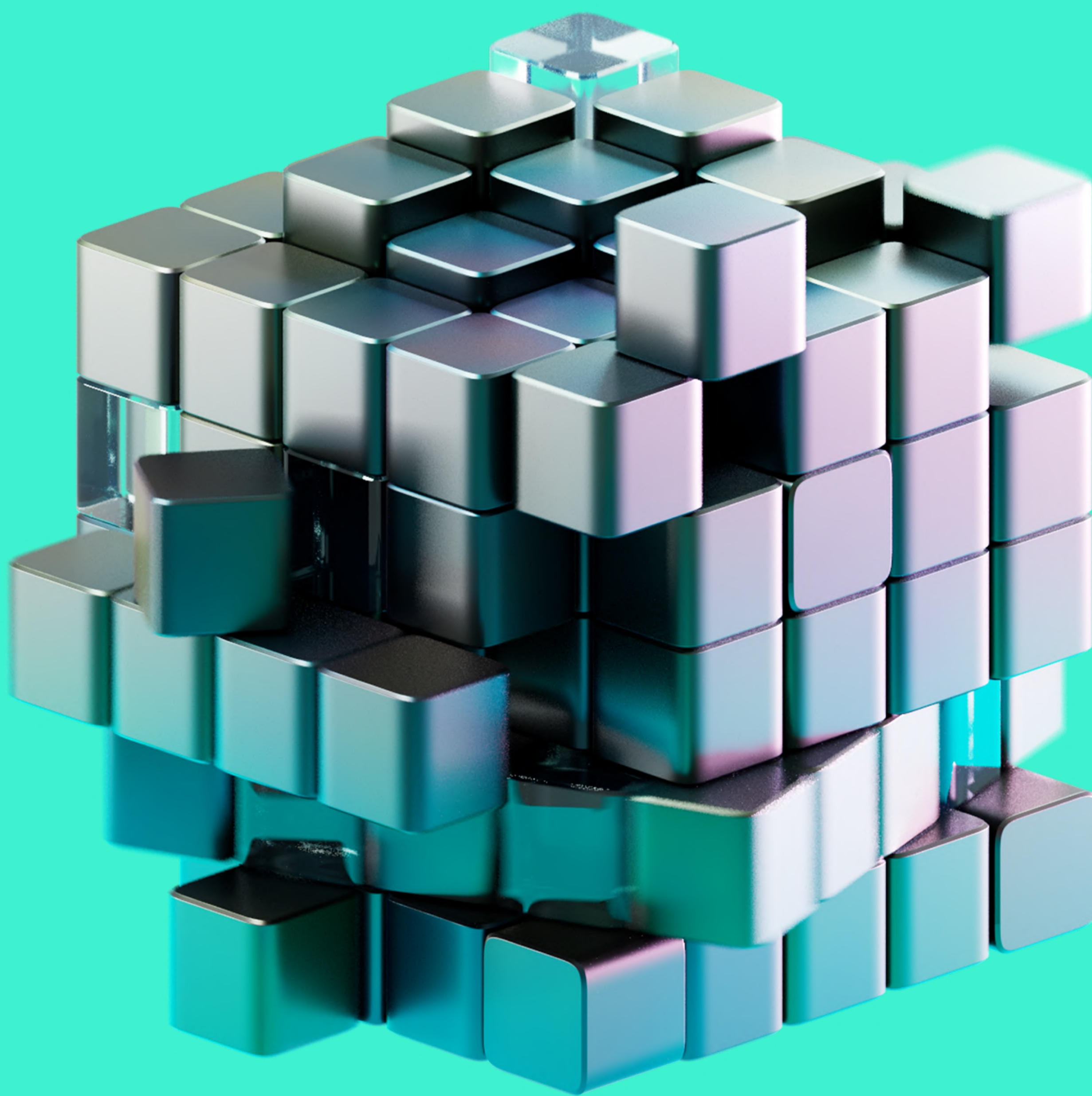


# HACKEN SECURITY REPORT

A Turbulent

20

23



# Table of contents

1. Introduction	3
2. Year in Review	4
Executive Summary	5
More Sophisticated Attacks in 2023	5
2023 Hacks Breakdown	8
Assessing the Impact	10
Affected Networks	12
Geography of Exploits	13
Looking Ahead: Predictions for 2024	14
3. Response and Solutions	16
Audit Coverage	17
Bug Bounties	18
Real-Time Monitoring	19
Secure Hot Wallets	19
Browser Extensions	19
4. Conclusions and Recommendations	20



# Highlights

\$1.9B

was the total yearly losses reached.

50%

of the stolen value due to access control issues.

\$275M

was drained from protocols through flash loan attacks.

20%

of stolen funds were returned.

# Introduction

Imagine you're on vacation when an unexpected alert appears on your phone: an unauthorized transaction from your wallet. The shock deepens as you discover your hot wallet is empty, hacked. This was a grim reality for too many crypto enthusiasts and builders this year.

This report aims to dissect these incidents, understand their implications, and offer insights to foster a safer crypto environment. The source of data for this analysis was primarily [De.FI Rekt database](#). Some parameters from this source were adjusted and updated to align with our research objectives. Furthermore, additional data concerning team responses to these incidents, bug bounties, and details of existing audits—including the relevance of each audit and bug bounty—were collected through a collaborative effort involving [Trust Army](#) and the Hacken research team.

# YEAR IN REVIEW



## Executive Summary

In 2023 Incidents ranged from abundant rug pulls to half-year-long breaches in centralized businesses. **Attack sophistication increased in both technical execution and variety of impact.**

While concerning, these incidents were smaller in scale compared to the catastrophic losses faced by crypto companies in 2022. But if we take a closer look at the number and type of incidents, the dynamics of 2023 are concerning.

