Immunefi

HACKING DEEP DIVE
BNB CHAIN

PREPARED BY IMMUNEFI

Hacking Deep Dive: BNB Chain

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 on BNB Chain since its inception in September 2020.

INTRODUCING BNB CHAIN

BNB Chain, formerly known as Binance Smart Chain, is a blockchain network launched by the cryptocurrency exchange Binance. BNB Chain offers smart contract functionality and compatibility with the Ethereum Virtual Machine (EVM).

Since its launch in September 2020, BNB Chain has rapidly evolved, achieving several key milestones. By February 2021, it experienced a surge in users and transactions, showcasing its scalability and efficiency. By August 2021, BNB Chain had surpassed Ethereum in daily transaction volume, solidifying its position as a leading blockchain platform. These data points highlight the rapid growth and adoption of BNB Chain, setting the stage for further advancements in the DeFi space. As of June 2024, BNB Chain's TVL sits at $4.9 billion—the third largest chain by total value locked.

SECURITY OVERVIEW

In total, we have seen a loss of **$1.64 billion** on BNB Chain since its inception. $1.27 billion was lost to hacks across 168 specific incidents, and $368 million was lost to fraud across 228 specific incidents. Most of the sum was lost through four specific incidents, including BNB Chain itself, Venus Protocol, Qubit Finance, and Uranium Finance.

BNB Chain has also been a popular network for rug pulls. Despite efforts to maintain security, a surprising number of users attempt fraudulent activities in the form of rug pulls on the network. Overall, the volume of fraud on the BNB Chain was 2.3x that of Ethereum.

A brief introduction to Rug Pulls

OVERVIEW

Rug pulls are by far the most common type of fraud in DeFi. A rug pull is when a project creates an image of credibility to attract outside capital through token sales or other means with the sole purpose of stealing those deposited user funds and disappearing.

Rug pulls can be divided into **Hard Rug Pulls** and **Soft Rug Pulls**. This report considers both.

HARD RUG PULL

A hard rug pull occurs when developers insert a backdoor or minting function in the protocol codebase, enabling them to drain user funds from smart contracts easily.

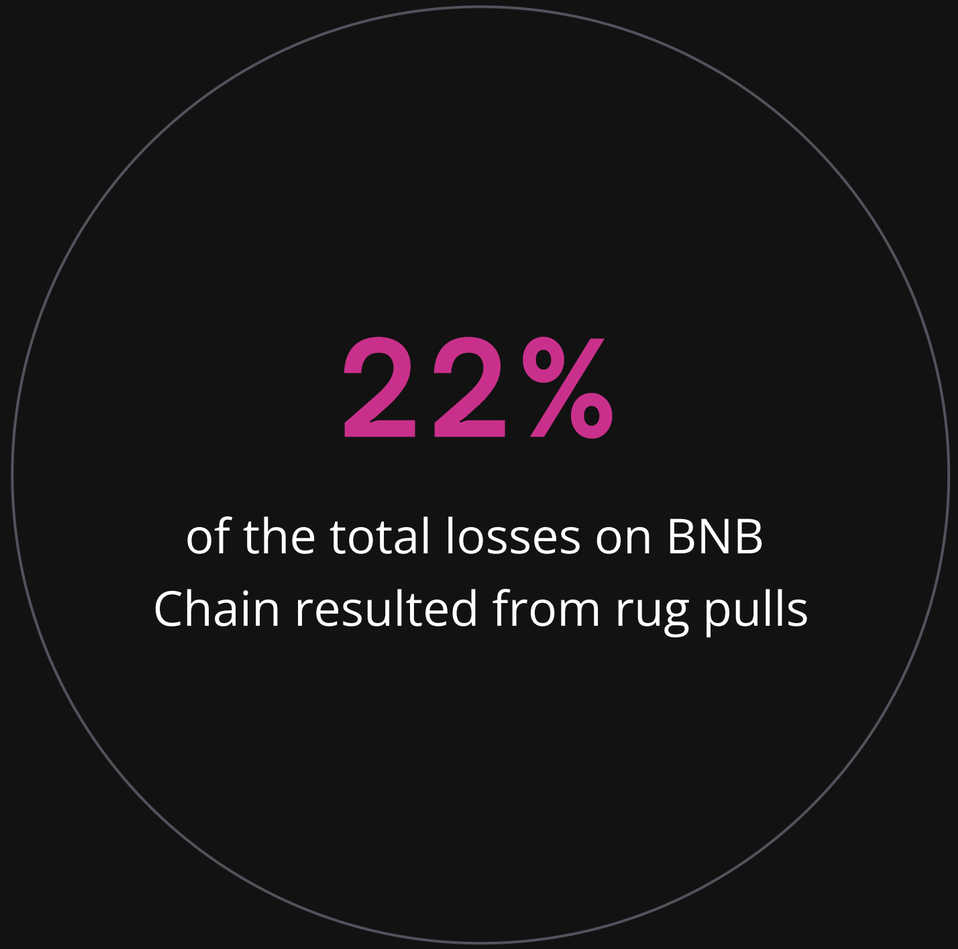
In some cases, a single developer exploits a backdoor in the protocol, while in others, all developers are involved. Rug pulls may be executed all at once, leading to a very clear picture on-chain of what happened. Alternatively, they may be hidden, resulting in funds being drained very gradually or discreetly.

