Immunefi

CRYPTO LOSSES Q3 2022

CRYPTO LOSSES IN Q3 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 Q3 2022.

Overview

The global web3 space was valued at $3 trillion in 2021, and with billions locked across different smart contracts, 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 alleged fraudulent protocols and founders who have performed a rug pull in Q3 2022. We have located 39 such instances, including both successful and semi-successful hacking attempts, as well as fraud.

In total, we have seen a loss of **$428,718,083** across the web3 ecosystem in Q3 2022. We have seen a loss of **$398,912,483** to hacks across 30 specific incidents, and a loss of **$29,805,600** to fraud across 9 specific incidents in Q3 2022. Most of that sum was lost by 2 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. Unlike in previous quarters, fraud was the cause of loss only for 9 projects, with the total figure amounting to $20,674,359**.**

These numbers represent a 62.9% decrease compared to Q3 2021, when hackers and fraudsters stole **$1,155,334,775**.

Immunefi

TOP 10 LOSSES IN 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

* the team behind Raccoon Network and Freedom Protocol and Teddy Doge allegedly performed a rug pull.

Get the full dataset here

About Immunefi

Immunefi is the leading bug bounty and security services platform for web3, which features the world's largest bounties. Immunefi guards over $60 billion in user funds across projects like Synthetix, Chainlink, SushiSwap, PancakeSwap, Bancor, Cream Finance, Compound, Alchemix, Nexus Mutual, and others. The company has paid out the most significant bug bounties in the software industry, amounting to over $60 million, and has pioneered the scaling web3 bug bounties standard. For more information, please visit **https://immunefi.com/**

Major Exploits in Q3 Analysis

Most of the Q3 loss sum was lost by 2 specific projects, Nomad Bridge and Wintermute, totaling **$350,000,000**. Together, these two projects represent 79,85% of Q3 losses alone.

Nomad Bridge

$190 million

On August 2nd, 2022, Nomad Bridge, a cross-chain communication standard that enables transfers of tokens and data between chains, suffered a major exploit leading to $190 million being drained out of the protocol. Nomad's hack quickly became referred to as a "chaotic" one, as in this particular case, there wasn't a singular malicious actor exploiting the vulnerability. Rather, there were many different people and MEV bots involved.

The hack was different from previous hacks that happened to the Ronin Network and to the Horizon Bridge. The surprising aspect of the vulnerability was that it was an easy-to-reproduce attack. All that was required to exploit it was to copy the original hacker's transaction and change the original address to a custom one. Simple copy-paste. Many malicious users wanted a piece of Nomad's pool. That's why the attack cannot be attributed to just one malicious actor, as many people participated in it after they figured out they could easily run the exploit as well.