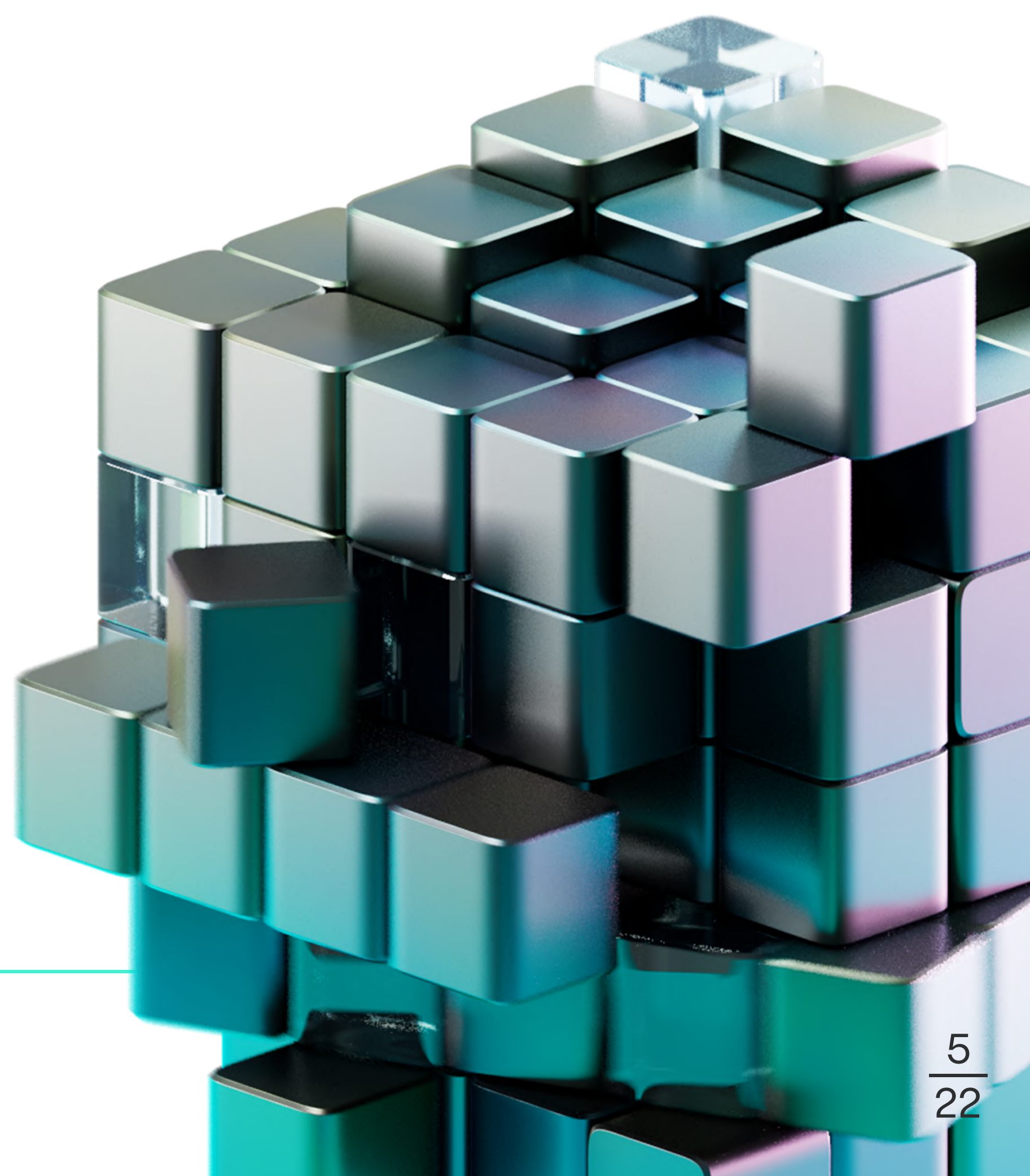
## More Sophisticated Attacks in 2023

2023 was marked by an onslaught of diverse attacks impacting almost every part of crypto infrastructure. These ranged from simple yet abundant rug pulls to elaborate half-year-long breaches in centralized businesses. There were multiple targeted multi-million dollar phishing attacks as well as private seed leakages in various forms.

The sophistication of exploits this year has not just been in their technical execution but also in their sheer variety and impact:

- A notable bug in a programming language that led to \$70 million in initial losses.
- A high-profile wallet breach, various Web2 attacks were successfully deployed to extract Web3 assets.
- A malicious library swap that made all apps using Ledger wallet connections briefly unsafe.

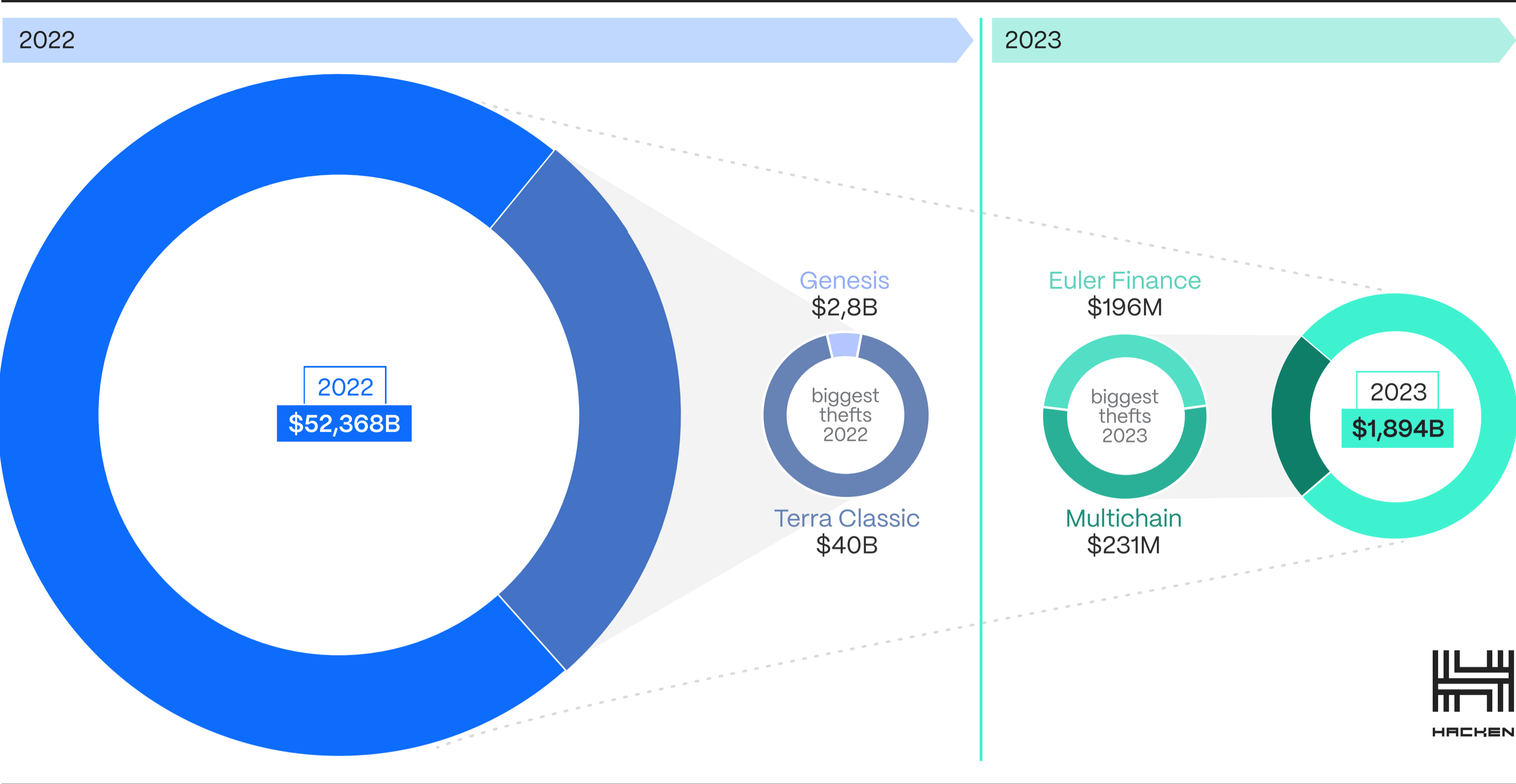
If a former employee with access to company's accounts can halt the whole DeFi sector just by uploading a piece of malicious code, there is still a lot of work to be done.



 Top 10 Crypto Hacks of 2023

PROJECT NAME	PROJECT TYPE	EXPLOIT	DATE	FUNDS STOLEN
Multichain	Bridge	Access Control	July 2023	\$231,129,033
Euler Finance	Lending and Borrowing	Flash Loan Attack	Mar 2023	\$196,000,000
Mixin Network	Infrastructure, CeFi	Access Control	Sep 2023	\$142,041,764
Poloniex	CEX	Access Control	Nov 2023	\$122,981,391
BonqDAO	Lending and Borrowing	Oracle Issue	Feb 2023	\$120,000,000
Atomic Wallet	Wallet	Access Control	June 2023	\$115,000,000
Heco Bridge	Bridge	Access Control	Nov 2023	\$86,284,430
Vyper Compiler	EVM Compiler	Reentrancy	July 2023	\$70,000,000
CoinEx	CEX	Access Control	Sep 2023	\$52,847,077
KyberSwap	DEX	Flash Loan Attack	Nov 2023	\$45,275,428

 Total Value Lost



With \$1.9 billion stolen in hacks and scams, the total value lost went down this year.

The biggest theft of 2023 involved Multichain, with \$231 million drained from the bridge. This pales in comparison to the 2022 Terra Luna fall, which burned over \$40 billion in value, triggering a cascade of collapses across the industry, including the overleveraged Genesis and Voyager with \$2.8 billion and \$1.2 billion in losses, respectively, and notable frauds like FTX and Celsius.

For direct comparison, 2022's Ronin Bridge breach, at \$625 million, is three times higher than this year's largest incident. In fact, if we look at all cases of funds lost due to hacks, scams, errors in code and logic in last two years, Multichain would not be in the top 10 of largest incidents of last two years.

Given the stark difference in evaluation of crypto assets, it's only natural that this year's figures are significantly lower. Last year, the entire crypto market lost two-thirds of market capitalization, and a large share was due to hacks, exploits, and scams. Moreover, **2023 was the first year exploited protocols recovered 20%, or \$400 million, of the stolen assets**, all thanks to rapid team response, hackers' goodwill, and heightened law enforcement.

