents a 62.9% decrease compared to Q3 2021, when hackers and fraudsters stole $1,153,390,775. Most of that sum was lost by two specific projects: Nomad Bridge, a cross-chain communication standard that enables transfers of tokens and data between chains, and Wintermute, a global crypto market maker. These projects together amounted to a total loss of $350,000,000.

Q4 2022

The total losses in Q4 2022 were **$1,620,138,807**. This number represents a 119.2% increase compared to Q4 2021 when hackers and fraudsters stole $739,243,793. Most of that sum was lost by two specific projects: FTX, a cryptocurrency exchange, and BNB Chain, a blockchain solution to build web3 dApps. These projects together amounted to a total loss of $1,220,000,000.

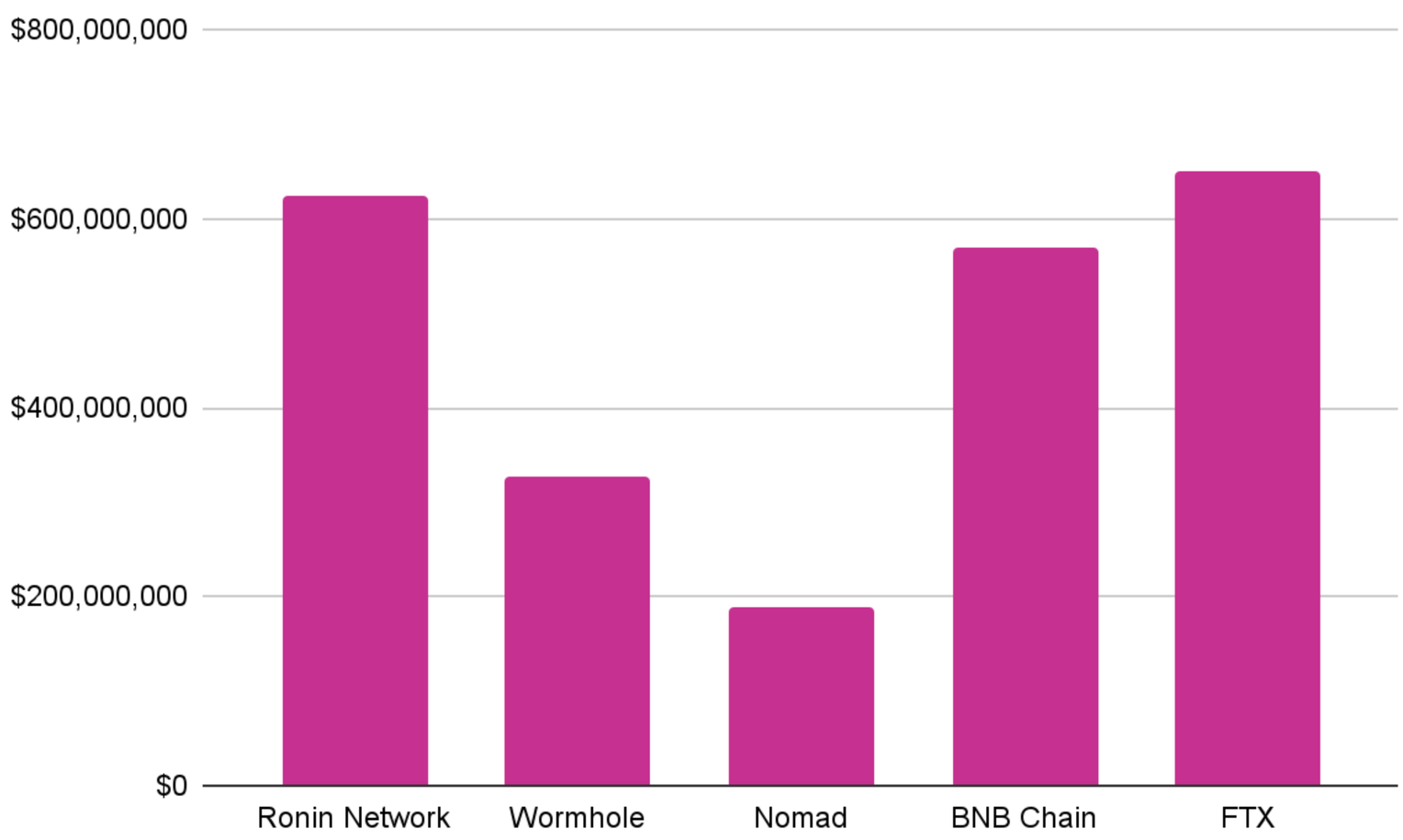
Losses by quarter 2021 vs. 2022

Overview



Major Exploits in 2022

The crypto industry has suffered some of the largest hacks in its history this year. The five major exploits of the year totaled **$2,361,000,000** alone, accounting for 59.8% of all losses in 2022.



