HACKEN

Blockchain Security Auditor

# WEB3 SECURITY REPORT

Q1 2024



# Table of contents

1. Highlights & Introduction 3

2. General Observations 4

3. Hack Overview 5

Hacks by Vulnerability Type 5

Hacks by Chains 8

Hacks by Project Types 8

4. Funds Recovered 10

5. Audited vs Unaudited Projects – What Do We Find? 12

General Analysis 12

Post-Audit Vulnerabilitie 12

Audit Scope and Relevance 12

6. Conclusions 13

Recommendations for Strengthening Web3 Security 13



# Highlights

**$824,405,224**
stolen
in Q1 2024

**$682,086,639**
lost to
access control hacks

**$443,773,698**
recovered or frozen
post-incident

**56%**
share of rug pulls
and smart contract vulnerabilities

In the first quarter of 2024, we witnessed 67 hacks totaling $824,405,224 stolen. Our research shows that **hackers are more active in targeting high-profile individuals and projects**. Access control stands out as the most frequent hack category by number of incidents and remains the most damaging hack category by funds lost, with $682,086,639 stolen. That's 83% of the total funds stolen in Q1 2024, with as many as 26 individual incidents.

Remarkably, $443,773,698 of the total stolen amount was recovered, signalling **a massive improvement** in the sector's ability to respond to and respond to hacks. Over 54% of the stolen amount was successfully frozen or recovered.

Our 2023 yearly report highlighted that access control was the main cause of 50% of all hacks. This trend continues in 2024, with access control remaining the most dominant vulnerability.

While rug pulls didn't cause a significant percentage of the total amount of funds lost, they stand equal to smart contract vulnerabilities, with 14 incidents each totaling 56% of all incidents.

While smart contract vulnerabilities alone didn't dominate this quarter, they played a big part in access control hacks, which caused the biggest exploits. Unrelated to access control, **purely smart contract-related hacks occurred mostly among smaller projects**, indicating security improvement among top-tier projects.

# Introduction

Hacken Research Department conducted an extensive study focusing on analyzing and contextualizing crypto hacks and scams that occurred during the first quarter of 2024. The study was based on a diverse range of primary sources, including audit information, responses from project teams, social media, and blog posts, as well as aggregated data from platforms such as De.Fi rekt.

# General Observations

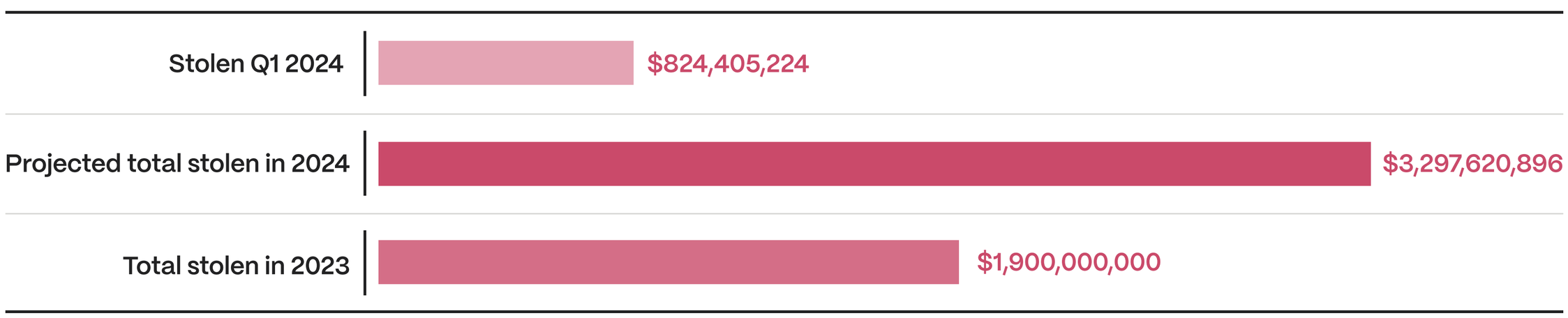
**These four big events accounted for 66% of the total funds lost.** This quarter's biggest security events were the gaming platform Playdapp suffering a $290,000,000 hack, Ripple's Chris Larsen wallet incident worth $112,000,000 at the time, the Orbit chain bridge hack, worth $80,000,000, and Munchables, the Web3 gaming protocol on Blast exploit worth $63,000,000.

Playdapp, Chris Larsen (Ripple), Orbit chain bridge, and Munchables were all access control breaches. Access control was the most damaging exploit type of Q1, as hackers gained unauthorized access to the most critical parts of the systems.

Tokens were the most frequent project type hacked, with 19 incidents, followed by others at 10 incidents and lending protocols at 9 incidents.

Gaming platforms were the most affected by funds lost, with Playdapp taking most of the statistics, followed by Munchables. The second category was breached wallets across high-profile users, DAOs, tokens, bridges, and CeFi platforms. Examples are Chris Larsen, Jeffrey Zirlin, and AirDAO

**Project Assets Stolen in 2024**




So far, in 2024, an increase in hacks and funds lost can be seen compared to the previous year of 2023. Why an increase?

