

Protecting Web3

2023 Security Insights

Q3

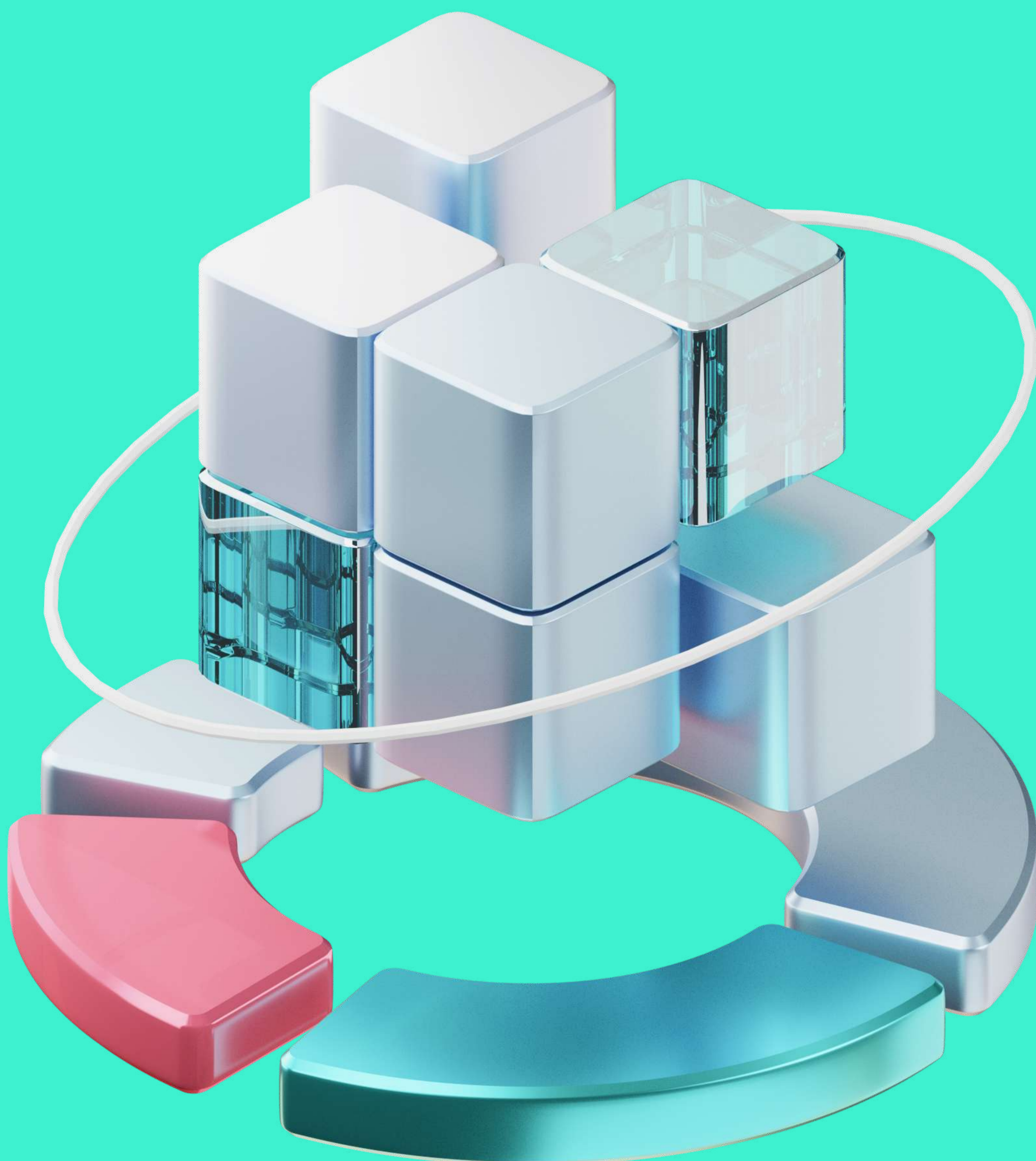


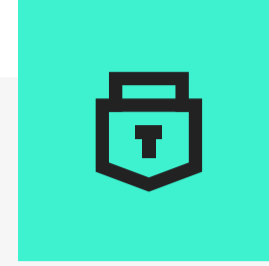
Table of contents

1. Highlights	3
2. Introduction	3
3. General Observations	4
4. Hacks by Types	5
4.1 Access Control Breach	5
4.2 Rug Pull	6
4.3 Reentrancy + Flash Loans	9
5. Hacks by Chains	10
6. Hacks by Project Types	11
7. Hacks of Audited Projects	13
7.1 When Audit Done Right	13
7.2 Reality Check: Audit Report Does Not Guarantee Security	14
8. Conclusions	15

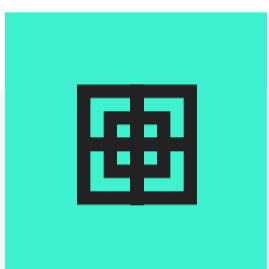
Highlights



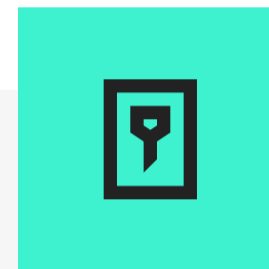
The quarter's 117 hacks totaling \$720 million stolen reveal systemic security shortcomings across the crypto industry.