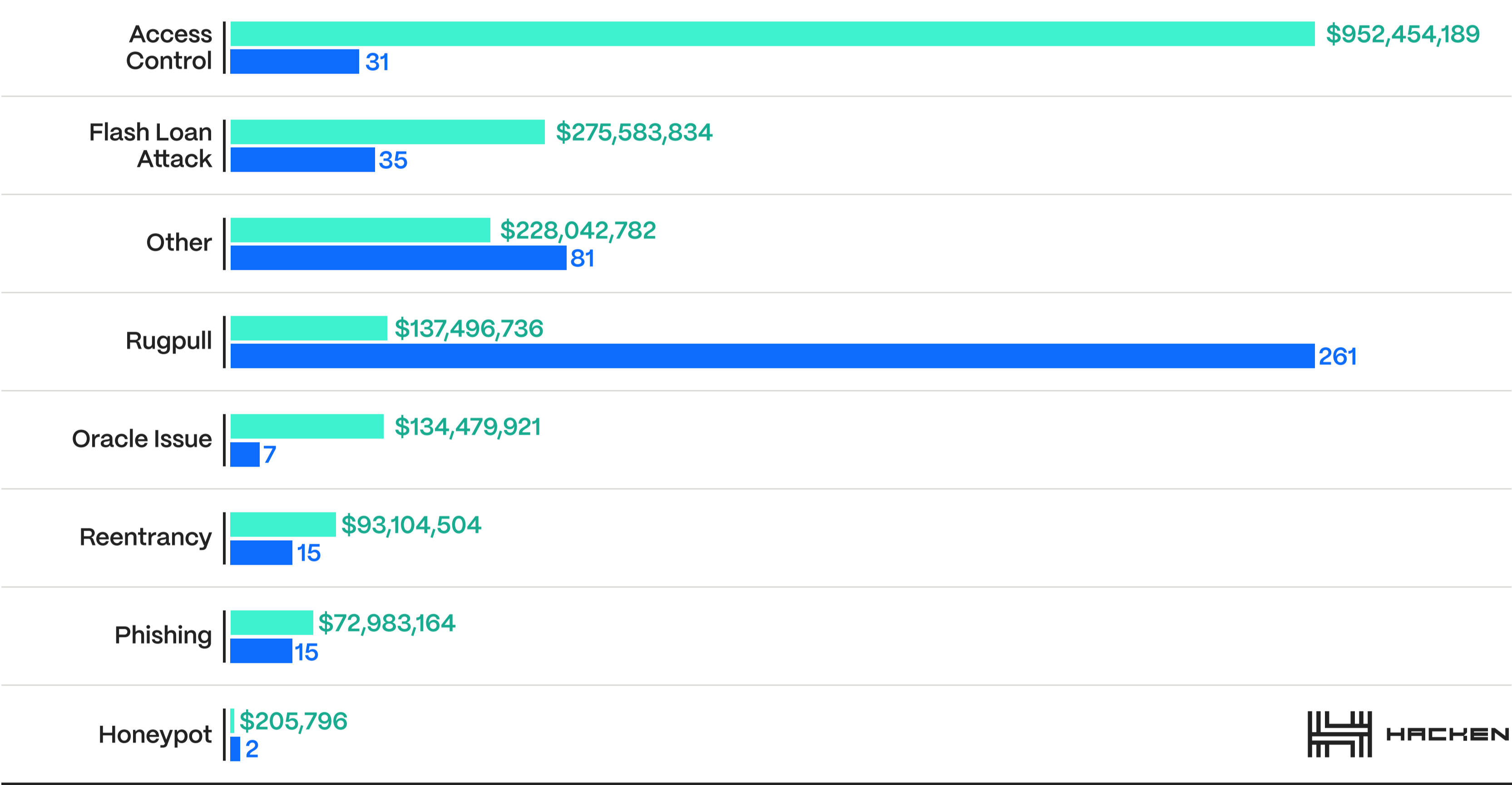
Cases of Value Loss



In this context, 2023, with its \$1.9 billion in losses, appears like a beacon of safety and best security practices. However, we recorded a **14% increase in the number of attacks** over the previous year, along with a significant surge in hack types. This calls for a closer examination of 2023’s exploits.

2023 Hacks Breakdown

Number of Incidents      Total Amount Stolen



## ■ Access Control Breach

By far, **the most damaging type of vulnerability this year** was Access Control. Unauthorized access to hot wallets by hackers or insiders accounted for half of all stolen funds, averaging \$31 million per incident. Besides Multichain's breach, three other significant but obscure hacks occurred, each netting north of \$100 million for the attackers. The specifics of these incidents remain unknown. This includes a security breach in Atomic Wallet.

Analysts [suggest](#) that a North Korean hacking group might be involved, deduced from the pattern of fund transfers between wallets. However, we believe that more evidence is needed to identify this hack as a state-sponsored wrongdoing, as these on-chain patterns of money laundering could be replicated by other hackers. Similar claims surround the Poloniex hack, where \$123 million in various cryptocurrencies vanished from the company's accounts. The Lazarus group is again [suspected](#), but notably, this attack did not impact customer funds.

## ■ Flash Loan Attacks

Flash Loan attacks have found ways to **manipulate pools of assets in their favor for \$275 million**. Among the victims of such attacks was Euler Finance, which was drained of \$196 million of liquidity, as well as the old-school protocols like Balancer, Yearn Finance, and KyberSwap. The latter case was also noteworthy since, after the attack, the hacker started to demand changes in the protocol's management.

## ■ Rug Pull

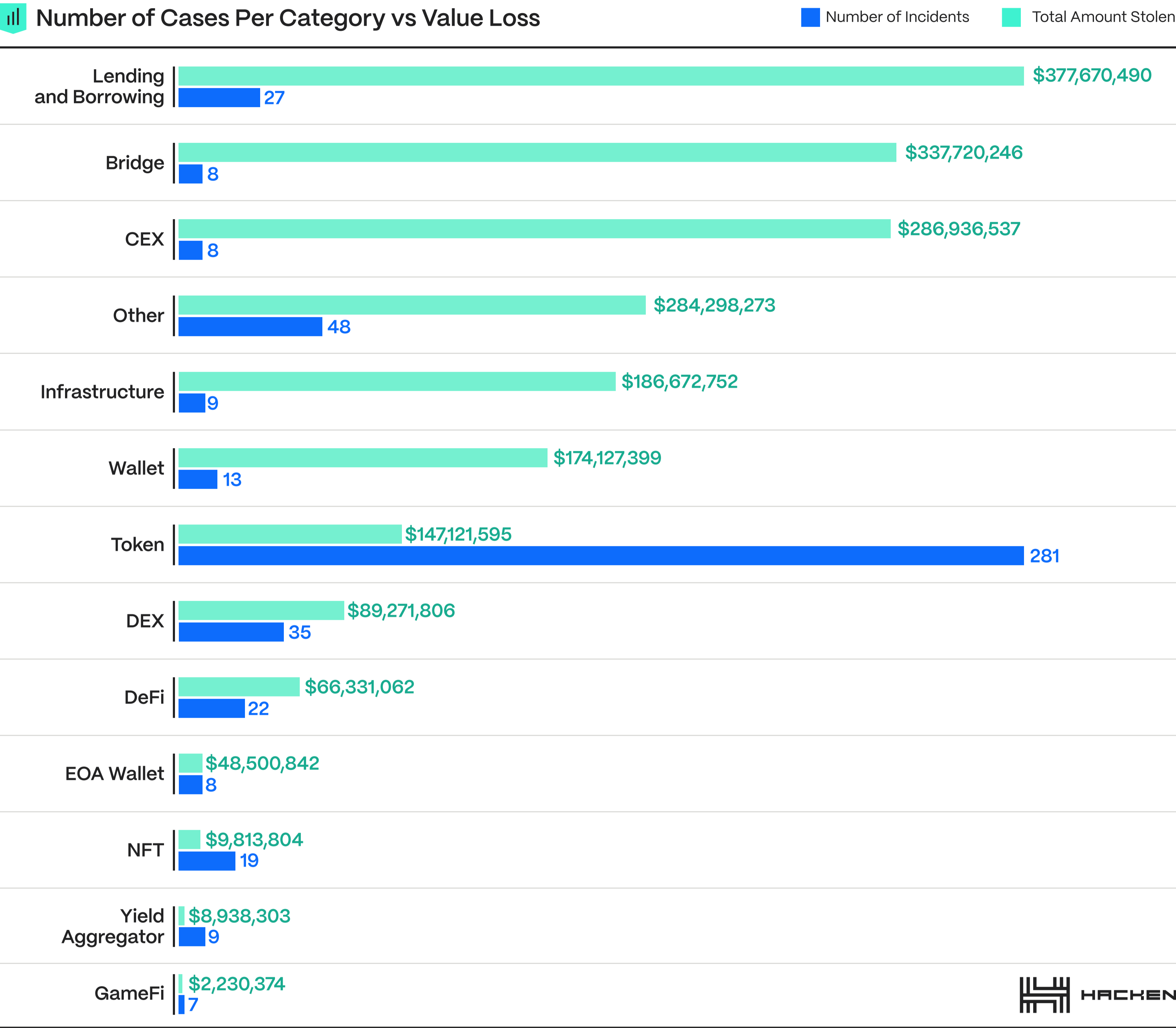
An important outlier this year was a class of scams called rug pulls. We've already explored how it works in our previous [report](#), but what's noteworthy is that **the number of such attacks was higher than all other registered exploits combined**. And though there were several large-scale cases of multi-million dollar fraud, most were in six figures. An attack of this kind netted \$566k on average, making it the second least damaging type after the closely related Honeypot scams.

