HACKEN

The Hacken 2024 Web3 Security Report

Unveiling key insights into crypto hacks, scams, and security best practices

hacken.io

Web3 Security Highlights in 2024

1. Access control exploits caused nearly $1.7 billion in losses, accounting for 78% of all crypto hacks – a sharp rise from 50% in 2023.

2. DeFi losses dropped by 40% compared to 2023, while CeFi losses more than doubled.

3. Phishing schemes led to an estimated $600 million in losses, with a notable surge in presale scams and celebrity-endorsed rug pulls.

4. Gaming and metaverse platforms represented 18% of Web3 hack-related losses.

5. Bridge hacks declined for the second consecutive year, showing a 94% drop from 2022 and a 70% drop from 2023.

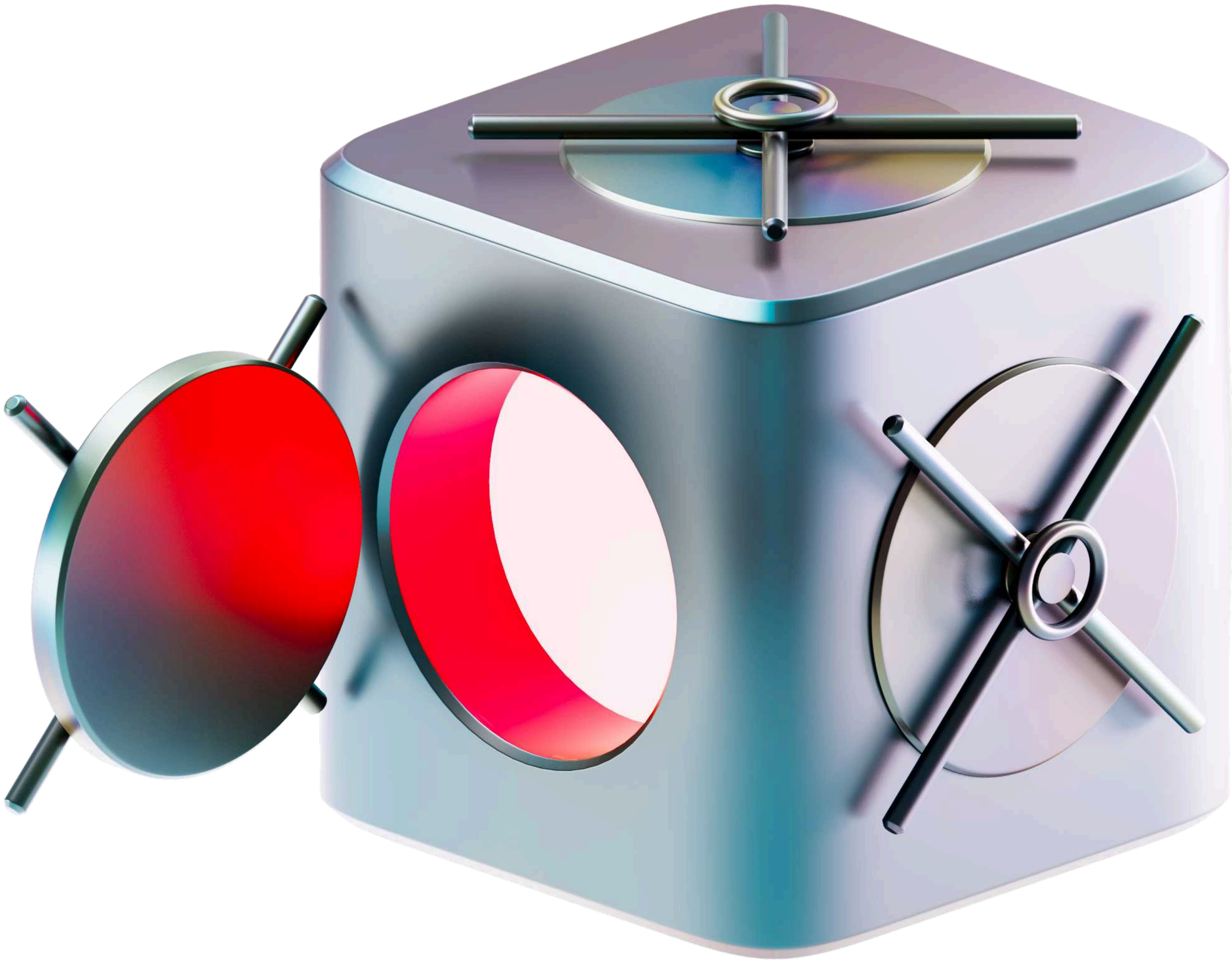
6. Solana has emerged as a hub for rugpulls, primarily driven by memecoins.

Introduction

2024 was another year of challenges and lessons for blockchain security. While the total losses from crypto hacks remained relatively stable compared to 2023 standing at more than $2.3 billion excluding phishing – the breakdown of exploit types reveals new and recurring vulnerabilities.

Access control exploits emerged as the single largest threat, accounting for 75% of all crypto hack losses (excluding phishing). This trend spanned across DeFi, CeFi, and gaming/metaverse platforms, highlighting dominance of the vulnerabilities regarding operational security and access management.

The data was collected from official resources of Web3 projects, including platforms like X, post-mortems, and aggregated databases of Web3 hacks, such as De.Fi Rekt Database and DefiLlama. Information on phishing-related losses was primarily sourced from ScamSniffer reports. Each entry was independently verified and validated by the Hacken Research Team to ensure accuracy and reliability.



Key Trends in Crypto Hacks

Access Control exploits dominance

Access control vulnerabilities were responsible for 75% of crypto hack losses, excluding phishing, across all sectors—DeFi, CeFi, and gaming/ metaverse. This highlights a pressing need for enhanced key management and operational security practices.

DeFi vs. CeFi trends

DeFi losses accounted for 20.4% of total crypto hack losses, while CeFi losses made up 30%. However, both sectors were heavily impacted by access control vulnerabilities, with nearly 50% of DeFi losses tied to this exploit type