SOFT RUG PULL

A soft rug pull occurs when developers sell off all their tokens and abandon the project, causing the token price to plummet.

IN-DEPT

Why has BNB Chain suffered the most rug pulls in the crypto ecosystem?



BNB Chain Losses

KEY TAKEAWAYS

- From 2020 to 2022, BNB Chain experienced a significant rise in total losses, surging almost 80% from 2021 to 2022 alone, reaching over $911 million in losses.
- However, starting in 2023, BNB Chain began to see a positive downward trend in total losses, dropping to $165 million, an 82% decrease year over year. While the entirety of the ecosystem witnessed a decline in the volume of losses in 2023, Binance's proactive measures to enhance security and interoperability contributed to a decrease in successful exploits. BNB Chain initiated a series of hard forks, such as the ZhangHeng, Plato, and Hertz upgrades, aimed at directly addressing vulnerabilities and improving compatibility.
- Despite these efforts, rug pull incidents continued to thrive compared to previous years.

RUG PULLS

- Since its inception, hacks have remained the primary cause of losses on BNB Chain, accounting for over 77% of total losses.
- Rug pulls, despite resulting in lower losses, still represent a significant portion of incidents and a considerable percentage relative to total losses on BNB Chain — particularly when compared with other chains.
- Despite the downward trend witnessed in 2023 across the ecosystem, rug pulls accounted for 44% of the total losses on BNB Chain in 2023. In comparison, rug pulls on Ethereum made up only 1.7% of total losses in 2023, marking a significant decrease from 4.4% in 2022.

PRIMARY CHAIN FOR RUG PULLS

- A review of the data shows most rug pulls occur on BNB Chain. The primary reason for this is that BNB Chain has faced a serious issue with developers using forked code. Its community has lacked a security-first approach and attracted many users looking for a quick way to earn money. While Binance has been able to seamlessly onboard users onto the chain, the downside is that they become prime targets for bad actors who try to leverage their lack of knowledge and experience.

Top 10 BNB Chain Ecosystem Losses

EXPLOITS

BNB Chain	$570,000,000
Venus Protocol	$200,000,000
Qubit	$80,000,000
Uranium Finance	$50,000,000
PancakeBunny	$45,000,000
Stake	$41,300,000
Spartan Protocol	$30,000,000
Transit Swap*	$28,900,000
Helio	$15,000,000
Elephant Money	$11,200,000

RUG PULLS

DeFiAI	$40,000,000
DeFi100	$32,000,000
Fintoch	$31,600,000
Meerkat	$31,000,000
StableMagnet*	$25,000,000
Harvest Finance*	$21,500,000
Raccoon Network*	$20,000,000
Flare	$17,000,000
Value DeFi	$11,000,000
Arbix Finance	$10,000,000

* Raccoon Network & Freedom Protocol

BNB Chain Major Exploits Analysis

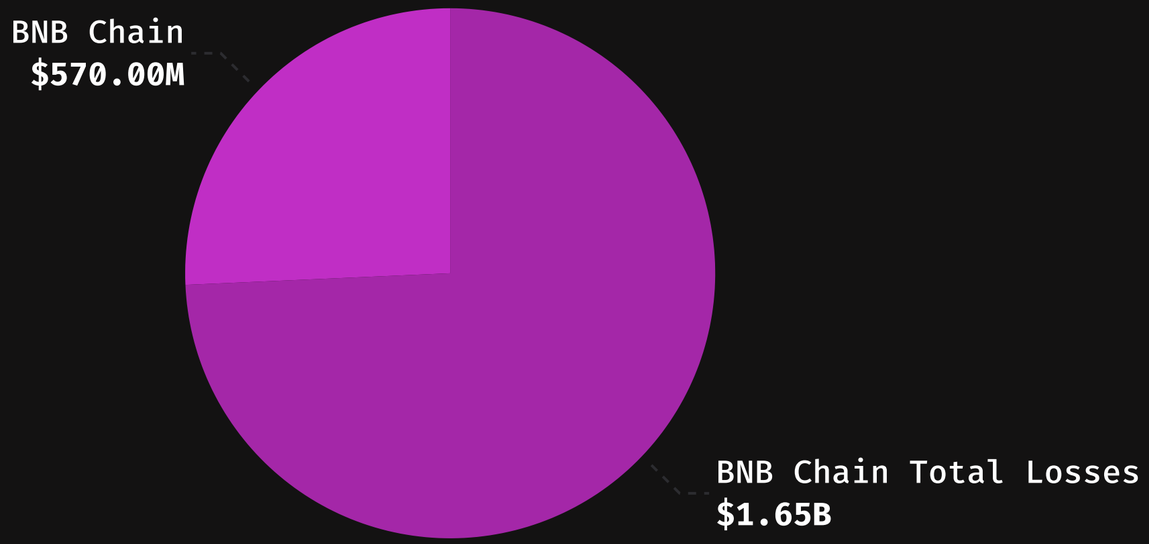
Most of the sum lost from exploits was lost through four specific incidents, including BNB Chain, Venus Protocol, Qubit Finance, and Uranium Finance, totaling **$900 million**. Together, they account for **54%** of the total historical losses on BNB Chain.