## ■ Other Exploits

Interestingly enough, uncategorized incidents **have netted a hefty \$195 million this year**. This category once again includes cases of notorious North Korean group activity. According to CoinsPaid's [post mortem](#), hackers spent six months before finally getting into their systems.

In a rare case of the SEC actually defending people, a charge against scammers from CoinDeal was moved forward. According to the agency, the company was a facade for extracting \$45 million from investors and spending it on a lavish lifestyle with real estate and a boat. Since federal agents have seized the assets the scammers bought, there is a possibility that a large portion of this sum will be returned.

# Assessing the Impact



## ■ Lending and Borrowing

This year presented a shift from the previous trend where centralized companies collapsed like dominos under the weight of bad debt. The most affected sector was Lending and Borrowing, primarily smart contract-based money markets.

These platforms amass substantial liquidity pools, lending to users against collateral. However, they became prime targets for hackers exploiting flash loans – a Web3 mechanism offering vast capital to be repaid in the same transaction. But why would anyone borrow money just to return it a few seconds later?

There are many legitimate reasons for flash loans – paying the debt with a higher interest rate on one platform and opening a collateralized debt position with smaller interest on the other, etc. But for attackers, it's a tactic to overflow liquidity pools, exploit pricing flaws, or corrupt oracles that provide crucial data, leading to disproportionate asset withdrawals.

A case in point is BonqDAO, where an attacker manipulated a token's price, minted a lot of stablecoins that used the first coin as collateral, and then dumped them into the market. Technically, this eroded \$120 million in value, yet the hacker cashed out only [\\$1.2 million](#) due to the limited liquidity of the printed stablecoin. The remainder was blocked, with affected parties compensated through newly minted tokens.

## ■ Bridges and CEXs

Bridges and CEXs are next in terms of stolen value. Because they benefit from large liquidity pools, these projects often attract hackers and insider threats. Despite fewer incidents, these platforms report substantial average losses of \$42 million and \$35 million, respectively.












## ■ Novel Cases

This year saw the first major vulnerability in the Vyper smart contract programming language, impacting multiple protocols simultaneously with initial losses of around \$70 million. Quick response and collaboration led to the recovery of most funds.

Another outlier traced back to the LastPass breach, where numerous seed phrases were exposed. Security experts [noted](#) that many of these belonged to seasoned crypto users, underscoring the widespread and varied nature of this year's security challenges.

# Affected Networks

## Top 10 Most Affected Chains

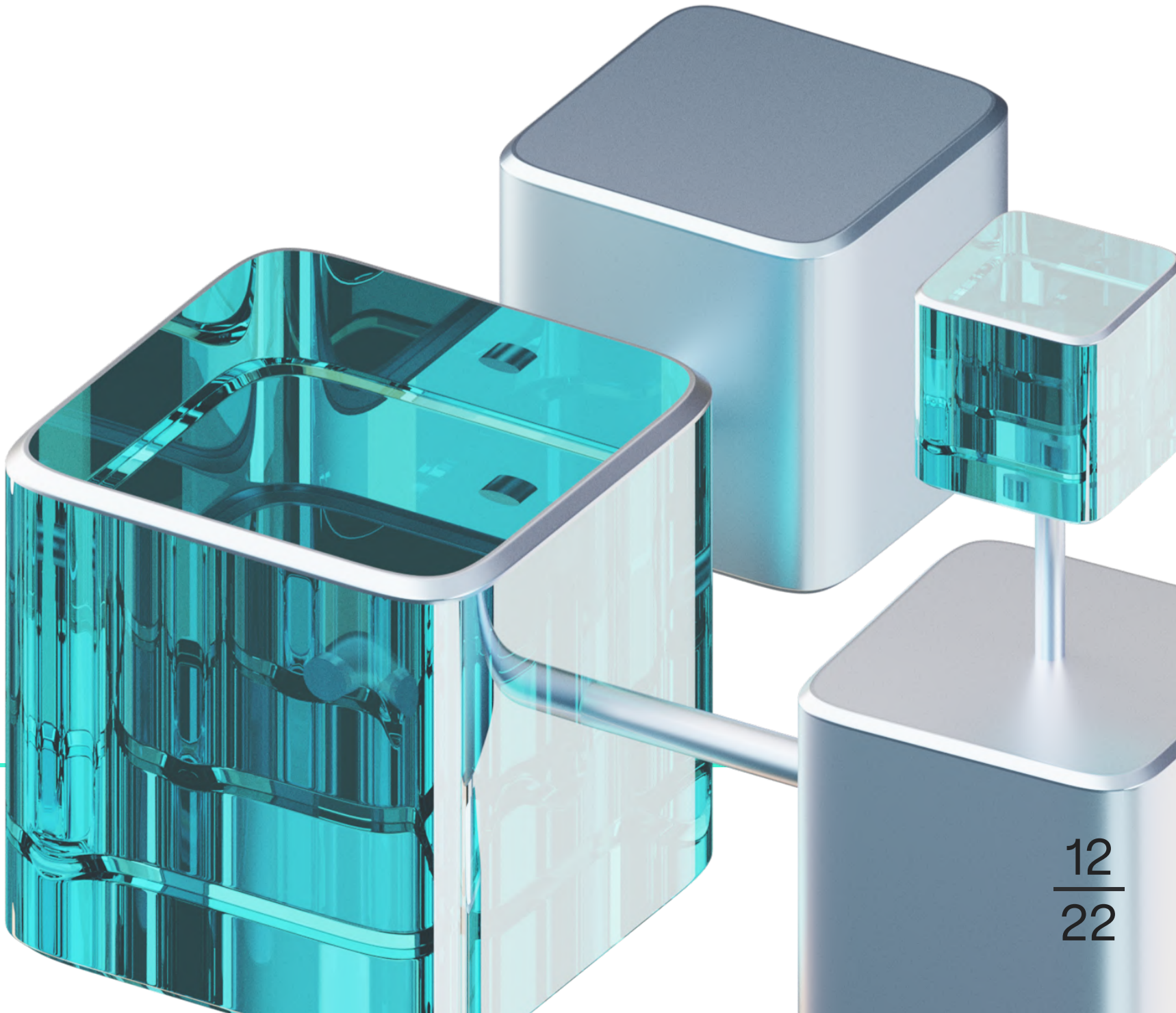
NETWORK	HACKS	CHAINS BY INCIDENT CATEGORY								
		Rug pull	Access Control	Reentrancy	Oracle Issue	Phishing	Flash Loan Attack	Honeypot	Other	
 BNB CHAIN	214	149	12	2	.	.	18	2	31	
 ETH	178	97	19	8	2	13	11	.	28	
 ARBITRUM	30	7	4	2	3	3	2	.	9	
 POLYGON	15	2	3	1	1	.	4	.	4	
 AVALANCHE	10	.	3	2	.	.	2	.	3	
 OPTIMISM	9	1	1	2	2	.	2	.	1	
 BASE	8	4	1	.	.	.	2	.	1	
 BTC	5	.	4	.	.	1	.	.	.	
 TRON	4	.	4	.	.	.	.	.	.	
 ZKSYNC	3	1	1	1	.	.	.	.	.	

