HACKEN

The Hacken 2025 Q1 Web3 Security Report

$2B Lost in 90 Days: Understanding What Went Wrong and What Comes Next

hacken.io

Web3 Security Highlights In 2025 Q1

1. $2 billion stolen in Web3 security incidents in Q1 2025 – a 96% increase from Q1 2024.

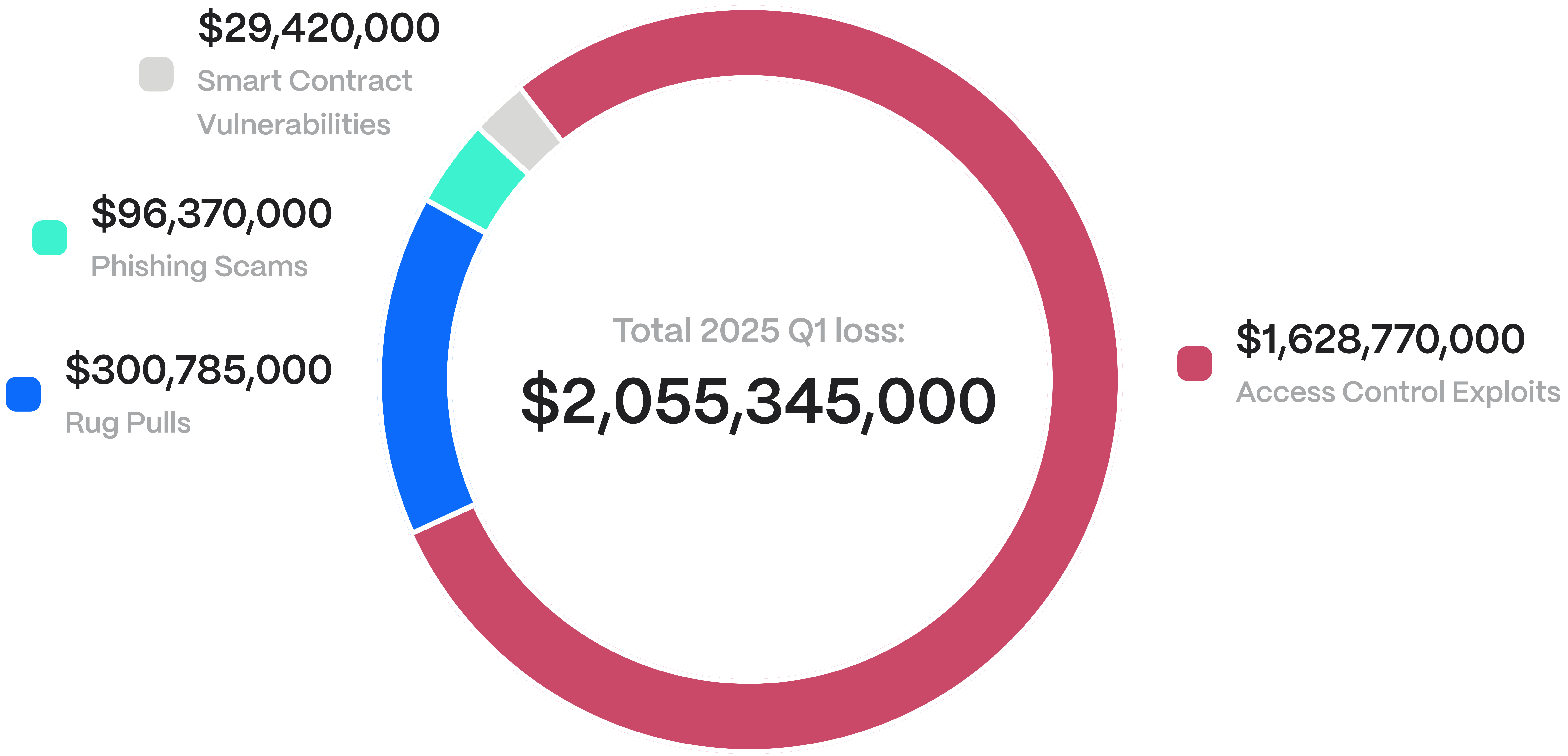
2. The biggest hack in the history recorded – Bybit $1.46 billion access control exploit.

3. Access control exploits were the dominant hack with 80% of the total value stolen.

4. Three consecutive quarters have seen the largest exploits originate from compromised multisig wallets, all involving Safe wallets.