BNB CHAIN

- In October 2022, BNB Chain suffered a direct exploit that resulted in a loss of $570 million. The exploit targeted the BSC Token Hub, a native cross-chain bridge, enabling hackers to withdraw BNB tokens off the network.

EXPLOIT IN FOCUS: CHAIN HALTED

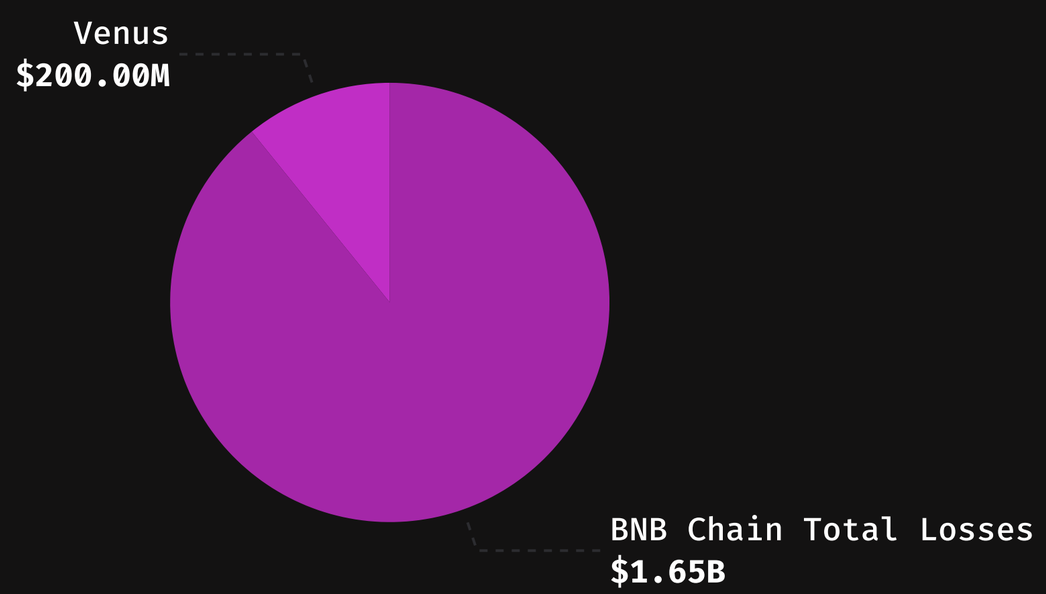
- After discovering the hack, BNB Chain validators unanimously decided to stop the blockchain's operation, halting further token transfers to other chains. Additionally, Tether blacklisted the attacker's address, freezing about $7 million in assets that were moved from the chain. The blockchain was then restored with a hotfix release primarily aimed at preventing the attacker from transferring more stolen BNB tokens off-chain.



BNB Chain Major Exploits Analysis

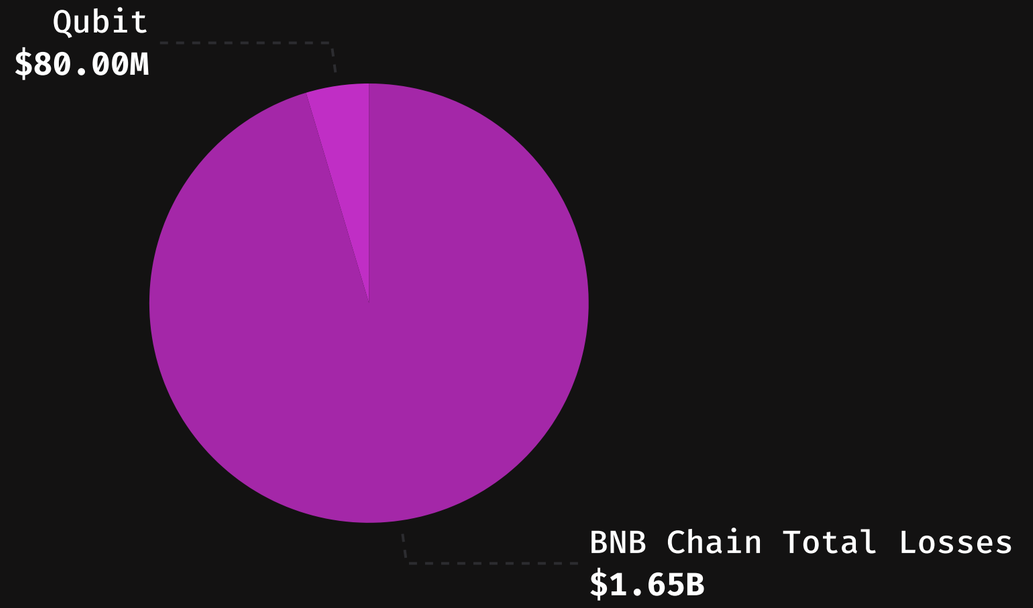
VENUS

- In May 2021, BNB Chain project Venus Protocol suffered a $200M loss, due to a price manipulation of the protocol’s native token XVS, which caused a massive liquidation.