Wintermute

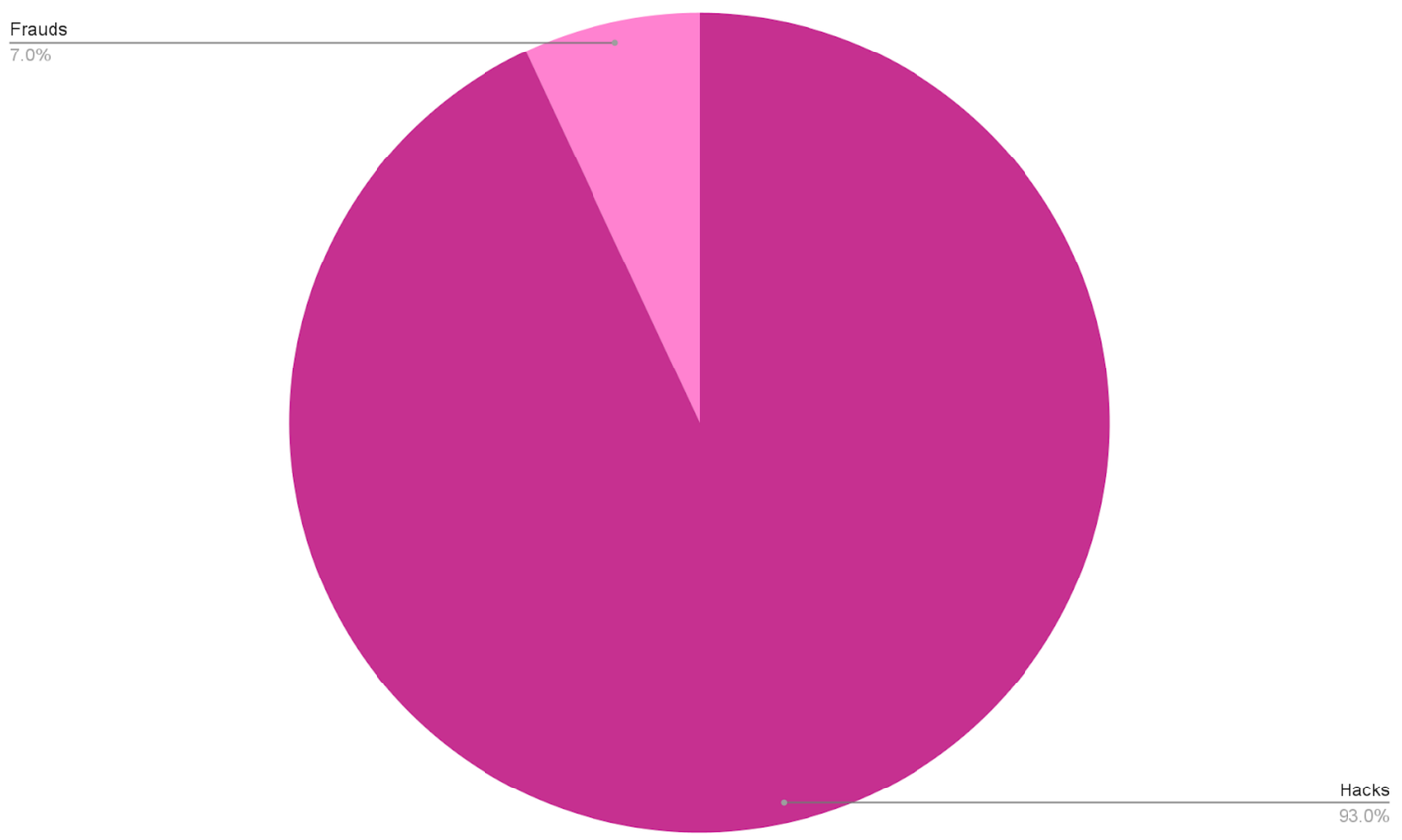
$160 million

On September 20th, 2022, Wintermute, a global crypto market maker, lost $160 million in a hack relating to its decentralized finance operation, in a hot wallet compromise. Although suffering a major exploit, Wintermute's lending and over-the-counter (OTC) services were not affected, and the company's CEO Evgeny Gaevoy, said that the company remained solvent with "twice over" $160 million remaining in equity.

Wintermute provides liquidity on more than 50 exchanges and trading platforms, including Binance, Coinbase, FTX, Kraken, and decentralized platforms Dydx and Uniswap. It is also an active investor, having invested in projects such as Nomad, HashFlow, and Ondo Finance.

Hacks vs. Frauds Analysis

In the Q3 of 2022, 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 only 7% of the total losses in the Q3 2022, while hacks account for 93%.



Overview

Hacks

In total, we have seen a loss of **$398,912,483** to hacks in Q3 2022, across 30 specific incidents. These numbers represent a 67.3% decrease compared to Q1 2022, when losses caused by hacks totaled $1,218,500,867, and a 38.7% decrease compared to Q2 2022, when $650,269,602 was lost.

When compared to the losses of Q3 2021, where losses caused by hacks totaled $994,489,686, we've witnessed a 59.9% decrease.