5. Smart contract vulnerabilities accounted for $30 million, just under 2% of total loss.

6. The $LIBRA rug pull, involving the Argentine President, drained $300 million from traders.



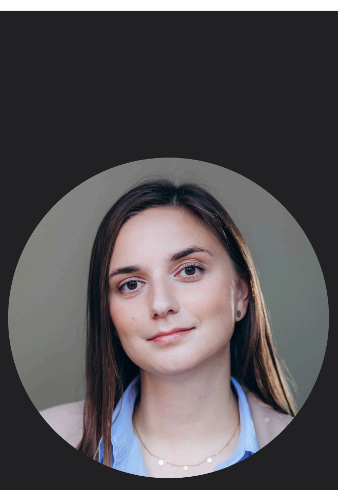
Introduction

The first quarter of 2025 saw continued attacks on the Web3 ecosystem, with even the biggest centralized and decentralized players falling victim to operational failures, access control weaknesses, and in a few cases, social engineering.

The most critical takeaway this quarter is not the rise of any new exploit technique, but rather the continued effectiveness of existing attack vectors – especially through the exploitation of multisig operational weaknesses.

While smart contract vulnerabilities remain a threat, most damage is now caused by failures in people, processes, or permission systems.

This report presents a categorized breakdown of the quarter's incidents, identifies trends, and highlights a growing need for operational maturity across protocols and CeFi platforms.



Yevheniia Broshevan

Hacken Co-Founder & CBDO

X linkedIn

"This quarter marks an alarming moment for the industry — $2 billion lost, driven mostly by operational failures, not smart contract bugs. The persistent pattern of multisig-related incidents show that access control and signer security must become the absolute priority for every serious Web3 project."

Key Trends In Crypto Hacks

HACKED

Q1 2025 was defined by a continuation of a dangerous trend: the largest and most damaging exploits continue to originate from compromised multisig-based operations.

The largest incident this quarter—and in history—was the Bybit hack, where signers were tricked into authorizing a malicious transaction via a compromised Safe{Wallet} frontend – resulting in a loss of $1.46 billion.

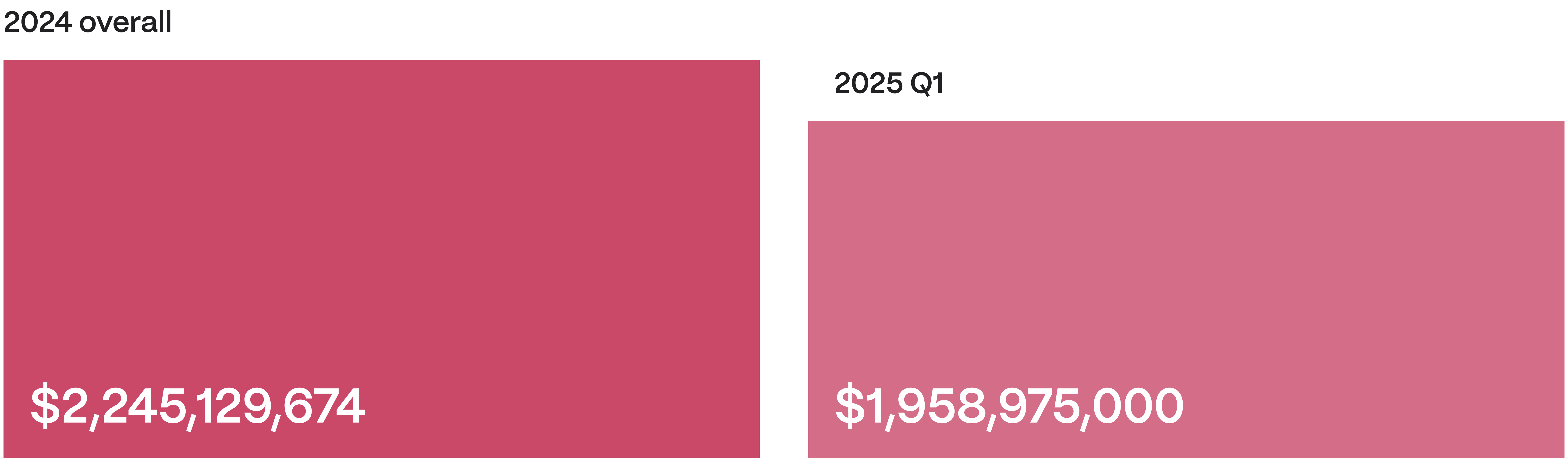
This marks the third straight quarter where the largest exploit was a multisig-related event, following Radiant Capital in Q4 2024 and WazirX in Q3 2024.