Gaming & Metaverse hacks

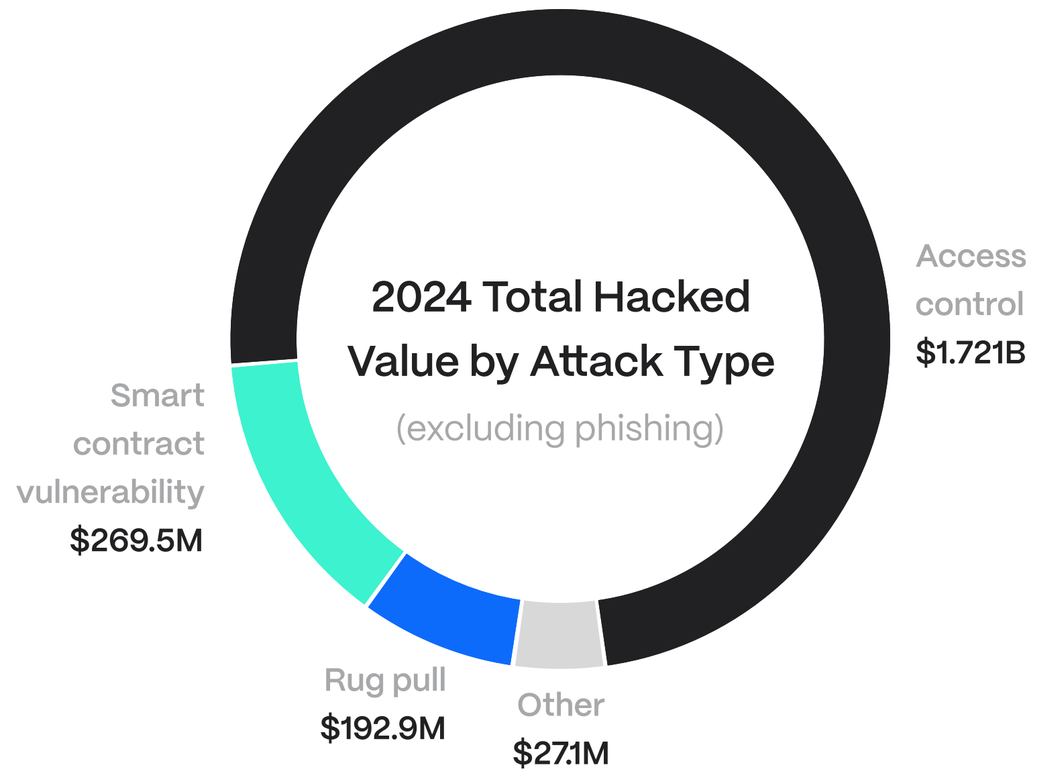
Gaming and metaverse platforms represented 21% of total losses, driven mainly by the $290 million PlayDapp hack back in Q1. This sector demonstrated a mix of traditional exploit methods and evolving vulnerabilities.

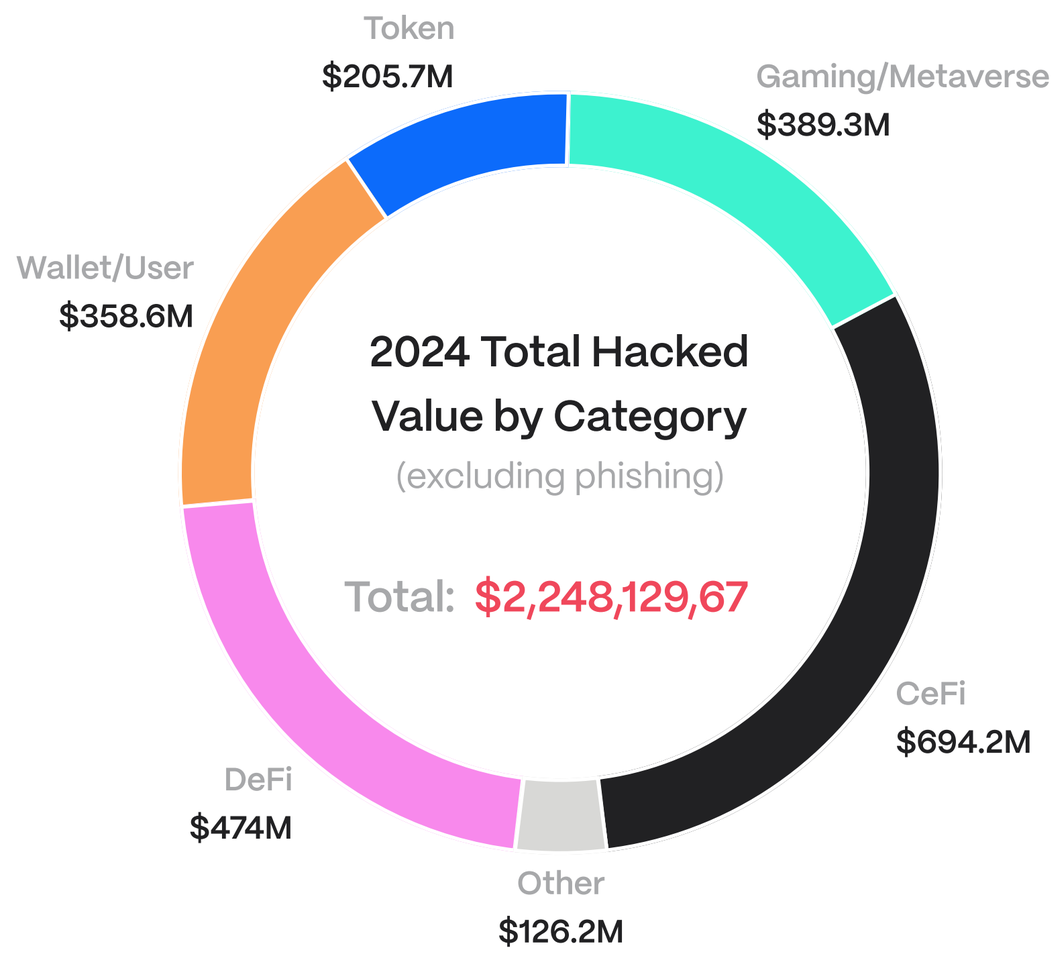
Bridges kept tendency to be more reliable

Bridge-related losses declined significantly to $117 million, down from $330 million in 2023 and $1.9 billion in 2022, reflecting improved security measures in cross-chain protocols.

Operational security concerns

Number of DNS hijacking was increased, underscoring the need for Web3 projects to prioritize broader security measures beyond on-chain protections.



