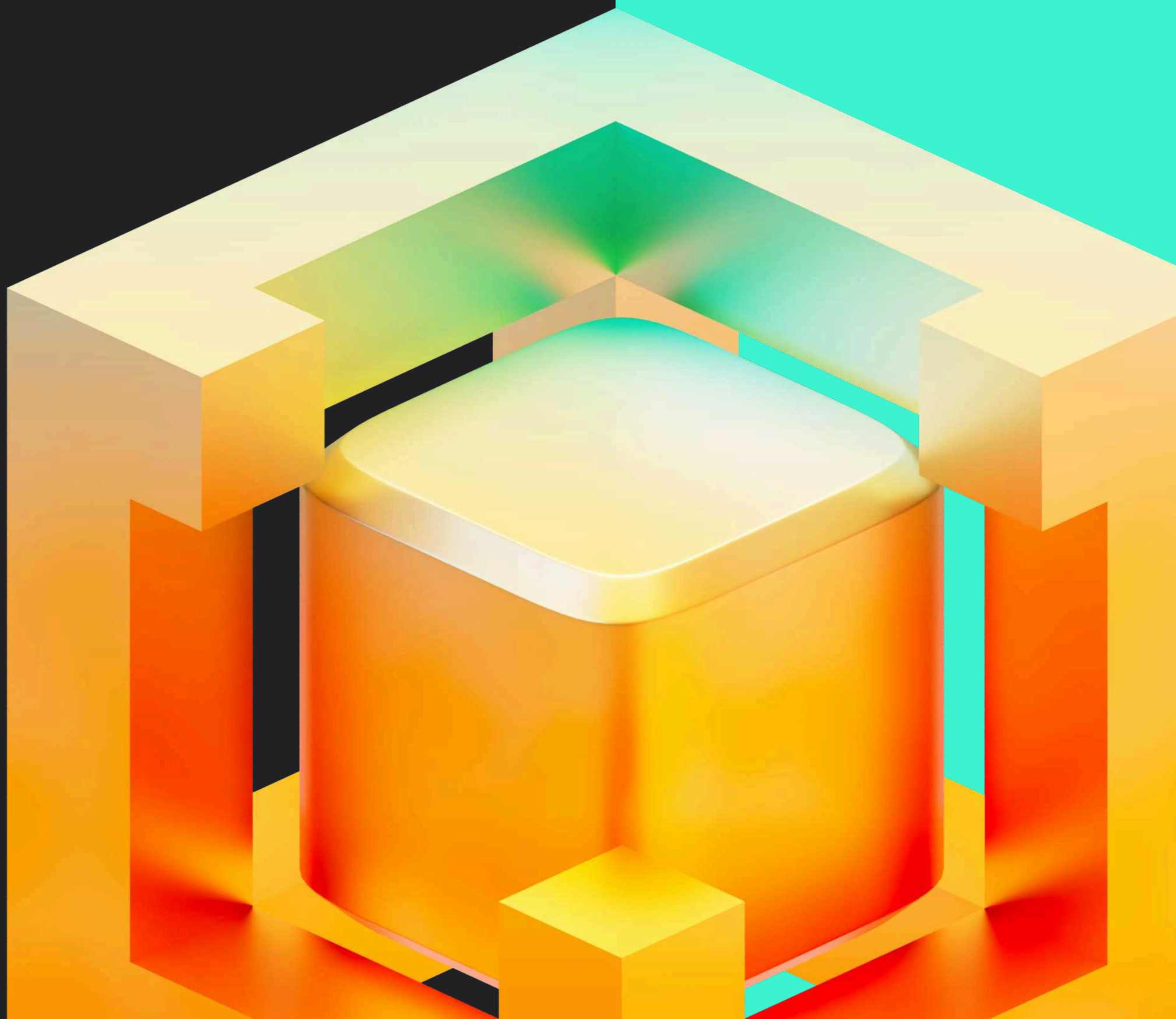
BNB CHAIN

HACKEN

BNB Chain Security Report 2024

Expert insights from Hacken, a trusted blockchain security auditor



hacken.io

BNB Chain Yearly Security Highlights

1. **Security Strengthened and Hacks Decreased:**
Stolen funds fell 70%, from $161M to $47M in 2024.