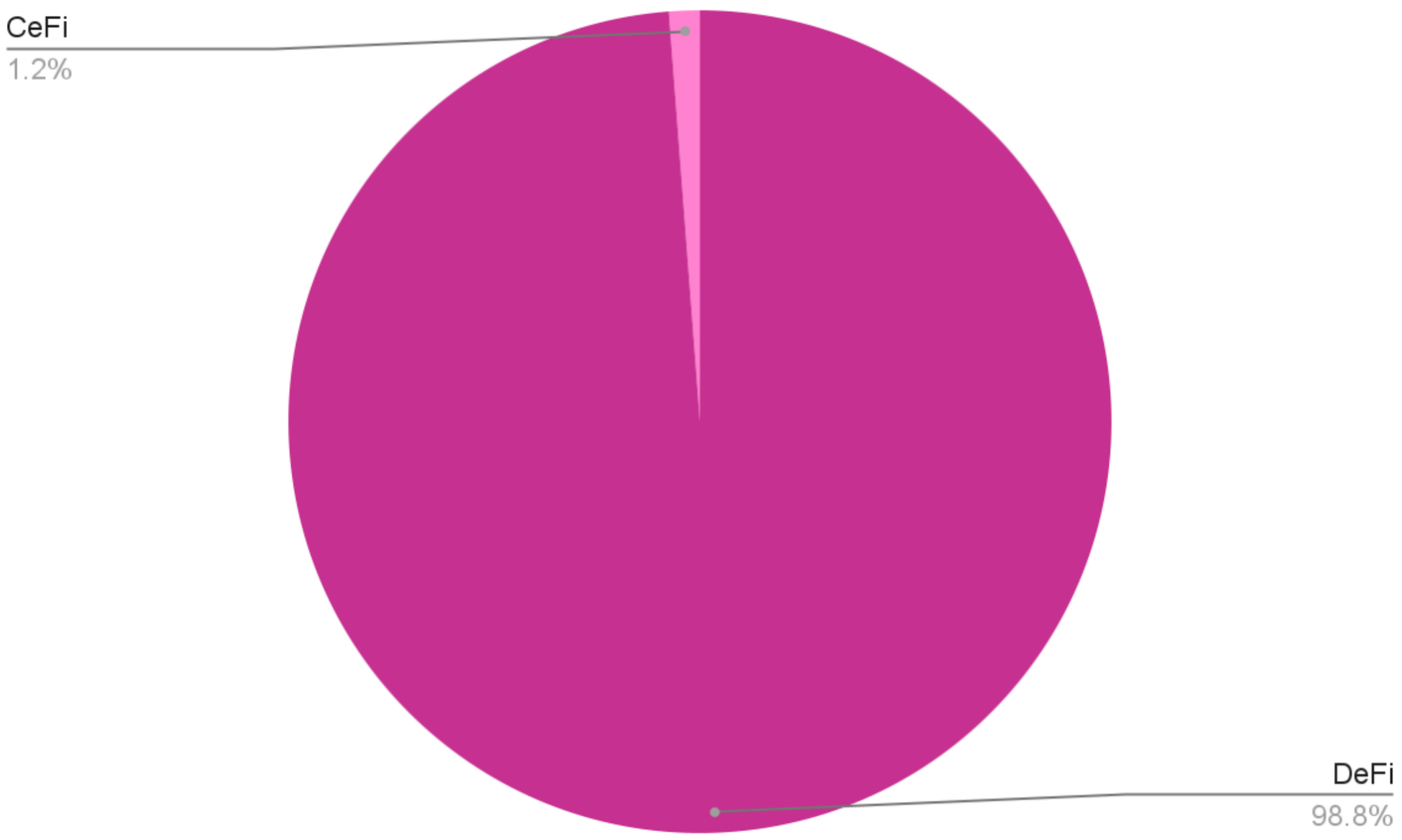
Fraud

In total, we have seen a loss of **$29,805,600** to fraud in Q3 2022, across 9 specific incidents. These numbers represent a 170.9% increase compared to Q1 2022, when losses caused by frauds, scams, and rug pulls totaled $11,000,000 and a 838.9% increase compared to Q2 2022, when $3,174,359 was lost.

When compared to the losses of Q3 2021, where losses caused by frauds, scams, and rug pulls totaled $160,845,089, we've witnessed a 81.5% decrease.

DeFi vs. CeFi Analysis

In the Q3 of 2022 DeFi continues to be the key target for exploits as compared to CeFi. DeFi represents 98.8% of the total losses, while CeFi represents 1.2% of the total losses.



Overview

DeFi

DeFi has suffered **$423,423,783** in total losses in the Q3 2022, across 36 incidents.
In Q2 2022, DeFi suffered losses totaling $670,608,280 across 49 incidents, representing a 36.8% decrease in losses when compared with Q3 results.

