HACKEN × HackenProof

WEB3 SECURITY REPORT



2024

hacken.io | We Make Web3 A Safer Place

Table of contents

1. General Observations 3

2. Overview of Hacks 4

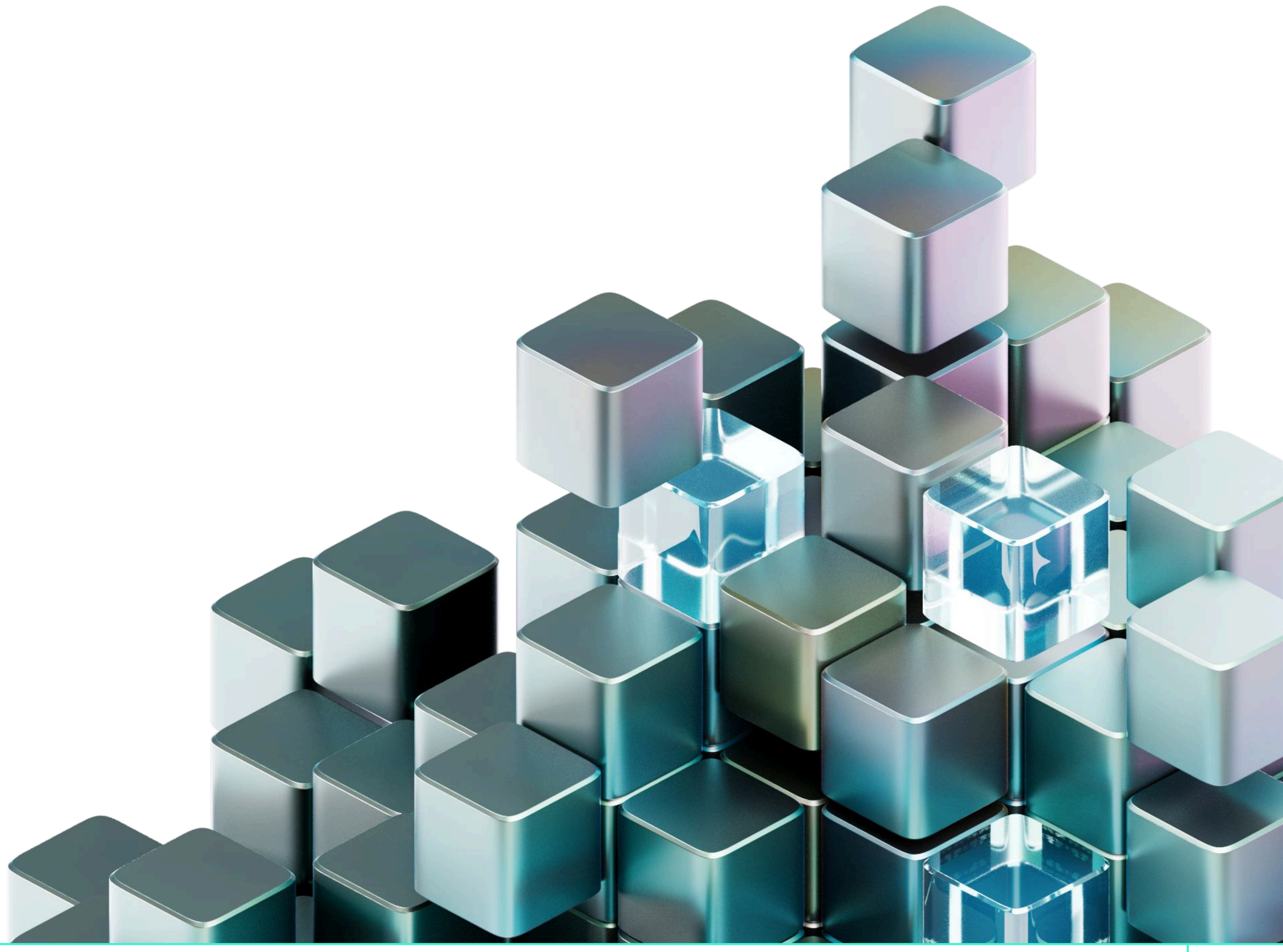
Types of Attacks 4

Types of Projects Affected 5

Funds Recovery 8

3. Security Measures of Projects Hacked 8

4. Conclusions 10



General Observations

Highlights

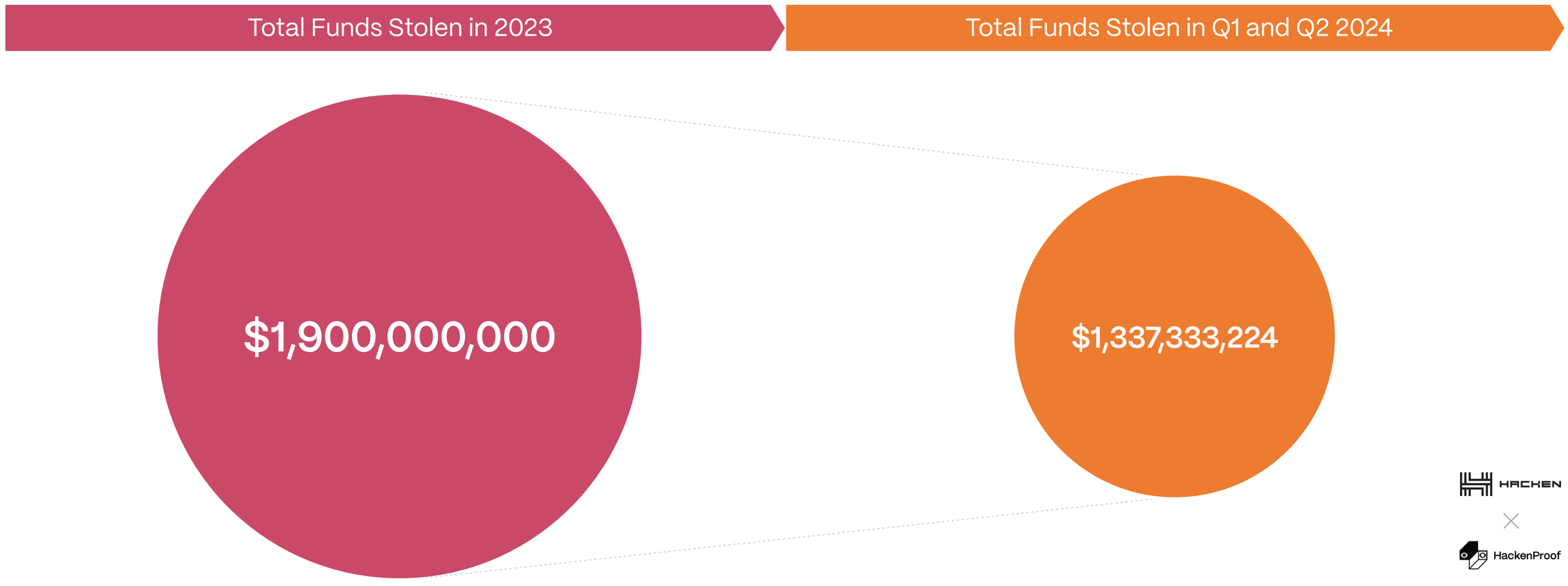
Q1 2024		Q2 2024
$824,405,224	Funds Stolen	$512,928,000
$380,631,526	Funds Lost	$165,496,712
67	Number of Incidents	41
$290,000,000 Gaming platform Playdapp	The Biggest Hack	$300,000,000 Crypto Exchange DMM Bitcoin

In the second quarter of 2024, we witnessed a significant decrease in the number of hacks compared to the first quarter. Is it a glimmer of hope amid the gloom?

The researchers from Hacken and HackenProof teams collaborated to analyze the data, aiming to equip the community with insights and observations on what the figures really mean and the recent trends observed. We relied on the following sources of information: DefiLlama and De.Fi REKT Database.