Access control breaches remain the most financially damaging hack category, with each exploit costing tens of millions on average.



Rug pulls are the most frequent attack vector, preying on hype and greed to siphon liquidity from unassuming investors.



Smart contracts continue to harbor risks even after audits, pointing to the need for recurring multi-auditor due diligence.

Introduction

Hacken reviewed De.Fi's [REKT database](#) to identify the most prevalent crypto hacks and scams of Q3 2023. Additionally, [Trust Army](#), Web3 researchers that are part of the Hacken community, collected public data like audits and team responses. Through this analysis, we aim to provide crypto users with essential insights while also helping to fortify the blockchain ecosystem.

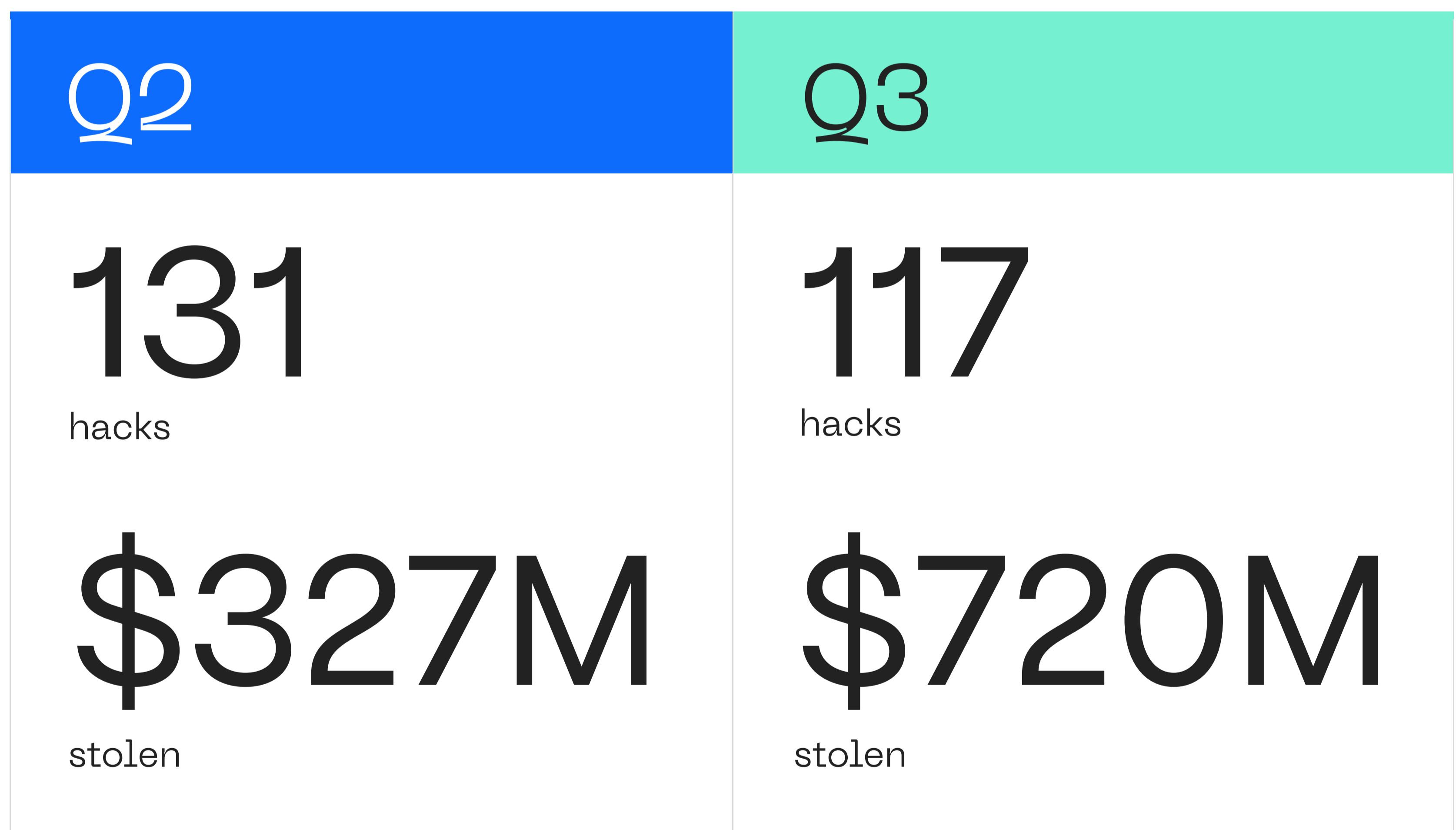


General observations

The biggest hack this quarter was a **\$231M exploit of the Multichain** bridge. This isn't Multichain's first mishap, having previously faced two attacks. Another notable incident involved a bug in the Vyper compiler, leading to \$70 million in losses from large projects including Curve Pools, Alchemix and JPEG'd. Thankfully, quick action and good communication allowed 90% of the funds to be returned.