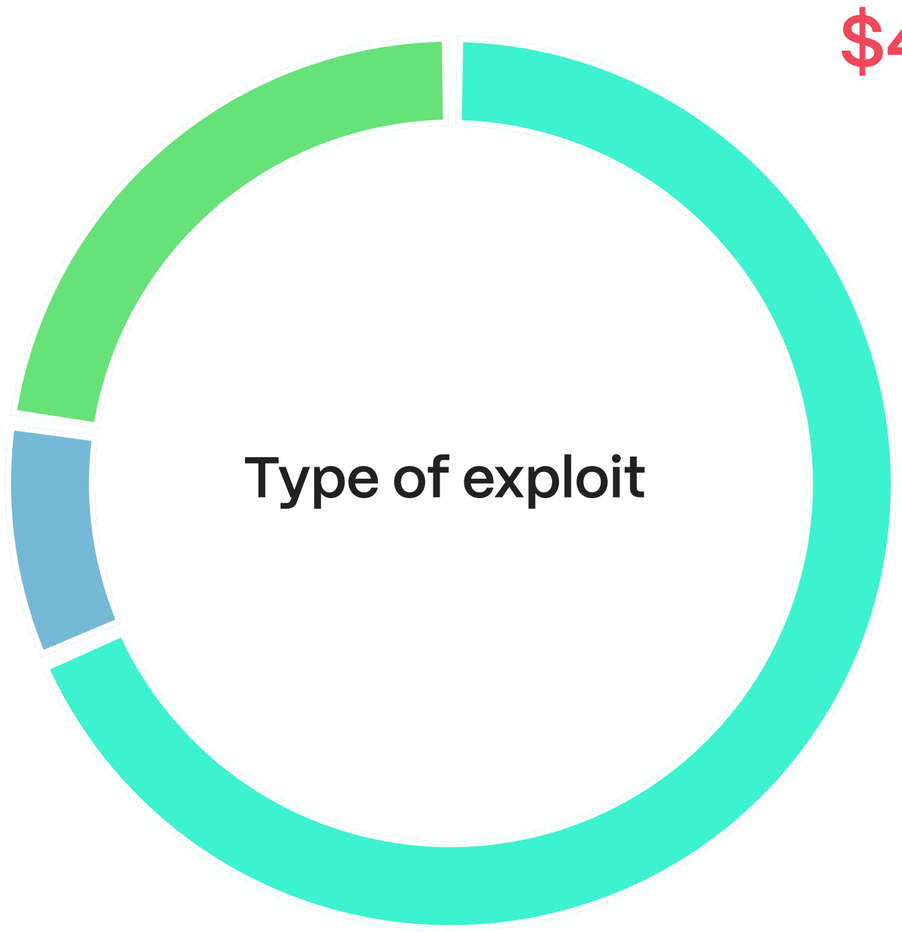
2. **Dominant Threat:**
Access control exploits caused 69% of all yearly losses.

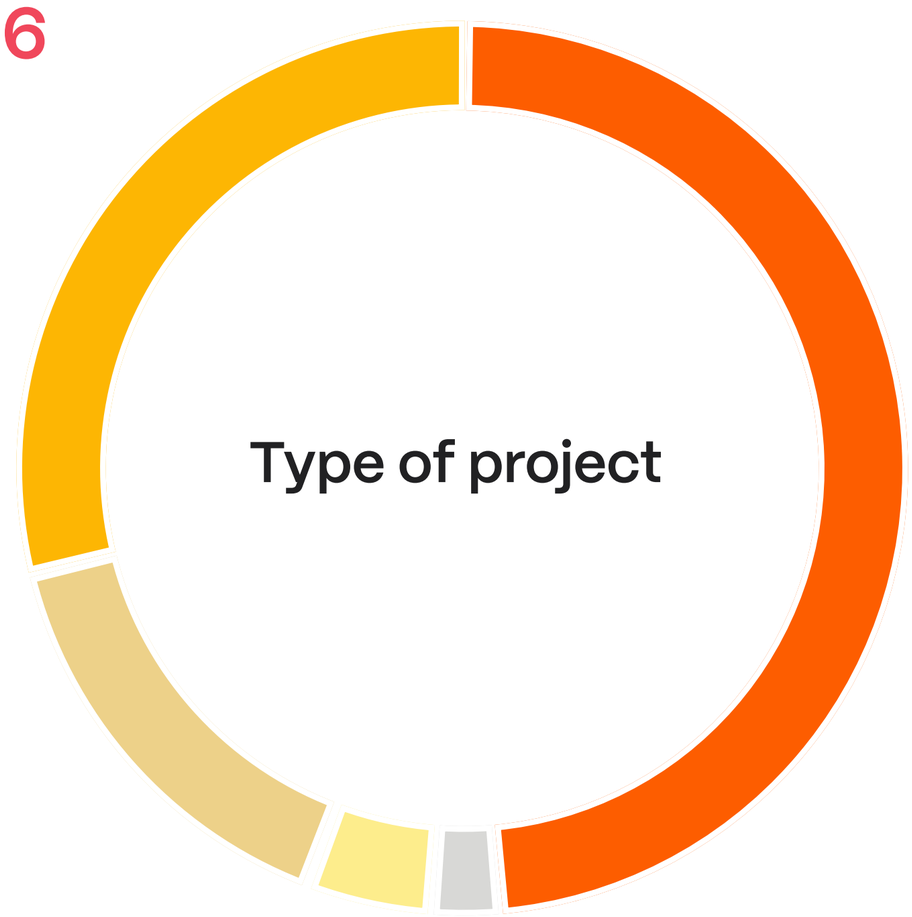
3. **Biggest Hack:**
The Radiant $21M security breach involved malware injection.