**While numerous factors are at play, two significant ones should be considered:**

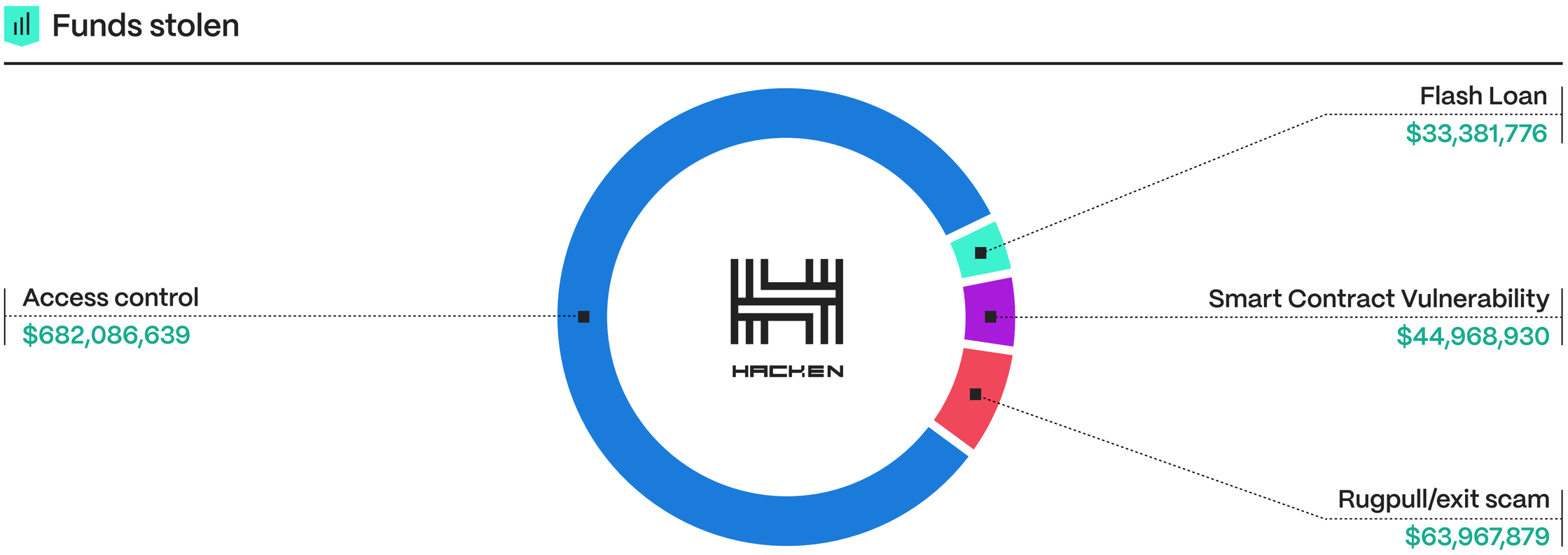
**1.** The market has a general "bull market" sentiment which usually follows with increased activities.
**2.** The market is maturing with new and vulnerable protocols launching across "under-discovered" verticals (gaming, RWA/tokenization, new DeFi apps and more).

# Hacks by Vulnerability Type

In Q1 2024, we saw four main hack types occurring:

- Access control
- Flash loans
- Smart contract vulnerabilities
- Rug pulls/exit scams

**Access control came out as this quarter's biggest vulnerability**. In addition to being the biggest hack type by the number of incidents, it was the most devastating by the number of funds lost, accounting for 83% of the total hack types by funds lost and 40% by the number of incidents.




**Several hypotheses underlie these statistics:**

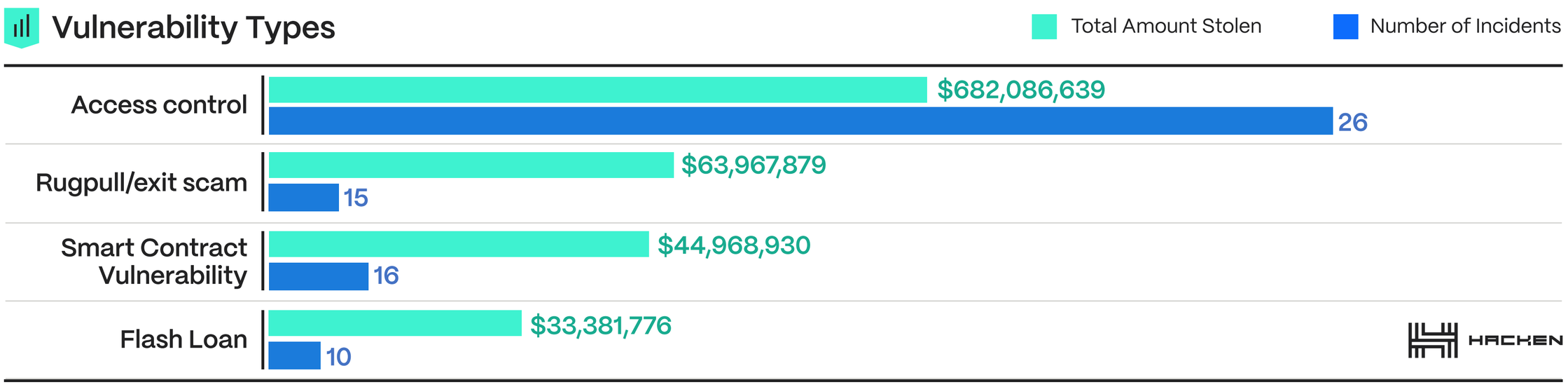
- High-profile Web3 projects are improving their audit and smart contract security.
- Hackers are becoming increasingly sophisticated in targeting the central points of vulnerability of high-value individuals and projects through phishing and social engineering methods. People are the biggest vulnerability, and targeting humans remains the most profitable strategy.
- While smart contract vulnerabilities remain a major factor in the number of incidents, the value stolen is quite low. This indicates that these hacks are targeted at up-and-coming "low-value" projects that can't afford or don't prioritize extensive audits in their stage.