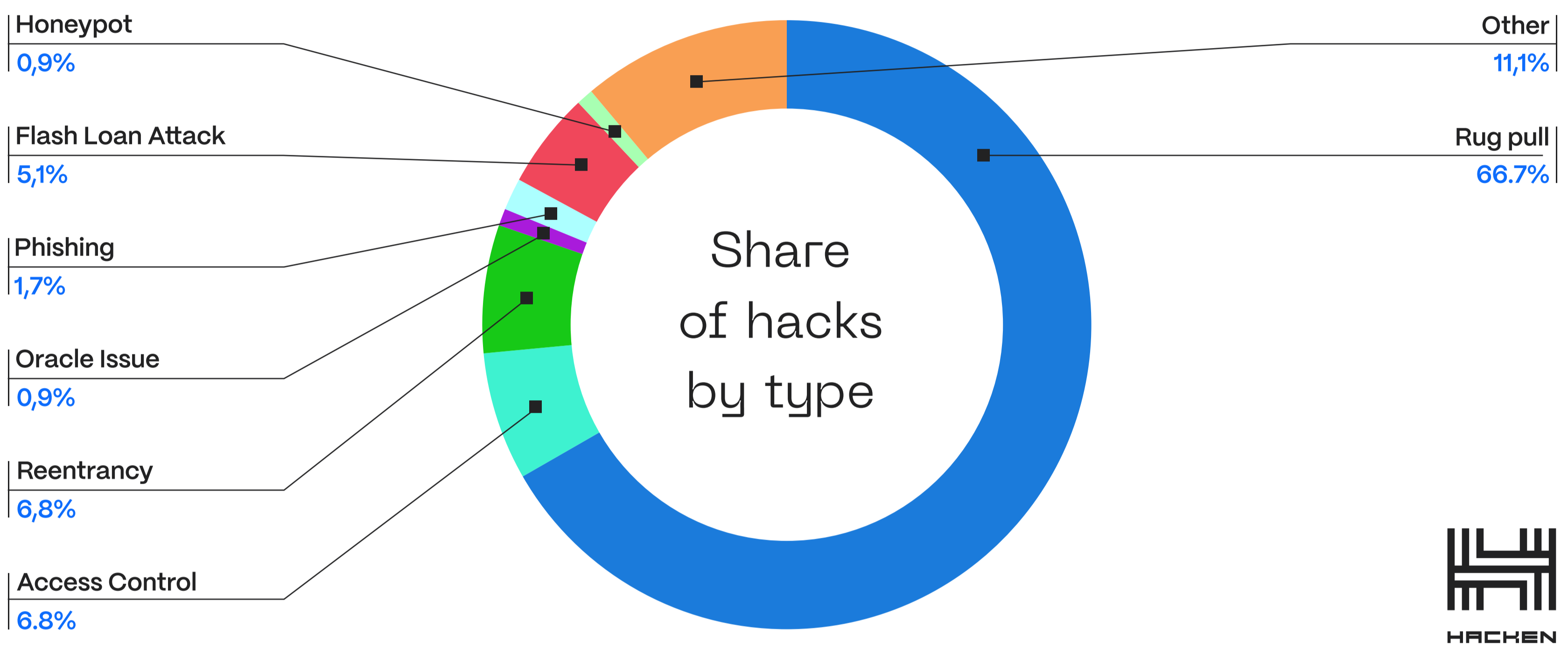
A quick response from the team can be an important make or break scenario. Our Trust Army data reveals that genuine teams typically respond within **24 hours** of a hack, which, with proper communication, can lead to most funds being recovered.

The most damaging exploit type was Access Control, causing **\$449 million in losses** from just 8 incidents. This underlines that beyond code vulnerabilities, the human factor remains the most exposed part of the crypto industry.



Hacks by Types

In Q3, the crypto landscape witnessed a diverse range of security breaches. The lion's share of the losses, with a significant 65%, came from Access Control attacks. Smaller yet noteworthy segments – Rug pull and Reentrancy + Flash Loans made up over 20%. With these forms of attacks dominating the scene, it's imperative to zoom in.



Access Control Breach

- Access control is the most damaging type of exploit with the highest total losses and only a handful of incidents. Gaining control over a seed phrase allows hackers to extract assets from both smart contracts and Externally Owned Addresses (EOAs).
- **EOAs** are particularly at risk since seed phrases are their sole protection. With a private key, attackers can seize assets across chains and various addresses originating from that key. Moreover, many projects store substantial assets in EOAs, incentivizing attackers to create elaborate schemes for massive gains.
- Similar to Multichain, Mixin Network lost **\$142 million** due to an access control attack. The protocol stored their private keys in a cloud database, which was breached in September.
- On average, access control exploits led to \$58 million in losses each, becoming the most profitable attack vector. This vulnerability accounted for **two-thirds of all funds lost** this quarter
- Notably, Q2's largest hack, involving Atomic Wallet, was also an access control breach with \$115 million lost, so the trend stays the same.