In total, $1.98 billion was stolen this quarter: almost an entire amount lost throughout 2024 ($2.25B).

- Access control failures make up the vast majority of hacks.
- Smart contract vulnerabilities caused only $29.4 million in losses.
- Phishing attacks and scams accounted for a considerable 5% share.

An unusually impactful rug pull tied to the politically-promoted $LIBRA token drew widespread attention, with estimated realized PnL of over $300 million by insiders. The token soared after being promoted by Argentina's president and collapsed shortly after insiders dumped their positions.

DeFi protocols lost a combined $81 million, in line with the decreasing trend over the past year. Key incidents included Infini ($50M, access control), zkLend ($9.6M, smart contract vulnerability on Starknet), and a social engineering attack on Ionic ($12.3M).

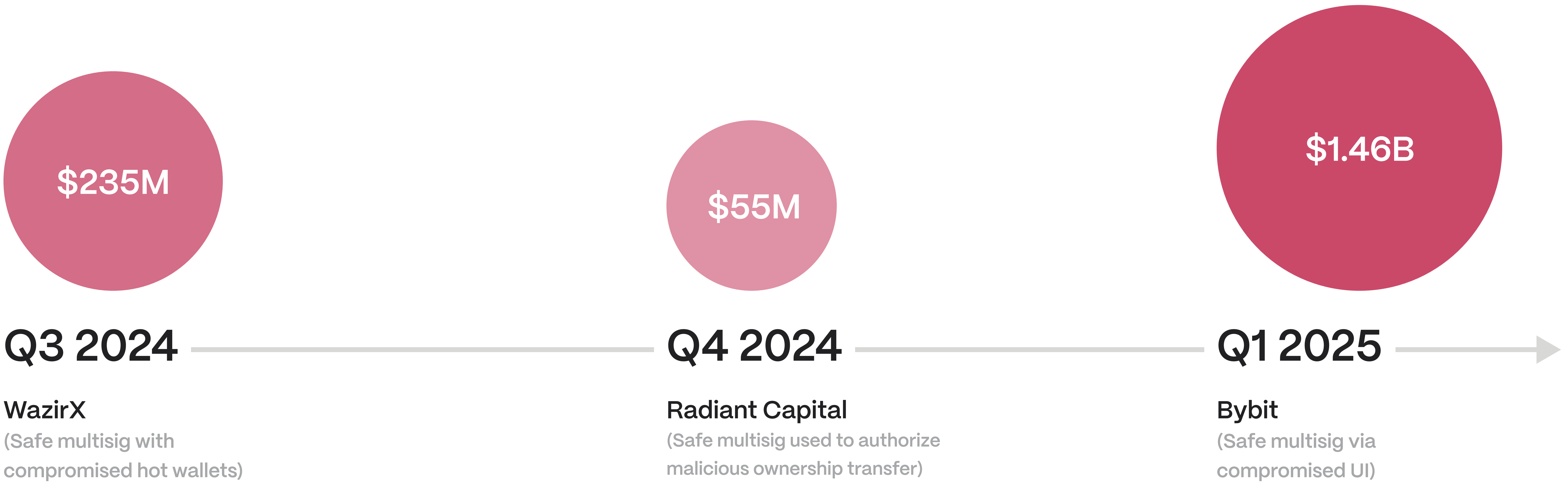


Total loss excluding Phishing

Multisig Failures – Three Quarters of Catastrophe

The largest exploit of Q1 2025 — the $1.46B Bybit hack — was a direct result of a compromised signer interface (Safe{Wallet}), allowing attackers to propose and propagate a malicious transaction. The malicious proposal manipulated the Safe's delegate call setup to seize control of the wallet.

This was not an isolated case. It marks the third straight quarter where the most damaging exploit stemmed from multisig usage:



Each of these relied on Safe multisig infrastructure. The commonality across cases is not a flaw in the Safe smart contracts themselves, but inadequate operational security, signer workflows, and transaction verification tools.

As protocols rely on multisigs for governance and fund control, these incidents highlight the urgent need for better signer tooling and alerting.