QUBIT

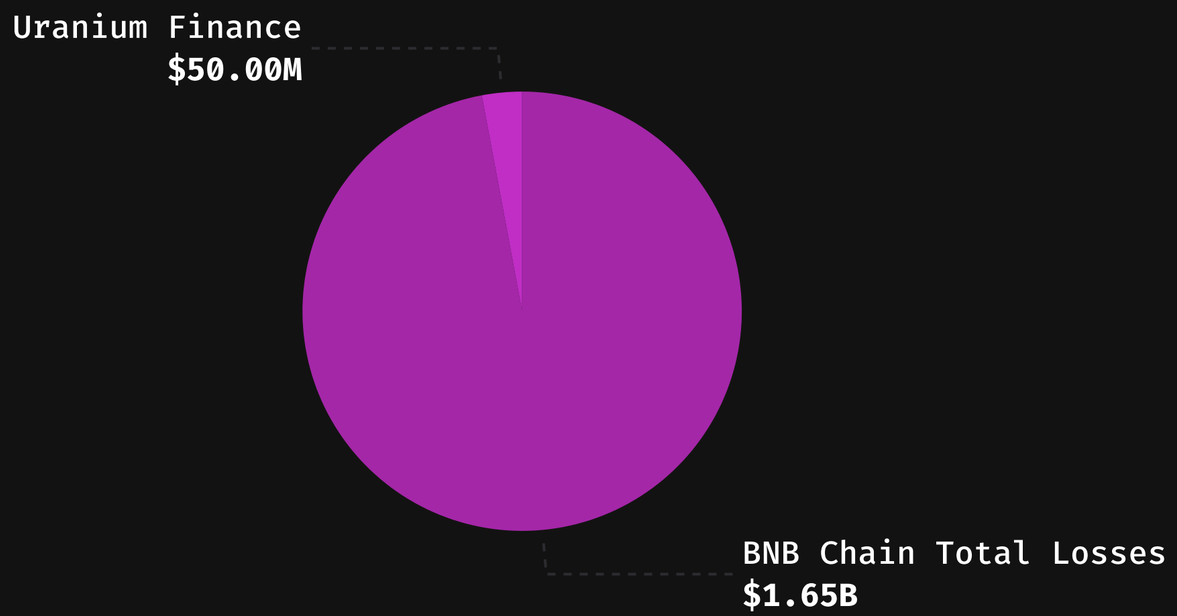
- In January 2022, DeFi protocol Qubit Finance suffered a $80 million loss. Hackers exploited QBridge and stole the entire quantity of the BNB tokens stored in the bridge.



BNB Chain Major Exploits Analysis

URANIUM FINANCE

- In April 2021, Uranium Finance, an automated market maker platform on BNB Chain, lost $50 million in an exploit, when an attacker used a calculation error in the code to siphon liquidity out of the protocol.



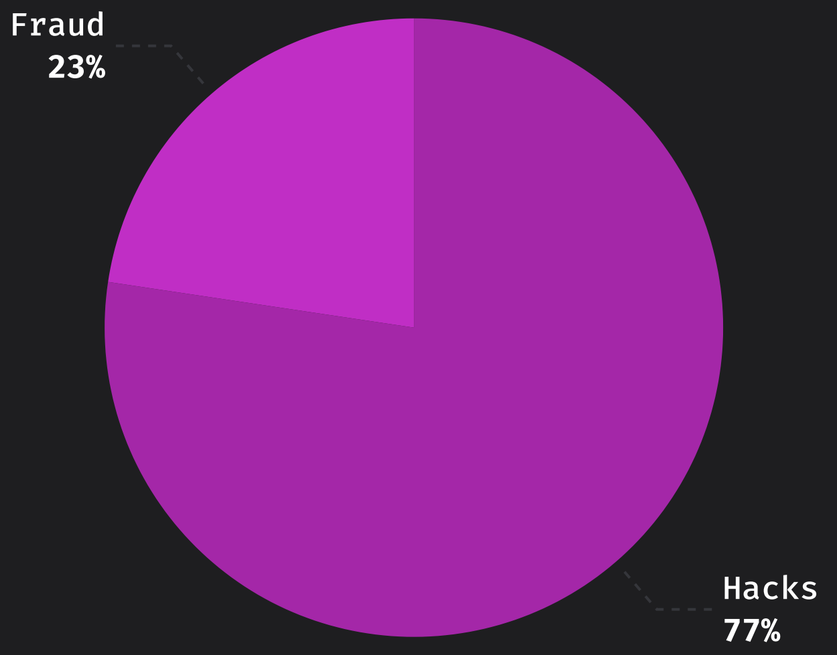
Hacks vs. Rug Pulls Analysis

Hacks continued to be the predominant cause of losses on BNB Chain, compared to fraud.

OVERVIEW

- **Hacks**
  In total, there was a loss of **$1,279,930,833** due to hacks across BNB Chain since its inception, comprising 168 specific cases.