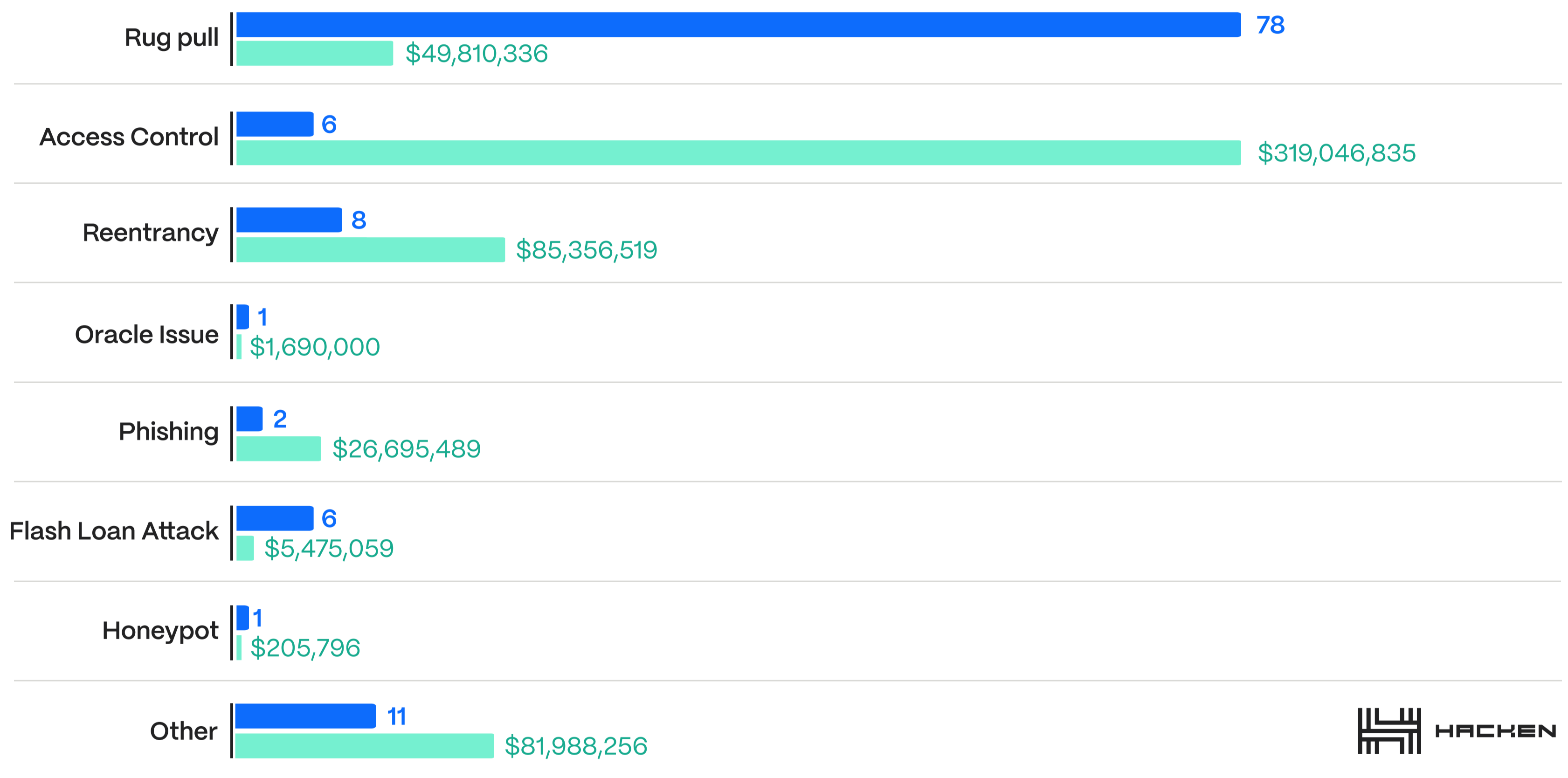
Rug pull

Another glaring trend is the prevalence of rug pulls – a type of exit scam characterized by a sudden withdrawal of liquidity, often accompanied by changes in tokenomics or the project's smart contract.

Understanding the anatomy of this scam is crucial because they make up **most exploits this year**. Despite the relatively low average check cashed by the malicious actors of \$638,594, it's one of the simplest scams to prevent.

Hacks by project category

Number of Incidents ■
Total Amount Stolen (\$M) ■



Rug pull_

Observation #1: Token Factories

The reason for so many rug pulls on the market is the ease with which they are created. Serial scammers use token factories that exhibit the same behavior to produce fraudulent tokens on a mass scale. An example of such a factory can be seen in the following [smart contract](#).

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0x7d87014fbe5fbaaf...	Create Token	17689269	97 days 3 hrs ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.12263948
0x488d9a1cac925be4...	Create Token	17688304	97 days 7 hrs ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.16154729
0x92601e169cf1d04b8...	Create Token	17688230	97 days 7 hrs ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.12326442
0x4f45416c12bf4d80c...	Create Token	17682694	98 days 2 hrs ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.08961986
0x0ff16fb414c1fb2bdd...	Create Token	17681462	98 days 6 hrs ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.0925137
0x2863945e2d6772c4...	Create Token	17681244	98 days 7 hrs ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.09171347
0x553df54800531dd8...	Create Token	17677110	98 days 20 hrs ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.08330409
0xcdef18d293221dfb1...	Create Token	17675774	99 days 1 hr ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.0828424
0xbba78daf78ae10786...	Create Token	17675007	99 days 4 hrs ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.06954994
0xa3e29d7370db09f5f...	Create Token	17667177	100 days 6 hrs ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.08801815
0x0879dc12396b545a...	Create Token	17667132	100 days 6 hrs ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.08741531
0x68f142ef1ce477e9d...	Create Token	17662577	100 days 22 hrs ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.07346025
0x1c49d36e17f97d52f...	Create Token	17661009	101 days 3 hrs ago	0x6007D8...16531C2a	0x5cfa8d...f9ada3e0	0 ETH	0.06993451

From the list of tokens created, we can choose any arbitrary token to see the similar pattern – a token is created, and then liquidity is added to the LP. After a few days of trading, liquidity is removed from pools with a premium.