4. **More Secure DeFi:**
DeFi losses, excluding the Radiant hack, were just 3.9%.

5. **Scam Alert:**
Rug pulls took $10M, mostly from newly issued or unaudited tokens.

Total
$47 316 116





$32 846 286
Access control

$10 464 544
Rug pull

$4 005 286
Smart contract exploits

$22 864 286
DeFi

$14 187 830
Token

$7 500 000
CeFi

$2 069 000
Gaming / Metaverse

$700 000
Wallet

What You Need To Know

In 2024, the BNB Chain grew more resilient. Total losses dropped from $161 million in 2023 to $47 million – thanks to better security practices and improved monitoring.

While isolated incidents occurred, proactive measures helped minimize overall impact. The Radiant Capital $21 million exploit underscored the ongoing risk of Access Control breaches.

Such exploits can quickly override a project's usual defenses, draining funds in a matter of minutes once ownership permissions are compromised.

The joint report by Hacken and BNB Chain analyzes the year's major attack vectors, highlights the project types most vulnerable to exploitation, and presents insights on preventing or mitigating future breaches.

With DeFi protocols hit hardest and rug pulls persisting, rigorous security audits, bug bounty programs, continuous monitoring, and swift incident response remained the first line of defense on BNB Chain in 2024.

- **Access Control Dominance**

  Attacks aiming at contract ownership or developer access led the pack this year, accounting for nearly 70% of total losses. Some attacks exploited multisig vulnerabilities, emphasizing the need for continuous security improvements, which BNB Chain actively addresses.

- **DeFi's Continuing Vulnerability**

  DeFi security has improved significantly, with losses decreasing from over 80% in 2023 to 48% in 2024, showcasing progress while highlighting areas for continued strengthening. This was mostly because of the Radiant Capital Access Control exploit, which had resulted in 44% of the total loss of the BNB Chain ecosystem in 2024.

- **Rug Pulls Still Common**

  Rug pulls made up more than 22% of the year's total losses, mostly affecting newly issued or lightly audited tokens. A sharp decline in rug pulls from $49M in 2023 to $10M in 2024 shows that enhanced scrutiny and community diligence are yielding positive results.

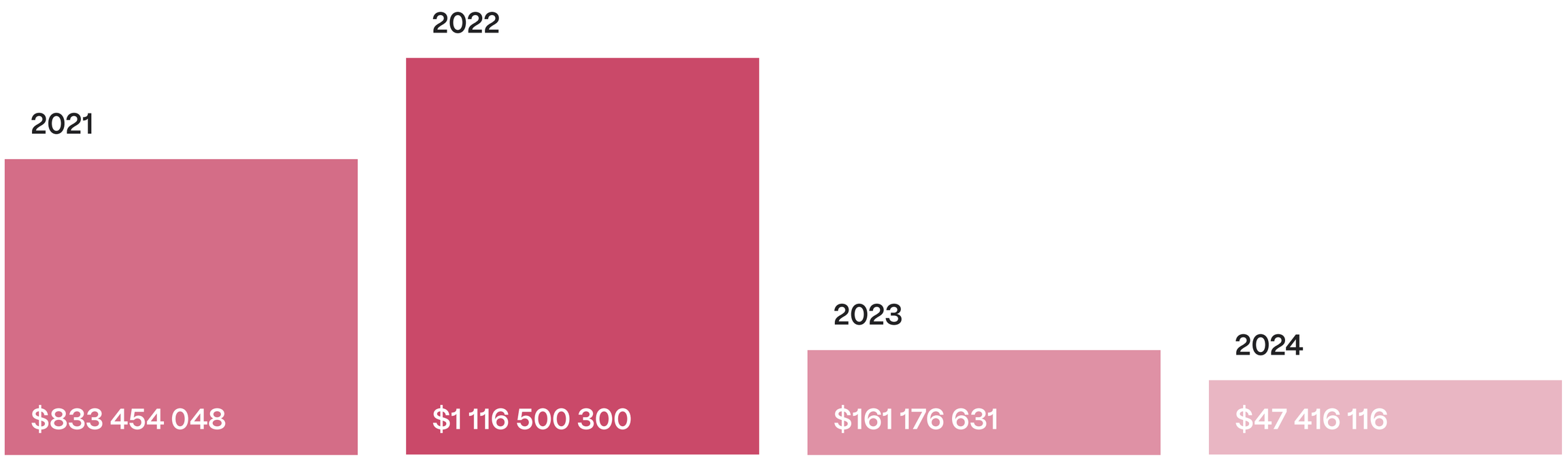
- **2024 vs. 2023**

  Total losses on BNB Chain dropped by around 70%, down from $161 million to $47 million. Smaller scams have significantly declined, demonstrating improved security measures. Isolated incidents like Radiant highlight the need for continuous vigilance, which BNB Chain remains committed to.