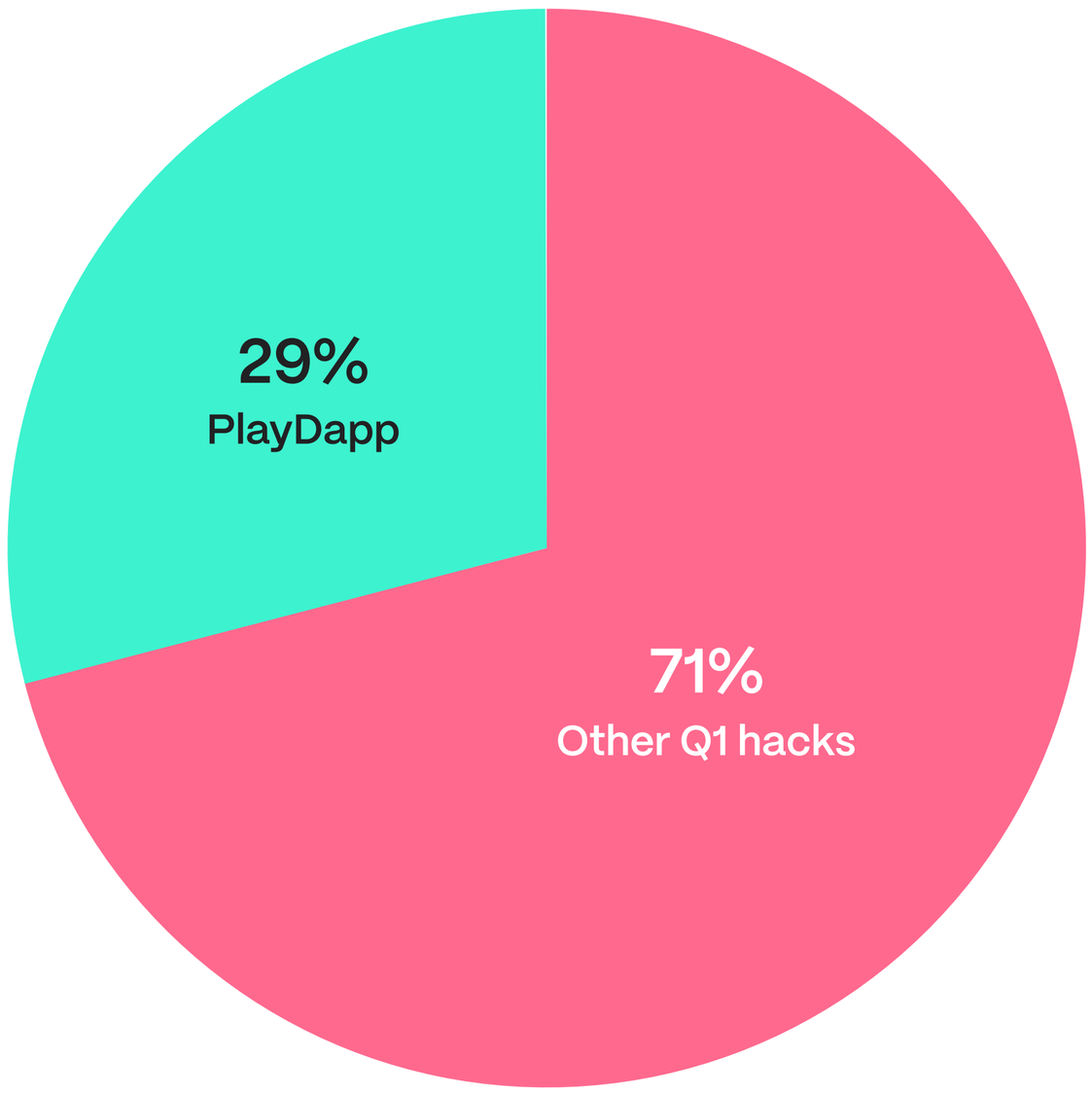


Year In Review: Biggest Rekt of Each Quarter

Let's uncover the key vulnerabilities exploited by attackers in the biggest hacks of 2024.

Quarter 1:

Total rekt	1 billion
Biggest hack	$290M – PlayDapp (Gaming/Metaverse)



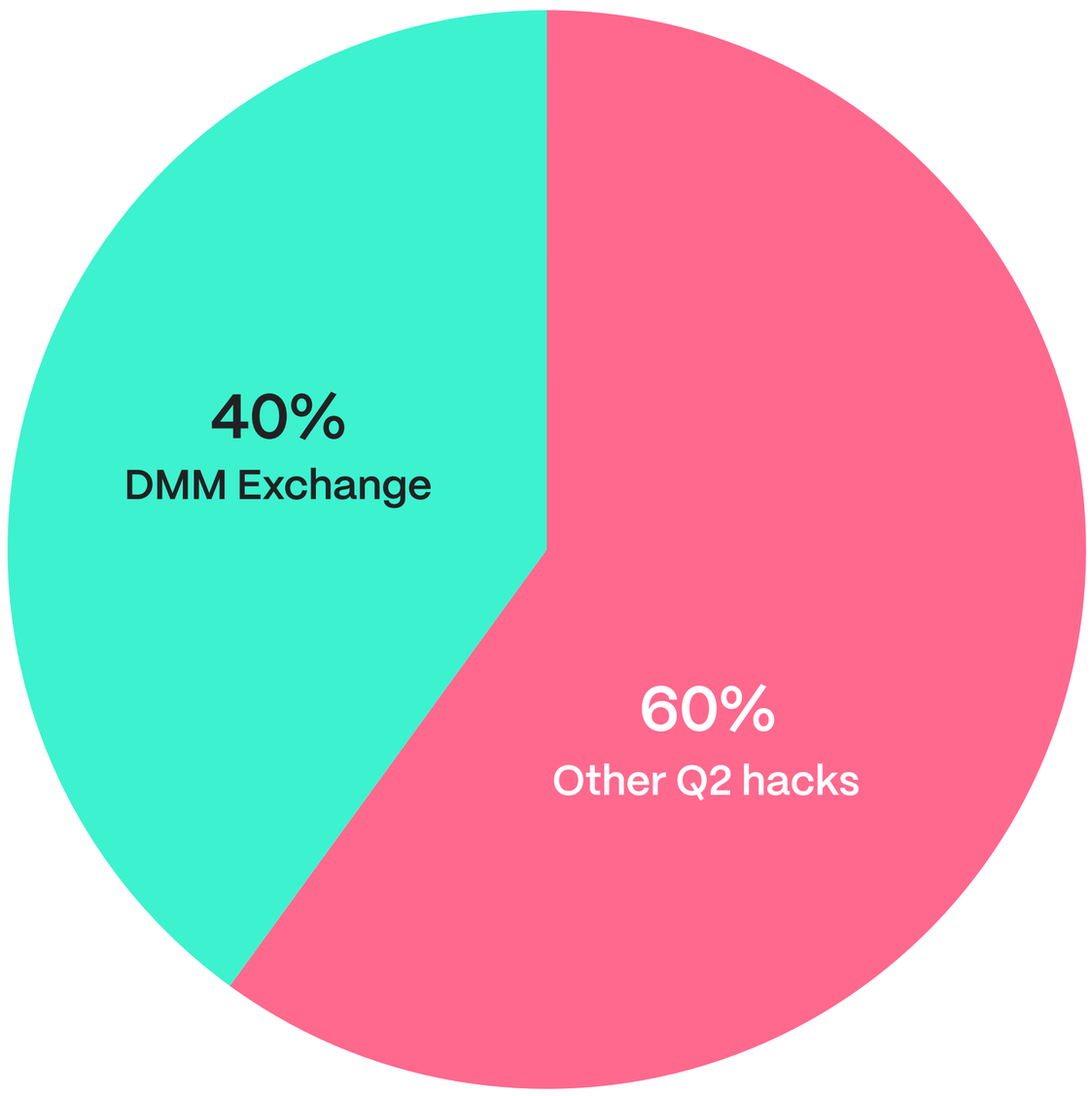
PlayDapp hack explained:

In February 2024, PlayDapp was hacked due to an access control vulnerability that allowed the attacker to make themselves a token minter. Over two attacks, they minted 1.8 billion PLA tokens worth $290 million, devaluing the token and causing massive losses.

PlayDapp froze tokens on exchanges, paused the vulnerable contract, and prepared for a token migration to mitigate the impact.

Quarter 2:

Total rekt	762.5 million
Biggest hack	$304M – DMM Exchange (CEX)



DMM Exchange hack explained:

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.