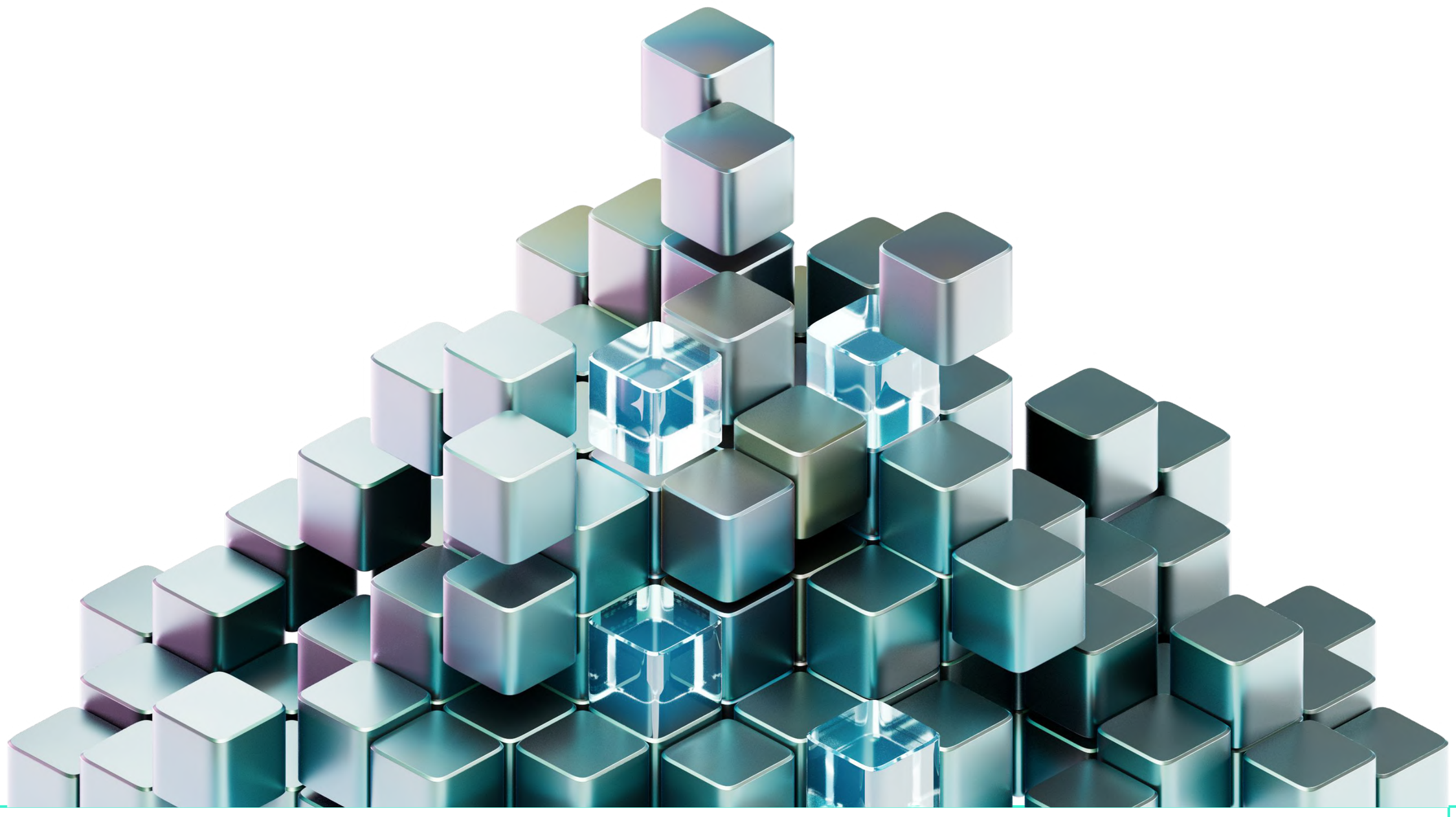
There seems to be an industry shift where hackers focus more on access control methods of hacking projects. Gaining unauthorized access to seed phrases or private keys allows attackers to drain assets from smart contracts and Externally Owned Addresses (EOAs), highlighting the critical vulnerability of EOAs' reliance on single keys for security.

Unlike previous quarters, where certain hacks stood out for their magnitude, this quarter saw a broader distribution of losses across incidents. This reflects a persistent and widespread challenge in securing access controls within the Web3 space.

Access control has also affected varied project types, showing that the vulnerabilities related to access control remain relevant to everyone, regardless of project type, whether in DeFi or CeFi. Beyond code vulnerabilities, the human element in Web3 projects remains the most vulnerable part of the industry.

Flash loan attacks also remain one of the instruments to find vulnerabilities in crypto projects, totaling $33,381,776. Some noteworthy hacks were the lending platforms Radiant Capital and Gamma Strategies, as well as WooFi token.