- **Incident Response: The Critical Factor**

  Effective, quick reactions to suspicious admin transactions or compromised signers can significantly reduce fallout. In Radiant's case, The Radiant incident demonstrated the importance of swift response mechanisms, reinforcing BNB Chain's commitment to enhancing governance and emergency protocols.

Stolen Funds Continue to Decline



Total losses on BNB Chain per year

In 2024, stolen funds on BNB Chain dropped for the second year in a row, falling from $161.2M in 2023 to $47.4M. This sharp decline reflects both improved security awareness and a shift in attackers' methods and targets. While incidents remain frequent, the average financial loss per attack has dropped to its lowest level in years.

High-value exploits are becoming less common on BNB Chain.

A breakdown of 2024 losses shows a shift from previous years, with DeFi projects accounting for 48.2% of stolen funds—down from over 80% in 2023. Token projects, CeFi platforms, gaming/metaverse, and wallets now share a greater portion of the risk, indicating that while DeFi security has improved, other sectors remain vulnerable.

Rug pulls on BNB Chain, once a major contributor to losses, saw a sharp decline in 2024. In 2023, they accounted for $49M in losses, whereas token-related incidents in 2024 resulted in $10M. This drop suggests that increased scrutiny and market caution are making it harder for scammers, as users are becoming better at identifying high-risk projects.

Access control issues, particularly multisig vulnerabilities, remain a major threat. The Radiant Capital attack demonstrated how sophisticated tactics can bypass cold storage. While overall losses have declined, hackers are refining social engineering methods that remain difficult to counter. With the rise of AI-powered impersonations—including deepfake voice, video, and live call scams—these threats will continue to be challenge.

Top 3 Biggest Hacks on BNB Chain in 2024

1 Radiant Capital – $21M

DeFi

Access Control

How Did The Hack Occur?

Radiant Capital experienced a $55M ($21M – on BNB Chain) security breach involving malware injected into developer devices. Hence, attackers were able to intercept and manipulate legitimate transaction approvals despite the use of hardware wallets.

The attackers exploited this to transfer ownership of Radiant's critical LendingPoolAddressesProvider contract and execute a multicall transaction on Arbitrum, which included upgrading the Lending Pool's implementation to malicious code and draining underlying assets from Radiant Markets contracts.

Incident Response

Radiant had an automated incident response system in place, provided by their security partner Hypernative. However, the pause command failed to stop the malicious contract upgrade.

This system was set to alert and pause operations if suspicious activities were detected. It triggered alerts for three key events: (1) the ownership transfer of the LendingPoolAddressesProvider, (2) the upgrade of the Lending Pool contract, and (3) the draining of $32 million in assets.

After detecting the attack on Arbitrum, Radiant quickly paused the Lending Pool on both the Ethereum network and BNB Chain.

However, the pause on Ethereum occurred first, despite BNB Chain having a higher total value locked.

The main flaw in the incident response was that the contract upgrade was possible even when the contract was paused. In the multicall transaction, the second operation involved upgrading the Lending Pool's implementation with malicious code.

This upgrade could be executed regardless of whether the Pool was in a "paused" or "unpaused" state, highlighting a critical security oversight enabling the hack.

The attack on the BNB Chain pool was fully executed in just 80 seconds.

The incident affected more than 10,000 victims due to infinite token approvals post-exploit, resulting in ongoing unauthorized fund transfers. New victims continue to emerge daily on both Arbitrum and BNB Chain, where the exploit occurred.

Security Recommendations From Hacken

CCSS Audit

to protect team endpoints from malware injection and phishing attempts

Extractor

A more reliable incident response solution designed to automatically trigger a built-in protection mechanism like instantly pausing the lending pool ≥

2 Gifto – $8.6M

Token Rug Pull

How Did The Rug Pull Occur?

The incident began when Binance announced that it would remove Gifto's token (GFT) from its platform on December 10, 2024. Instead of trying to fix the situation, the Gifto team quickly issued an extra 1.2 billion tokens. These new tokens, worth about $8.6 million, were sent to major exchanges within a few hours. The move flooded the market, and GFT price fell by 36% in just one day, leaving many retail investors confused and facing losses.