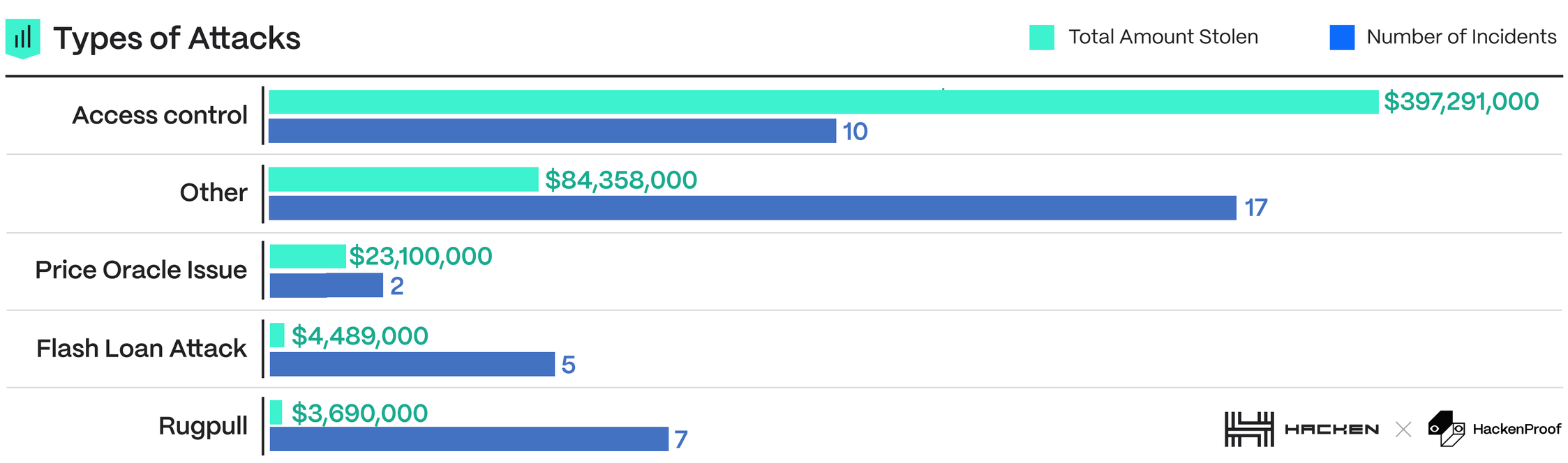
While at a glance the dynamics of the market seems beyond optimistic with the number of hacks almost half as much as the previous quarter, the situation appears more dire when considering the funds lost. The safety crypto crisis has only deepened, as the amount of funds drained from crypto projects in 2024 is already close to the total losses for the whole of 2023.