Ronin Network Q1 2022
$625 million

Wormhole Q1 2022
$326 million

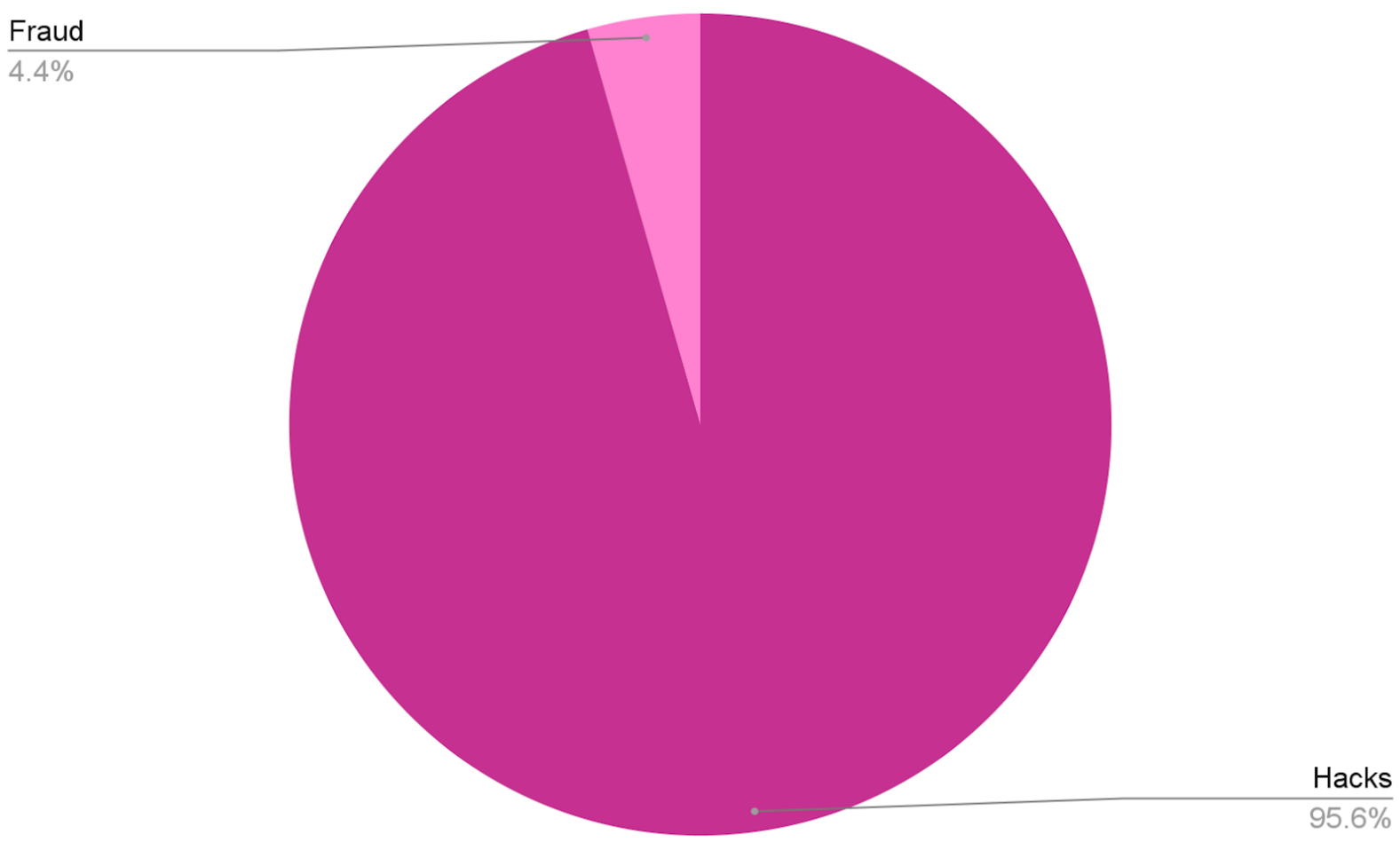
Nomad Q3 2022
$190 million

BNB Chain Q4 2022
$570 million

FTX Q4 2022
$650 million

Hacks vs. Fraud Analysis

In 2022, hacks continued to be the predominant cause of losses as compared to frauds, scams, and rug pulls. Fraud accounted for only 4.4% of the total losses in 2022, while hacks accounted for 95.6%.



Overview

Hacks

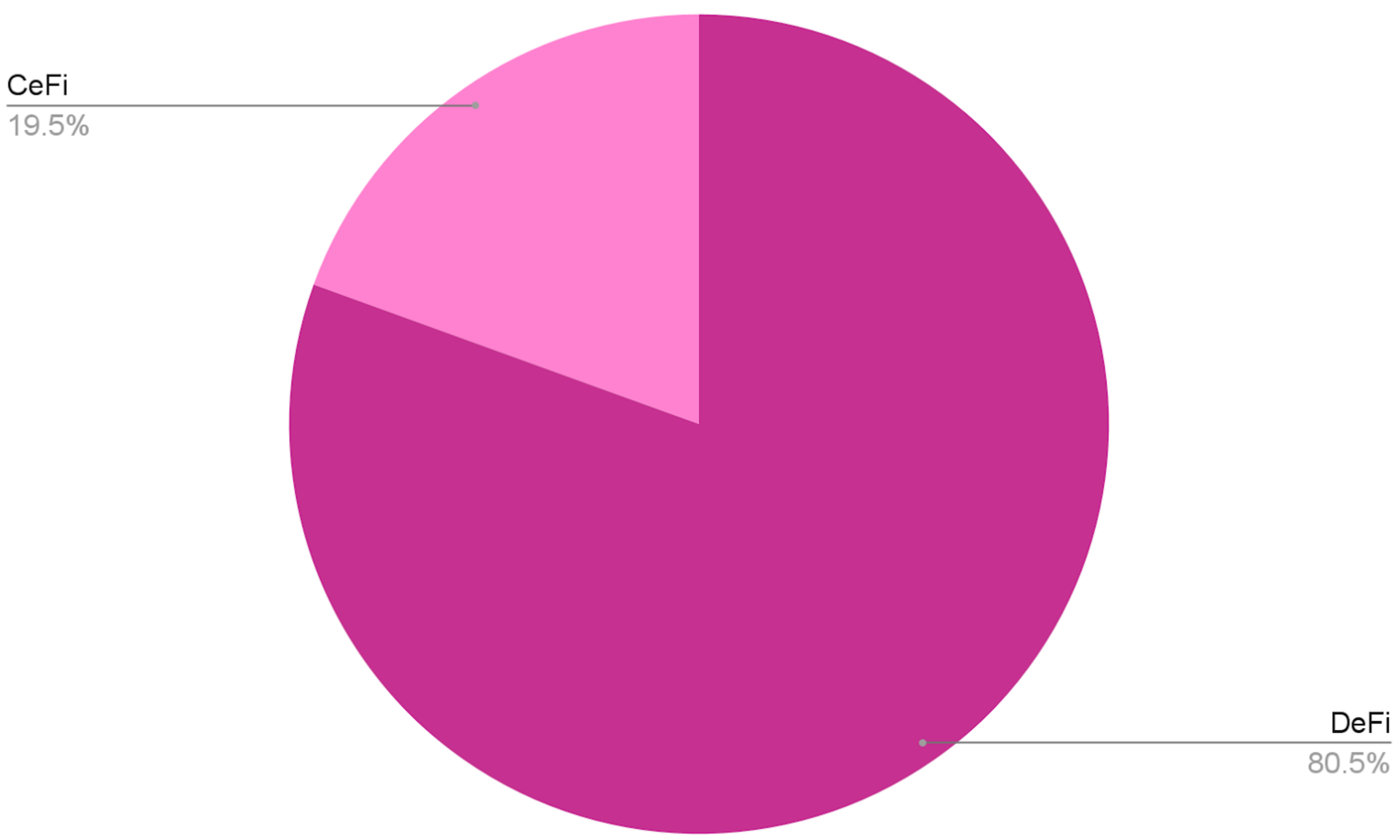
In total, we have seen a loss of **$3,773,906,837** to hacks in 2022, in 134 specific incidents. This number represents a 58.3% increase compared to 2021, when losses caused by hacks totaled $2,384,164,452, in 102 incidents.

Fraud

In total, we have seen a loss of **$174,949,200** to fraud in 2022, in 34 specific incidents. This number represents a 96.9% decrease compared to 2021, when losses caused by fraud totaled $5,704,173,787, in 14 incidents.

DeFi vs. CeFi Analysis

In 2022, DeFi continued to be the main target of successful exploits as compared to CeFi. DeFi accounted for 80.5% of the total losses, while CeFi accounted for 19.5%.



Overview

DeFi

DeFi has suffered **$3,180,023,103** in total losses in 2022, across 155 incidents. This number represents a 56.2% increase compared to 2021, when DeFi lost $2,036,015,896, in 107 incidents.