In what appears to be a form of market manipulation, the Gifto team took advantage of the time following the delisting announcement—a period when investors were already nervous—to flood the market with new tokens.

This sudden increase in supply caused the token's value to drop rapidly and undermined trust among investors. Some community members called for Binance to freeze the tokens or block the account to protect investors.

This event highlights the need for clearer rules and better control in the cryptocurrency market to prevent similar issues in the future.

3 CoinsPaid – $7.5M

CeFi · Access Control

How Did The Hack Occur?

CoinsPaid, an Estonian cryptocurrency payment service provider, suffered a unique phishing attack on January 5th, resulting in the theft of approximately $7.5 million on BNB Chain and Ethereum.

Attackers employed a fake job interview scheme, deceiving an employee into accepting a fraudulent job offer and downloading malicious software.

This granted the hackers access to CoinsPaid's internal systems and sensitive data. In a previous incident in July 2023, CoinsPaid was hacked for $37.3 million, forcing the company to shut down operations for four days.

Security Recommendations From Hacken

Virtual CISO

to enforce robust security policies, ensuring continuous team protection against social engineering attacks, malware injection, and phishing attempts ≥

Access Control Rampage

Nearly 70% of 2024 losses on BNB Chain–$32.9 million—were caused by access control exploits, including the breaches of Radiant Capital, CoinsPaid, Karastar, Narwhal, and Polyhedra. These types of attacks occur when attackers gain unauthorized access to key functions by compromising private keys or multisig wallets.

Security breaches enable attackers ownership or upgrade contracts with malicious code, draining massive funds.

This issue extends beyond BNB Chain—globally, access control exploits accounted for 75% of all hack losses in 2024, totaling $1.72 billion.

Recommendations for B2B Operational Security

To help prevent access control exploits, all BNB Chain projects should consider these security steps:

- **Enhanced MultiSig and Access Control Monitoring:**

  Set up continuous monitoring for MultiSig contracts. Use automated systems to check transaction signatures in real time and remove any compromised accounts immediately. This step can stop attackers before they complete a harmful transaction.

- **Robust Private Key Management:**

  Use strong methods for managing private keys. This includes using encrypted and decentralized storage and multi-layered authentication instead of relying on a single signature, which can easily be compromised.

- **Automated Incident Response Strategies (AIRS):**

  Go beyond simply pausing contracts during suspicious activity. Build an automated incident response system that can detect and react quickly to access control breaches. Tools like Extractor's Wallet Actions can help by automatically removing a compromised key from the MultiSig, reducing the time attackers have to cause damage.

- **Regular Security Audits and Adherence to Standards:**

  Perform regular security audits following recognized standards such as the Cryptocurrency Security Standard (CCSS). These audits will help identify weaknesses in access control and ensure that the security measures remain up to date.

The Case For Automated Incident Response Strategy

Nowadays, continuous transaction monitoring and rapid response measures are vital, especially for projects using upgradeable contracts. A proper Automated Incident Response Strategy (AIRS) monitors critical contracts, detects threats and anomalies in real-time, automatically mitigates attacks, and prevents catastrophic losses before they escalate.

> It's possible to save most of the assets from being completely drained by hackers.

To illustrate its effectiveness, we analyzed two security incidents on BNB Chain—Radiant Capital ($21M) and Polyhedra ($800K)—which targeted companies of different sizes and scales. These cases demonstrate how timely monitoring and automated responses could have stopped or minimized the damage.

100%
Prevention in Radiant Capital Hack

80%
Prevention in Polyhedra Hack

100% Prevention in Radiant Capital Hack

$21,000,000 / $21,000,000 Potentially Saved

The exploit was carried out using a multicall-type transaction on the Arbitrum network at 17:09:18 UTC. In this single, atomic operation, the attackers did several things: they transferred ownership of the LendingPoolAddressesProvider to a malicious contract, upgraded the Lending Pool with the new code, and then iterated over Radiant Market contracts to withdraw underlying assets. These contracts, similar to those used by Aave's V2, allowed the attackers to drain funds from all the markets by abusing the transferUnderlyingTo function.

Effective Incident Response Could Have Prevented 100% of the Loss

Radiant had an incident response system in place, yet it failed. The attack exploited a multisig vulnerability, and while Radiant eventually responded, the necessary action came 4 hours and 27 minutes too late, allowing attackers to drain $21M from the BNB Chain.

EXTRACTOR

Hacken Extractor is designed to analyze all possible attack scenarios and deliver the most resilient automated detection and response. With customized setup for each project, it ensures real-time monitoring, anomaly detection, and instant actions In Radiants case, Extractor would have directly targeted the MultiSig contract, preventing execution by swiftly removing compromised signatures across BNB Chain, Mainnet, and Base.