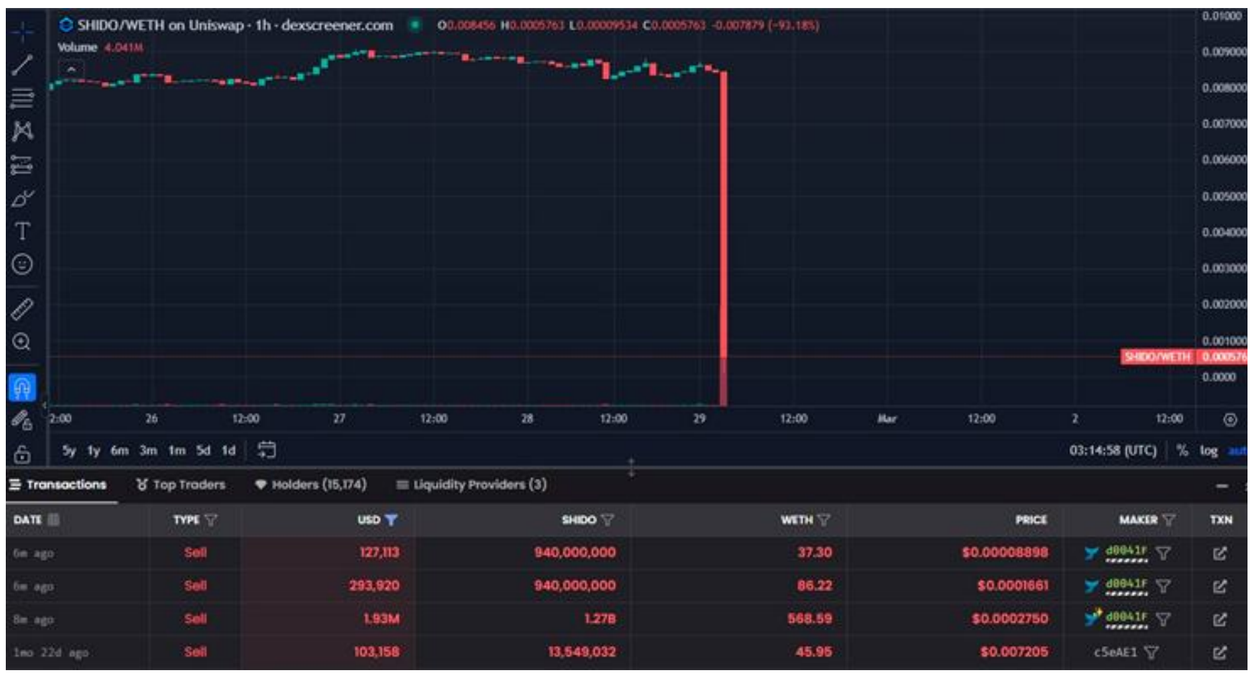



# Access Control Hack – Case Study by Hacken

SHIDO

In late February, the Shido layer-1 blockchain project suffered a major exploit on its Ethereum staking contract due to an access control vulnerability. An attacker was able to drain over 4.3 billion SHIDO tokens worth around $35 million from the contract.

→ Source




**Exploit Details:**
The attack unfolded when Shido's StakingV4Proxy contract ownership was unexpectedly transferred to a new address.

The new owner immediately upgraded the contract code to include a hidden withdrawToken() function. This allowed the attacker to withdraw the entire 4.3+ billion SHIDO token balance from the contract. Blockchain analytics linked the exploiter's wallet to funds originally bridged from Layerswap and Arbitrum.

As ZackXBT pointed out in a follow-up tweet, the admin's personal assets were withdrawn, showing the possibility that the attack was access control-based.

**Root Cause:**
A critical access control flaw permitted unauthorized transfer of the staking contract's ownership and subsequent upgrade to a malicious version of the contract code. This highlighted inadequate security controls around the protocol's key smart contracts.

**Impacts:**
The SHIDO token price plunged over 85% as the exploited funds were drained, wiping out tens of millions in value. Shido confirmed the exploited funds would be returned to affected stakers, but the incident severely impacted trust in the project as it prepared for the mainnet launch.