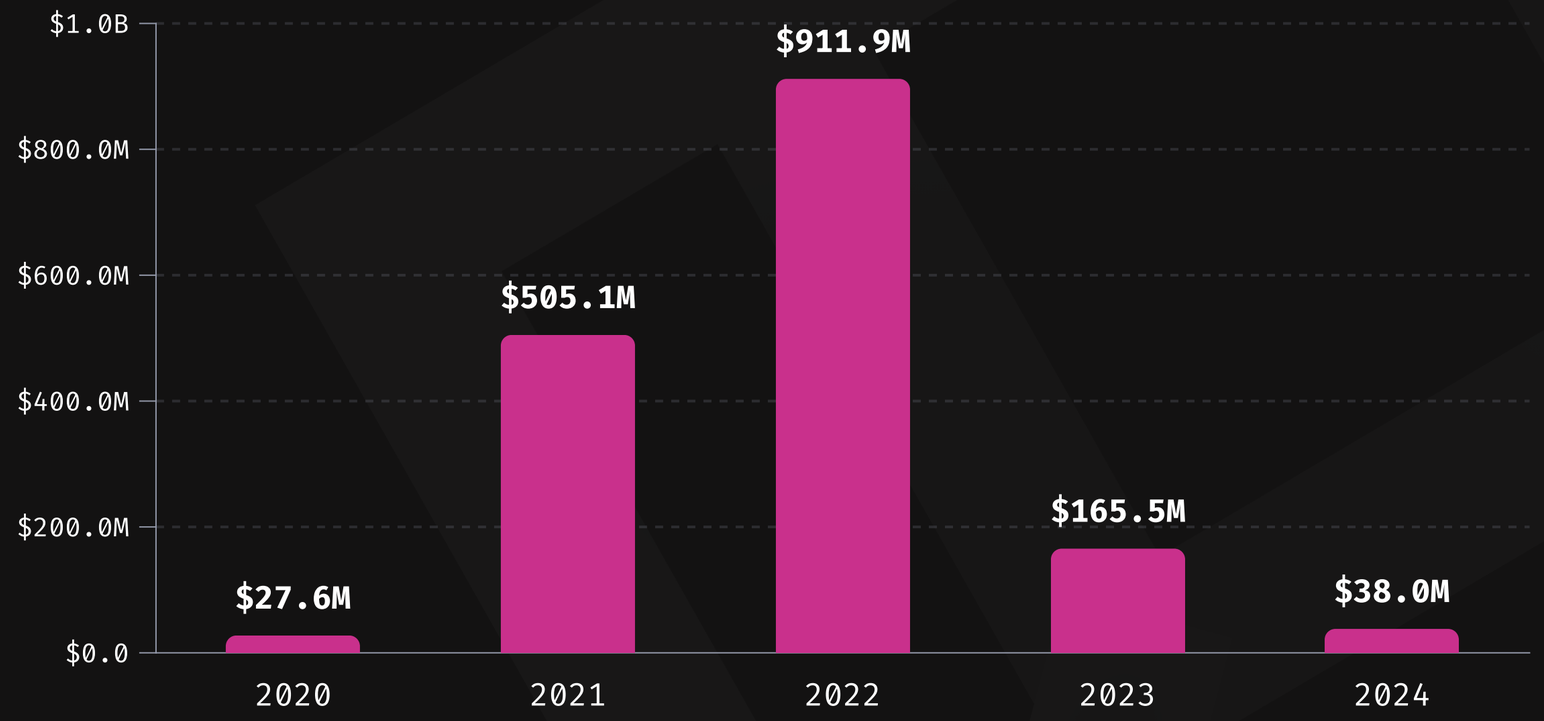
- **Fraud**
  In total, there were a loss of **$368,176,135** to fraud and rug pulls across BNB Chain since its inception, spanning 228 specific cases.