Transaction Hash: 0xf221b69f4cbb661c1d1d9fc54e183441c8f9c5786928f269f66d0c33076aab83

Status: Success

Block: 17662371 720745 Block Confirmations

Timestamp: 100 days 22 hrs ago (Jul-10-2023 09:27:35 AM +UTC) | Confirmed within 1 sec

Transaction Action: Remove 32.683085119231473162 ETH And 1,400,833,509.214759694327601143 NOVA Liquidity From Uniswap V2

Sponsored:

From: 0x6007D8d700004635340a40B990A4057a16531C2a

Interacted With (To): 0x7a250d5630B4cF539739dF2C5dAcB4c659F2488D (Uniswap V2: Router 2)

ERC-20 Tokens Transferred: 4

- From 0x6007D8...16531C2a To Uniswap V2: NOVA 37 For 204,939.01531919196766342 Uniswap V2... (UNI-V2...)
- From Uniswap V2: NOVA 37 To Null: 0x000...000 For 204,939.01531919196766342 Uniswap V2... (UNI-V2...)
- From Uniswap V2: NOVA 37 To 0x6007D8...16531C2a For 32.683085119231473162 (\$50,738.92) Wrapped Ethe... (WETH...)
- From Uniswap V2: NOVA 37 To 0x6007D8...16531C2a For 1,400,833,509.214759694327601143 Nova Token... (NOVA...)

Value: 0 ETH (\$0.00)

Transaction Fee: 0.002488851355286146 ETH \$3.86

Gas Price: 15.159838679 Gwei (0.000000015159838679 ETH)

Rug pull_

Observation #2: Most Don't Have Audits

When assessing if a project might prepare for an exit scam, it's crucial to check for an independent third-party audit. This audit can offer a detailed review of a token, pinpointing vulnerabilities and alerting investors. **Of the 78 rug pulls examined, only 12 reported having undergone any kind of audit.**

While a thorough audit might signal potential red flags, it doesn't always guarantee protection from exit scams. For starters, the project can undergo an audit and have an audit report, but with **a poor score**. Yet, users overlook this and consider the mere fact that the project was audited as sufficient.

As in the case of Magnate Finance, a key problem is that users often overlook audit results. The project had undergone an [audit](#), which clearly stated that a deployer could manipulate the token:

Ownership/admin privileges

Comptroller.sol

- ✓ Pause/Unpause minting, borrowing, transfer, and seize
- ✓ Set reward distributor, price oracle address
- ✓ Set close factor, collateral Factor, liquidation incentive, and marketborrow caps.
- ✓ Set borrow cap guardian address.

CToken.sol

- ✓ Set admin address
- ✓ Set comptroller address
- ✓ Set reserve factor

However, users didn't pay too much attention to the findings. Token owners continued to participate in protocol for almost 3 months after the audit results. And by the end of August, the deployer had removed liquidity from LPs in multiple transactions. As a result, we got the 2nd largest rug pull this quarter with over \$5 million stolen.

A similar situation has happened with DeFiLabs. An auditor has [found](#) multiple cases of centralization risk within their contracts, but the unresolved issues failed to raise sufficient concern among users.

PDL-01	Centralization Risks in Policy.Sol	Centralization/Privilege	● Major	Acknowledged
PDC-01	Centralization Risks in VPoolv5.Sol	Centralization/Privilege	● Major	Acknowledged

Rug pull_

[Rug Pull Observation #3: Common Pattern](#)

Rug pulls usually follow the same 5 steps:

- 1 Creation:**
 A developer creates a token, retaining control over its parameters.
- 2 Promotion:**
 They aggressively market the token, often using popular themes like meme-coins. Investors buy in, adding liquidity to pools.
- 3 Manipulation:**
 Once substantial liquidity accumulates, developers alter the token's rules, often inflating its supply to drain liquidity pools.


















In the case of \$IEGT, when the attacker [drained LP](#), the total token supply was increased from 5 million to 1 billion.
- 4 Farewell:**
 After draining funds, developers vanish, often cutting off all communication (the most sinister may even send a [farewell message](#)).
- 5 Crash:**
 The token's value plummets, leaving investors with near-worthless assets.

Reentrancy + Flash Loans_

Reentrancy and flash loan attacks often come hand in hand, and these categories brought a hefty penalty on many protocols: \$85 and \$5.8 million respectively. These attacks are much more technical in nature, and often go deep in exploring deployed smart contracts for finding a way to exploit faulty functionality.