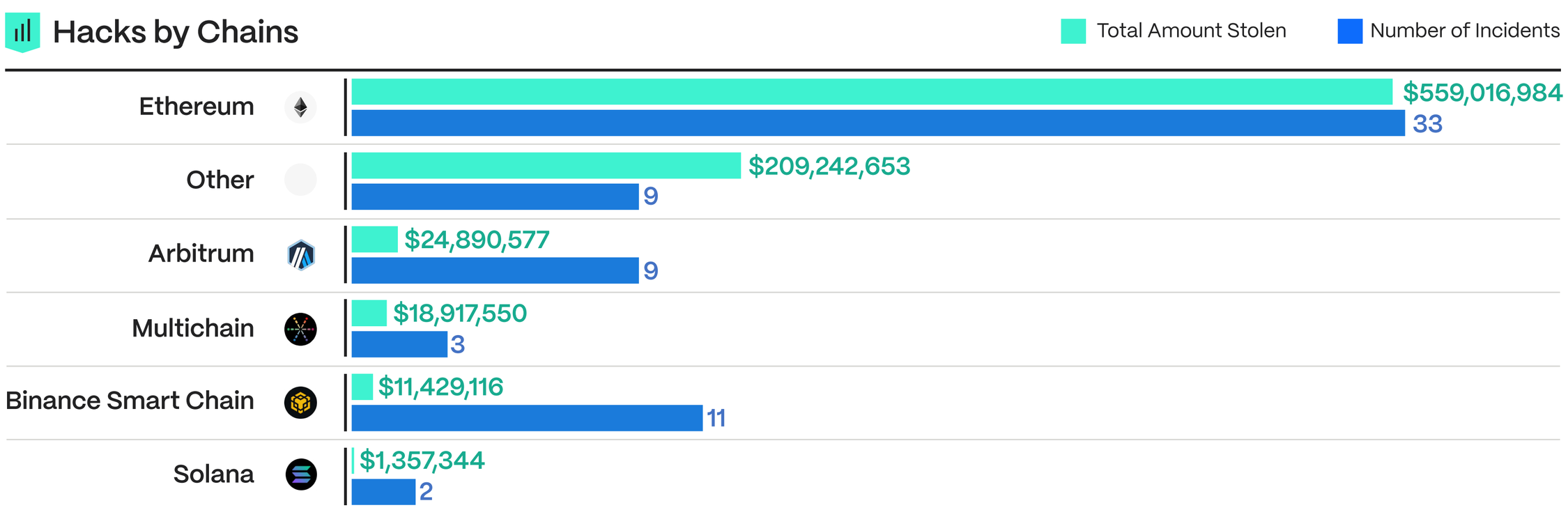
**Lessons Learned:**

1. Robust access controls and security restrictions around ownership/upgrade capabilities for critical contracts are paramount.
2. Continuous security monitoring and time locks on major contract changes can mitigate these types of attacks.
3. Centralized privileges like ownable contracts pose systemic risks that should be mitigated through decentralized governance.
4. Comprehensive smart contract audits and formal verification are essential, even pre-launch.

## Hacks by Chains

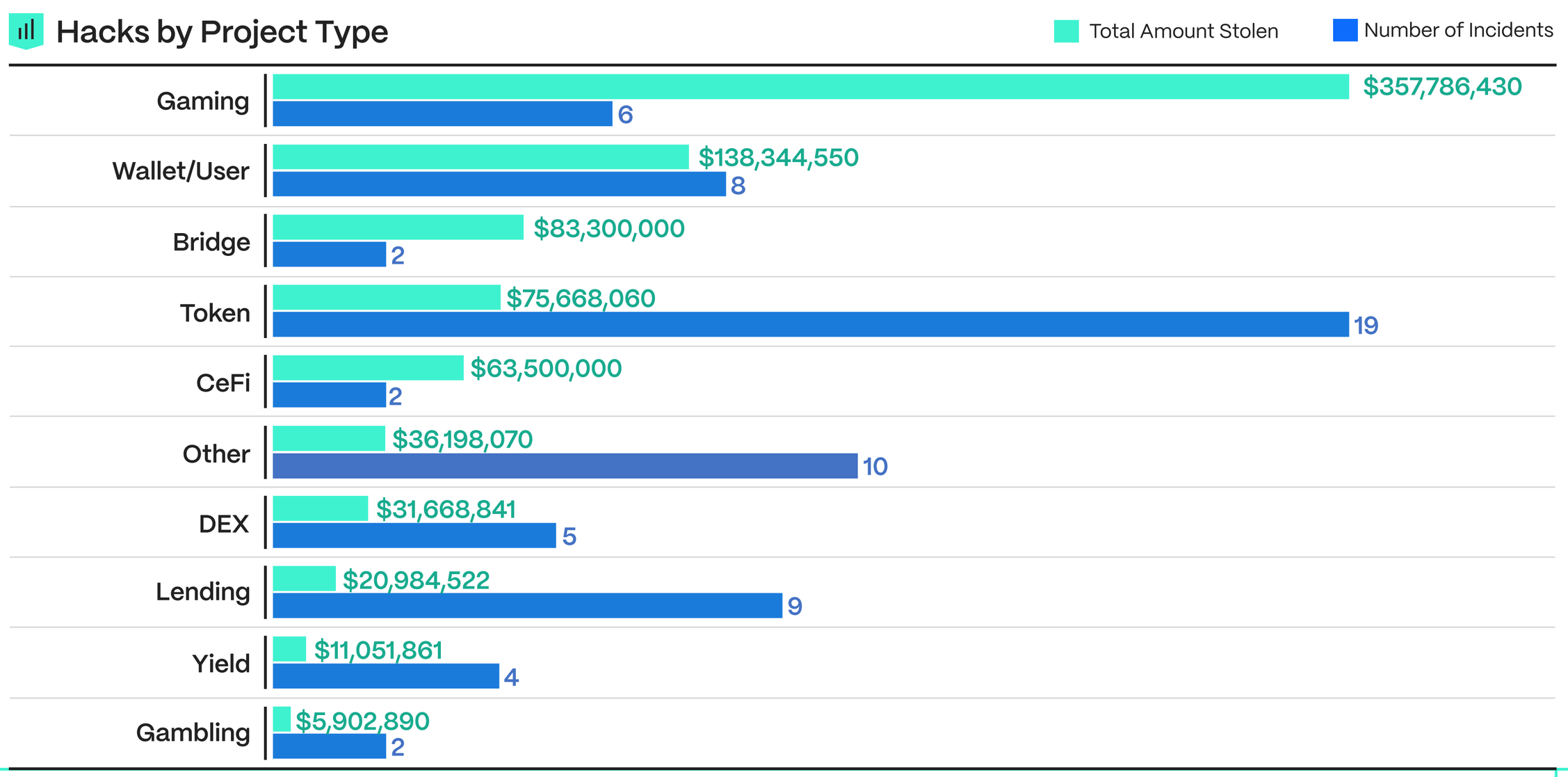
Our previous Q3 2023 report mentioned that "the larger the chain, the more it's targeted," a trend that continues this quarter. Ethereum has the most incidents, followed by Binance Smart Chain and Arbitrum. By the number of funds lost, Ethereum leads by far. The biggest event on Ethereum was the Playdapp hack.