80% Prevention in Polyhedra Hack

$800,000 / $1,000,000 Potentially Saved

Attackers gained access to Polyhedra's upgradeable cryptocurrency wallets by using a leaked key. They deployed a malicious implementation to the proxies of these wallets and then upgraded four wallet contracts with this harmful code. This allowed them to control the wallets and withdraw assets. In total, around $1 million in cryptocurrencies was exchanged for BNB tokens, with the most significant loss being $800K in $THE (Thena) tokens. Notably, the attacker withdrew the $THE tokens at the end of the withdrawal sequence.

Effective Incident Response Could Have Prevented 80% of the Loss

Again, an effective Attack & Incident Response System could have prevented 80% of the Polyhedra exploit. The attack's structure created a small detection window—the malicious implementation was deployed quickly, but the main $THE token withdrawal occurred last. This brief delay would have been enough for an automated system to detect the unauthorized wallet upgrades and trigger an immediate response before the final withdrawal.

For example, Extractor's real-time monitoring and automated threat detection would have instantly flagged the suspicious contract upgrade, allowing for rapid mitigation and securing funds before any significant losses occurred.

More Secure Bridges on BNB Chain

In 2024, bridge hacks on BNB Chain saw a dramatic 99% decline, with only one notable incident—the Polyhedra hack, which resulted in a $1 million loss. In 2023, cross-bridge vulnerabilities were exploited for nearly $100 million.

Hackers targeted these bridges because they lock large amounts of crypto assets on one chain to mint collateralized assets on another, creating an attractive target. These incidents were often the result of weaknesses in access control and smart contract vulnerabilities, which allowed attackers to exploit the bridges and steal funds.

The shift is largely due to enhanced security measures adopted by bridge projects.

- advanced consensus mechanisms
- modular designs
- cryptographic safeguards such as optimistic rollups and zero-knowledge proofs.

These improvements have strengthened access controls, reduced smart contract vulnerabilities, and separated transaction verification from execution and asset custody, making it harder for attackers to exploit weaknesses.

The 2024 decline in bridge hacks highlights the effectiveness of modern security architectures in cross-chain protocols, demonstrating that proactive security investments can significantly reduce risk in decentralized ecosystems.

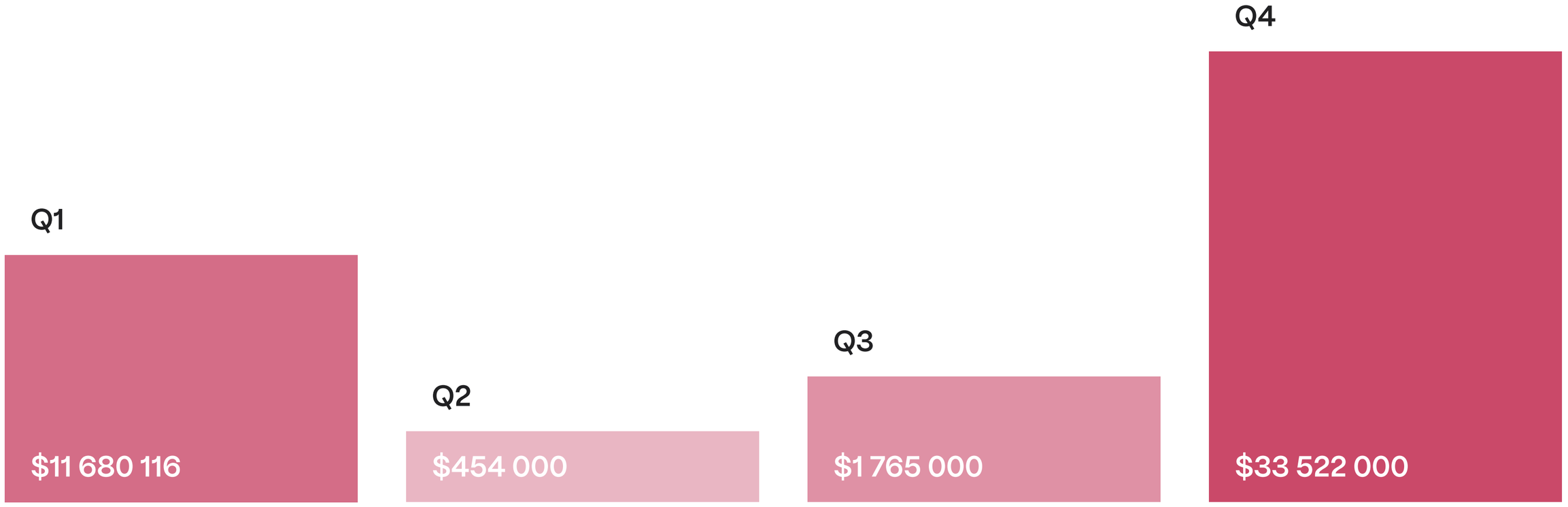
DeFi Losses, Excluding Radiant Hack, Were Just 3.9%

In 2024, DeFi losses on BNB Chain totaled $22.86M, or 48.22% of the $47.4M stolen. However, $21M came from Radiant Capital's hack, heavily skewing the data. Without this outlier, DeFi losses were just $1.86M—a dramatic drop from $128M+ in 2023, when DeFi accounted for over 80% of the $161.2M lost on BNB Chain.