CeFi

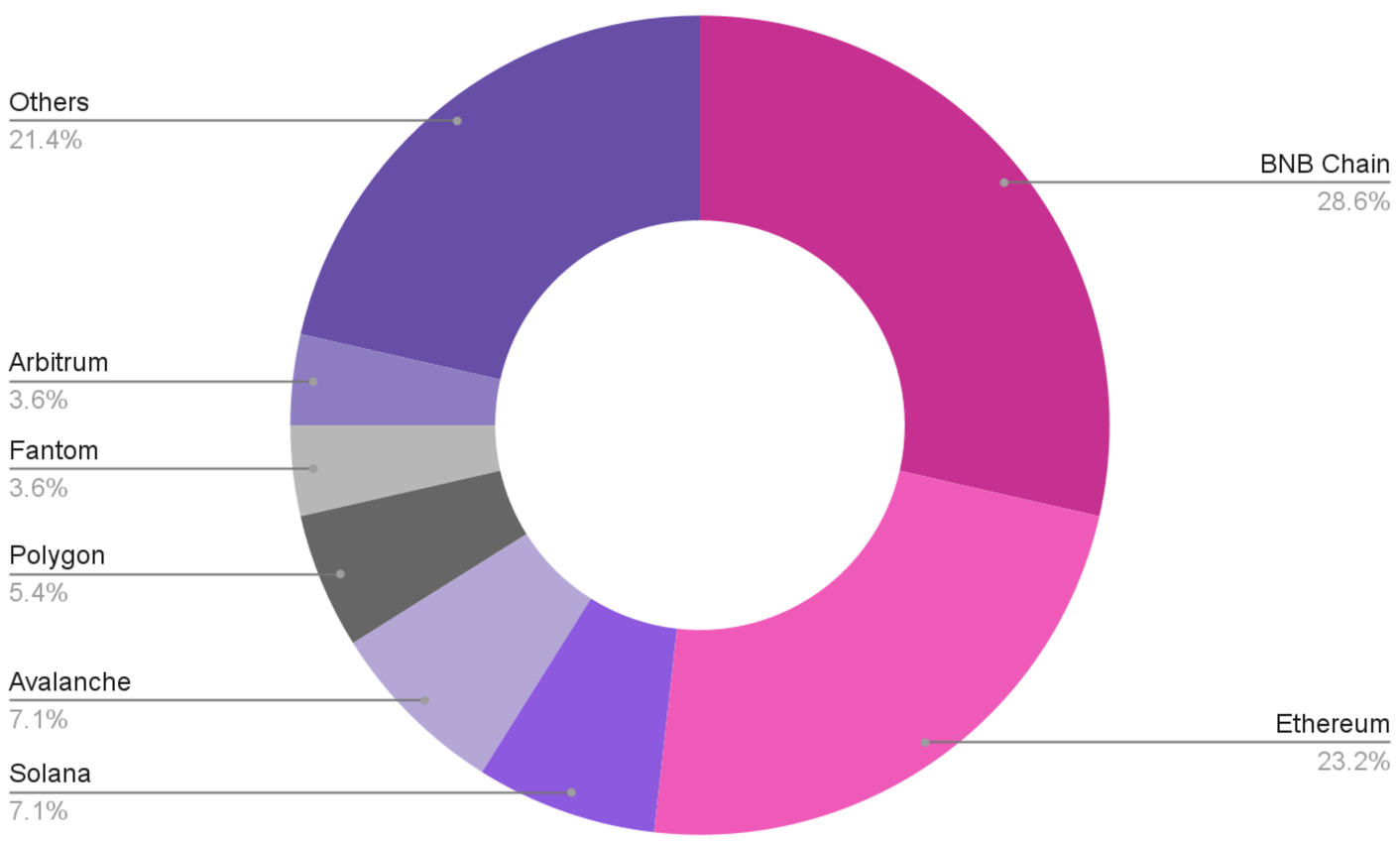
CeFi has suffered **$5,294,300** in total losses in the Q3 2022, across 3 incidents.
In Q2 2022, CeFi suffered losses totaling $90,000 across 1 incident, representing a 5782.6% increase when compared with Q3 results.

CeFi Safety

It’s harder to break into a centralized exchange like Binance and Coinbase, as they’ve invested a lot of resources into security. Given their basic infrastructure setups, pulling money out of a centralized exchange often requires hackers to jump through far more hoops than pulling money out of a vulnerable DeFi protocol. In other words, vulnerable DeFi projects are much more low-hanging fruit for malicious hackers, and the authorities are less likely to become involved when a no-name protocol is hacked. There are also far more DeFi protocols than centralized exchanges or CeFi projects, resulting in a much greater attack surface.