Assets Stolen in 2023 vs. 2024



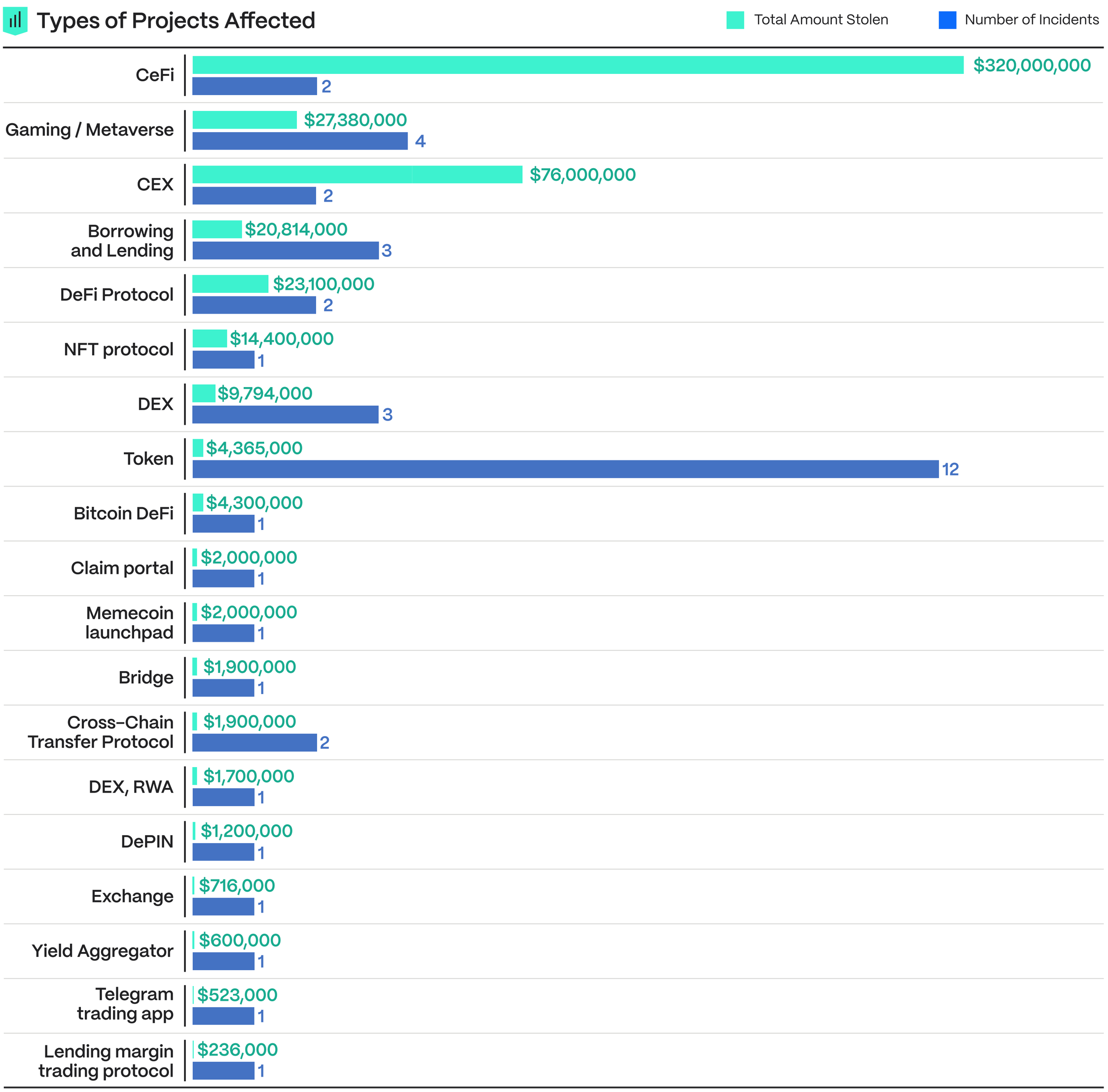
Overview of Hacks

Types of Attacks

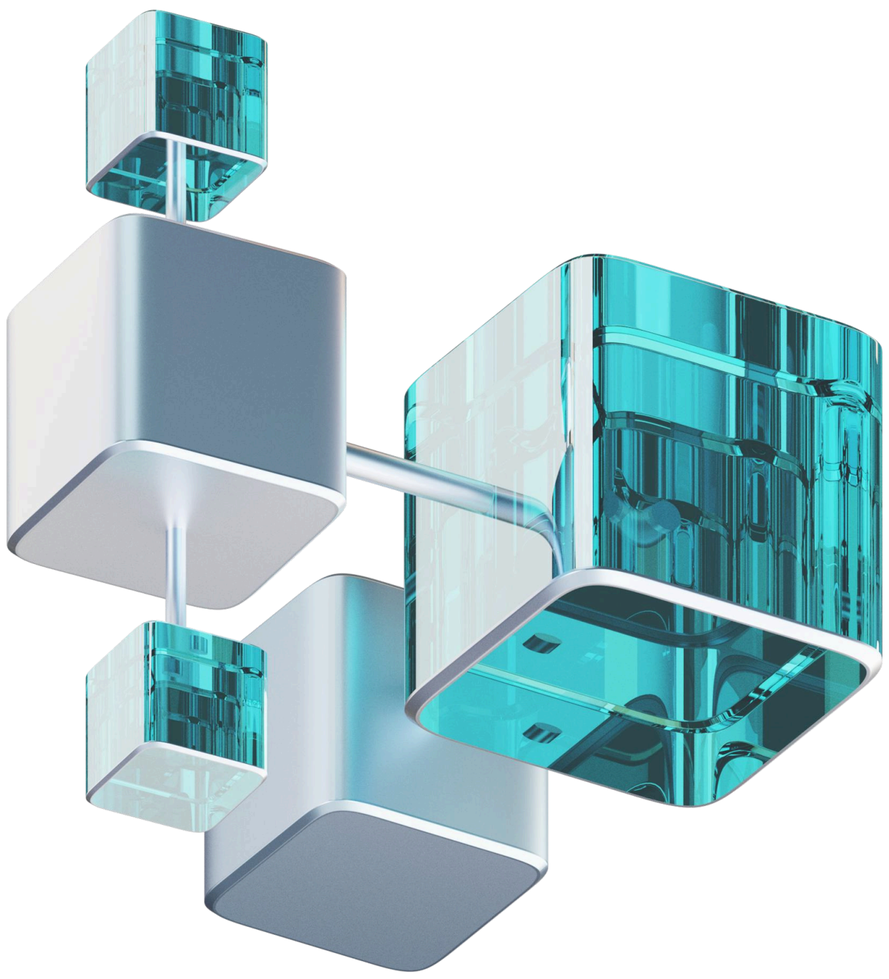


Our 2023 yearly report highlighted that access control was the main cause of 50% of all hacks. This trend continued in Q1 2024, with access control remaining the most dominant vulnerability. Notably, in Q2 2024, Access Control was not prevalent in terms of the number of cases, but this type of attack caused the industry's biggest losses, amounting to **397.2M**.