A review of blockchain networks most impacted by exploits reveals BNB Smart Chain (BSC) and Ethereum as the predominant targets, each for distinct reasons.














**BNB Chain** recorded 214 incidents, mainly rug pulls, attributed to its large user base, low fees, and ease of capital movement, making it an attractive target for large-scale, cost-effective malicious activities.

**Ethereum** experienced 176 incidents, ranging from classic rug pulls to sophisticated flash loan attacks, reflecting its status as a pioneering yet embattled blockchain platform. Its role as an innovation leader also introduced unique exploits, including unnoticed code errors. An example is the 2023 Yearn Finance attack, exploiting a dormant smart contract vulnerability from 2020 that referenced the wrong address, leading to an \$11 million loss.

Smaller platforms had their share of incidents, too. For example, Arbitrum faced 30 incidents, often related to access control, highlighting vulnerabilities in newer networks.



 Geography of Exploits

										
COUNTRY	AMOUNT OF HACKS	FUNDS STOLEN	Rug pull	Access Control	Reentrancy	Oracle Issue	Phishing	Flash Loan Attack	Honeypot	Other
 USA	25	\$249,581,056	.					.		
 Singapore	13	\$302,637,581	.		.	.	.	.		
 UK	5	\$201,062,733	.		.	.	.	.		
 China	4	\$19,226,612	.		.	.	.	.	.	.
 Estonia	4	\$154,330,228								
 Hong Kong	4	\$195,935,183	.		.	.	.	.	.	
 Australia	4	\$12,452,727	.	.		.		.		
 Portugal	3	\$2,296,586	.	.	.	.	.	.		
 Cayman Islands	3	\$33,762,582	.		.	.	.	.	.	
 Switzerland	2	\$2,283,829	.	.	.	.	.	.	.	
 Russia	2	\$3,076,112	.	.		.	.	.	.	.
 Seychelles	2	\$29,767,463	.		.	.	.	.	.	.
 Cyprus	1	\$6,227,977	.	.	.	.	.	.	.	
 Chile	1	\$115,595	.		.	.	.	.	.	.
 Mexico	1	\$29,195	.	.	.	.	.	.	.	.
 Sweden	1	\$235,462	.	.	.	.	.	.	.	
 Panama	1	\$459,094	.	.		.	.	.	.	.
 Italy	1	\$3,254,850	.	.		.	.	.	.	.
 St. Vincent and the Grenadines	1	\$22,851,804	.		.	.	.	.	.	.
 Austria	1	\$900,000	.	.	.	.	.	.	.	.
 Uruguay	1	\$7,197,240	.		.	.	.	.	.	.
 Curaçao, Netherlands	1	\$41,408,903	.		.	.	.	.	.	.
 Germany	1	\$264,000	.	.	.	.	.	.	.	
 France	1	\$452,114	.	.	.	.	.	.	.	.

Our investigation into the places of incorporation of the hacked companies, while limited by data availability, successfully covered two-thirds of the stolen funds.

**Singapore and the USA** emerged as significant hotspots for cyber exploits, possibly due to the highest fintech activity there. Singapore experienced 13 incidents, totaling \$302 million in losses. The USA had 25 cases with \$249 million in losses.

**Estonia and Hong Kong**, despite fewer incidents, saw significant financial consequences from cyber exploits. Each reported four attacks, averaging \$39 million and \$49 million per hack, respectively. The global spread of incidents, from the UK to the Cayman Islands, reflects the borderless nature of blockchain vulnerabilities.

# Looking Ahead

## Predictions for 2024

### Layer 2s

With the rise of Layer 2s, we will likely see a lot of experimentation and risk-seeking liquidity shifting from **Ethereum to these new solutions and blockchains**. Companies tend to audit base smart contracts only on the mainnet but neglect similar audits on new networks. We must reverse this typical pattern, otherwise new blockchains would create more vulnerabilities for hackers.

The expected increase in new protocols and liquidity during the upcoming bull run could result in more incidents than in 2023, not as a regression but as a natural outcome of growth and experimentation. The focus should be on learning from past mistakes and utilizing established security tools.

### Access Control and Flash Loans

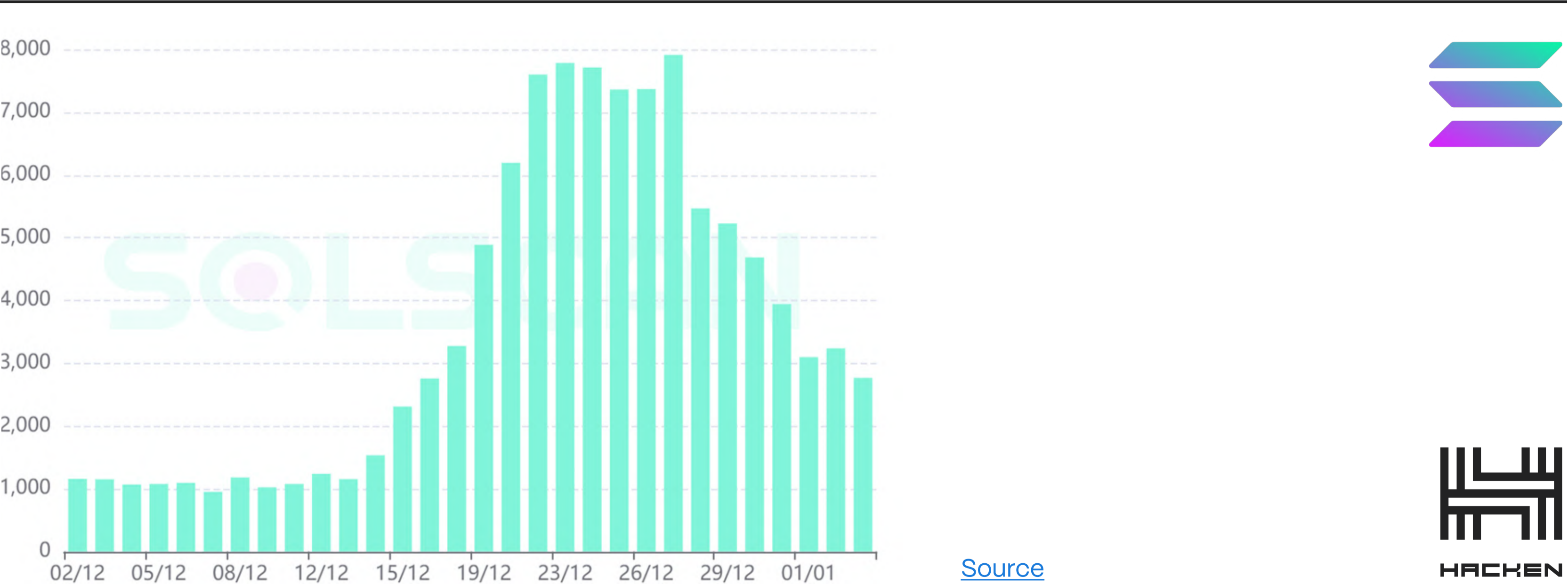
Access control breaches and flash loan attacks, significant in 2023, will probably **remain major security concerns**. Increased investment in securing these areas, possibly through more stringent auditing, multi-signature wallets, adherence to the CCSS standard for private key management, and advanced proof-of-reserves.

### Rug pulls

Rug pulls, frequent but less financially impactful per incident, are becoming a standard risk. Addressing them will require improved due diligence and community education to help retail investors recognize and avoid scam projects.

Particularly concerning is the expected surge of rug pulls on networks like Solana. **An indicator of this trend is the creation of approximately 100,000 new tokens on Solana in just December**, hinting at potential vulnerabilities and risks associated with such rapid expansion.