CeFi

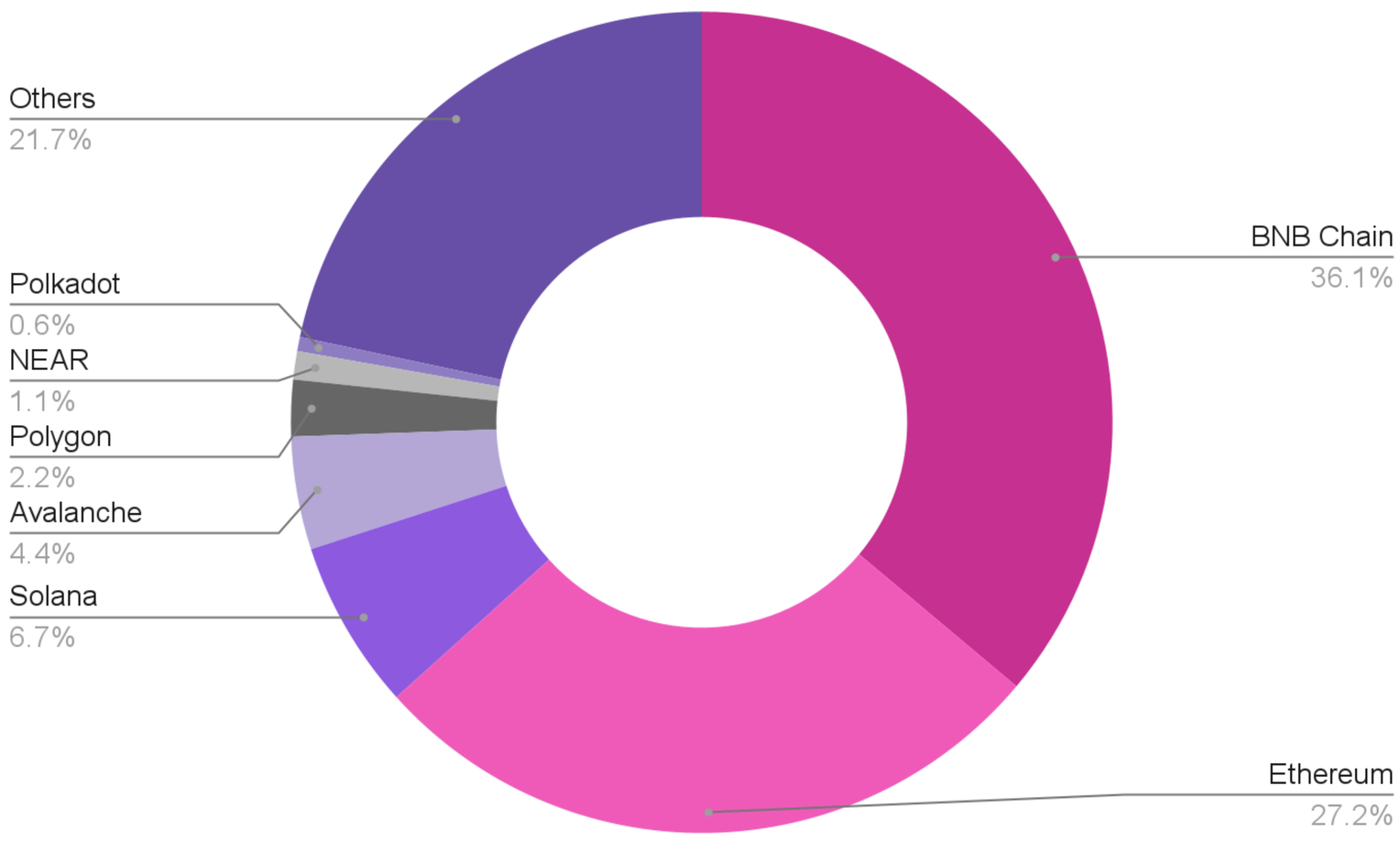
CeFi has suffered **$768,832,934** in total losses in 2022, across 13 incidents. This number represents a 87.3% decrease compared to 2021, when CeFi lost $6,052,322,343, in 9 incidents.

Losses by Chain

BNB Chain and Ethereum were the two most targeted chains in 2022.

BNB Chain suffered the most individual attacks with 65 incidents, representing 36.1% of the total attacks across targeted chains. This number represents a 51.2% increase compared to 2021, when BNB Chain witnessed 43 attacks.

Ethereum witnessed 49 incidents, representing 27.2% of the total incidents across targeted chains. This number represents a 8.9% increase when compared to 2021, when Ethereum witnessed 45 attacks.



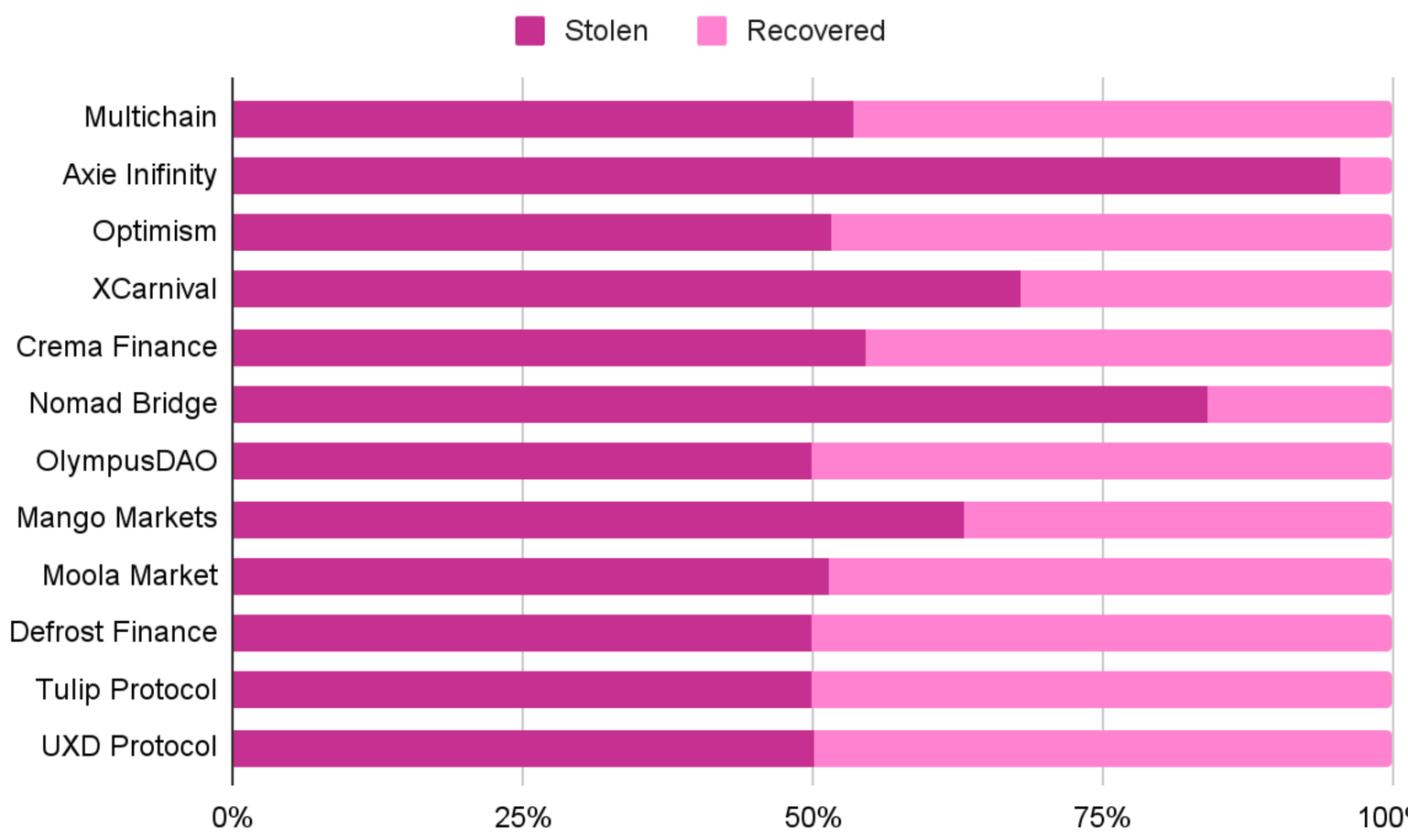
Overview

BNB Chain and Ethereum represented more than half of the chain attacks in 2022 at 63,3%. Solana came in third with 12 incidents, representing 6.7% of total attacks across chains. Avalanche followed with 8 incidents, representing 4.4%. Polygon with 4 incidents, representing 2.2%. NEAR with 2 incidents, representing 1.1%. Polkadot with 1 incident, representing 0.6%.