Types of Projects Affected



In the CeFi category, we included projects that combine FinTech and DeFi elements. The two incidents are:



- **The Rain Exchange** hack occurred due to a failure to secure private keys, allowing the attacker to generate valid digital signatures for transactions. On April 29, 2024, $14.8 million was transferred from several Bitgo wallets to two wallets, converted to BTC and ETH. The exchange did not disclose the hack until two weeks later when it was exposed by blockchain sleuth ZachXBT. Rain then issued a statement, declaring implementation of additional security measures and covering the stolen funds to ensure safety of user funds.

- **The DMM Bitcoin** incident is one of the few BTC-related hacks and one of the biggest, accounting for the majority of funds stolen in the entire quarter and becoming the largest incident of the year so far. It happened in May 2024 and resulted in a loss of approximately $305 million. The hack involved a large transfer of 4502.9 BTC to an unknown wallet, followed by redistribution to multiple addresses. Potential causes include compromised private keys, signing processes, or address poisoning. The incident highlights the need for robust security measures like multi-signature wallets, cold storage, and decentralization of funds to protect against such high-value breaches.

Token category is prevalent in the number of hacks. It can be attributed to the rapid growth and innovation in the blockchain and DeFi sectors, which often outpaces security measures, leaving new projects vulnerable to exploits. Many of these projects deploy complex smart contracts that may contain undiscovered vulnerabilities. Additionally, some prioritize launching quickly over thorough security audits, leading to overlooked security gaps. The increased sophistication in social engineering tactics has allowed attackers to gain access to critical administrative accounts and sensitive information, further exacerbating the problem.

Moreover, the lack of experience in secure coding practices among new development teams and the lucrative nature of successful attacks, which offer significant financial rewards, motivate hackers to target these projects. The trust within the blockchain community is also exploited through phishing and rug pull scams, deceiving even seasoned investors. The global and decentralized nature of blockchain projects makes it challenging to enforce standardized security measures and regulations, highlighting the need for improved security practices and vigilant community awareness to mitigate such risks.

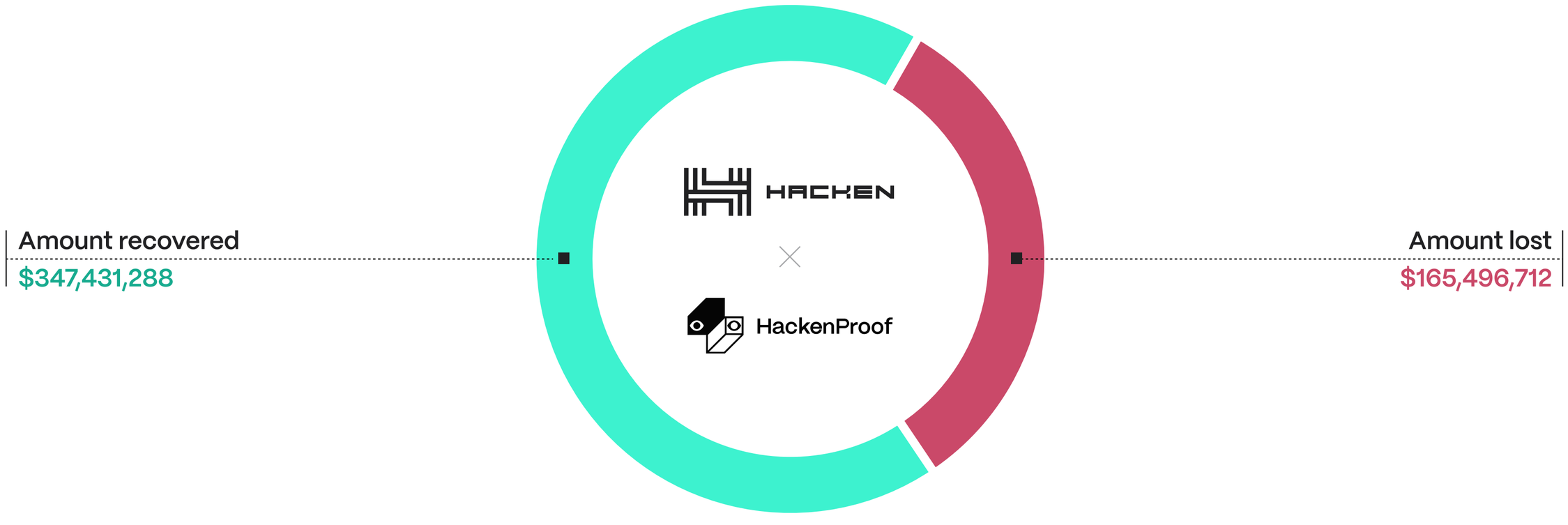
Why do so many projects get hacked?