BNB Chain Losses

YEARLY OVERVIEW

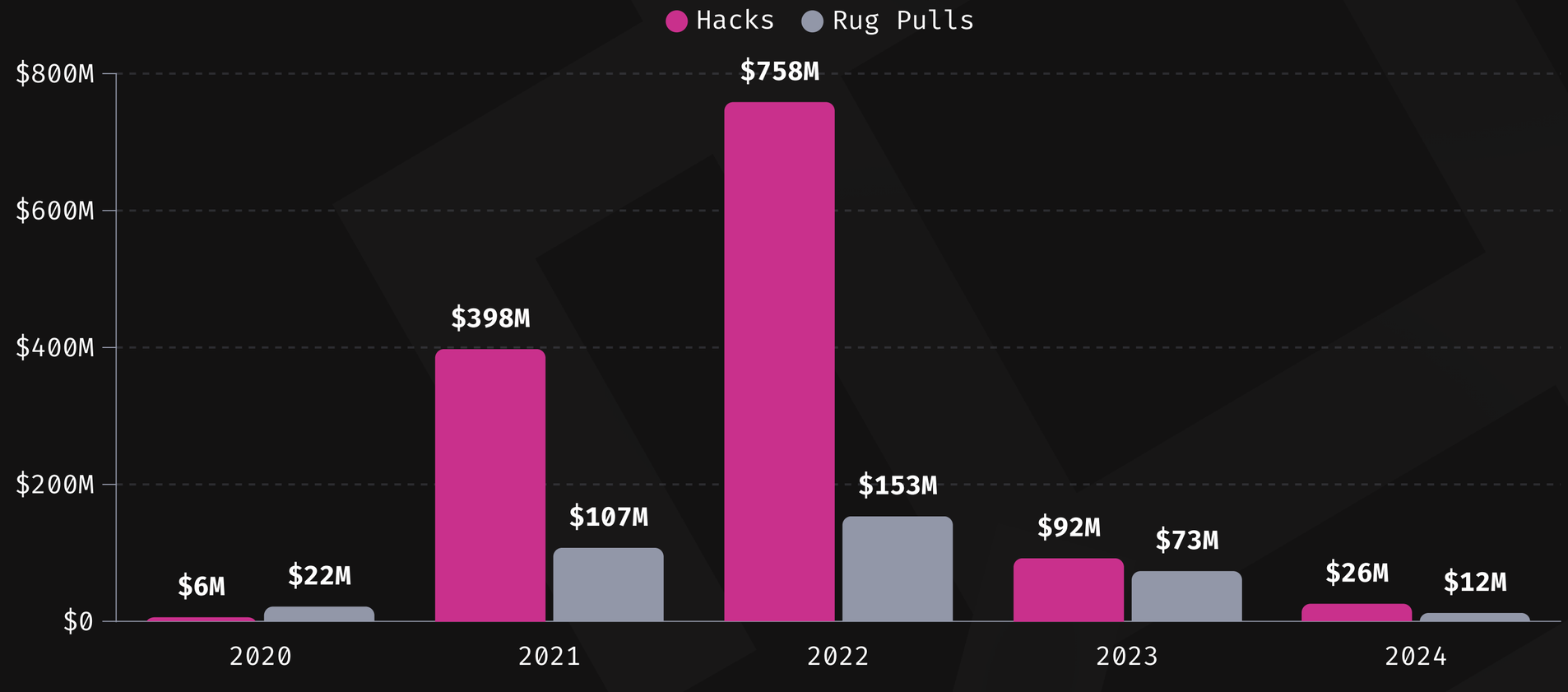
- Overall, we have seen a loss of **$1.64 billion** across BNB Chain, involving 396 specific incidents since its inception in September 2020. The majority of that sum was lost in 2022 across 147 cases totaling $911 million, followed by a $505 million loss in 2021 and a $165 million loss in 2023.



BNB Chain Losses

YEARLY OVERVIEW: HACKS VS. RUG PULLS

- Hacks continue to be the predominant cause of losses across BNB Chain compared to frauds, scams, and rug pulls. In total, there was a loss of **$1,279,930,833** due to hacks across 168 cases, while **$368,176,135** was lost in 228 fraud incidents.



IN-DEPTH

BNB Chain vs Ethereum

2.3x

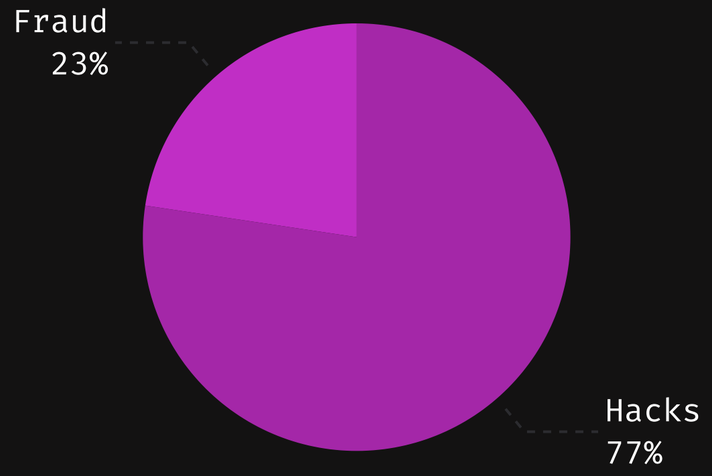
volume of frauds and rug pulls occurred on BNB Chain compared to Ethereum since 2020*