Losses by chain

The two most targeted chains in Q3 2022 were BNB Chain and Ethereum. BNB Chain suffered the most individual attacks with 16 incidents, representing 28.6% of the total losses across targeted chains, and Ethereum witnessed 13 incidents, representing 23.2% respectively.



Overview

BNB Chain and Ethereum represent more than half of the chain losses in Q3 2022 at 51.8%. Solana and Avalanche come in third both with 4 incidents, each representing 6.8% of total losses across chains. Polygon follows with 3 incidents, Fantom and Arbitrum with 2 incidents each.

Remaining chains like Optimism, Gnosis, Polkadot, Aurora, and others together represent 21.4% of the total chain incidents, all with single incidents.

Losses by Chain

BNB Chain is still attracting a developer community that creates a lot of copies of Ethereum protocols, and it also attracts a lot of users who want to earn quick money. Forked code can contain vulnerabilities, and we've seen cases before where developers on BNB Chain will modify forked code without much knowledge of the underlying program structure, which introduces novel vulnerabilities that then get exploited.

Additionally, many of the security traditions and culture that exist within the Ethereum developer community do not yet exist within the BNB Chain community. Vulnerabilities that you see less and less in Ethereum protocols still crop up on BNB Chain. Over time, if BNB Chain manages to attract more serious developer talent, these security traditions will eventually grow.

Multiple Chain Incidents

It's rare to find a single smart contract-based attack method that equally affects all the different chains of a project, and these cases are no exception. With Impermax Finance, the attack vector was a private key compromise, which affected team wallets on different chains. It was not a smart contract exploit that allowed a hacker to pull funds out of contracts on different chains. With Celer Network, the exploit was a DNS attack that allowed a malicious hacker to redirect users to a Celer frontend that that hacker-controlled. Once the users interacted with that hacker-created frontend–regardless of the chain–their funds were gone.

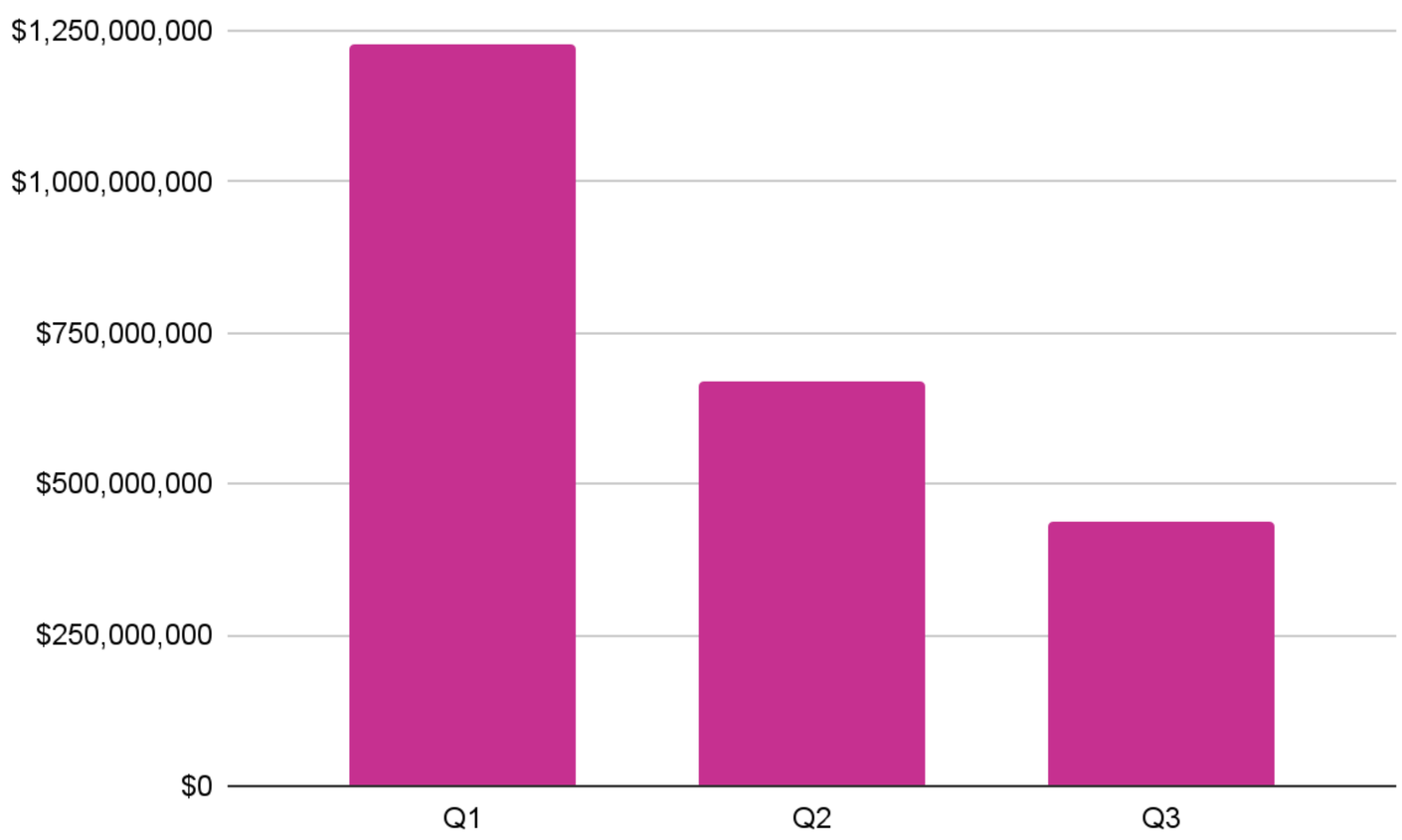
When a project has its smart contracts drained simultaneously across all chains that it operates on, the probability actually increases that it was a rugpull, although it is not a definitive indicator.