Noteworthy incidents from smaller chains were Animoca Brands GAMEE token on Polygon access control hack of $16,352,814.00, resulting from an unauthorized GitLab access containing the private key and a vulnerability in the recoverERC721s() function). In addition, Ripple co-founder Chris Larsen's wallet breach of $112,000,000 took place on the Ripple blockchain, a hack accounting for almost 15% of the funds stolen this quarter.




## Hacks by Project Types

The first quarter of the year witnessed security incidents across a variety of project types. From token projects and gaming platforms to DEXs and lending protocols, all project types remain vulnerable, often to the same vulnerabilities.



- **Token projects** emerged as the biggest target in Q1, suffering a staggering 19 incidents resulting in over $75 million worth of funds being drained. The tokens incidents accounted for were mostly rug pulls, with a minority resulting from flash loans and access control.

- **Gaming projects** were hit six times, and $357 million was stolen. This highlights the exposure of gaming assets and in-game currencies to exploitation, a relatively new risk for the gaming industry, which has never had to consider in-game assets being stolen.

- **Decentralized exchanges (DEXs)** faced five incidents, losing close to $32 million as these trading platforms hold large amounts of liquidity. Yield platforms lost $11 million in four attacks.

- **The DeFi ecosystem** remains a major hotspot for attackers. Eight incidents, amounting to $21 million in losses, hit lending protocols hard, as their complex financial incentives and composability make them challenging to secure.

- **Bridge exploits** caused $83 million in damages across two incidents. The Orbit chain hack was the most damaging one, affecting around 95% of the total funds for this category. Bridge hacks are not new, with many incidents in 2022 and 2023. Bridges usually hold substantial amounts of assets with quite complicated cross-chain smart contracts and vulnerable admin privilege contracts.

- **Centralized trading platforms** and wallet infrastructure providers each suffered 2 incidents, collectively losing nearly $73 million – displaying that custodial risks persist even as DeFi grows.

- **Gambling dApps** saw around $6 million siphoned in 2 hacks.

- Perhaps most notably, **the "Other" category** comprising new innovations like unique smart contract standards had 10 incidents totaling $36 million in losses. As Web3 evolves rapidly, cutting-edge deployments face heightened risks due to unaudited and untested codebases. This underscores how emerging Web3 projects without battle-tested code are particularly vulnerable.

## Key Takeaways

Gaming platforms remain a target for hackers, leading the statistics by funds lost, while token hacks lead by the number of incidents. Investors and traders become victims of token rug pulls while lending protocols are emerging as lucrative for attackers. In addition, wallet breaches occurred across high-profile users and DAOs, tokens, bridges, and CeFi platforms. Although leading verticals emerged, this quarter saw a wide distribution of hacks and scams across project types and a fairly distributed sequence across project types defined.

# Funds Recovered

In Q1, $443,773,698 were successfully recovered or frozen from various cryptocurrency hacks and exploits, totaling 54% of the amount stolen. **This substantial recovery effort represents a notable improvement in the industry's ability to respond swiftly and effectively to hacks, exploits, and theft**. From hackers returning funds in return for bounties (Seneca Protocol hack and Dolomite) to white hat hackers such as @coffeebabe_eth front running the hackers themselves (Blueberry protocol hack) and returning the funds.

Due to the PlayDapp team's fast response and the token's illiquid nature, $253,900,000 out of $290,000,000 stolen has been frozen. This incident stands out among others, but even if excluded from the total picture, Web3 projects still managed to recover 23% of funds stolen this quarter.

Proactive measures from teams and white hat hackers facilitated the recovery of stolen funds and mitigated the potential for further losses and disruptions within the affected ecosystems. While the total amount hacked during this period reached a staggering $824,405,224, **recovering over half of the stolen funds is an immensely positive step toward enhancing the cryptocurrency landscape's security and resilience**.

Other aspects of the recovery process involved innovative and decisive actions, such as freezing tokens to prevent further unauthorized transfers, minting new tokens to replace those affected by specific exploits, and deploying new smart contracts to secure assets against further vulnerabilities.