BNB Chain vs. Ethereum

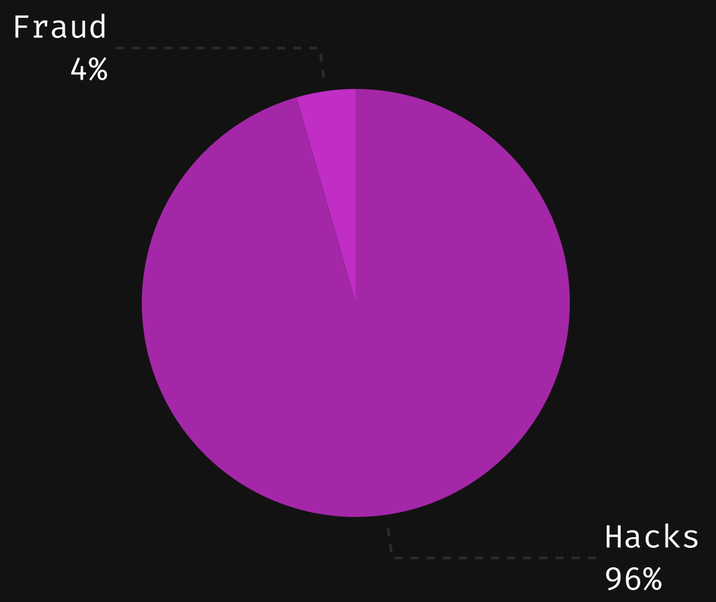
OVERVIEW

- In total, we've seen $1.64 billion in losses across BNB Chain, with 23% lost due to rug pulls. While Ethereum losses were twice as high as those on BNB Chain, totalling $3.6 billion, only 4.4% were due to rug pulls.
- Despite the significant difference in overall losses, the frequency of hacks and rug pulls, and the number of cases across the networks, are almost the same. This indicates that BNB Chain remains a preferred target for rug pulls.