Remaining chains like Gnosis, Cronos, Arbitrum, Fantom, and others together represented 21.7% of the total chain attacks.

Funds recovery

In total, **$204,157,000** has been recovered from stolen funds in 12 specific situations. This number makes up 5.2% of the total losses in 2022.



Overview of cases

Multichain
Stolen
$3 million
Recovered
$2.6 million

Axie Infinity
Stolen
$625 million
Recovered
$30 million

Optimism
Stolen
$16 million
Recovered
$15 million

XCarnival
Stolen
$3.8 million
Recovered
$1.8 million

Crema Fin.
Stolen
$9.6 million
Recovered
$8 million

Nomad
Stolen
$190 million
Recovered
$36.4 million

OlympusDAO
Stolen
$212,000
Recovered
$212,000

Mango Mark.
Stolen
$114 million
Recovered
$67 million

Moola Mark.
Stolen
$9.1 million
Recovered
$8.6 million

Defrost Fin.
Stolen
$12 million
Recovered
$12 million

Tulip Protocol
Stolen
$2.5 million
Recovered
$2.5 million

UXD Protocol
Stolen
$20 million
Recovered
$19.9 million

Immunefi

CRYPTO LOSSES IN Q4 2022

In focus

Overview of the volume of crypto funds lost by the community due to hacks and scams in Q4 2022, as assessed by Immunefi.

Overview

In total, we have seen a loss of **$1,620,138,807** across the web3 ecosystem in Q4 2022. **$1,499,813,207** was lost to hacks, across 43 specific incidents, and **$ $120,325,600** was lost to fraud, across 12 specific incidents. Most of that sum was lost by two specific projects: FTX, a cryptocurrency exchange, and BNB Chain, a blockchain solution to build web3 dApps.

This number represents a 119.2% increase compared to Q4 2021 when hackers and fraudsters stole **$739,243,793**.

TOP 10 LOSSES IN Q4 2022

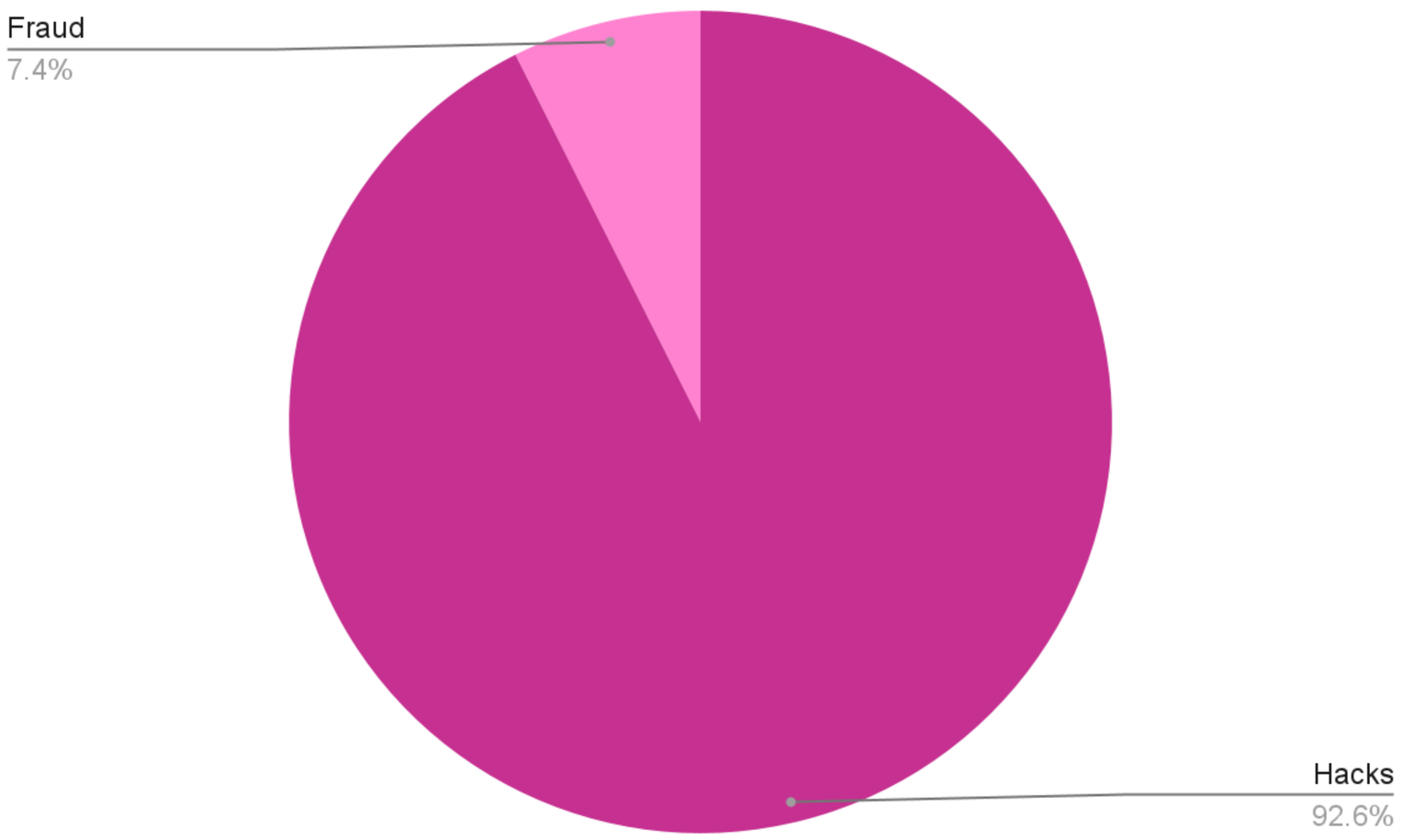
FTX	$650,000,000
BNB Chain	$570,000,000
Mango**	$100,000,000
mgnr*	$52,000,000
DeFiAI	$40,000,000
Transit Swap	$28,900,000
Deribit	$28,000,000
UXD Protocol**	$20,000,000
Flare	$18,500,000
Helio	$15,000,000

Get the full dataset here

* The team behind mgnr allegedly performed a rug pull. **Mango Market later recovered $67 million of the stolen funds. UXD Protocol later recovered over $19 million of the stolen funds.

Hacks vs. Fraud Analysis

In Q4 of 2022, hacks continued to be the predominant cause of losses as compared to fraud, scams, and rug pulls. Fraud accounted for only 7.4% of the total losses in Q4 2022, while hacks accounted for 92.6%.