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 did occur.

CRYPTO LOSSES YTD

The team at Immunefi, the leading bug bounty and security services platform for web3 which protects over $60 billion in user funds, continuously assesses the volume of crypto funds lost by the community due to hacks and scams during the respective quarters of the year.

In total, we have seen a loss of **$2,328,917,230** across the web3 ecosystem YTD.



Overview

Q1 2022

The total loss in Q1 2022 was **$1,229,500,867**. These numbers represented almost a 7.9x growth compared to Q1 2021, when hackers and fraudsters stole $154,609,199. Most of that sum was lost by 2 specific projects, Ronin Network, known for the Axie Infinity game, and the Wormhole bridge. The total loss of these two projects alone reached $951,000,000.

CRYPTO LOSSES YTD

Q2 2022

The total loss in Q2 2022 was **$670,698,280**. These numbers represented almost a 1.5x growth compared to Q2 2021, when hackers and fraudsters stole $440,021,559. Most of that sum was lost by 2 specific projects, Beanstalk and Harmony Horizon. The total amount of loss of these two projects alone reached $282,000,000.

Q3 2022

In total, we have seen a loss of **$428,718,083** across the web3 ecosystem in Q3 2022. These numbers represent a 62.9% decrease compared to Q3 2021, when hackers and fraudsters stole **$1,155,334,775**. Most of that sum was lost by 2 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. The total amount of loss of these two projects alone reached $350,000,000.

Numbers Down

There are numerous reasons why the total value of losses has decreased.

- Developers are getting smarter over time and also more experienced. Security has moved from a side concept to a main concept.
- Bug bounties and other security innovations have saved countless billions of funds from being hacked by blackhat hackers.
- More well-established protocols are standing the test of time and becoming safer.
- Poorly managed projects, which often also have poor security, are being weeded out by the bear market.
- The total value of losses is down because the total value of crypto is down as a result of economic trends.

It’s too early to tell which one of these reasons has played a decisive role in bringing down the total value of losses, so it’s too early to celebrate any progress that has been made. Hacks are still happening, including some incredibly high-value ones. It’s important to stay vigilant and continue to invest in security.

Immunefi

Funds Recovery

In total, **$93,800,000** has been recovered from stolen funds, across 6 specific situations. This number makes up **4%** of the total losses YTD.