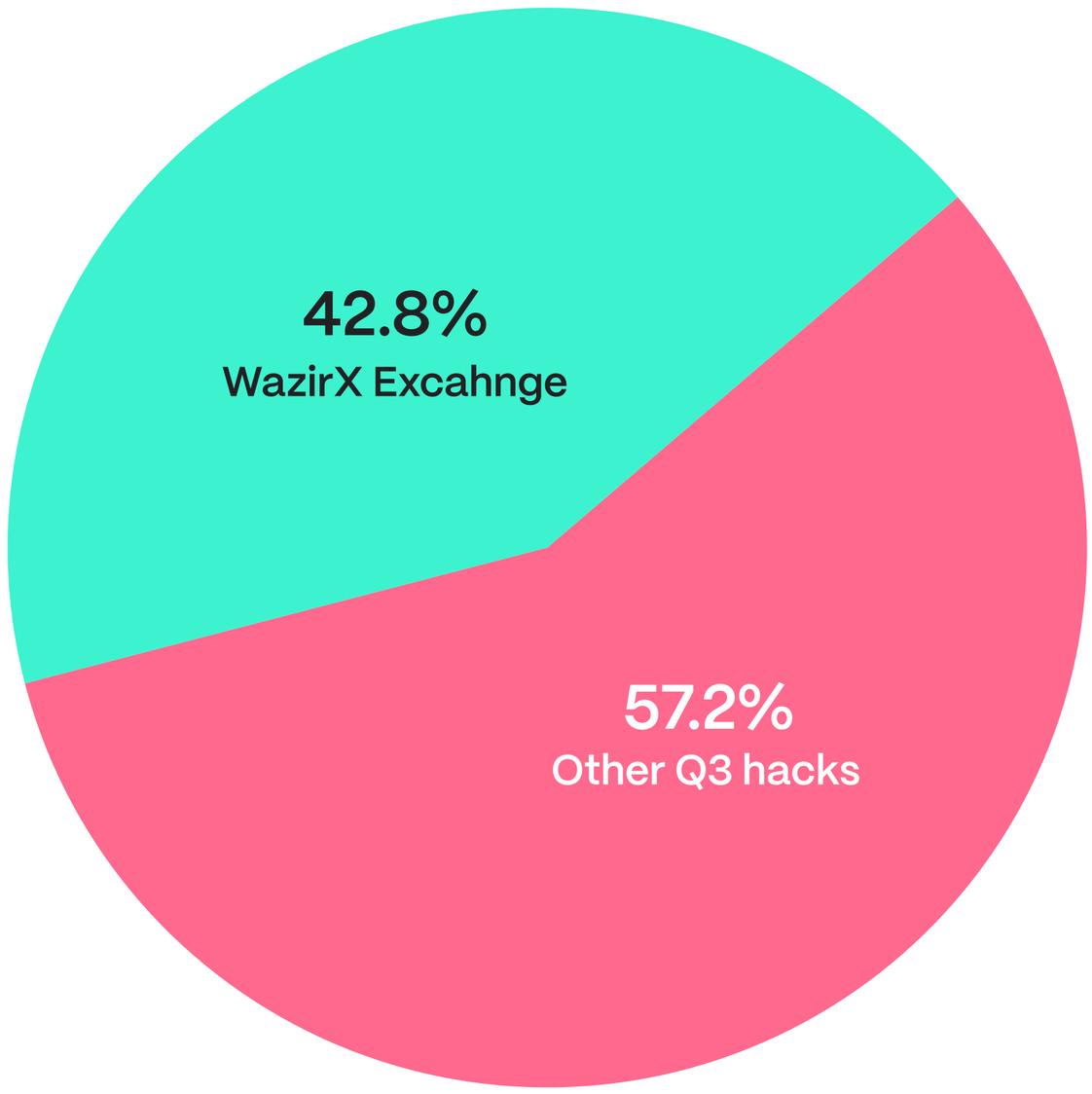
The hack involved a large transfer of 4502.9 BTC to an unknown wallet, followed by redistribution to multiple addresses. Potential causes include compromised private keys, signing processes, or address poisoning.

The incident highlights the need for robust security measures like multi-signature wallets, cold storage, and decentralization of funds to protect against such highvalue breaches.

In Hacken's Web3 2024 Q2 security report, we have not reported the losses from Solana Pre-sales scams, which occurred in April, as there was not enough data to state about that incident at the moment. In our current 2024 yearly report, we added $122.5m pre-sale scams to total Q2 losses.

Quarter 3:

Total rekt	538 million
Biggest hack	$230M – WazirX Exchange (CEX)



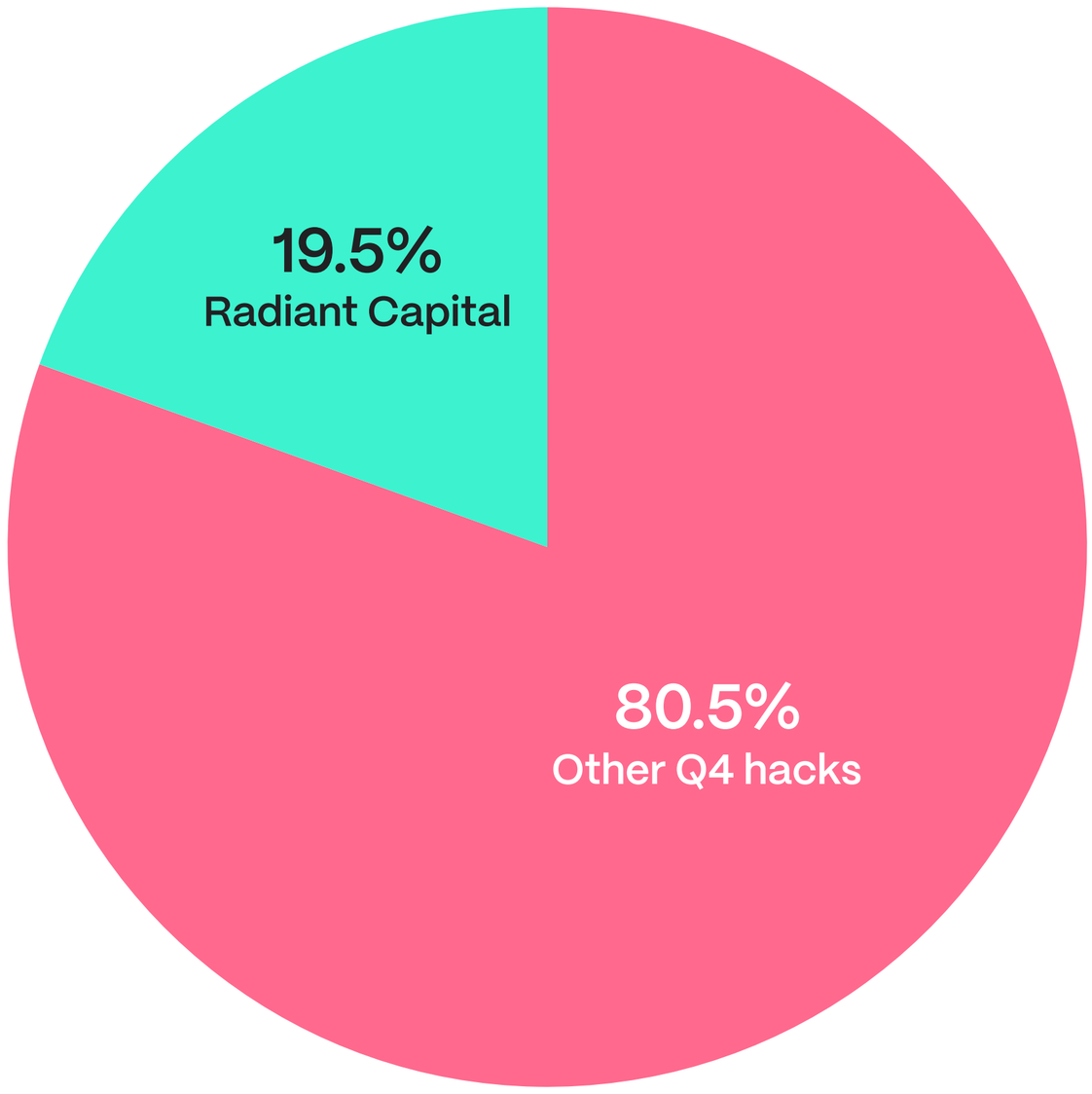
WazirX Exchange hack explained:

Despite employing a robust multiparty security system, the exchange suffered a breach due to unauthorized fund movements from their wallets. WazirX utilized a Gnosis Safe multisig wallet requiring 4 out of 6 signatures for transactions. Five of the keys were managed by WazirX, while the sixth was held by Liminal, a digital asset custody provider.