Token	Why this happened?	What was affected?	Is it fixed now?
Condom Token	Exploit in the smart contract's minting function.	Token supply was manipulated, resulting in inflation.	Yes, developers patched the contract and relaunched it with enhanced security.
DegenFox	Social engineering attack targeting the development team.	Administrative access was compromised, leading to unauthorized transactions.	Partially; security protocols were updated, but some funds are still unrecovered.
SAGA	Vulnerability in the staking protocol.	Users' staked funds were stolen.	Yes, the protocol was audited and fixed; users were compensated.
Empower AI Rug	Malicious exit by the developers.	Entire project funds were siphoned off.	No, the developers disappeared, and funds are unlikely to be recovered.
FENGSHOU	Flaw in the decentralized finance (DeFi) lending protocol.	Loan collateral was manipulated, causing significant financial losses.	Yes, the flaw was corrected and the protocol was relaunched.
NovaMind	Cross-site scripting (XSS) attack.	User data was compromised, leading to unauthorized access.	Yes, security measures were enhanced, and affected users were notified.
OSN	Insufficient input validation in the smart contract.	Contract logic was bypassed, causing token mismanagement.	Yes, the issue was addressed with a smart contract upgrade.
Fake Lifeform	Phishing attack on users.	Users' private keys were stolen, leading to fund loss.	Yes, awareness campaigns were conducted, and security features were added.
Galaxy Fox	Exploit in the liquidity pool.	Liquidity was drained, causing a crash in token value.	Yes, the exploit was patched, and the liquidity pool was restored.
Fake PIToken	Clone phishing scam mimicking the original project.	Investors were defrauded by the fake project.	Yes, the fake project was taken down, and legal actions are in process.
WINR	Flash loan attack.	Manipulated market prices led to large-scale fund extraction.	Yes, the protocol was adjusted to prevent similar attacks in the future.
YYS Token	Internal fraud by a team member.	Significant portion of project funds was embezzled.	Yes, the team member was removed, and funds were partially recovered.

Funds Recovery

For the second consecutive quarter, the silver lining amid the alarming rate of theft in crypto is the amount of funds recovered. This time, the industry managed to recover more than half of assets targeted by scammers and hackers.