Hacks by Chains

The chain distribution follows a predictable pattern: the larger the chain, the more it's targeted. Ethereum mainnet leads with **73** hacks, **54** of which are rug pulls. BSC is next with **33** breaches, **24** being rug pulls. Despite BSC being a tenth of Ethereum's, it has half as many scams. The newer Layer 2, Base, saw 6 hacks, including **4** rug pulls.

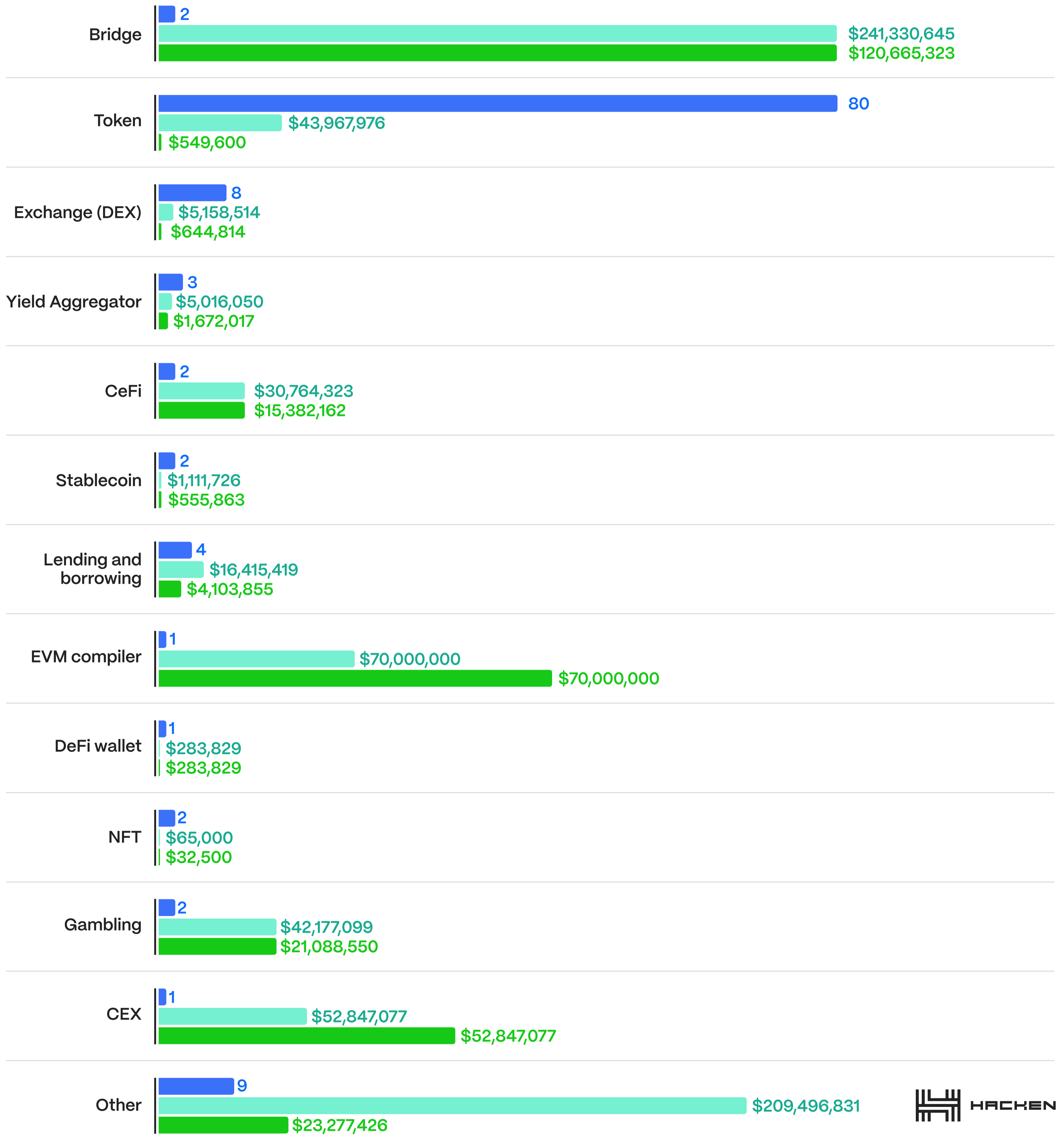
NETWORK	HACKS	CHAINS BY INCIDENT CATEGORY							
		Rug pull	Access Control	Reentrancy	Oracle Issue	Phishing	Flash Loan Attack	Honeypot	Other
 ETH	76	52	7	5	.	2	4	.	5
 BSC	34	24	3	.	.	.	2	1	4
 BASE	6	4	1	1
 POLYGON	4	.	2	1	1
 OPTIMISM	4	.	1	2	.	.	1	.	.
 ARBITRUM	4	.	2	.	1	.	.	.	1
 AVALANCHE	4	.	3	1
 FANTOM	2	.	1	.	.	.	1	.	.
 TRON	2	.	2
 BTC	2	.	2
 METIS	1	.	1
 CRONOS	1	.	1
 MOONBEAM	1	.	1
 ZKSYNC	1	.	.	1
 BTCCASH	1	.	1
 RIPPLE	1	.	1
 XDAG	1	.	1

Most of the attacks tend to happen on **1 to 2 different networks**. However, with access control attacks we see that it affects all the networks this address has assets on. Once a private key gets exposed, it does not matter where the cryptocurrency is located – the whole stash is compromised.