The attacker managed to manipulate the system, obtaining signatures from three WazirX signers and one from Liminal, allowing them to upgrade the wallet to a malicious contract and siphon off the funds.

Quarter 4:

Total rekt	282 million
Biggest hack	$55M – Radiant Capital (Lending and Borrowing)



Radiant Capital hack explained

Radiant Capital experienced a $55M security breach involving malware injected into developer devices, enabling attackers 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.

Access Control Exploits: The Dominant Threat of the Year

Private key theft remains the most significant security threat year after year. In 2024, access control exploits—closely tied to private key compromises—accounted for nearly 75% of total crypto hack losses, up from 50% in 2023. This translates to nearly $1.7 billion lost across Web3, a sharp increase from less than $1 billion the previous year.

In comparison, smart contract vulnerability exploits contributed just 14% of the total losses in 2024, underscoring the dominant threat posed by unauthorized access and private key theft.

Even more concerning is the fact that access control attacks consistently ranked as the dominant threat across every category of Web3, underscoring their pervasive threat for every project.

- ### CeFi

  The largest hack of the year was in CeFi, caused by access control vulnerabilities. Most damages from access control hacks occurred in centralized exchanges, with DMM Exchange and WazirX being the most significant incidents, resulting in combined losses of over $500 million.

- ### DeFi

  In addition to immediate financial damage, access control exploits in DeFi also led to smart contract management compromises.

  The Radiant Capital $55M incident affected nearly 10,000 victims due to infinite token approvals, resulting in ongoing unauthorized fund transfers. New victims continue to emerge daily on both Arbitrum and BNB Chain, where the exploit occurred.

- ### Gaming/Metaverse

  This sector was heavily impacted by access control vulnerabilities, with the PlayDapp exploit ($290M) being the most damaging hack in Q1.

Why Does It Keep Happenning – Private Key Compromise

Insecure private key management platforms

Victims often relied on third-party private key management services that lacked robust security practices. Some platforms stored keys in centralized systems without proper encryption or distributed storage, creating a single high-value target for attackers.

Single-signature vulnerabilities

Many wallets and platforms used simple single-signature schemes, turning them into a single point of failure. In one notable DeFi case, a compromised private key allowed an attacker to drain millions in assets without requiring any additional approvals.

Social engineering attacks

Attackers frequently impersonated wallet providers or support teams, tricking users into revealing their private keys or seed phrases. The success of these scams often came down to inadequate user education and the absence of clear verification methods to authenticate legitimate communication channels.

Insecure backups

Private key backups were often stored in unsecured environments, such as unencrypted cloud drives or poorly protected physical locations. Attackers who gained access to these backups were able to swiftly compromise associated wallets.

How Can Businesses Protect Their Private Keys

This surge in access control exploits across all sectors underscores the urgent need for robust operational security, stricter access management protocols, enhanced multisig management, and Automated Incident Response Strategies. In parallel, organizations and individuals must place greater emphasis on private key security, considering more robust standards and guidelines to mitigate the underlying issues.

Adopting the Cryptocurrency Security Standard (CCSS) provides a structured approach to these challenges. CCSS recommendations include multi-layered security measures, periodic security audits, and stringent access control guidelines. By adhering to CCSS, organizations can better protect the generation, storage, and management of private keys, ultimately reducing the frequency and severity of Access Control-related breaches.

whitebit Achieves CCSS Level 3 Certification with Hacken

The CCSS has become the benchmark for securing cryptocurrency systems, offering a robust framework for exchanges, applications, and custody solutions. Designed to complement existing standards like ISO 27001, CCSS introduces best practices tailored for the unique requirements of cryptocurrencies, ensuring resilience and trust across digital asset platforms.

In 2024, WhiteBIT, one of Europe's leading crypto exchanges, achieved CCSS Level 3 certification—the highest level of compliance—through an extensive audit conducted by Hacken. This rigorous process included an evaluation of 41 aspect controls critical to cryptocurrency security.

In an environment where Access Control failures now drive the majority of crypto-related losses, addressing the root cause—particularly private key compromise—offers a clearer path to security and stability across the blockchain ecosystem.

DeFi 2024 Losses: Trends and Key Highlights

This year, the DeFi sector witnessed a reduction in losses compared to 2023, most notably thanks to more secure bridges. While 2023 recorded $787 million in total DeFi losses, 2024 saw this amount decrease to $474 million, marking a 40% reduction.

	2023	2024
Smart contract vulnerabilties	$448M	$255M
Access control exploits	$339M	$219M
Total	$787M	$474M

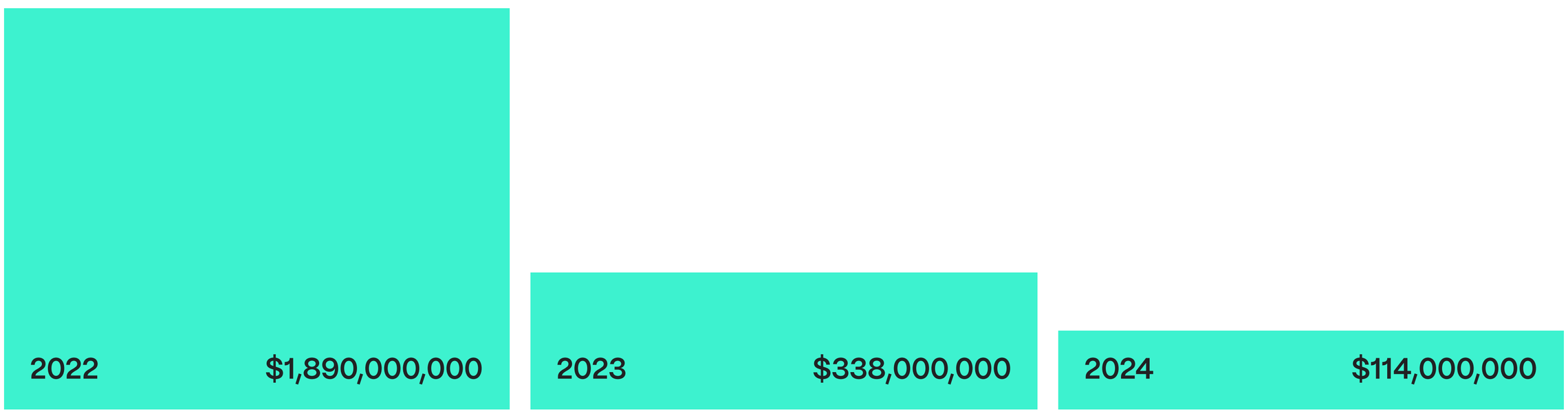
DeFi Hacks in 2023 vs 2024

Cross-Chain Operability Got More Resilient

The reduction in bridge exploit losses played a key role in the overall decline of DeFi-related losses.