### Lost vs. Recovered Funds



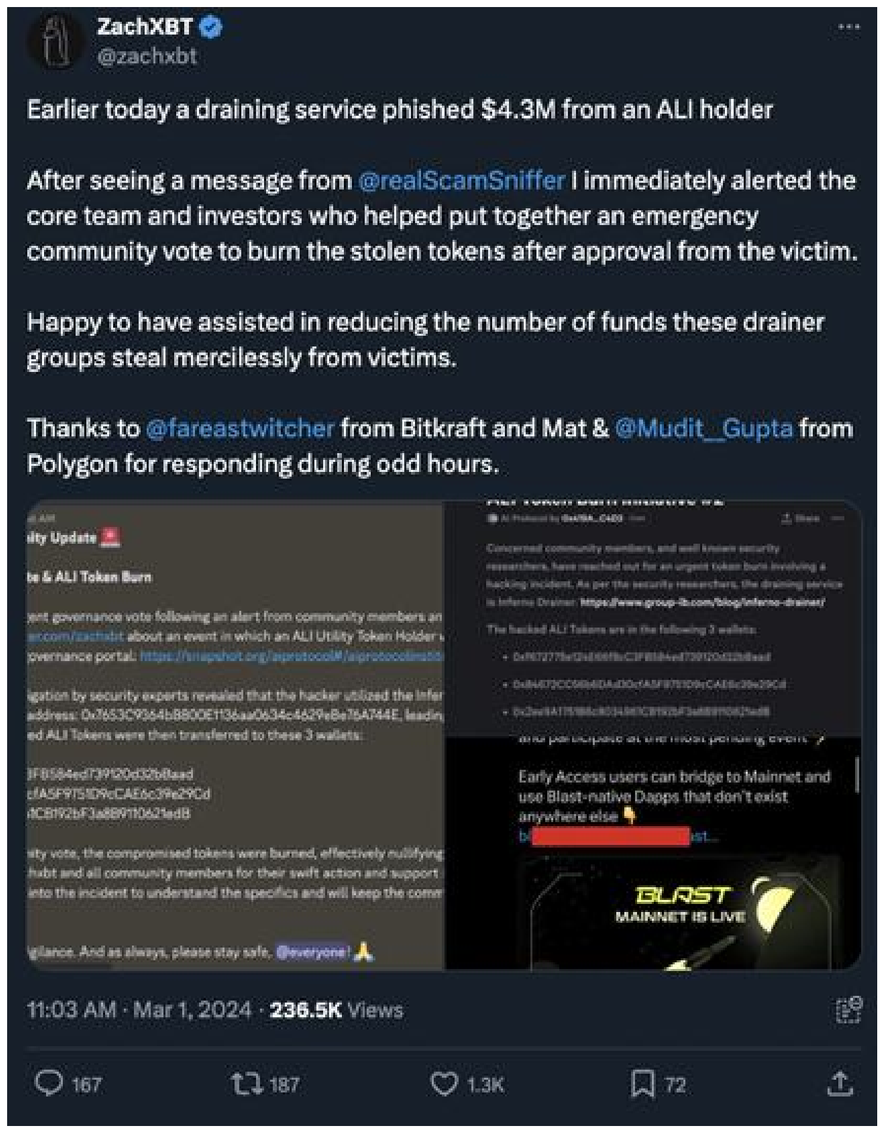
## Funds Recovered: Case Study of $ALI token

The $ALI incident was an example of a phishing exploit. A hacker used the Inferno Drainer to compromise a wallet containing 113 million ALI tokens worth $4.3 million. The cryptocurrency vigilance community swiftly responded. On-chain analyst @ZachXBT and other community members alerted the ALI core team after detecting the breach.

The ALI team organized an emergency governance vote to neutralize the threat. The community collectively burned the compromised $113 million of stolen ALI tokens. By proactively burning those tokens, they effectively rendered them unusable by the hacker and recovered the funds from the exploit.

**ZachXBT stated:** "After seeing a message from Scam Sniffer, I immediately alerted the core team and investors who helped put together an emergency community vote to burn the stolen tokens after approval from the victim."

This incident highlighted the importance of having communication with Web3 security teams and individuals like ZachXBT, ensuring swift coordination between teams and token holders– Decentralized projects' ability to respond quickly through governance mechanisms is often long; in this case, a decision was made in time to burn the stolen tokens. The collective crisis response allowed ALI to "recover" the $4.3 million that was targeted by the phishing attack. By making the stolen funds unusable by the hacker, the protocol could effectively mint new.