 Number of newly created tokens in December 2023 on Solana



## ■ Token Factories

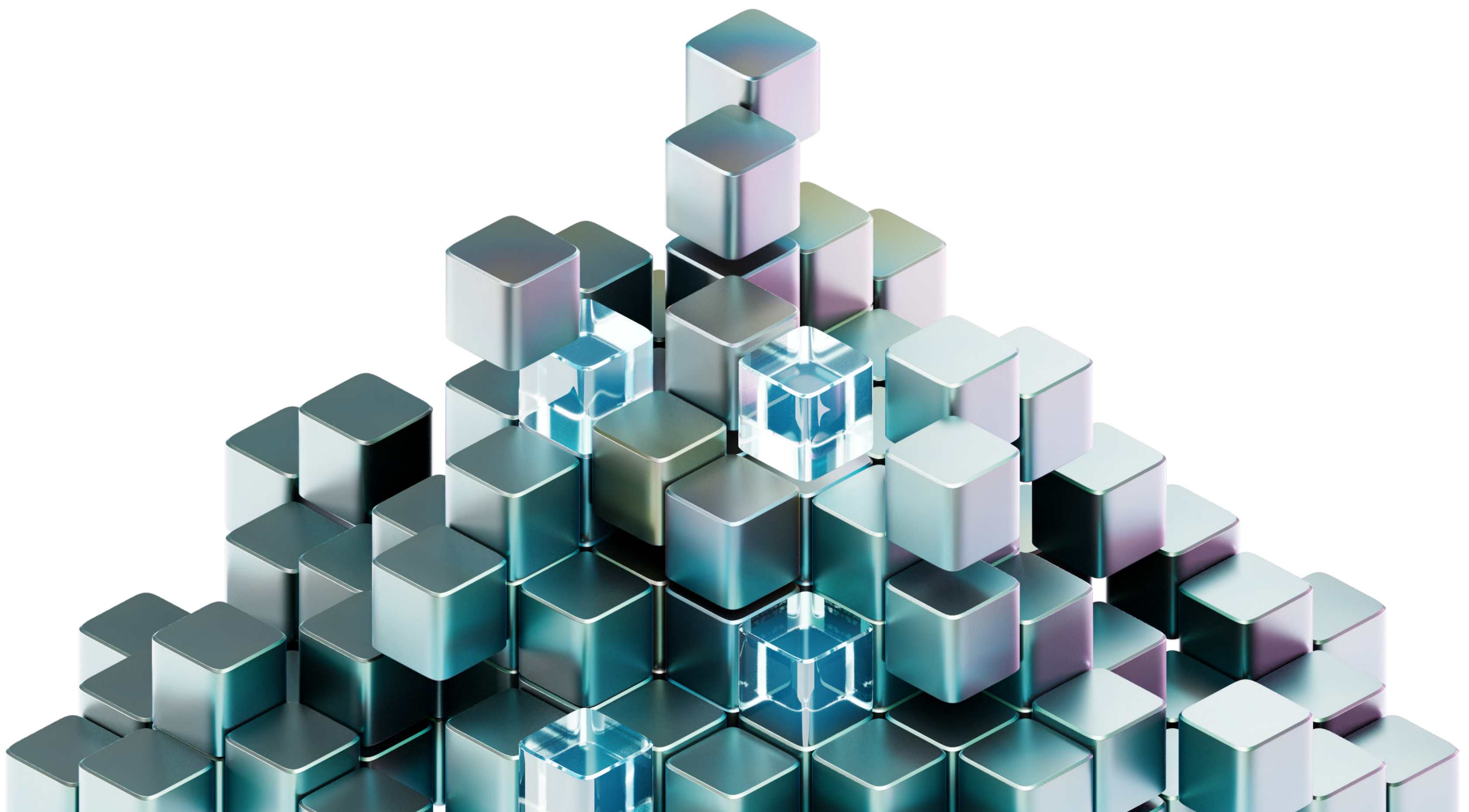
The trend of creating new tokens, notably spurred by **the success of \$BONK and other meme coins**, has expectedly been hijacked by rampant pump-and-dump schemes. Some creators are deploying over [300 tokens daily](#), capitalizing on initial value spikes before moving on to the next token.

## ■ Front-End Attacks

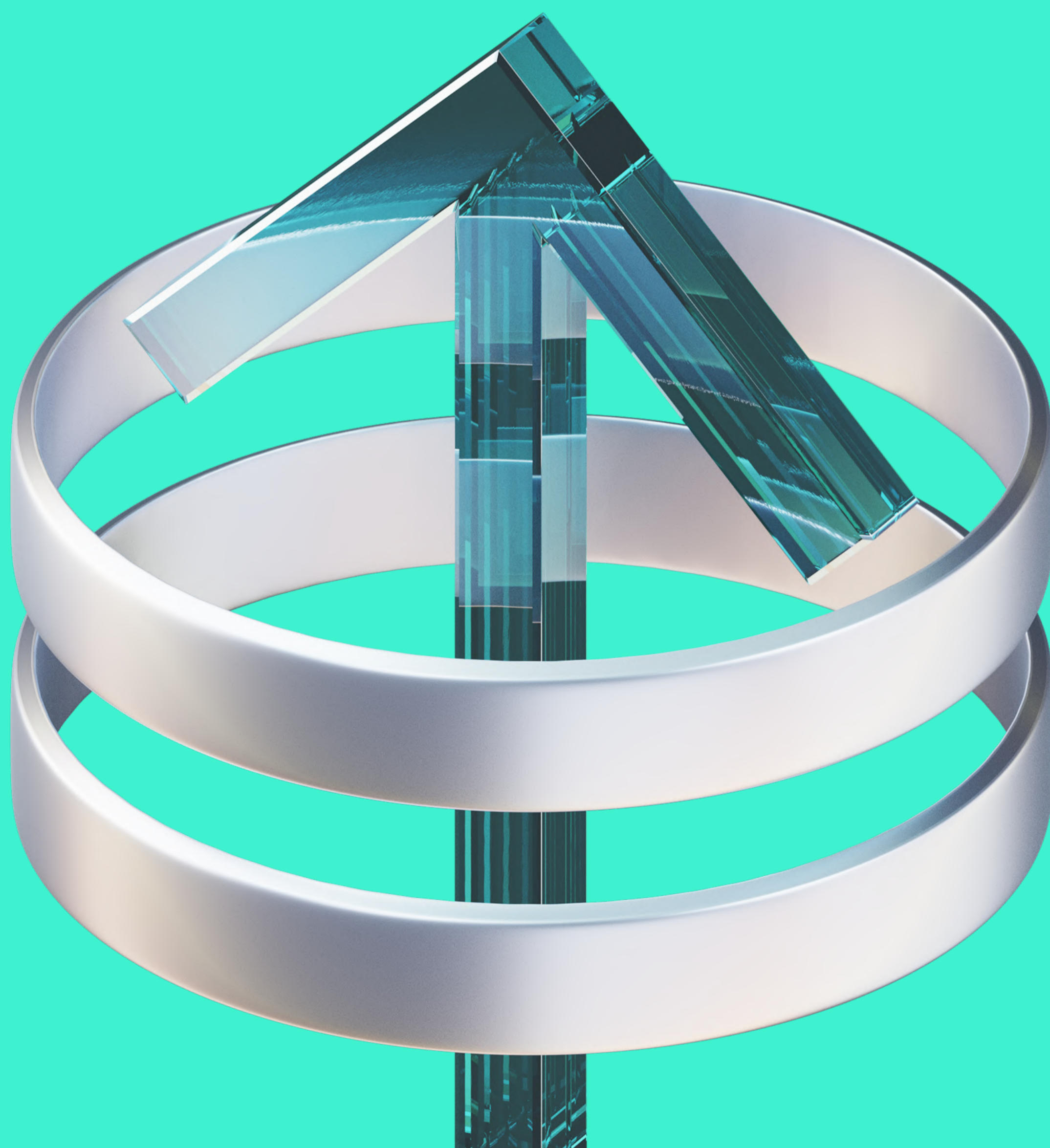
In 2024, we anticipate a rise in front-end attacks, which don't require deep Web3 knowledge. Such attacks involve **injecting malicious code or redirecting tokens to attackers' wallets through compromised websites or dApps**. Notable incidents like the Balancer and Velodrome hacks highlight this vulnerability, where losses occurred due to front-end compromises.

## ■ Attack Diversity

The variety and complexity of exploit types we've seen this year is also something developers should keep in mind. We expect attackers to employ a wider range of methods, from sophisticated smart contract exploits to social engineering. Security measures must be equally diverse and robust.