Multichain
Stolen
$3 million
Recovered
$2.6 million

Axie Infinity
Stolen
$625 million
Recovered
$30 million

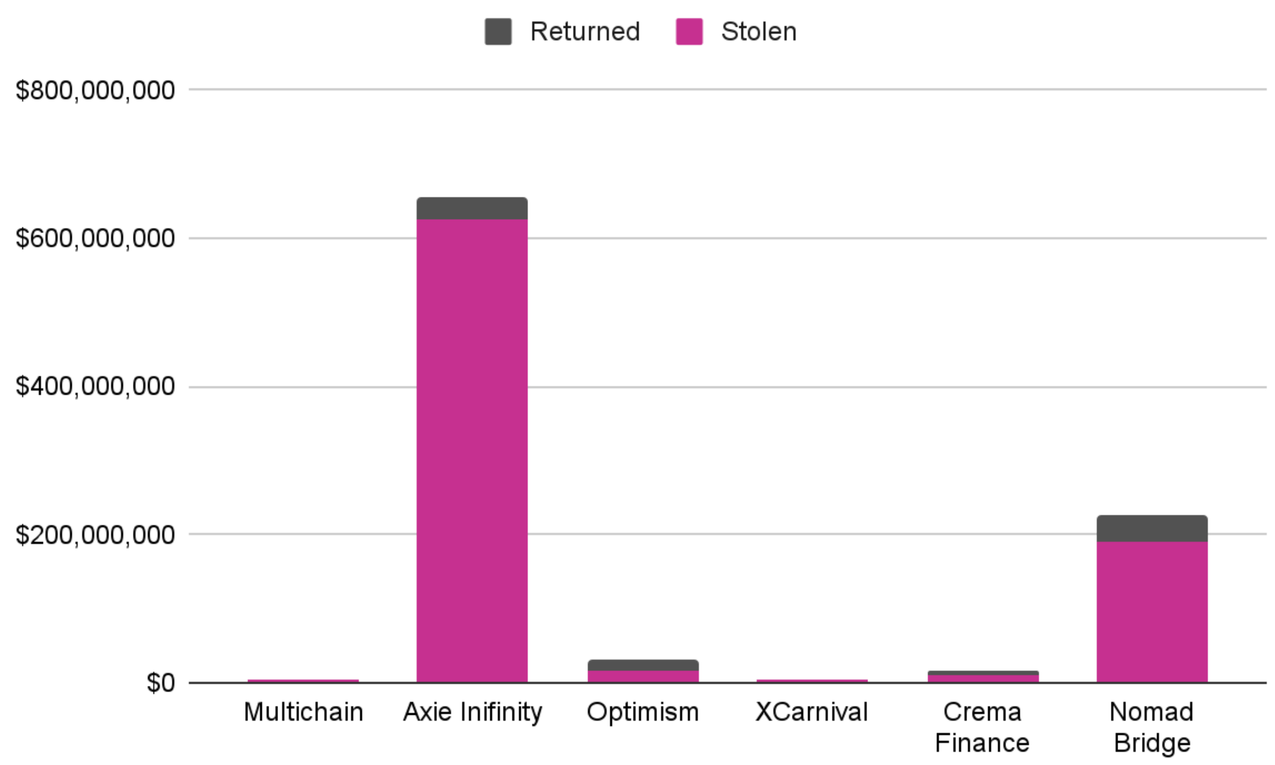
Optimism
Stolen
$16 million
Recovered
$15 million

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

Some of the biggest hacks, such as the Axie Infinity one, have come from organizations like the Lazarus Group, which is backed by North Korea. These groups will never return any funds, as they have state support and are largely immune from prosecution. Other malicious hackers are spread across the world, and so even if law enforcement knows the identity of a hacker, it's not always easy to prosecute that person or affect a return of funds. Furthermore, hackers are becoming more and more professional in their DeFi hacking, leaving fewer traces for investigators to pick up on. It's clear there is room for improvement here.



Immunefi

Immunefi is the leading bug bounty and security services platform for web3 protecting over $60 billion in user funds. Immunefi boasts 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 the code of particular projects 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 **$60 million** in total bounties, while saving over **$25 billion** in user funds.

Total bounties available

Immunefi offers over **$132 million** bounties available.

Supported projects

Trusted by established, multi-billion dollar projects like Chainlink, Wormhole, MakerDAO, Compound, Synthetix, and more, Immunefi now supports 302 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.

If you're a developer thinking about a bug-hunting career in Web3, we got you. Check out our ultimate blockchain hacking guide, and start taking home some of the $132M in rewards available on Immunefi — the leading bug bounty platform for Web3.