Hacken Recommends: Automated Incident Response

Learn more ↗

Hacken Extractor can automatically detect and prevent multisig exploits with its advanced Safe Multisig Monitor and TVL Monitor capabilities.

The Safe Multisig Monitor is purpose-built to track and validate transactions from Safe Multisig wallets, keeping a constant eye on key activities – retrieving signers, confirming signatures, and executing transactions. It verifies transaction hashes and signatures, flagging mismatches or anomalies with severity-based alerts.

A more reliable incident response solution designed to automatically trigger a built-in protection mechanism like instantly pausing the lending pool >

Together, these detectors form a vigilant frontline, catching Access Control threats as they emerge. But Extractor goes further with automated prevention: it can limit or pause outflows, transfer ownership to a secure contract, initiate key rotation, remove compromised signers, or reassign proxy admin rights – all in real time.

Lessons From Recent Multi-Sig Incidents

For three consecutive quarters, the largest exploits in Web3 have stemmed from multi-sig-related events. While this may give the impression that multi-sig wallets are a weak point, the reality is quite the opposite — multi-sigs are indispensable for Web3 stability. By contrast, this is a wake-up call to harden its design, implementation, and surrounding infrastructure.

What Is a Multi-Sig?

A multi-signature (multi-sig) wallet is a wallet that requires multiple private keys to authorize a transaction instead of relying on a single key. These keys can be distributed between devices, individuals (co-signers), or a combination of both.

Multi-sig wallets are commonly implemented through smart contracts, supporting flexible schemes such as 2-of-3, where two approvals out of three possible keys are needed for a transaction to be valid.

Why Is It Needed?

The core purpose is to separate responsibility, reduce single points of failure, and make unauthorized fund movements significantly harder. Multi-sigs are an essential component of Web3 security infrastructure, especially for projects managing large treasuries, operational funds, or protocol-governed assets.

If They Use Multi-Sig Wallets, Why Are Projects Still Getting Hacked?

While multi-sig wallets are widely trusted due to their reliance on smart contracts, they are not immune to threats. Vulnerabilities may not only stem from flaws in the smart contracts themselves but also from weaknesses in off-chain components and the operational security layer.

Bad actors continuously search for alternative attack vectors, aiming to exploit any weak link in the system. A notable example is the Bybit incident, where the Lazarus Group compromised the web interface used to manage the wallet.

Key lesson for Web3 projects

Securing digital assets requires more than just secure on-chain code — the entire infrastructure, from front-end interfaces to internal processes, must be equally hardened, as all it takes is a single weak spot to wreck the entire system.

Best Security Practices for Using Multi-Sig Wallets

- **Minimize smart contract complexity and attack surface**

  Use purpose-built multi-sig contracts tailored to your needs, supporting only essential operations (e.g., native and ERC-20 transfers) and avoiding unnecessary features like generic delegatecalls. This reduces the attack surface and simplifies auditing.

- **Implement human-readable signing**

  Adopt EIP-712 typed data signatures wherever possible. They allow signers to clearly see and verify the transaction details they are approving, reducing the risk of blind-signing malicious or unexpected payloads.

- **Secure off-chain components**

  The web interfaces, SDKs, and other tools used to interact with multi-sigs must be treated as part of the security perimeter. Implement safeguards such as JavaScript pinning, integrity checks, and supply chain security controls.

- **Use hardware wallets**

  Require signers to use hardware wallets that can display and verify EIP-712 messages directly. Even if a signer's computer is compromised, hardware wallets add an important layer of protection by exposing the actual data being signed.

- **Establish policy checks and monitoring**

  Complement the on-chain logic with off-chain transaction policies, anomaly detection, and signer activity monitoring. This enables teams to spot suspicious transactions early and enforce additional safeguards when needed.

- **Account for human factors**

  Security is not only technical — education and operational discipline are equally important. Signers should be trained to avoid blind-signing, verify transaction data carefully, and follow secure key management practices.

Access Control Exploits: 83% of Losses

ACCESS BREACHED

Access control failures led to $1.63 billion in losses this quarter — the single most damaging category by far.

Centralized Exchanges (CeFi):

$1.46B
Feb 21, 2025

BYBIT

malicious Safe transaction signed via compromised frontend.

$85M
Jan 23, 2025

phemex

hot wallet compromise across multiple chains including Ethereum, Solana, BTC, BNB Chain, Sui, Aptos.