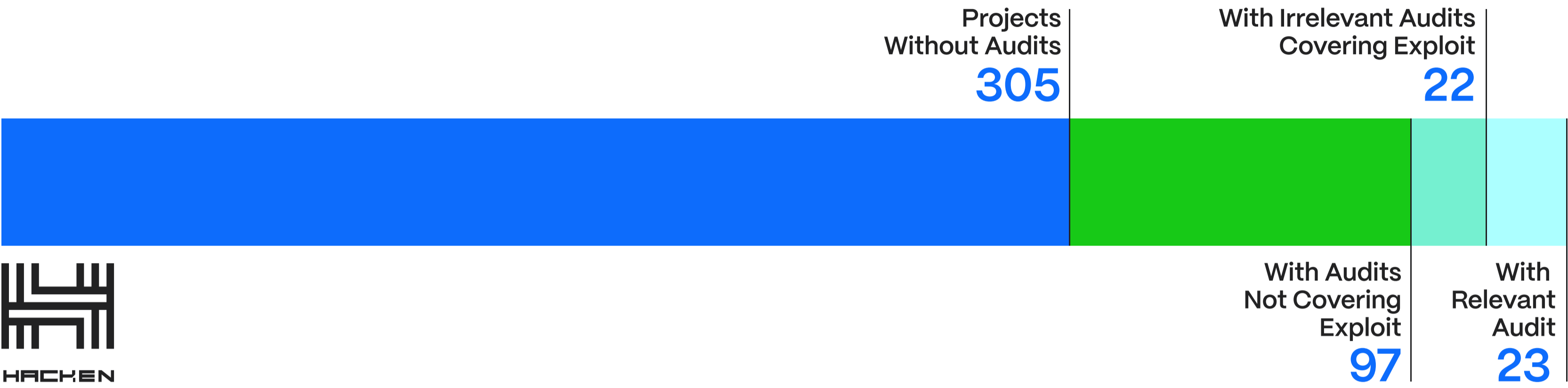


# RESPONSE AND SOLUTIONS



It might look like the crypto industry has no means of protecting its assets – but this can’t be further from the truth. **The crypto industry is actively enhancing user and investor protection**, evidenced by the continual improvement and availability of sophisticated security solutions.

 Audit Coverage



In 2023, **only 10% of exploited contracts underwent any form of audit, and merely half of these were relevant**, matching the deployed blockchain code. Hence, the data suggests that independent third-party assessments of the code and architecture significantly lower the chances of exploits in audited code.

Along with it, in a range of cases, scope of audit included the effected smart contract, though the audited and deployed code differ. Which means that the code was changed after an audit, which makes all the security measures pointless. In the graph above these cases are counted as the ones with irrelevant audits covering exploits.

This year's data also highlights instances where companies faced breaches shortly after deploying new smart contracts, only to seek audits post-incident. Conducting a pre-deploy third-party check is a must for firms handling large crypto asset pools.

The reactive approach to security in the crypto industry, instead of a proactive one, is exemplified by two cases in early 2023. Revert Finance experienced a breach of its exploited contract in February, leading to a [security audit](#) of the same contract in March. Similarly, FEG Token also underwent an [audit](#) only a few weeks after its security incident.

Despite auditors' efforts, reentrancy attacks – exploiting vulnerabilities to withdraw assets repeatedly – breached 26% (4 out of 23 in total) of smart contracts with relevant audits. **This emphasizes the need for auditors to intensify efforts in detecting such errors.** Other vulnerabilities, like oracle issues and flash loan attacks, despite relevant audits, had breach rates of 14% and 11%, respectively. The difference in breach rates might be attributed to the greater sophistication and knowledge required for conducting oracle manipulation and flash loan attacks compared to reentrancy attacks.

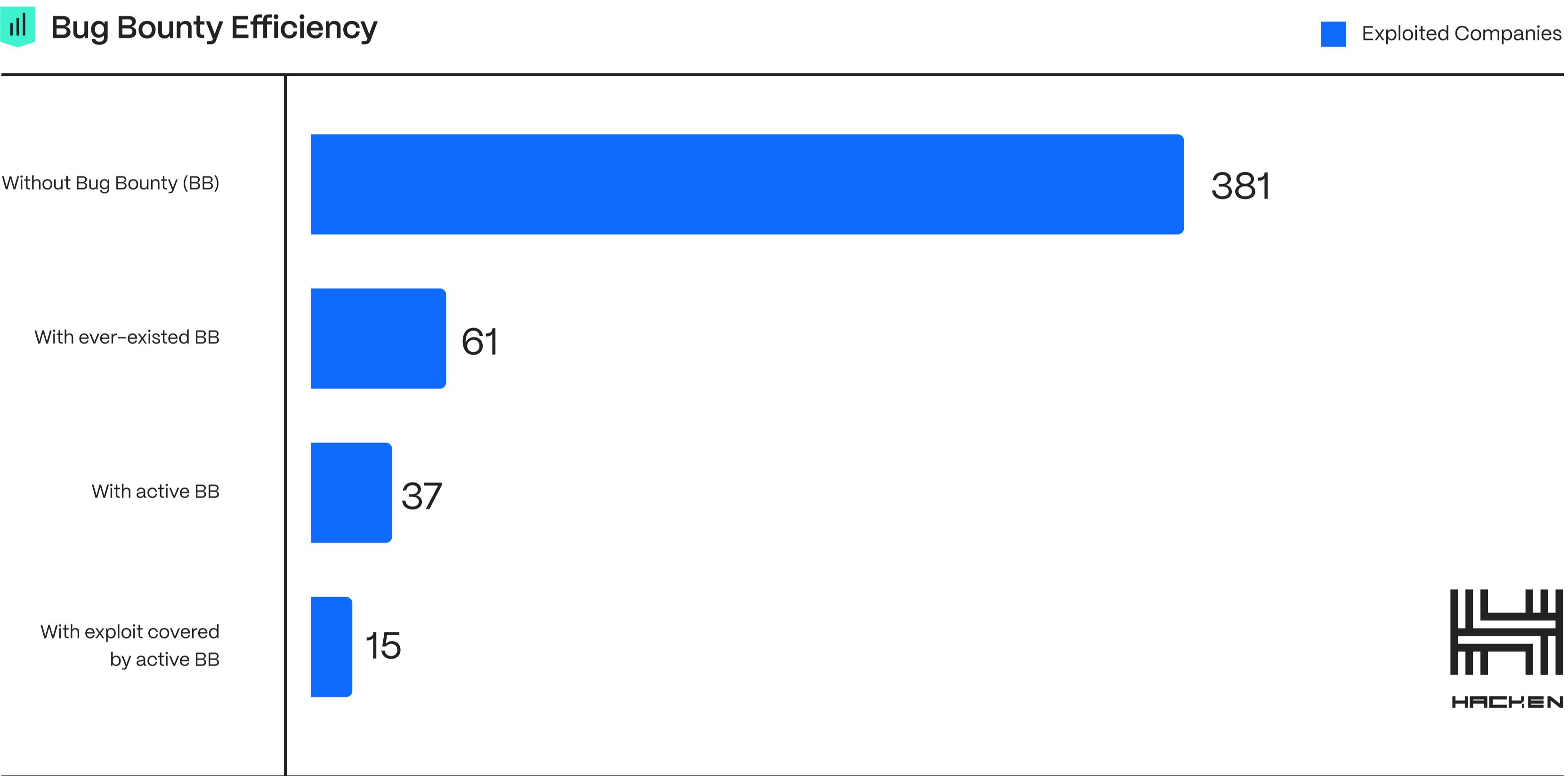
■ Rug pulls and Audits

Notably, **only 6% of rug pull projects had any form of audit**, underlining the importance of audit verification as a crucial part of due diligence for crypto investors. However, caution is advised against relying on low-quality assessments or partial audits.

■ Final Thoughts

These observations stress **the critical need for rigorous, comprehensive audits**. Moreover, implementing on-chain insurance and having skin in the game can increase the efficiency of auditing space, and it would be interesting to see the evolution of this tool.

# Bug Bounties



Only **15% of hacked companies had any bug bounty program**. Among these, just 7% had an ongoing bug bounty program covering the exploited smart contracts when the hack occurred.