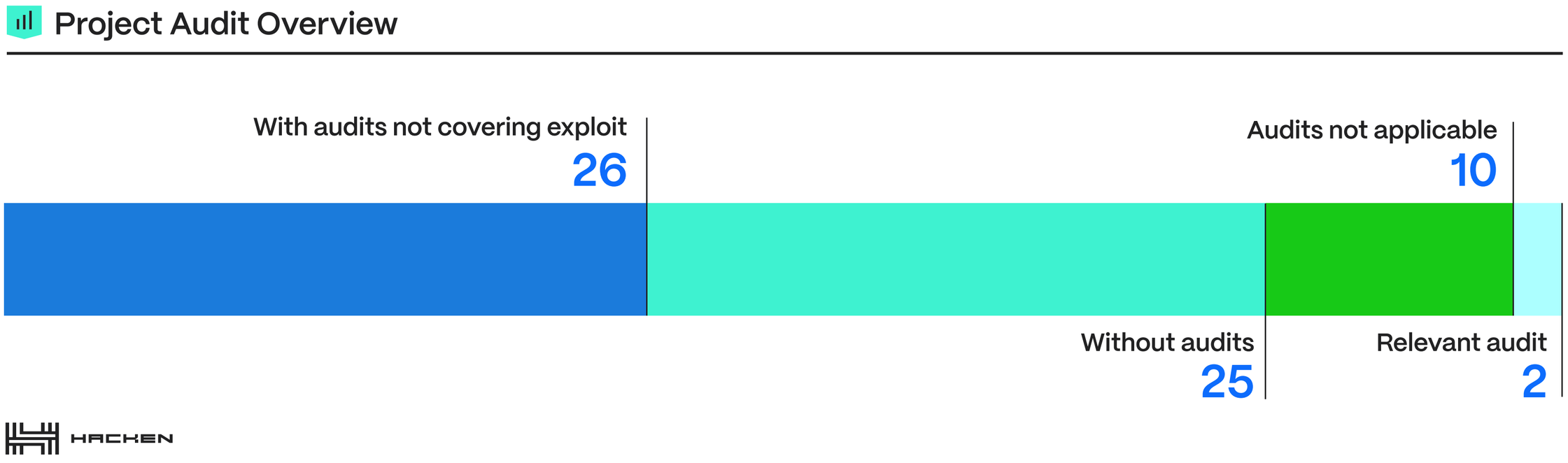





## Audited vs Unaudited Projects – What Do We Find?

**General Analysis**

Research reveals statistics about smart contract audits in the Web3 space during the first quarter. Of the projects included in this report, only 44% had undergone a smart contract audit, while 56% had not. Analyzing this further, we see that for audited projects, only two projects had an audit relevant to the hack. This shows that audits work, as most issues get resolved. However, this quarter's exploits also ranged from issues outside of audits, such as flash loans and access control issues.




A pattern emerges among the projects that get exploited even though they were audited, highlighting a bad practice within the Web3 ecosystem: Code commits, deployments, or upgrades after and outside audits cause exploits. This gap often leaves room for vulnerabilities absent and not included during the audit phase.

**Post-Audit Vulnerabilities**

The common theme among many hacks is exploiting vulnerabilities introduced in project architecture that occurred after the initial audit, including deploying new modules or features (e.g., Socket's new module), changing existing contracts (e.g., Unizen's updated contract), and not auditing relevant deployed contracts.

**Audit Scope and Relevance**

In some cases, the audits did not cover the specific components or features exploited in the hacks. For example, the Abracadabra hack involved a rounding error in smart contracts, which was not included in the audit focused on GMX V2 Market Integration.

This underlines the necessity for continuous security monitoring, auditing every piece of code and upgrades, and adopting security best practices throughout the development lifecycle. The findings also highlight that even a small code upgrade can cause major protocol devastation. The Socket Protocol hack and others are an example of this.

Audits do not guarantee immunity against exploits. Some but few projects that underwent audits were still compromised. However, **it becomes clear that most issues include reliance on outdated audits and post-audit alterations introducing new vulnerabilities**. Some are due to incomplete audits that fail to cover all aspects of the project. This reality check emphasizes that while audits are essential for identifying and mitigating security risks, they are not infallible for a Web3 project. Continuous vigilance, regular updates to audit scopes, and a multi-audit approach are critical for ensuring the ongoing security of Web3 projects.

# Conclusions

In summary, the first quarter of 2024 witnessed significant security challenges in the crypto space, with $824 million lost due to hacking incidents. Despite this, the recovery of 54% of stolen funds reflects a notable improvement in incident response within the Web3 space, signaling a growing commitment to enhancing security measures. However, with projected losses from hacks and exploits expected to exceed $3 billion if not addressed, there is an urgent need to act quickly. The increase in hacking incidents compared to previous years can be attributed to various factors, including the current bull market sentiment and the emergence of vulnerable protocols in under-discovered verticals.

Moving forward, prioritizing security and fostering collaboration is crucial for building a resilient Web3 ecosystem and mitigating future risks. The rise in targeted attacks against tokens, lending platforms, and bridges emphasizes the urgent need for decentralized and resilient governance and operational frameworks.

## Recommendations for Strengthening Web3 Security:

- Complement Audits with Comprehensive Measures: While audits are crucial, they offer only a snapshot of your system for a given date. To enhance resilience, Web3 projects should conduct audits on a regular basis and combine them with security assessments, on-chain monitoring, and bug bounty programs.

- Prioritize Continuous Security Practices: Educating Web3 builders on secure coding and fostering a security culture are vital for mitigating risks beyond audits. Continuous collaboration between developers and security teams ensures ongoing vigilance.

- Embed Security Across Teams: Security should be integral to the builder's mindset, extending beyond isolated systems to encompass cross-chain interactions, wallet security, and dependency codebases.

## Sources used for numbers and statistics:

- de.fi/rekt-database
- quillaudits.com/tools/quillmonitor
- neptunemutual.com/hack-database/
- defillama.com/hacks
- twitter.com
- @Certik, @Cyvers & @h3idilao

HACKEN

Blockchain Security Auditor

# We Make Web3 A Safer Place



| | | |
|---|---|---|
| **6**<br>Years of expertise | **1,000+**<br>Clients | **180+**<br>Partners |
| **1,500+**<br>Audited projects | **50+**<br>Crypto exchanges | **100+**<br>Team members |

HACKEN.AI | TRUST ARMY | EXTRACTOR | HACKEN PROOF