Overview

Hacks

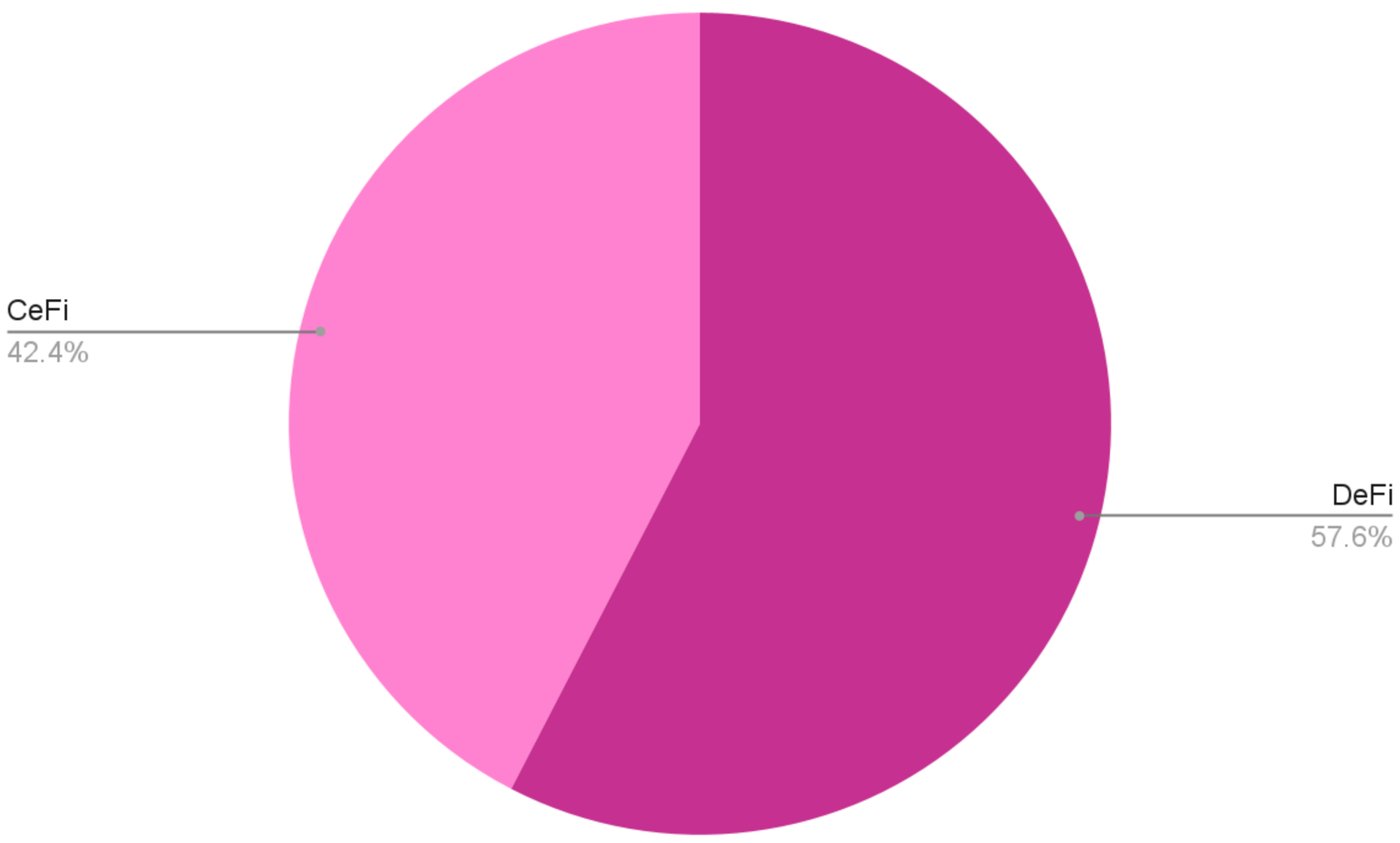
In total, we have seen a loss of **$1,499,813,207** to hacks in Q4 2022, in 43 specific incidents. This number represents a 106.3% increase compared to Q4 2021, when losses caused by hacks totaled $727,243,793, in 18 incidents.

Fraud

In total, we have seen a loss of **$120,325,600** to fraud in Q4 2022, across 12 specific incidents. This number represents a 902.7% increase compared to Q4 2021, when losses caused by fraud totaled $12,000,000, in 1 incident.

DeFi vs. CeFi Analysis

In Q4 of 2022, DeFi continued to be the main target of successful exploits as compared to CeFi. DeFi accounted for 57.6% of the total losses, while CeFi accounted for 42.4% of the total losses.



Overview

DeFi

DeFi has suffered **$933,040,173** in total losses in 2022, across 50 incidents. This number represents a 133.2% increase compared to 2021, when DeFi lost $400,025,828, in 16 incidents.

CeFi

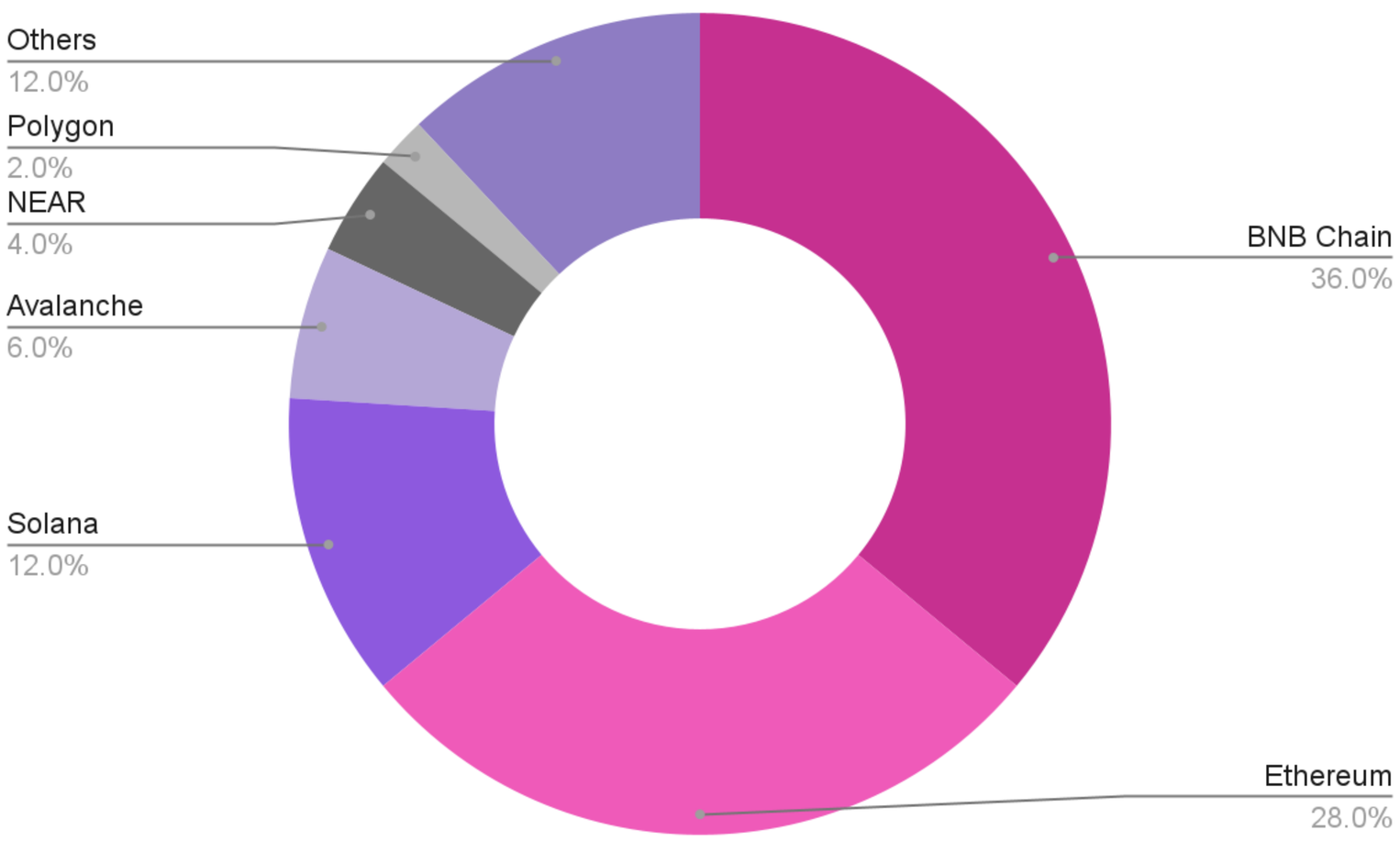
CeFi has suffered **$687,098,634** in total losses in 2022, across 5 incidents. This number represents a 102.6% increase compared to 2021, when CeFi lost $339,217,965 in 3 incidents.