Many hacked protocols learned the hard way that not having a bounty can cost them 10% liquidity, which is commonly a price hackers ask for returning stolen funds. This highlights the critical need for comprehensive and well-scoped bug bounty programs, especially for projects with large capital pools.

## ■ Self-Hosted vs Third-Party

The average minimum payout in third-party programs is 3x higher than self-hosted, with the maximum reward about 40% higher. Reward size was [found](#) to be a key factor for hackers when choosing bug bounties to pursue.

The increasing complexity of attacks and the effective report rate (the percentage of reports that point to a valid bug), such as [HackenProof's](#) 35%, point to a growing number and proficiency of white hat hackers in the industry. However, self-hosted programs have shown a lower efficacy in catching critical bugs, mostly due to lower exposure and smaller talent pools.

## ■ Final Thoughts

Utilizing a third-party platform for hosting bug bounty programs enhances the likelihood of identifying vulnerabilities, thereby reducing the risk of incurring unofficial 10% return fees typically demanded by hackers for recovered assets.

## Real-Time Monitoring

Real-time threat identification tools like [Forta](#) and [Extractor](#) monitor smart contracts and their interactions for potential threats, ensuring immediate response to any irregularities or breaches. All-day surveillance is essential for detecting most issues.

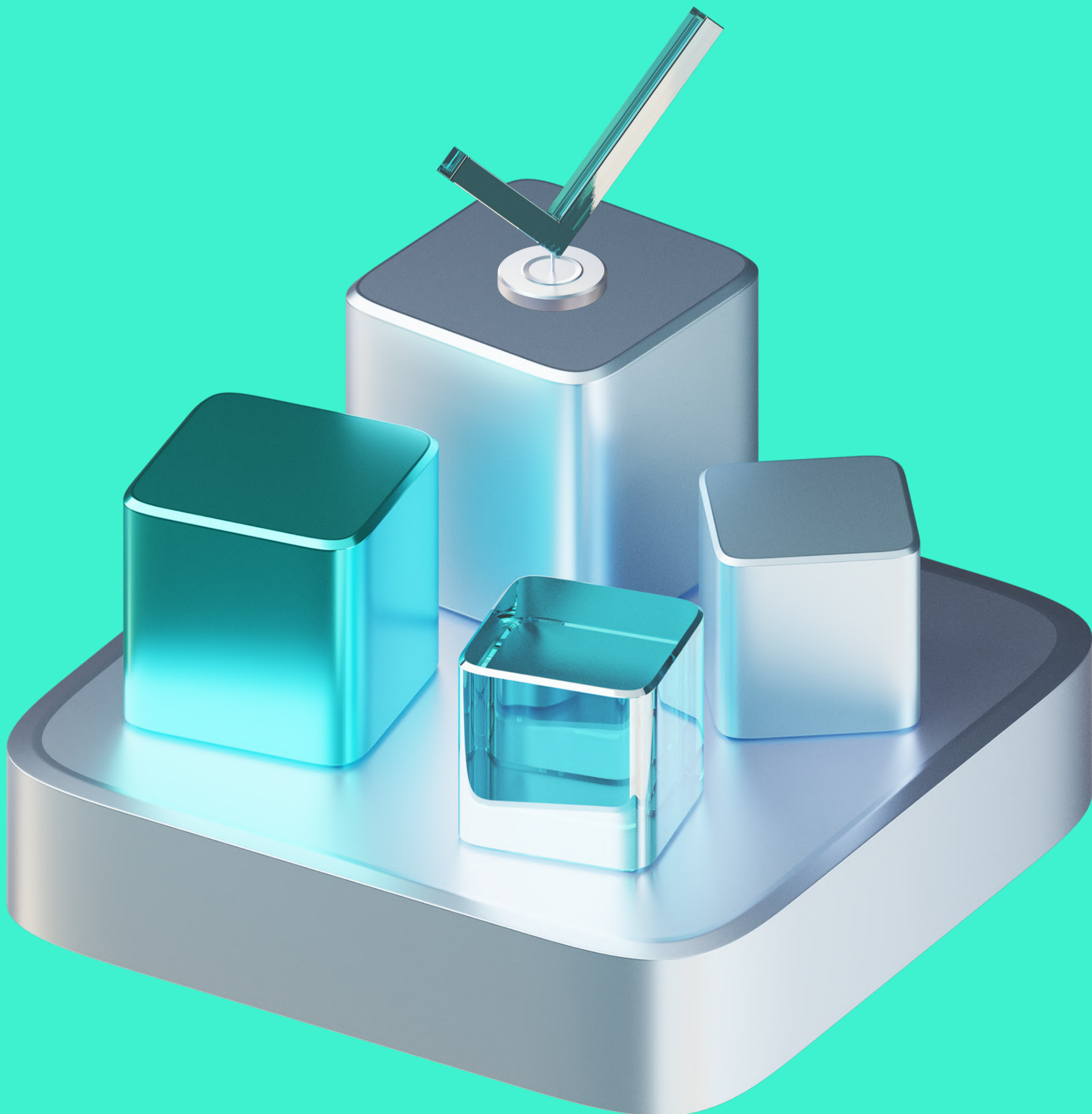
## Secure Hot Wallets

On the user side, the security efforts of [Metamask](#), [Rabby](#), and a few other [wallets](#) deserve attention. Security-first wallets offer warnings against potential threats and simulate transactions to help users understand the implications of their actions before real execution. Not all features are practical for an average user yet, but developing such capabilities is vital.

## Browser Extensions

Security options for retail investors are expanding. [Wallet Guard](#), for example, scans websites for malicious elements like drainers, adding a layer of checks against front-end attacks. Another example is [Web3 Antivirus](#), a web extension protecting from phishing attacks, malicious smart contracts, and other threats.

# CONCLUSIONS AND RECOMMENDATIONS



2023 was marked by significant access control breaches, emphasizing the need for heightened wallet security and internal system controls. The diversity of attacks witnessed signals an alert for unconventional threats, necessitating a comprehensive security approach that combines technical strategies and human awareness.

A notable improvement in 2023 was the enhanced breach response mechanisms, leading to substantial asset recovery. This highlights the effectiveness of rapid response and collaboration but also stresses the ongoing vulnerabilities in human trust and due diligence, evidenced by persistent rug pulls and scams. These incidents underline the importance of community awareness and education.

## Looking Ahead to 2024

As we look towards 2024, the horizon is mixed with optimism and caution. We are seeing the explosion of new Layer 1 and Layer 2 solutions, modular blockchains, and interchain messaging and other seemingly promising technologies. The crypto landscape continues to evolve, and it demands adaptive and robust security measures.

The dynamic nature of cryptocurrency security in 2023 sets a foundation for the industry to evolve and adapt. Embracing these insights and best practices is essential for fostering a more secure and resilient blockchain ecosystem as we enter 2024.

2024 Security Trends	Recommendations
<ul style="list-style-type: none"><li>• Access control breaches and flash loan attacks to remain key concerns.</li><li>• Rug pulls to continue as a standard risk, with a surge on networks like Solana.</li><li>• Growth in token factories leading to rampant pump-and-dump schemes.</li><li>• A potential rise in vulnerabilities due to neglecting audits on new networks as risk-seeking liquidity and experimentation attention shifts from Ethereum to Layer 2 solutions.</li><li>• Rise in front-end attacks targeting web interfaces and dApps.</li><li>• Broadening range of attack methods, from smart contract exploits to social engineering.</li></ul>	<p><b>To improve security in 2024, businesses should invest in:</b></p> <ul style="list-style-type: none"><li>• Comprehensive auditing and ongoing monitoring</li><li>• Proactive security culture via bug bounty programs</li><li>• Stringent access controls like multisig wallets</li><li>• Security-rich features for wallets and extensions</li><li>• Collaboration within the industry for collective defense and swift asset recovery</li><li>• Better scam education for communities. Educate users not to sign any message from their wallet if they don't trust it and to always check the website's extension and name before interacting.</li></ul>

As the industry grows, proactive and resilient security measures will be essential to prevent costly incidents in the upcoming bull run.

# We Make Web3 A Safer Place



6

Years of expertise

1,000+

Clients

180+

Partners

1,500+

Audited projects

50+

Crypto exchanges

100+

Team members