Hacks by Project Types

Hacks by type

Number of Projects ■
 Total Amount Stolen ■
 Average Per Incident ■



Project types with the biggest number of incidents

1 **Tokens** emerged as the most targeted project type, with 80 attacks. The core issue? Many tokens give full control to just one person. This allows them to make big changes on a whim, often leading to these scams. A possible solution? Instead of one entity in charge, have a group (like team members, custodial services, DAO members) control major decisions using multisig wallets. This reduces the risks of centralized admin rights where parameters can be changed arbitrarily

2 **Bridges** suffered a lot, with two projects totaling \$241 million in stolen assets.

3 This quarter has seen two **Stablecoins** being hit by liquidity drains. This controversial type of asset has many different architectures, each with its own sets of risks and vectors of attack.

In the case of Palm USD, an unaudited staking smart contract had a mismatch in dynamic between its functions, allowing for the attacker to buy and withdraw more coins than intended.

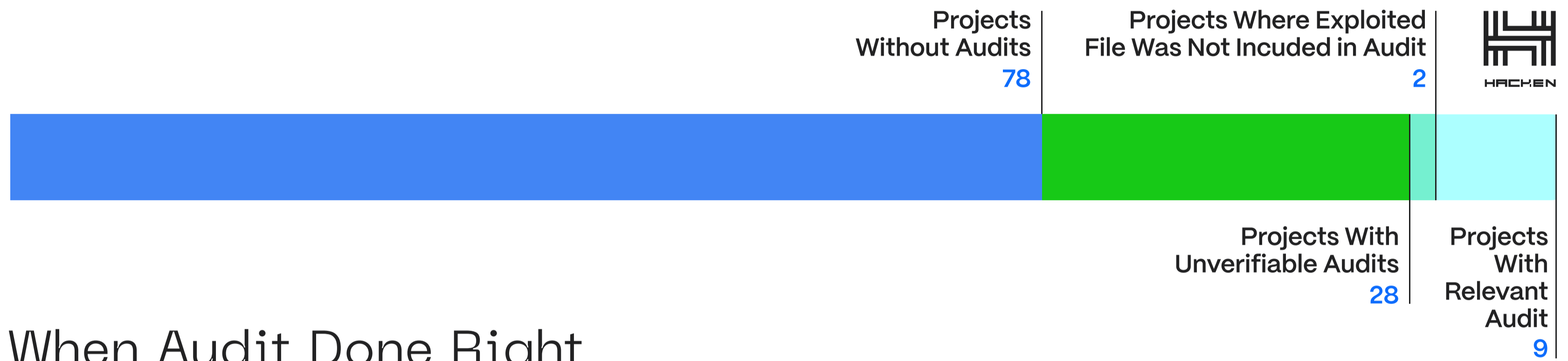
In the case of LUSD by Linear, the attacker found a breach in supporting smart contracts and managed to print an arbitrary amount of wrapped tokens. After obtaining derivative coins, they sold tokens on PancakeSwap and Ascendex pools, draining liquidity pools, causing a \$200k loss.

4 **Other** projects, which included entities like crypto payment providers Mixin Network and CoinsPaid, had its share of challenges, particularly massive phishing scams resulting in an average loss of \$24 million.

In a nutshell, while tokens faced the most attacks, it's clear that no crypto business is immune. Every project, big or small, needs strong security measures to guard against potential threats.