While it remains a key category for security breaches, many DeFi projects have improved their risk management and security measures, resulting in considerably lower losses.

$21 000 000	$1 864 286
Radiant Capital	Other DeFi platforms

Quarterly Breakdown of Losses on BNB Chain in 2024



Q1 saw losses reach $11.68 million, primarily due to the CoinsPaid incident.

Q2 recorded a dramatic drop to just $454,000, marking a period of relative stability.

Q3 reported moderate losses of $1.77 million, reflecting a lower-risk period with fewer high-value exploits.

Q4, however, experienced a sharp surge, with losses soaring to $33.52 million, driven by major incidents such as the Radiant and Gifto exploits.

The Q4 spike underscores the volatility of security threats, demonstrating how a few high-profile breaches can drastically shift the landscape. These fluctuations highlight the critical need for continuous monitoring, proactive security measures, and adaptive defense strategies to mitigate risks throughout the year.

Scam Alert:
Fewer Rug Pulls But Still Common

In 2024, rug pulls on BNB Chain declined significantly compared to 2023, with total losses dropping to $10 million. This reduction reflects improved market vigilance and more thorough due diligence by both investors and project teams.

BNB community is learning from past incidents and taking extra steps to avoid high-risk projects.

However, rug pulls remain a persistent threat, primarily affecting newly issued or lightly audited tokens. These projects often lack proper security reviews, making them easier targets for malicious developers looking to exploit unsuspecting investors.

1

One notable case in 2024 was the incident involving Gifto. After Binance announced its decision to delist the token, the Gifto team issued an additional 1.2 billion tokens, which were quickly dumped on the market. This action led to a sharp 36% drop in the token's price, leaving many retail investors with substantial losses. Although this incident did not involve a traditional hack or access control exploit, it is classified as a rug pull because the team manipulated token supply to profit at the expense of the market. Compared to 2023, similar events have been less frequent, suggesting that both project developers and investors are becoming more cautious.

2

Another significant case was with Narwhal's token. Initially reported as an exploit, further analysis revealed that the situation was more consistent with an exit scam—a form of rug pull. The token experienced two major price slippages within two days, culminating in a near 99% drop in value. Investigation showed that the same wallet, linked to the Narwhal deployer, was behind both slippages. The coordinated movement of funds, which included deposits into Tornado Cash, confirmed that this was a deliberate effort to exit the project rather than a random security breach. This case, along with Gifto's, illustrates how rug pulls continue to evolve and how attackers change their tactics to exploit vulnerabilities in the market.

The decline in rug pulls in 2024 signals stronger investor awareness, better project scrutiny, and improved risk management. However, ongoing security and due diligence remain crucial to giving scammers zero chances on the BNB Chain.

What It Means for BNB Chain Security

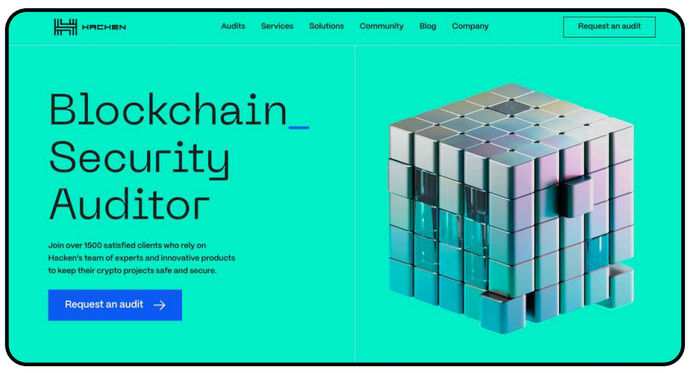
Security on BNB Chain significantly improved in 2024, with advanced cryptographic safeguards, modular security designs, and automated monitoring helping to reduce losses.

Access control vulnerabilities remain the top threat, responsible for 69% of total losses. These exploits enable attackers to bypass security measures, seize ownership control, and drain funds within minutes.

The persistence of such breaches highlights the need for stronger multisig protections, real-time monitoring, and stricter organizational policies to prevent unauthorized contract upgrades, private key compromises, and critical security failures.

With significant progress, a single exploit can impact months of security advancements, highlighting the importance of continuous vigilance, automated incident response, and regular proactive audits.