The total value stolen from bridges dropped from 1.89 billion in 2022, $338 million in 2023 to just $114 million in 2024. Bridges—historically top target for hackers—show significant improvement in terms of security.

In fact, bridge attacks have become less impactful. They are targeted less, and bridge developers increasingly integrate Multi-Party Computation (MPC) and Zero-Knowledge (ZK) cryptography.



Bridges losses over the years

Exploring DeFi Hacks by Attack Types

	Q1	Q2	Q3	Q4	Total
Smart contract vulnerabilties	$66,279,706	$93,800,000	$77,426,000	$17,090,000	$254,595,706
Access control exploits	$114,845,989	$28,500,000	$12,700,000	$63,220,000	$219,265,989

Access control issues, particularly the loss of private keys by team members at any level, remain a critical concern in the broader Web3 environment. Two of the largest DeFi hacks in 2024 were caused by access control vulnerabilities:

Radiant Capital

$55 million stolen, impacting 10,000 users due to infinite token approval issues.

Orbit Bridge

$80 million stolen, marking the largest DeFi hack of the year.

Smart contract hacks encompass reentrancy attacks, general vulnerabilities, flash loan exploits, and oracle issues. Losses from smart contract vulnerabilities totaled $255 million in 2024, a significant improvement from $448 million in 2023.

This reduction is largely attributed to the growing adoption of rigorous security audits and bug bounty programs, which are increasingly becoming standard components of DeFi project security roadmaps. However, critical vulnerabilities in smart contracts persist, with reentrancy attacks identified as the leading threat. The most significant exploit in 2024 was a $27 million reentrancy attack on the Penpie protocol.

How Can DeFi Projects Improve Their Security

Excluding bridge-related incidents, loss figures for 2023 and 2024 are relatively comparable.

To address ongoing vulnerabilities, the Cryptocurrency Security Standard (CCSS) provides a comprehensive framework to mitigate risks, including:

- **DRBG Compliance (1.01.3)**

  Ensuring secure cryptographic key generation

- **Key Storage (1.03)**

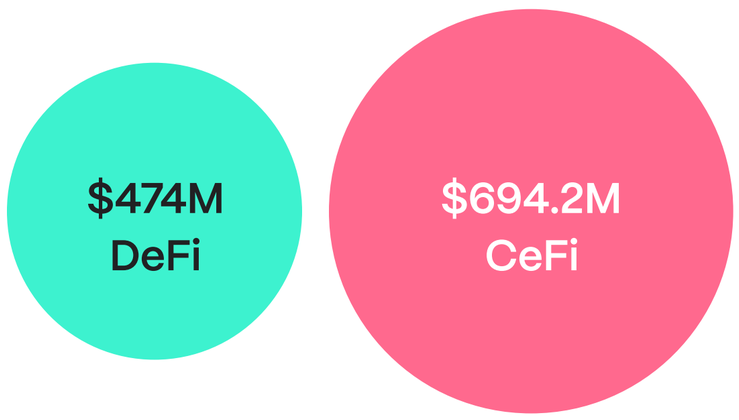
  Enforcing encrypted storage and restricted access to primary keys.

- **Multi-signature schemes and distributed key management**

  Reducing reliance on a single point of control and strengthening overall system resilience.

By implementing these controls, DeFi projects can significantly enhance their security posture and mitigate risks associated with both access control and smart contract vulnerabilities.

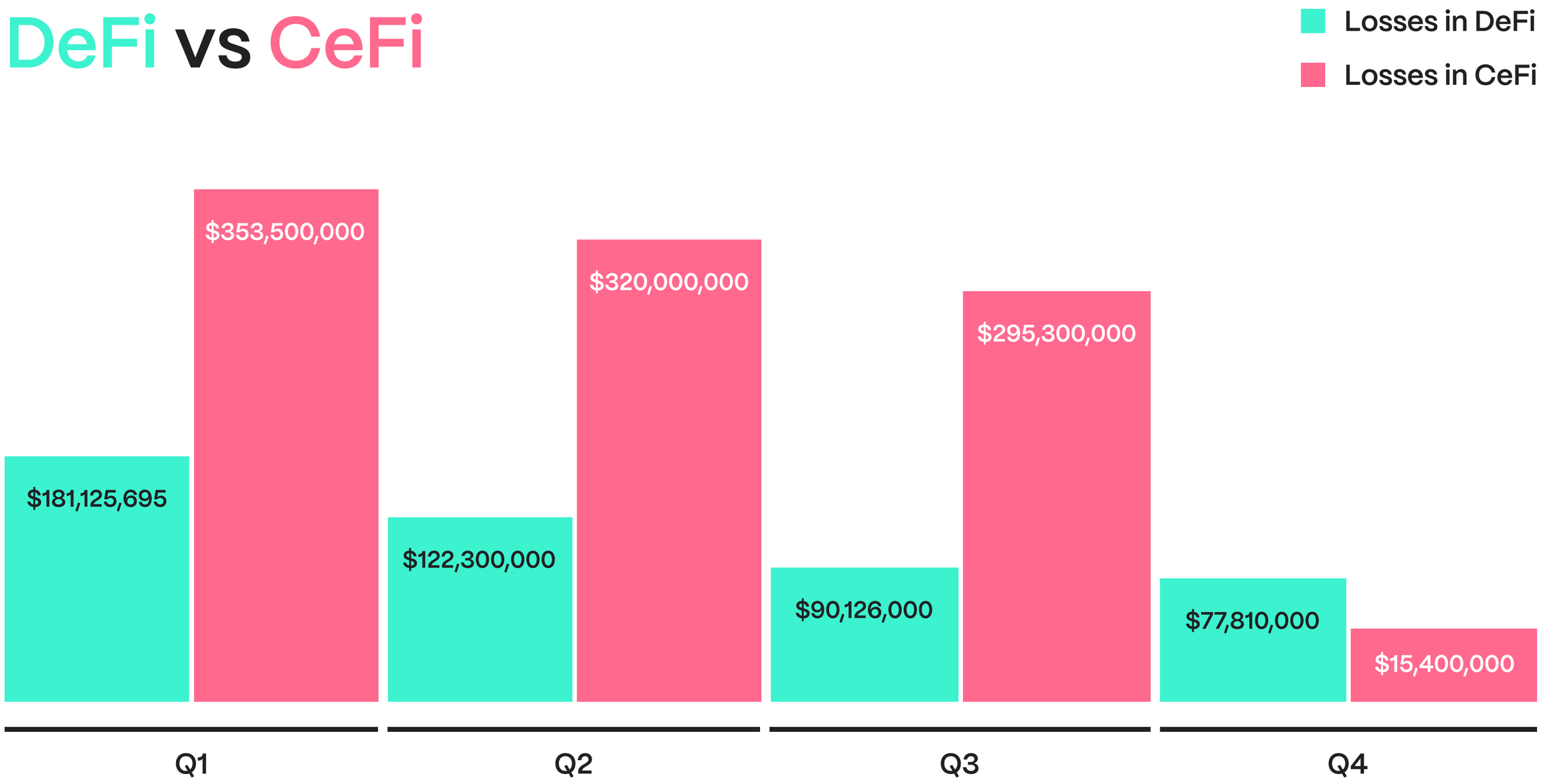
DeFi Got Safer, While CEXs Faced Challenges



DeFi vs CeFi Hacks in 2024

In 2024, the crypto security landscape highlighted a stark contrast between DeFi and CeFi trends. DeFi losses decreased significantly, from $787 million in 2023 to $474 million this year, marking a 40% decline. This improvement reflects the growing adoption of advanced security techniques like zk cryptography and MPC, especially in bridge development.