Hacks of Audited Projects

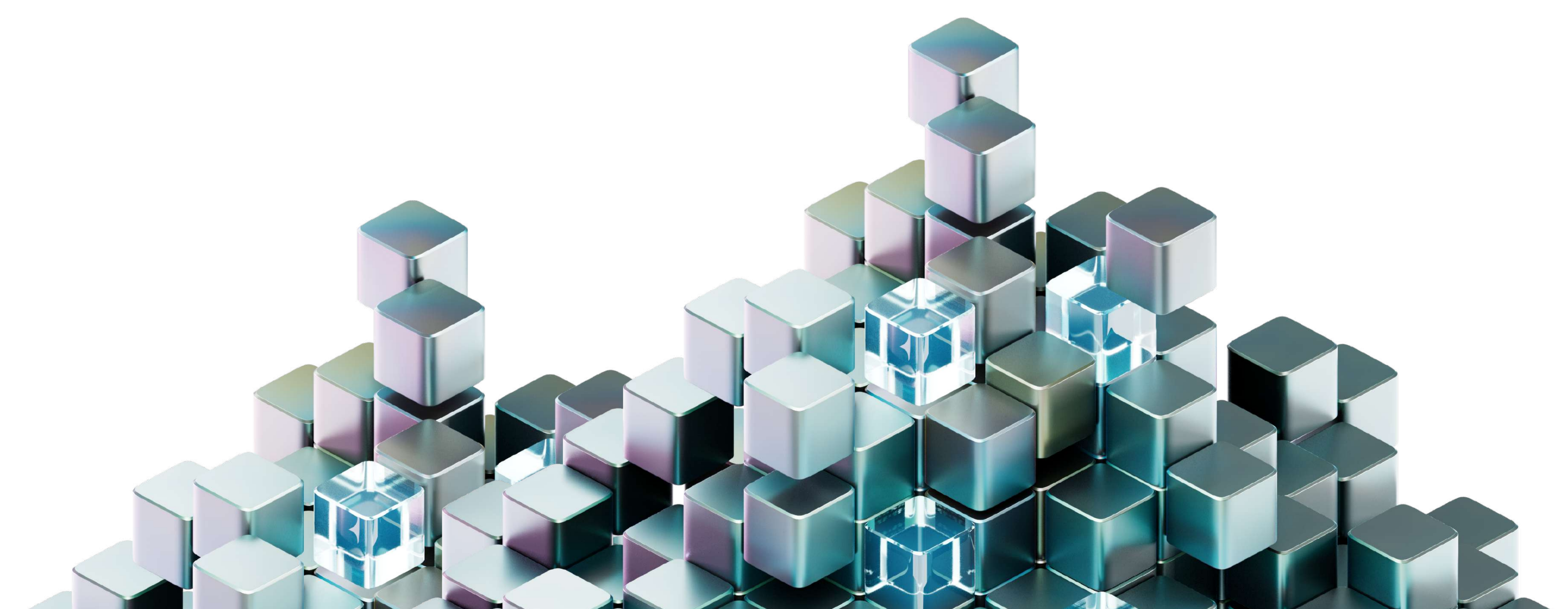
One way to prevent or, at least, drastically decrease the possibility of exploitation is smart contract auditing. However, even audited projects aren't immune. We delved into the details of hacked projects that had undergone audits to identify what went wrong and what could be done differently.



When Audit Done Right_

When done right, audits can serve as a vital line of defense, highlighting critical issues that projects should address. Key red flags an audit can uncover include:

- **Centralization Risks:** An audit can shed light on major centralization dangers. It's imperative to consult a company's audits as they often highlight these risks.
- **Address Discrepancies:** Discrepancies between the addresses of audited and traded tokens can be another revealing red flag. Notable instances of this were seen in the [DubaiCEO](#) & [Dogecoin3.0](#) exit scams.



Reality Check: _

[Audit Report Is Not A Guarantee Of Security](#)

Despite the protective nature of audits, not all audited projects are safeguarded against vulnerabilities. Among the 117 hacks we analyzed, 39 projects (including 11 rug pulls) claimed they had an audit.

Diving deeper, we identified several reasons why audits didn't stop exploits:

1

Outdated Review:

Relying on old audits for non-upgradable smart contracts can be detrimental.

A case in point is Balancer. Despite having multiple high-profile audits done in 2021, changes in the DeFi landscape rendered some of their older security measures obsolete. When a significant vulnerability was detected, Balancer attempted to move liquidity from the affected pools, but couldn't act swiftly enough. This lag culminated in a flash loan attack, resulting in almost \$2 million in losses.

2

Post-Audit Alterations:

A recurrent issue is when projects adjust their code after an audit. Any changes post-audit render the previous evaluations moot.

This exact scenario played out with Arcadia Finance. They were audited by Nethermint on March 2nd, 2023, but the contracts deployed five days later on Ethereum Mainnet and Optimism had glaring deviations from the audited code.

3

Incomplete Audits:

Another concern is when diligent companies inadvertently omit certain files from their audit's scope.

Exactly Finance, despite their exhaustive 13+ audits, overlooked the DebtManager.sol file. An exploit in this peripheral contract led to a severe \$7.2 million reentrancy attack.

4

Overlooked Vulnerabilities:

Finally, even the most thorough audits can sometimes miss vulnerabilities. These oversights remind us of the importance of perpetual learning, refining our expertise, and adhering to best practices. A prudent strategy would be to employ multiple auditors, amplifying the probability of detecting critical vulnerabilities.

In essence, while audits play a crucial role in enhancing security, they aren't foolproof. The responsibility remains on both auditors and projects to remain vigilant, updated, and open to iterative learning.

Conclusions

Reflecting on this quarter's crypto trends, three primary insights stand out:

- 1 Access Control Vulnerabilities:**
While less frequent, these breaches result in significant financial damage, averaging tens of millions per incident. Safeguarding against single points of failure with tools like multisig wallets, distributed key storage, and role-based permissions are crucial.
- 2 Rug Pulls Remain Prevalent:**
These scams exploit those drawn by quick profit prospects. It's vital to analyze token ownership, liquidity conditions, and audit outcomes before diving in. Favor projects with renounced admin controls, community-led finances, and steer clear of tokens from unidentified developers with default settings.
- 3 Continuous Vigilance with Smart Contracts:**
Audits aren't foolproof. Even thoroughly checked code can conceal vulnerabilities. It's wise to adopt a multi-auditor approach and remember: changes made post-audit nullify prior findings. With new threats surfacing regularly, ongoing audits of active contracts are a must.

The analysis of this quarter's hacks underscores the ongoing need for enhanced blockchain security awareness and action among users, projects and auditors.



We Make Web3 A Safer Place



6+

Years of expertise

1,000+

Clients in total

180+

Partners

1,200+

Audited projects

50+

Crypto exchanges

100+

Team members