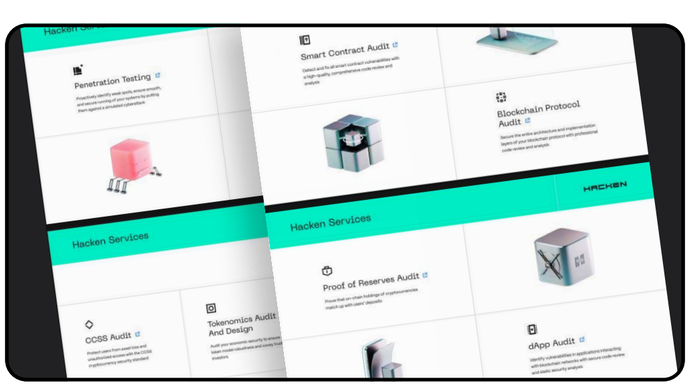
Hacken | Trusted Security Partner for BNB Chain



Learn More About Hacken

Your trusted blockchain security auditor for BNB Chain. Learn how you can strengthen resilience, prevent exploits, and build trust with Hacken.

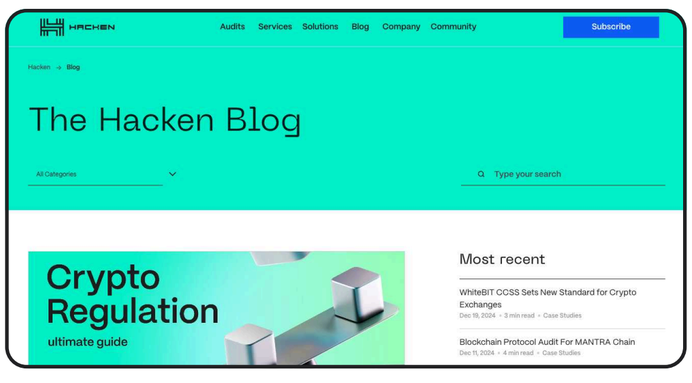
hacken.io



Discover Security Solutions

From smart contract audits to penetration testing, Hacken delivers the most robust security framework for BNB Chain projects.

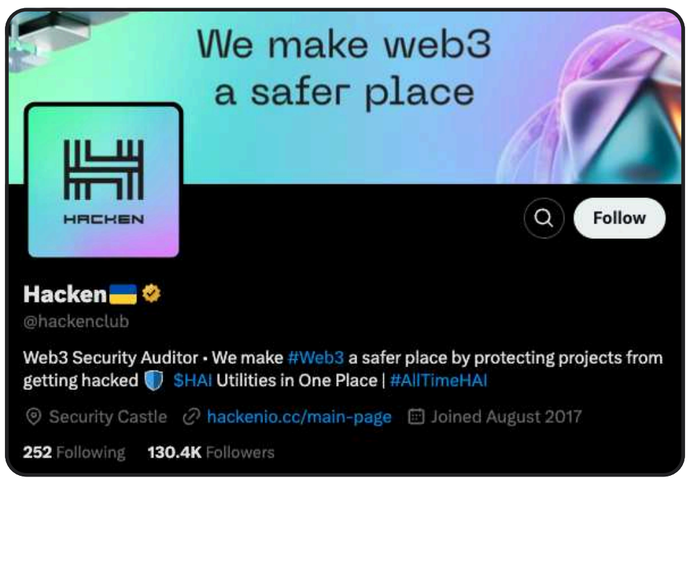
hacken/solutions



Access Educational Resources

Stay ahead of risks with Hacken’s tools and resources—because knowledge is your first line of defense.

hacken.io/research



Support a Safer Web3

Join Hacken’s security community. Stay updated, get involved, and advocate for blockchain security.

x.com/hackenclub

HACKEN

Making Web3 a safer place

About Hacken

Hacken is a trusted blockchain security auditor making Web3 safer for investors and businesses worldwide.

Our Story

Our journey started in 2017, as a small Ukrainian group of bug hunters. Over the years, Hacken has grown into a global leader in blockchain security, evolving alongside the industry and actively shaping it. Today, the biggest protocols and ecosystems choose Hacken as their security partner – the best recognition of the value we bring to Web3.

Our Value

We offer a comprehensive suite of blockchain security solutions, including security audits, compliance support, and more. Together, these create the most robust security framework for Web3 that combines operational excellence with battle-tested processes, protecting billions in digital assets.

Our commitment goes beyond business offerings—we actively champion transparent and reliable digital innovation. Subscribe to Hacken Digest for a host of educational and knowledge-sharing resources, including quarterly and annual security reports.

For media inquiries

marketing@hacken.io

Visit our website and follow us on social media

hacken.io linkedin.com/hacken x.com/hackenclub