DeFi vs CeFi



On the other hand, CeFi losses surged dramatically, more than doubling from $339 million in 2023 to $694 million in 2024, accounting for nearly a third of all crypto incidents that year.

Breaches predominately originated from centralized exchanges and were overwhelmingly linked to access control exploits, exposing critical gaps in operational security practices.

Gaming and Metaverse Hacks

In 2024, gaming and metaverse projects experienced significant losses, totaling $389 million, or nearly 20% of all crypto hacks. Most stemmed from access control exploits.

The largest rekt in this category was the PlayDapp exploit in Q1, where attackers gained unauthorized minting rights to steal $290 million. This stands as the biggest gaming/metaverse hack of the year. Two other prominent hacks occurred on the Blast L2, a platform that was gaining traction in Q1:

Munchables Exploit	$62.5 million (Access Control)
Super Sushi Samurai Exploit	$5 million (Access Control)

Together, these three cases account for 358 million, or more than 80% of all gaming/metaverse losses in 2024. The concentration of losses in Q1 highlights the sector's struggles with securing access management, especially on newer ecosystems like Blast, which also faced several rugpulls.

Protecting Web3 Gamers

Proper access control can be ensured through the Cryptocurrency Security Standard (CCSS), which mitigates risks like insecure key generation, inadequate key storage, and weak multi-signature or distributed key management.

$600M Lost in Phishing – How to Protect Yourself?

Phishing scams resulted in over $600 million in losses this year, shoshowcasing the growing sophistication of social engineering attacks in the Web3 space. This includes an absurd $129 million address poisoning attack in November. While in this case the stolen funds were later recovered, most incidents go unreported, let alone resolved, highlighting the pervasive and critical risks phishing schemes pose to the Web3 ecosystem.

Address Poisoning on Tron Blockchain

On Nov 13, a Web3 user have fallen to an address poisoning phishing scam, transferring 129.6M USDT to the scammer's address.

User's address **TMStAjRQHDZ8b3dyXPjBv9CNR3ce 6q1bu8**

Scammer's address **THcTxQi3N8wQ13fwntF7a3M88BEi 6q1bu8**

In the address poisoning attack, the attacker generated a malicious address with the same last characters as the victim's legitimate address. The attacker sent small, irrelevant transactions (e.g., 1 USDT) to the victim's address, creating a false transaction history in the victim's wallet. When the victim mistakenly used the fake address to send funds, the money was gone.

Most Dangerous Scams of 2024

Fake Airdrops and Links

Scammers created fake X accounts or compromised legitimate ones to post fraudulent links to airdrops. Victims who interacted with these links often unknowingly approved token transfers, allowing attackers to drain their wallets.

Permit Exploits

In some phishing schemes, victims were prompted to sign transactions granting token approvals through malicious smart contracts. Attackers leveraged these approvals to drain funds.

How to Protect Yourself From Crypto Scams?

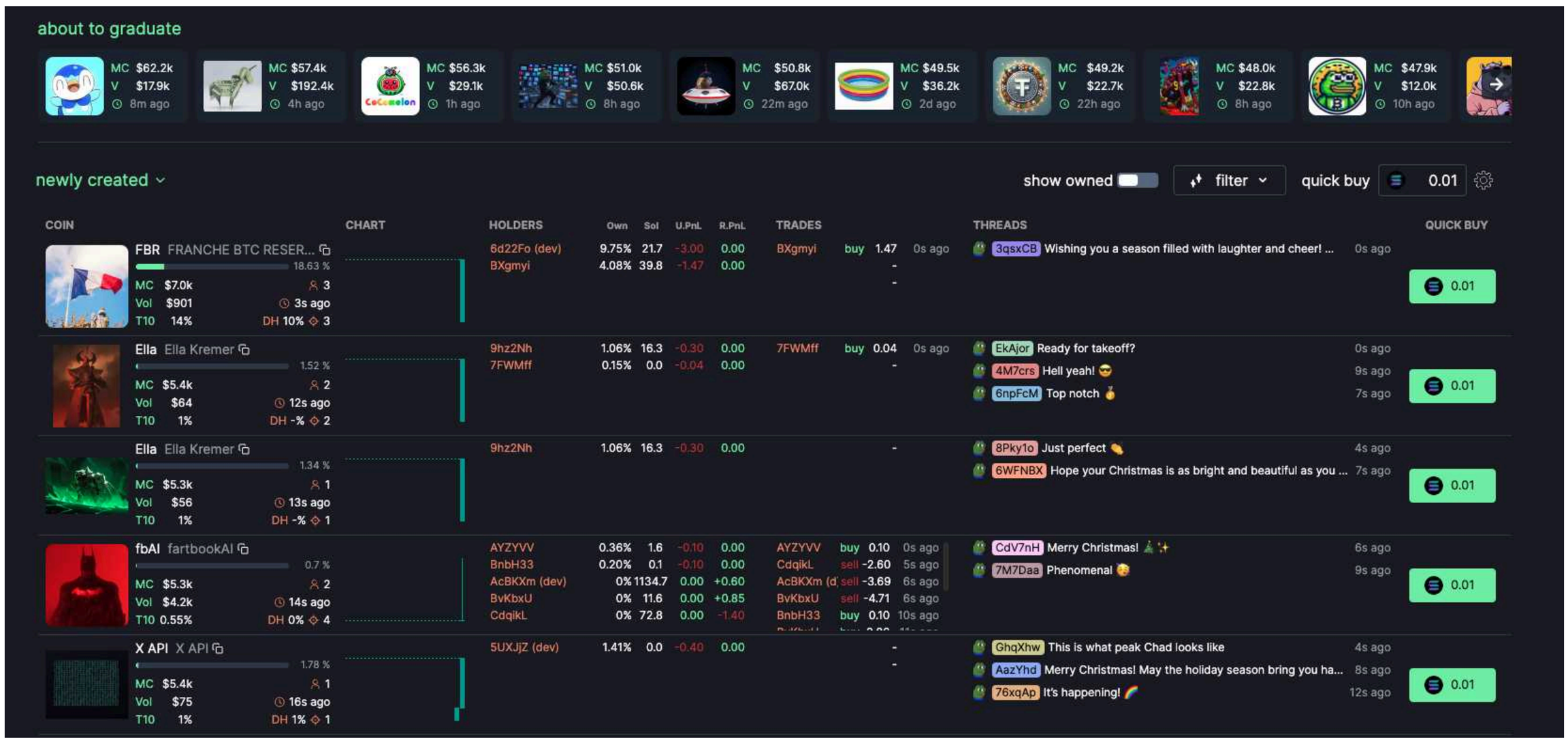
- Always double-check addresses directly from your wallet or a trusted source, avoiding reliance on transaction history or clipboard entries.
- Never share your wallet's seed phrase or private keys. No legitimate service will ever ask for them.
- Avoid clicking links that claim to offer free tokens, especially on social media. Always verify such claims through official channels.
- Ensure you're using official wallet apps and browser extensions.