Losses by Chain

The two most targeted chains in Q4 2022 were BNB Chain and Ethereum.

BNB Chain suffered the most individual attacks with 18 incidents, representing 36% of the total attacks across targeted chains. This number represents a 260% increase compared to Q4 2021, when BNB Chain witnessed 5 attacks.

Ethereum witnessed 14 incidents, representing 28% of the total attacks across targeted chains. This number represents a 55.6% increase when compared to Q4 2021, when Ethereum witnessed 9 attacks.



Overview

BNB Chain and Ethereum represented more than half of the chain attacks in Q4 2022 at 64%. Solana comes in third with 6 incidents, representing 12% of total losses across chains. Avalanche followed with 3 incidents, representing 6%. NEAR with 2 incidents, representing 4%. Polygon with 1 incident, representing 2%.

Remaining chains like CELO, Optimism, and others together represented 13.6% of the total chain attacks.

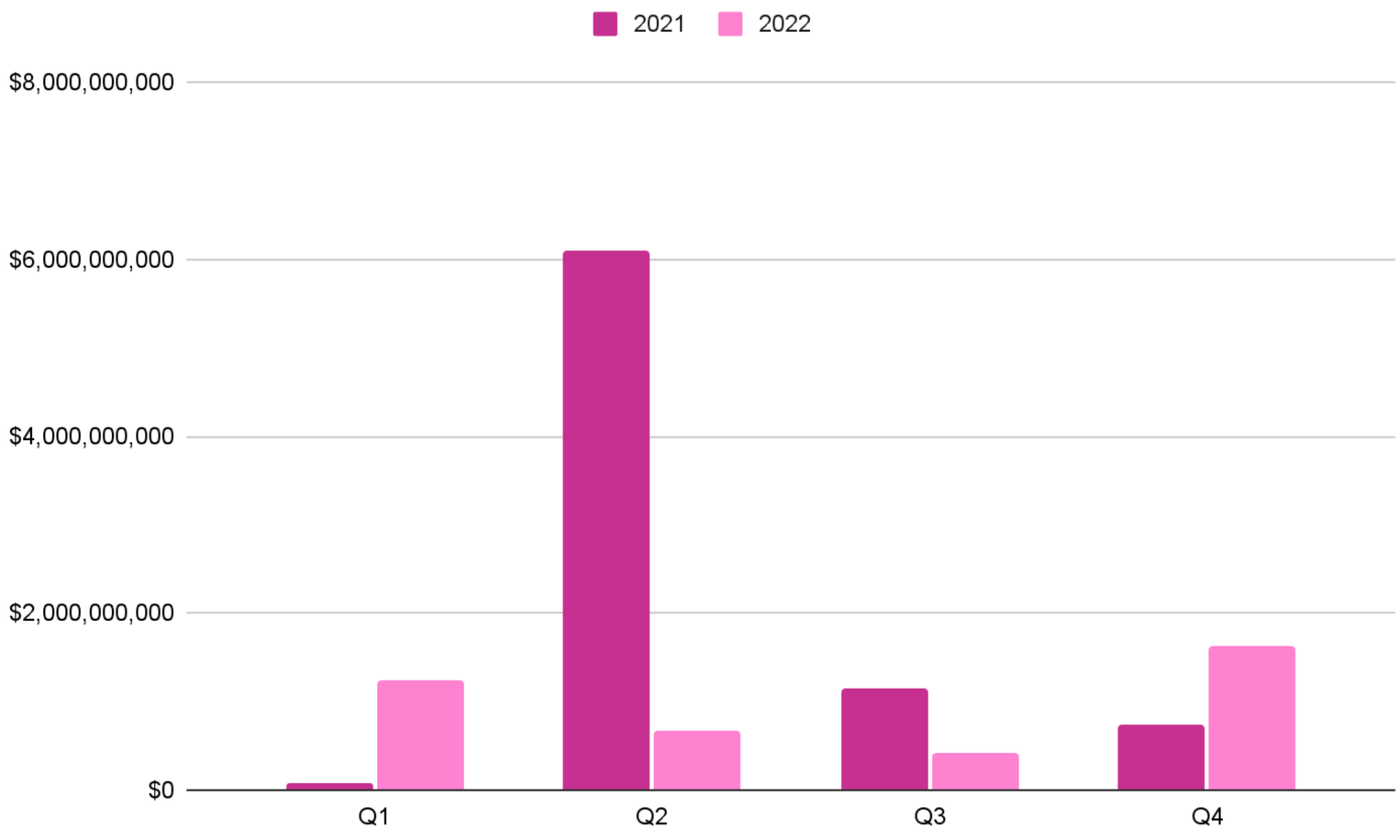
Immunefi

CRYPTO LOSSES IN 2021 vs. 2022

A visual comparison

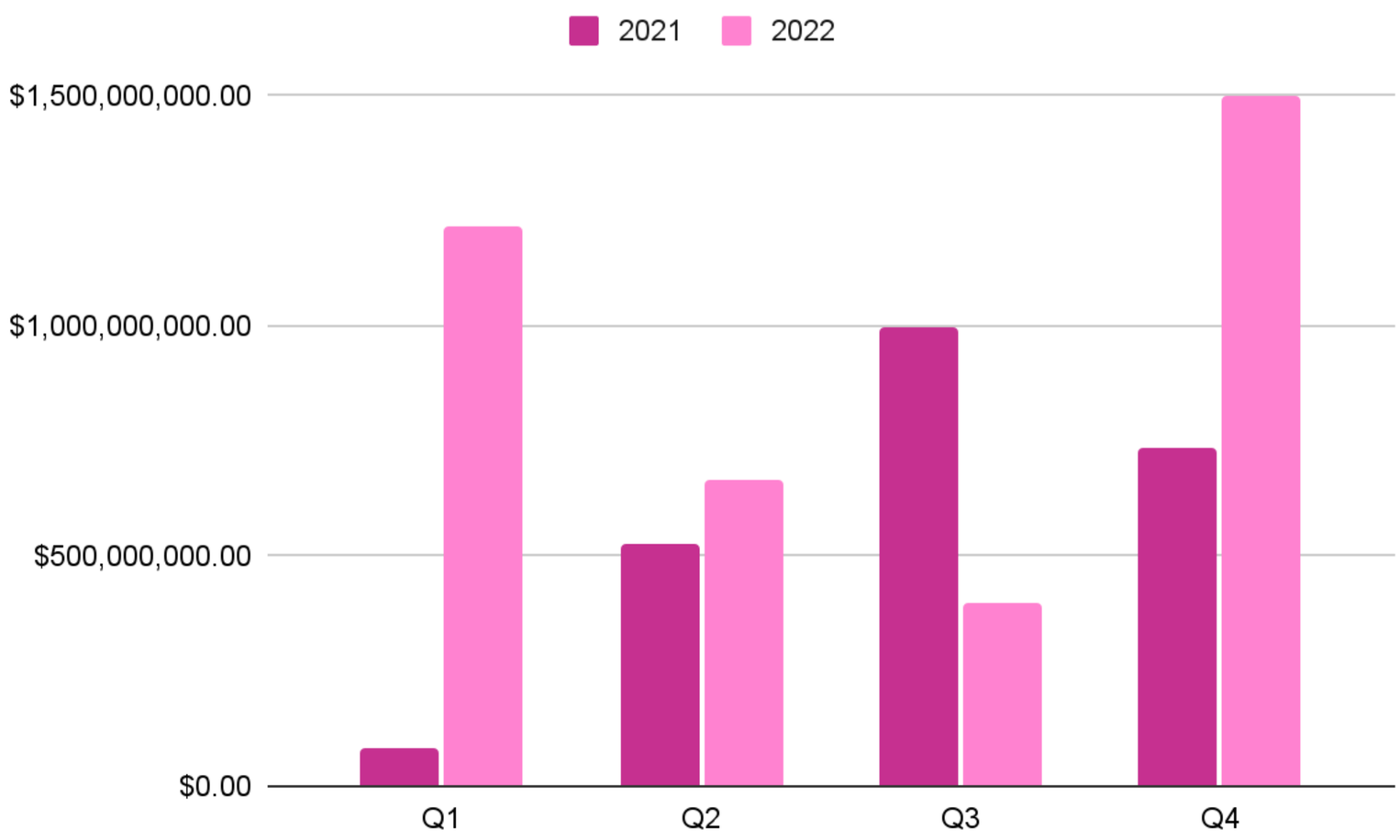
Immunefi has created a comprehensive visual comparison for its analysis of losses by categories between 2021 and 2022. It contains the charts broken down by category, year and quarter, as well as the corresponding datasets for each chart.