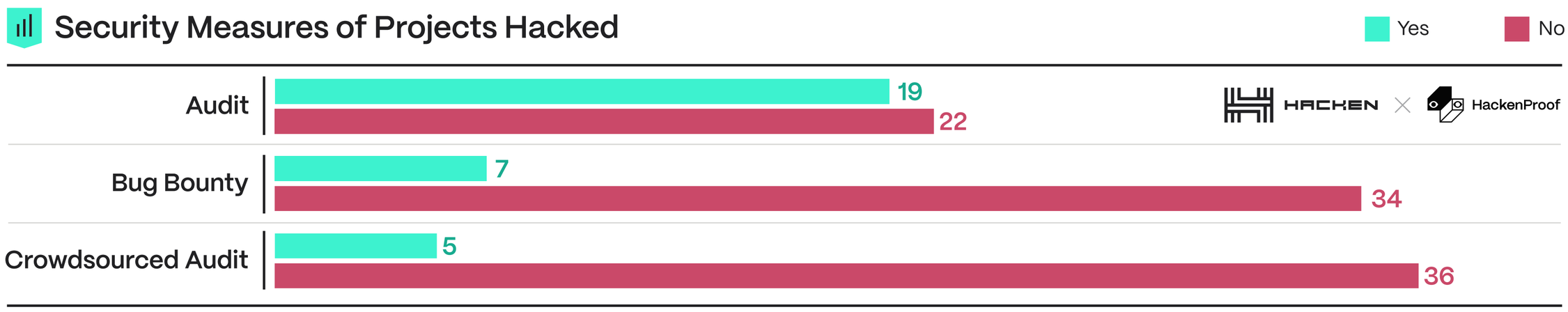
Funds Lost vs. Funds recovered

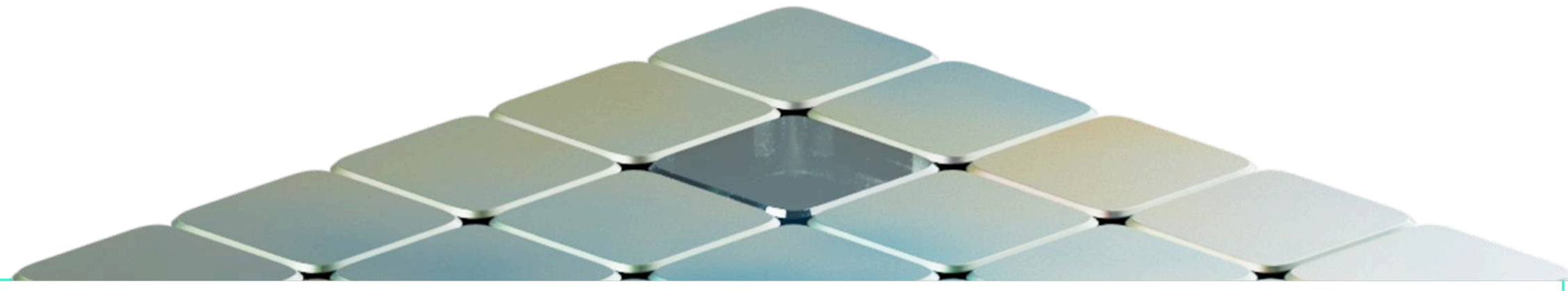


Security Measures of Projects Hacked

We continue to observe a lack of security measures in hacked projects.