Memecoins and Rugpulls

Rugpulls remain a significant issue in the crypto space, with their patterns evolving noticeably over the past year. On BNB Chain, the number of rugpulls has dropped significantly, from nearly 150 reported cases in 2023 to just 10 this year. This decline reflects the evolving methods of malicious actors to adapt to trends and benefit from them. Thus, Solana has emerged as a hub for rugpulls, primarily driven by meme coins.

pump.fun not so fun

On Solana, over 4 million tokens were created via tools like pump.fun, enabling anyone to launch tokens with minimal effort.



Memecoin rug pulls on Solana typically involve developers controlling large portions of a token's supply while users supply $SOL to liquidity pools in exchange for memecoins. Developers quickly dump their holdings, draining the liquidity pool and leaving investors with worthless tokens.

Facilitated by Solana's low transaction fees and high-speed network, these schemes are executed rapidly, often within minutes or hours. While individual amounts may be relatively small, the aggregated impact on investors has been significant, highlighting the risks associated with speculative token markets.

Presale Scams

One notable trend this year has been presale scams. According to crypto investigator ZachXBT, 27 presale scams tied to Solana meme coins siphoned over $122.5 million back in April 2024, making this a significant contributor to the ecosystem's losses.

Celebrity-Endorsed Scams

Celebrity-backed rugpulls have also marked 2024, particularly in the first half of the year. These tokens exploited the names and influence of public figures to inflate value before rugging.

HAWK Token

In early December 2024, Haliey Welch, known as the "Hawk Tuah Girl", launched a memecoin cryptocurrency HAWK on the Solana blockchain.

The token's market capitalization surged to approximately $490 million shortly after its release but plummeted by over 90% within hours, leading to investor losses and allegations of a rug pull.

Derulo Token

In June 2024, pop star Jason Derulo promoted a meme coin named "JASON" to his 3.5 million followers on social media platform X (formerly Twitter).

Shortly after its launch, the coin's value decreased by over 70%, leading to investor losses and allegations of a rug pull.

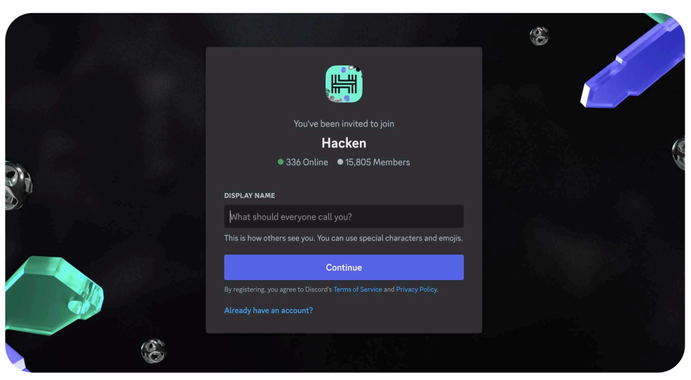
Jenner Token

In May 2024, Caitlyn Jenner launched the "JENNER" meme coin on the Solana blockchain.

The token's value plunged by over 65% shortly after its release, resulting in investor losses and accusations of a rug pull.

The prevalence of memecoin rugpulls and celebrity-endorsed scams highlights the evolving nature of crypto fraud. While traditional rugpulls often relied on more elaborate schemes, these new tactics leverage social influence and the accessibility of blockchain tools to scam Web3 users. The rise of such scams underscores the critical need for better investor education in order to understand the risks possessed with trading memecoins.

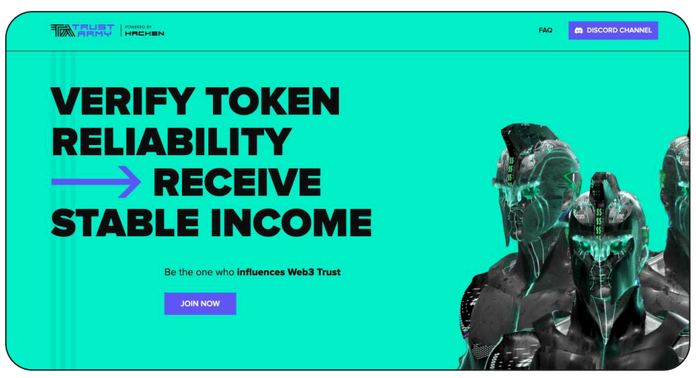
Empowering Crypto Users To Tackle Fraud



Join HAI Discord Community

Stay informed about the latest scams, fraud tactics, and best practices to safeguard your investments. Learn how to conduct thorough due diligence before trading memecoins or engaging with blockchain projects.

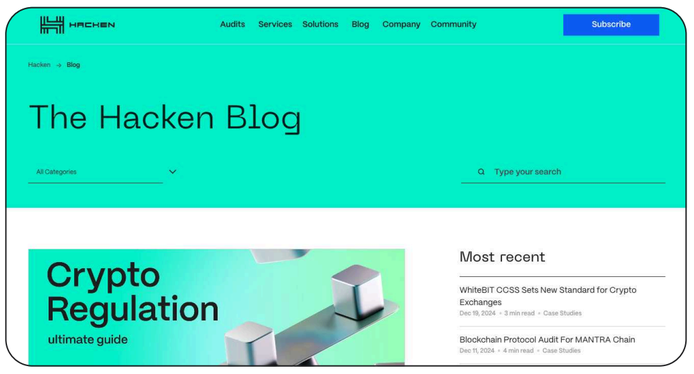
discord.gg/hacken →



Join the Trust Army

Become a watchdog for the crypto ecosystem. By joining Hacken's Trust Army, you can contribute to identifying fraudulent activities and promoting transparency in the Web3 space.

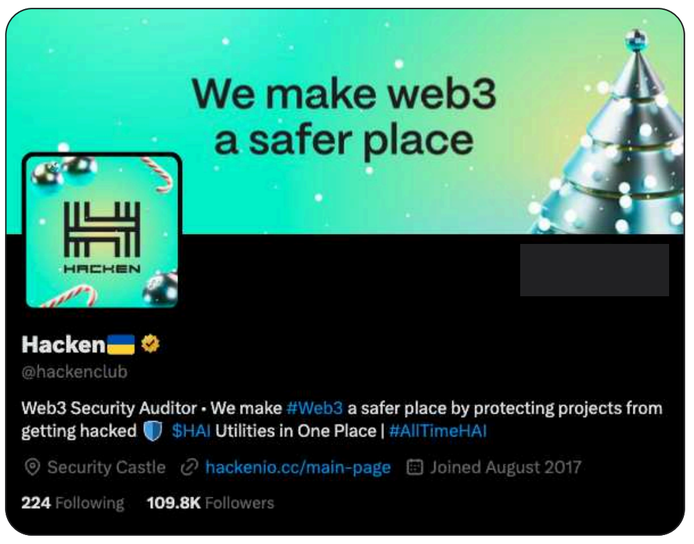
trustarmy.com →



Access Educational Resources

Explore Hacken's tools and resources to better understand the risks associated with speculative tokens like memecoins. Educating yourself is the first line of defense against evolving crypto fraud tactics.

hacken.io/research →



Support a Safer Web3

Collaborate with security-focusd community to advocate for stronger standards and practices in crypto security. Your participation can drive a more trustworthy and transparent blockchain ecosystem.

x.com/hackenclub →

These educational initiatives help crypto investors navigate the evolving crypto landscape with confidence while contributing to the fight against fraud and scams.

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 newsletter 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