Losses by quarter



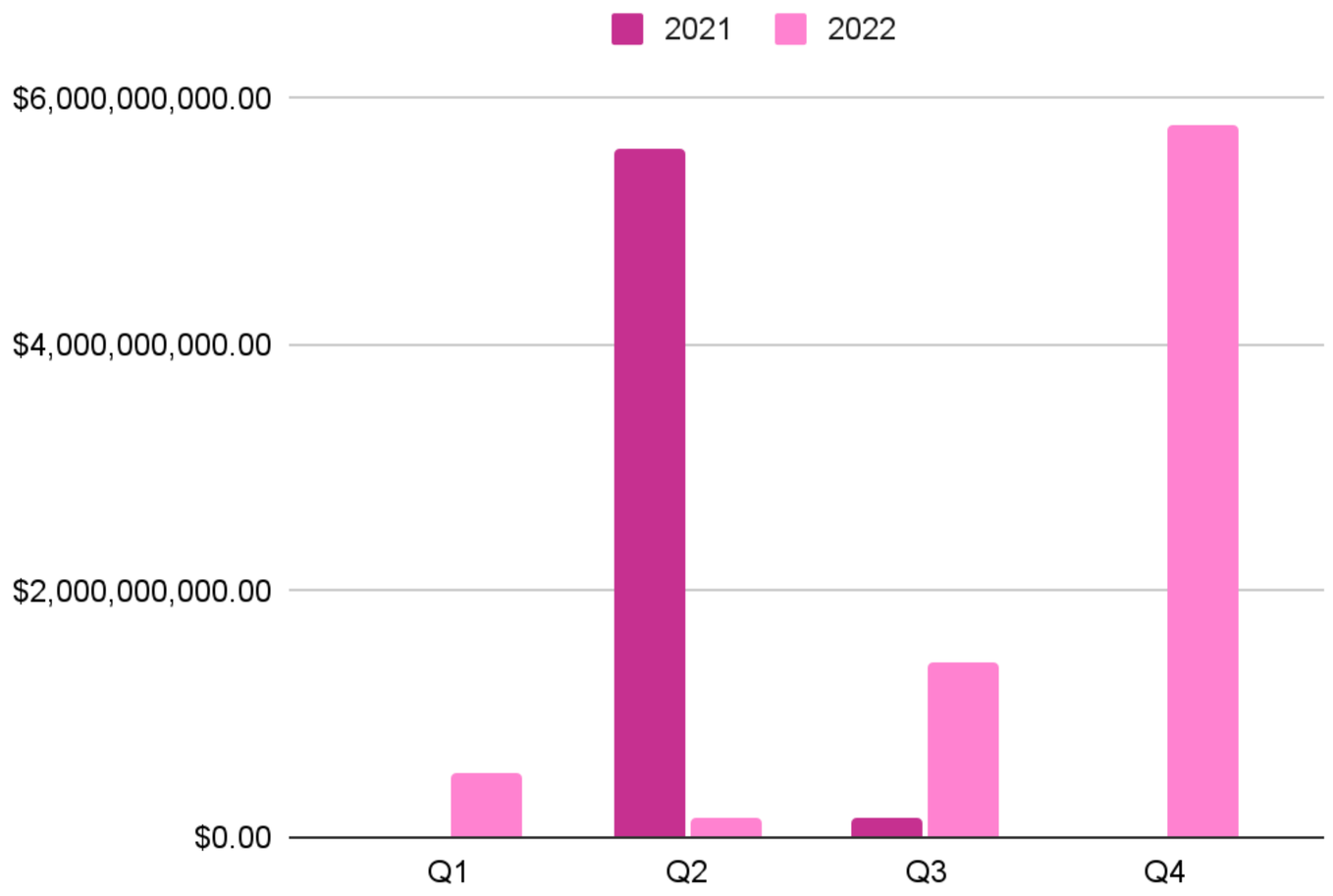
Hacks vs. Fraud

Hacks



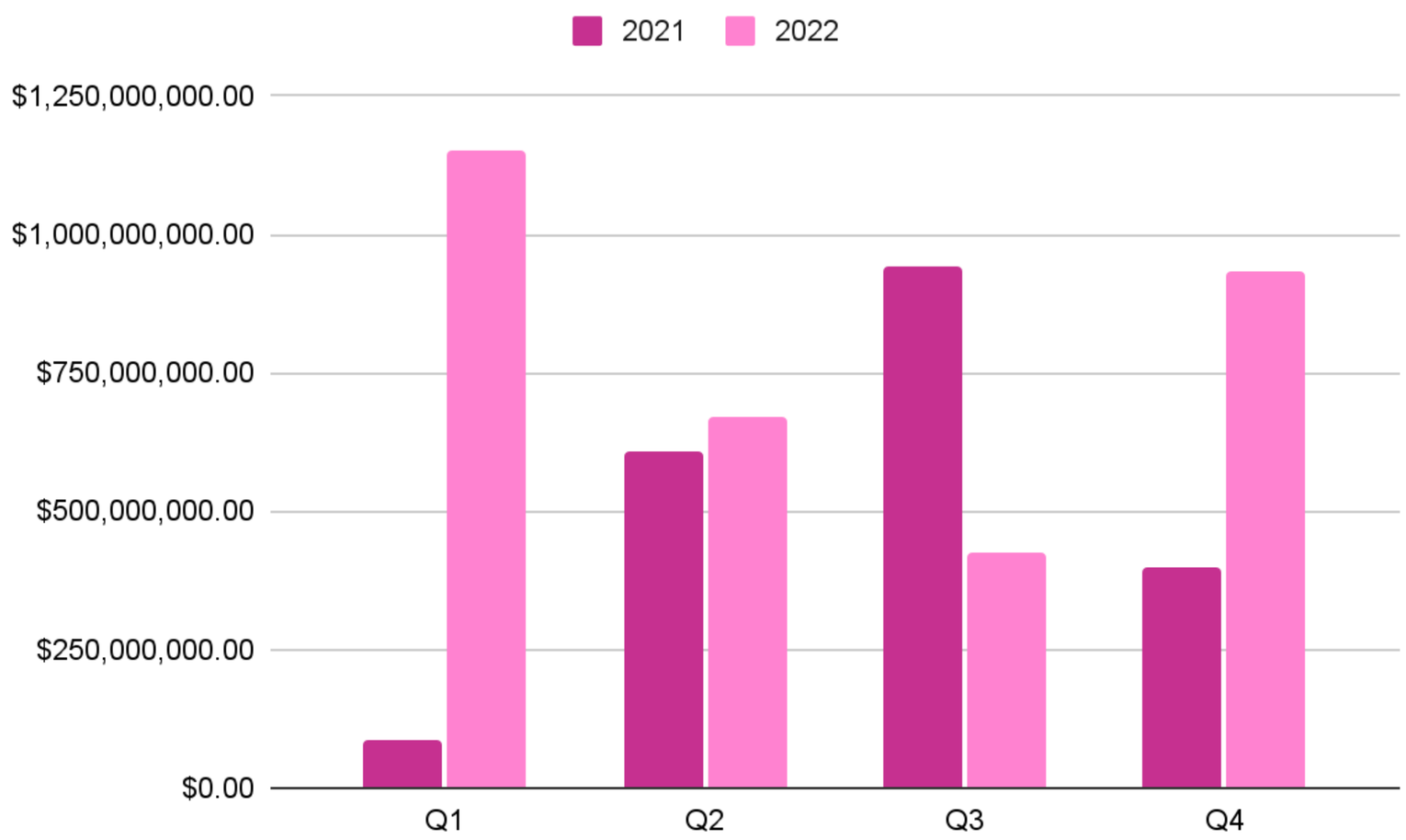
Hacks vs. Fraud

Fraud



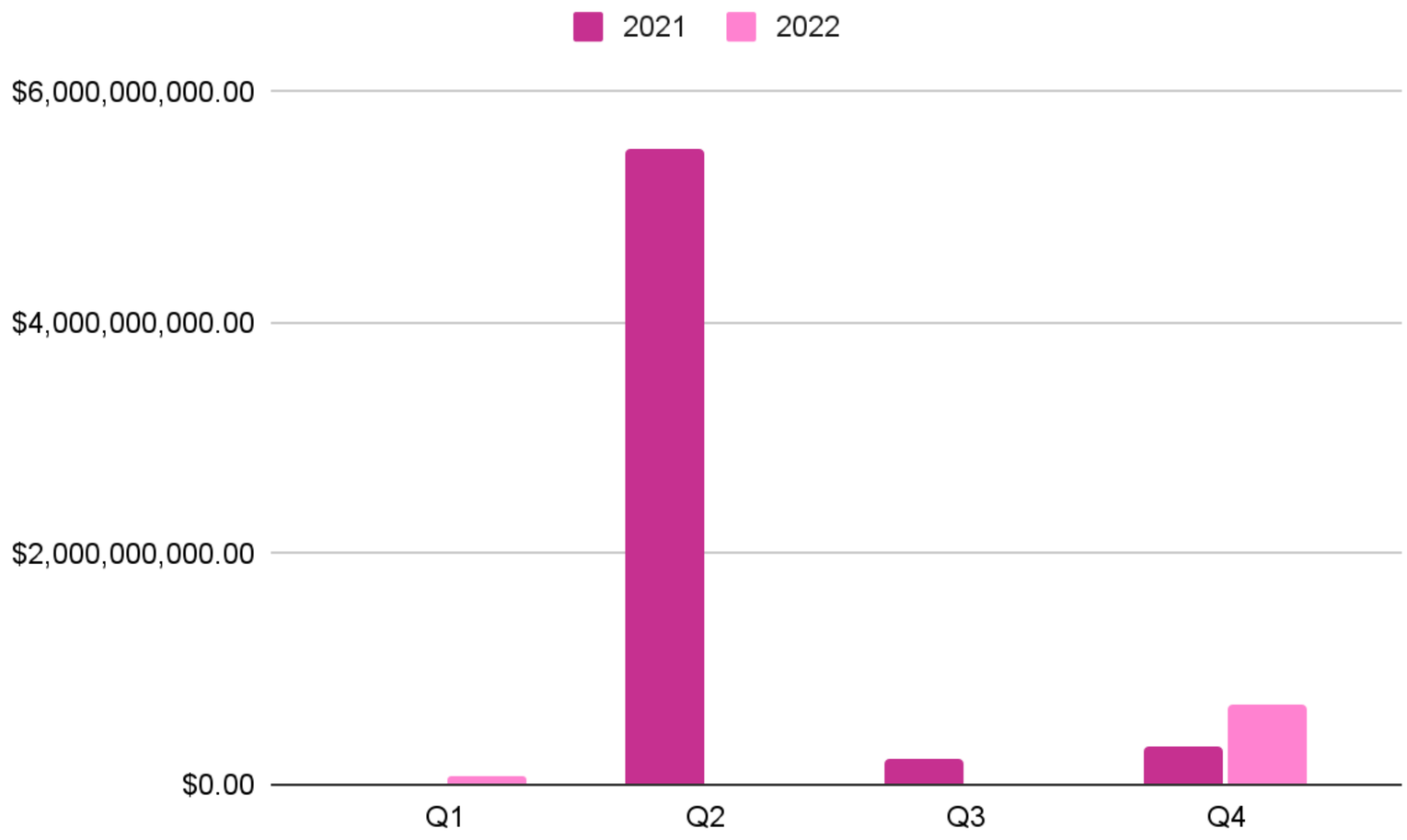
DeFi vs. CeFi

DeFi



DeFi vs. CeFi

CeFi



Crypto Losses in 2021 vs. 2022

Losses by quarter

	2021	2022
Q1	$86,002,208	$1,229,500,867
Q2	$6,109,701,463	$670,498,280
Q3	$1,155,334,775	$428,718,083
Q4	$739,243,793	$1,620,138,807

Hacks

	2021	2022
Q1	$81,575,125	$1,218,500,867
Q2	$524,701,463	$667,523,921
Q3	$994,489,686	$398,912,483
Q4	$735,243,793	$1,499,813,207

Frauds

	2021	2022
Q1	$4,927,083	$11,000,000
Q2	$5,585,000,00	$3,174,359
Q3	$160,845,089	$29,805,60
Q4	$13,400,000	$120,325,600

DeFi

	2021	2022
Q1	$85,957,208	$1,153,060,867
Q2	$609,701,463	$670,498,280
Q3	$940,331,397	$423,423,783
Q4	$400,025,828	$933,040,173

CeFi

	2021	2022
Q1	$45,000	$76,440,000
Q2	$5,500,000,000	$0
Q3	$213,059,378	$5,294,300
Q4	$339,217,965	$687,098,634

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 **$65 million** in total bounties, while saving over **$25 billion** in user funds.

Total bounties available

Immunefi offers over **$144 million** in available bounty rewards.

Supported projects

Trusted by established, multi-billion dollar projects like Chainlink, Wormhole, MakerDAO, Compound, Synthetix, and more, Immunefi now supports 301 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 decentralised 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.

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 $144M in rewards available on Immunefi — the leading bug bounty platform for web3.

https://immunefi.com/