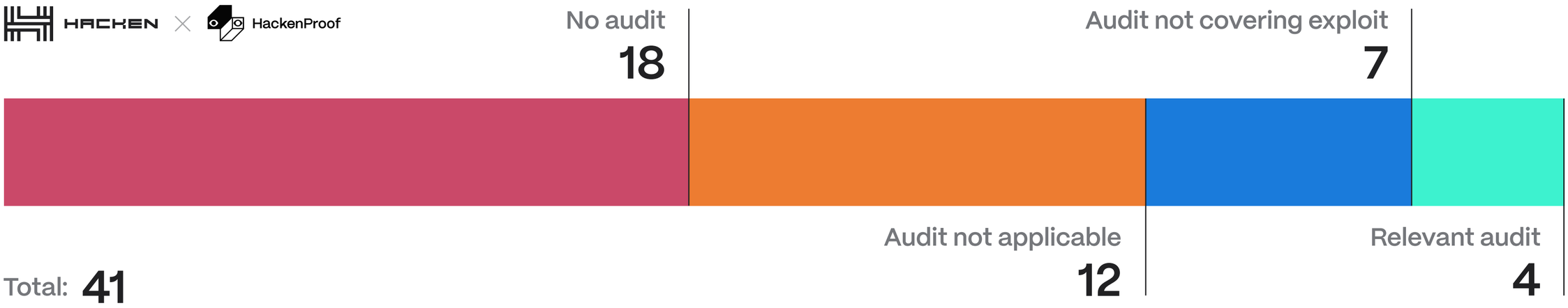
Security Measures of Projects Hacked





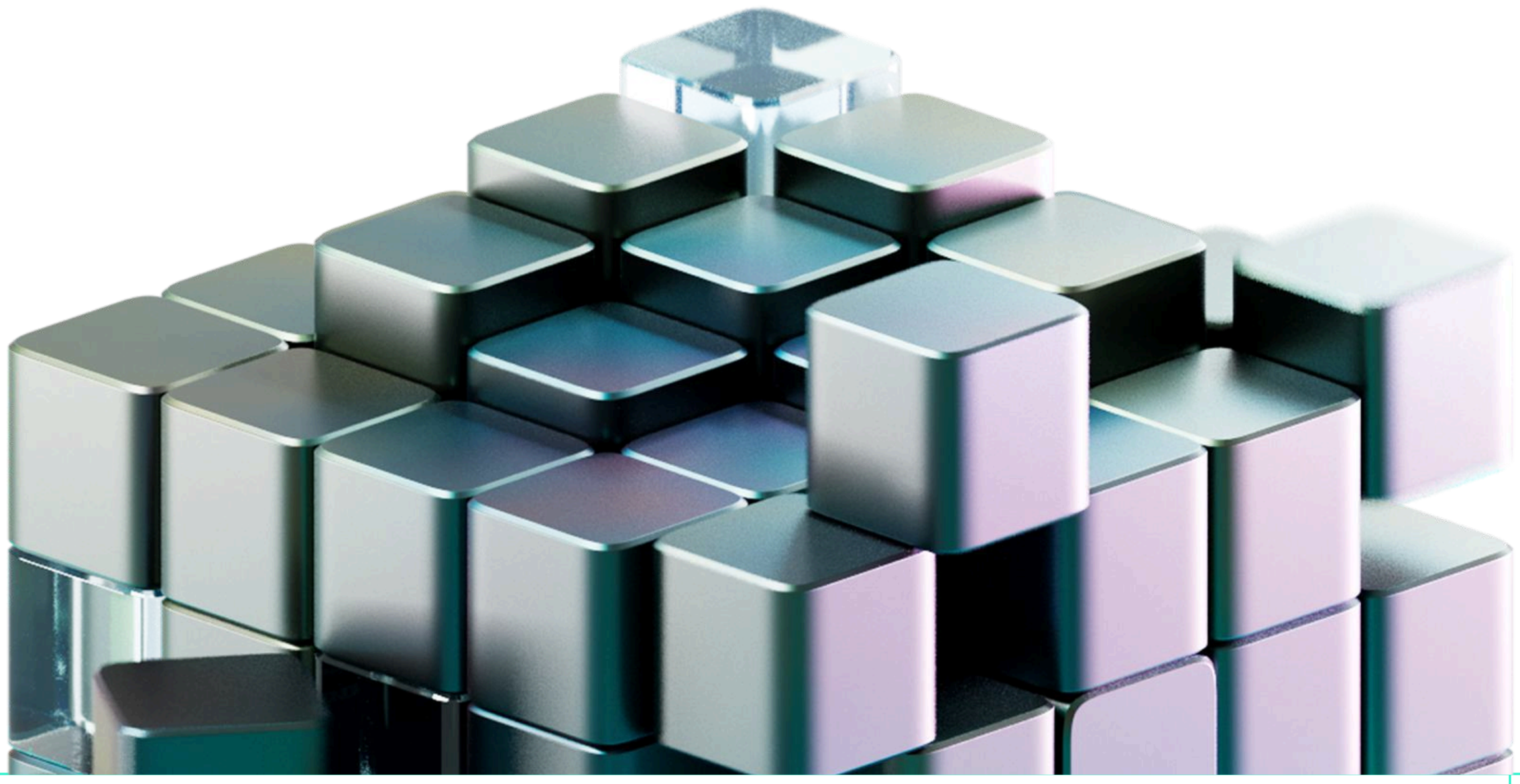
The number of projects that underwent a security audit appears to have increased since last quarter. However, upon analyzing the audit scope and comparing it with the hack details, we observed that projects still do not pay sufficient attention to this crucial security measure.

Audit Relevancy



While no security measures can guarantee total protection for a project, a security-first approach is crucial to combat bad actors and black hats. The best practice is to combine several security measures to ensure multi-layered protection.

The responsibility for making crypto secure lies with all parties involved. Projects should prioritize security, security providers must innovate new tools and methodologies, and regulators need to establish fair and transparent rules that address real-life challenges.



Conclusions

- **Reduction in Hacks:** Q2 2024 saw a significant decrease in the number of crypto hacks compared to Q1, indicating a potentially positive trend in security.

- **Increase in Financial Losses:** Despite fewer hacks, the total amount of funds lost in Q2 2024 nearly matched the total losses for all of 2023, suggesting that the severity of attacks is increasing.

- **Access Control Vulnerability:** Access control issues, though less frequent in Q2, resulted in the largest financial losses, underscoring the importance of robust access control mechanisms.

- **CeFi Incidents:** Notable incidents in the CeFi category, such as the Rain Exchange and DMM Bitcoin hacks, highlighted critical vulnerabilities in private key management and the need for advanced security measures like multi-signature wallets and cold storage.

- **Token Project Vulnerability:** The rapid growth in the blockchain and DeFi sectors has outpaced security measures, making token projects especially vulnerable to sophisticated attacks and social engineering tactics.

- **Improvement in Fund Recovery:** A positive development is the industry's success in recovering or freezing more than half of 77% of stolen assets in Q2 2024, emphasizing the progress in response and recovery efforts.

HACKEN × HackenProof

We Make Web3 A Safer Place



6 Years of expertise	**1,000+** Clients	**180+** Partners
1,500+ Completed audits	**50+** Crypto exchanges	**100+** Team members

HACKEN.AI · TRUST ARMY · EXTRACTOR · HackenProof