BNB CHAIN



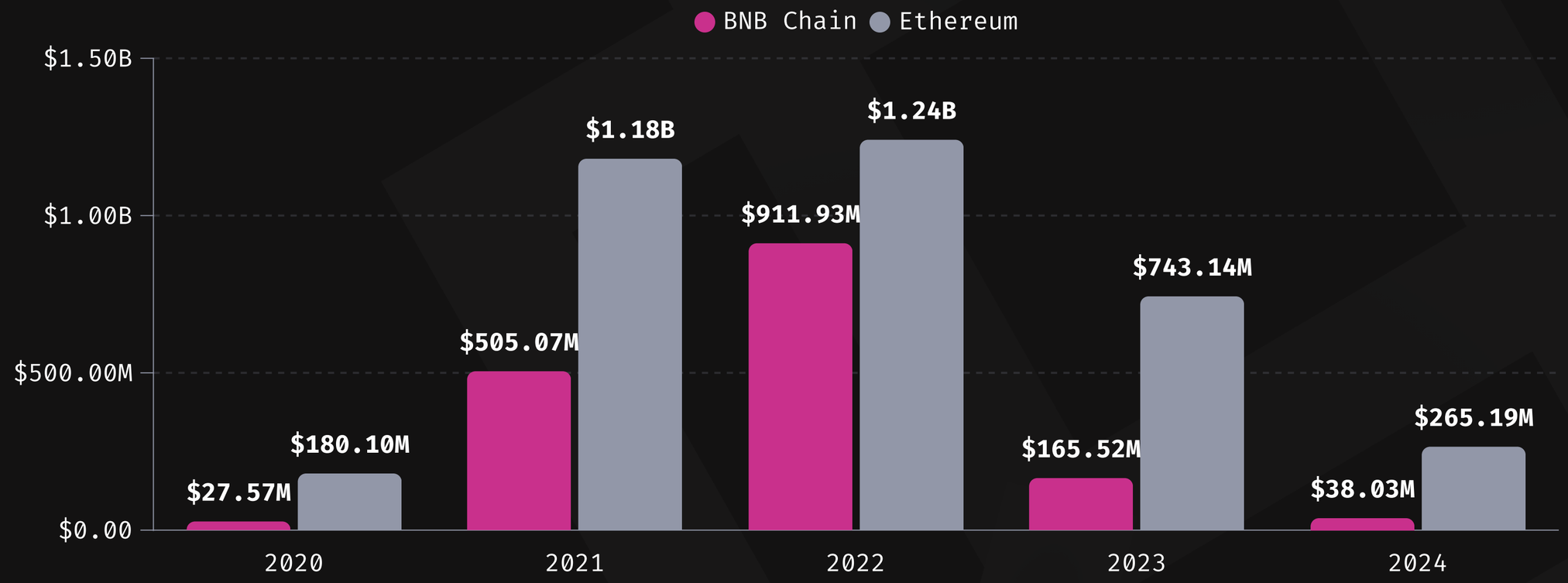
ETHEREUM



BNB Chain vs. Ethereum

YEARLY OVERVIEW: TOTAL LOSSES

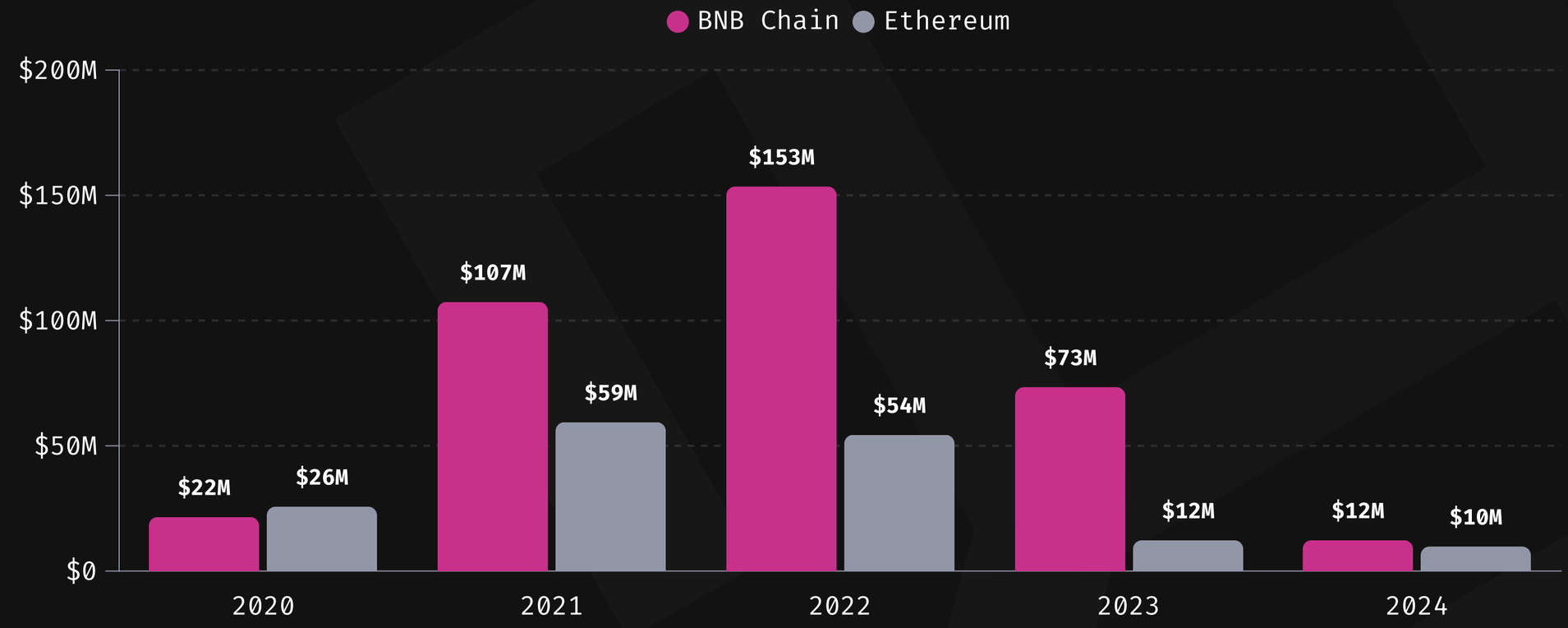
- Overall, Ethereum surpassed BNB Chain in total losses, with $3.6 billion lost across 286 cases since 2020, compared to $1.65 billion lost across 396 cases on BNB Chain since its inception in September 2020.



BNB Chain vs. Ethereum

YEARLY OVERVIEW: FRAUD

- While the total losses on Ethereum surpassed those on BNB Chain, the number of fraud cases on BNB Chain is nearly 4.5 times higher. In terms of fraud, BNB has consistently surpassed Ethereum since its inception in September 2020, until 2024 YTD.
- Since 2020, there have been 50 observed fraud cases on Ethereum, totaling $161 million, while 228 cases have been recorded on BNB, totaling $304 million. The majority of the fraud losses on BNB Chain occurred in 2022 at $153 million, followed by 2021 with $107 million and 2023 with $73 million.



IN-DEPTH

Security Approach to Rug Pulls

Mitigating Rug Pulls

OVERVIEW

While some projects show clear red flags early on, rug pulls are becoming increasingly sophisticated, with scammers employing a variety of tactics. This makes them harder to detect and allows them to lure investors and regular users over a period of months. Situations often arise where even projects that create an aura of credibility and openly communicate exploits or hacks are still under the community's suspicion of having executed a rug pull.

SECURITY APPROACH

Signs of a potential rug pull might include false claims of audits or resistance to implementing ongoing code review or bug bounties, centralized token control and distribution, inactive community engagement, promises of unusually high returns, and lack of a genuine use-case.

- **Research:** thoroughly assessing a project before investing is crucial. A comprehensive examination of the project's digital presence such as website and social media, the roadmap and associated materials, along with research about the team behind the project might reveal signs of suspicious activity.
- **Security:** it is important to assess whether a project showcases legitimate security measures and openly addresses the topic. Third-party code audits and bug bounty programs are good evidence that the project takes security seriously, as it is difficult to hide backdoors with third-party review.
- **Community:** a strong and engaged community can be a positive sign, but it's important to directly engage and assess whether it is actively involved in the project's roadmap and holding it accountable.
- **Pressure:** it can be a signal of a potentially fraudulent project when there's unusually aggressive marketing and selling, pressuring investors and promising unrealistic returns on investment.

Immunefi

Immunefi is the leading onchain crowdsourced security platform which protects 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 **$163 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.

Notes:

- *The volume of losses has been calculated since 2020, with the losses specifically for BNB Chain calculated since its inception in September 2020.
- The Total Value Locked (USD) data has been extracted from DefiLlama.
- *Top 10 BNB Chain Ecosystem Losses: $20 million in stolen funds were later recovered from the Transit Swap exploit, $9 million from Stable Magnet, $5.5 million from Deus Finance, $2.5 million from Harvest Finance, $720K from Palmswap, $465K from Allbridge, and $63K from MetaPoint.
- 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 $1163M in rewards available on Immunefi — the leading onchain crowdsourced security platform.

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