DeFi Access Control:

$50M
Feb 24, 2025

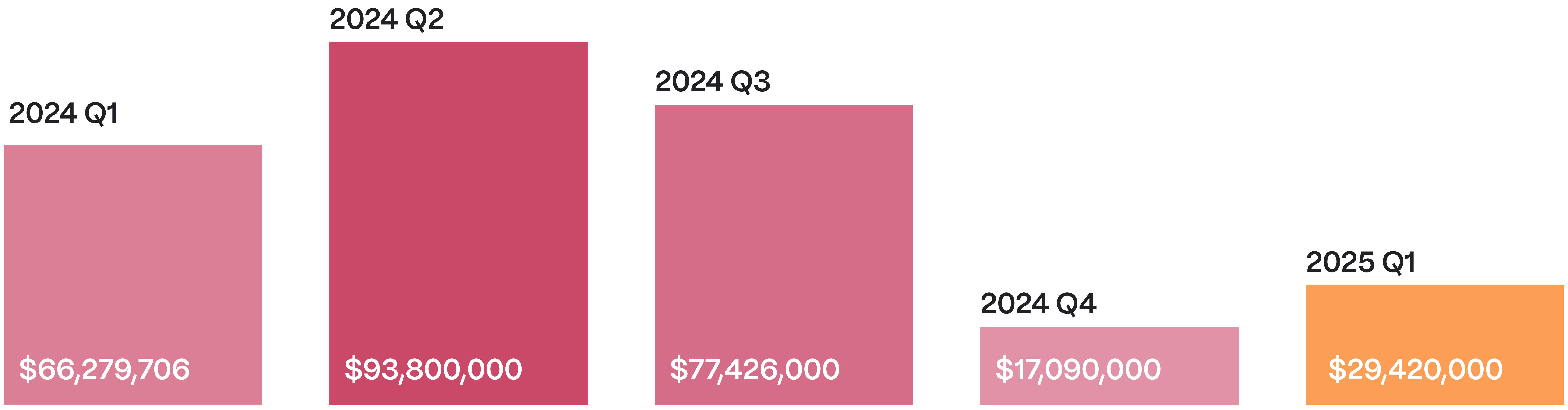
INFINI

developer retained administrative control over a deployed contract and drained funds from yield strategies after a long dormancy.

$9M
Mar 21, 2025

ZOTH

proxy upgrade controlled by an EOA, not a multisig; attacker upgraded contract and drained funds .



Smart Contract Vulnerabilities

Smart contract bugs accounted for just $29.4M (1.5%) of all losses. Still, several incidents stood out:

$9.6M

Feb 11, 2025

zkLend

rounding vulnerability in SafeMath allowed flashloan-driven price manipulation.

In this Starknet-based lending protocol, the attacker manipulated an internal exchange rate (the "lending accumulator") in an empty wstETH pool by cycling a tiny deposit and a flashloan repayment, which artificially inflated the accumulator's value.

Because the smart contract used SafeMath's integer division (which rounds down any fractional remainder), the calculation for burning the platform's zTokens during withdrawals became imprecise.
For more details, check out our video analysis.

$5M

Mar 4, 2025

1inch Fusion v1

old contract exploited; losses limited to resolvers, not users.

The 1inch Fusion v1 exploit involved an outdated smart contract and fortunately only affected resolvers (the independent bots that fill 1inch orders), not end-users. In this case, some resolvers were still running the deprecated Fusion v1 contract, which contained a vulnerability in its order settlement logic.

The attacker discovered a way to abuse this flaw – essentially by crafting a malicious transaction that bypassed normal restrictions – and was able to impersonate a resolver to execute swaps for huge profit.

Security Lessons and Mitigation Strategies For Smart Contracts

Review Your Arithmetic In Flash Loans

Rounding down can be dangerous in edge cases – developers must handle division carefully (e.g. use higher precision or rounding-up where appropriate) and set safeguards (like minimum liquidity or invariant checks) to prevent flashloan-driven price manipulation.

Keep Contracts Up-to-Date

The 1inch case shows the danger of running outdated code – always deprecate and replace vulnerable contract versions. Projects should actively encourage or enforce upgrades (through incentives or deactivation of old contracts).

Adopt a Strong Security Culture

Including bug bounties, thorough audits, and testing for unusual attack vectors (like flash loans or buffer overflows) can catch vulnerabilities before attackers do, thereby safeguarding user funds and protocol integrity.

Hacken Recommends: Automated Incident Response

Learn more ↗

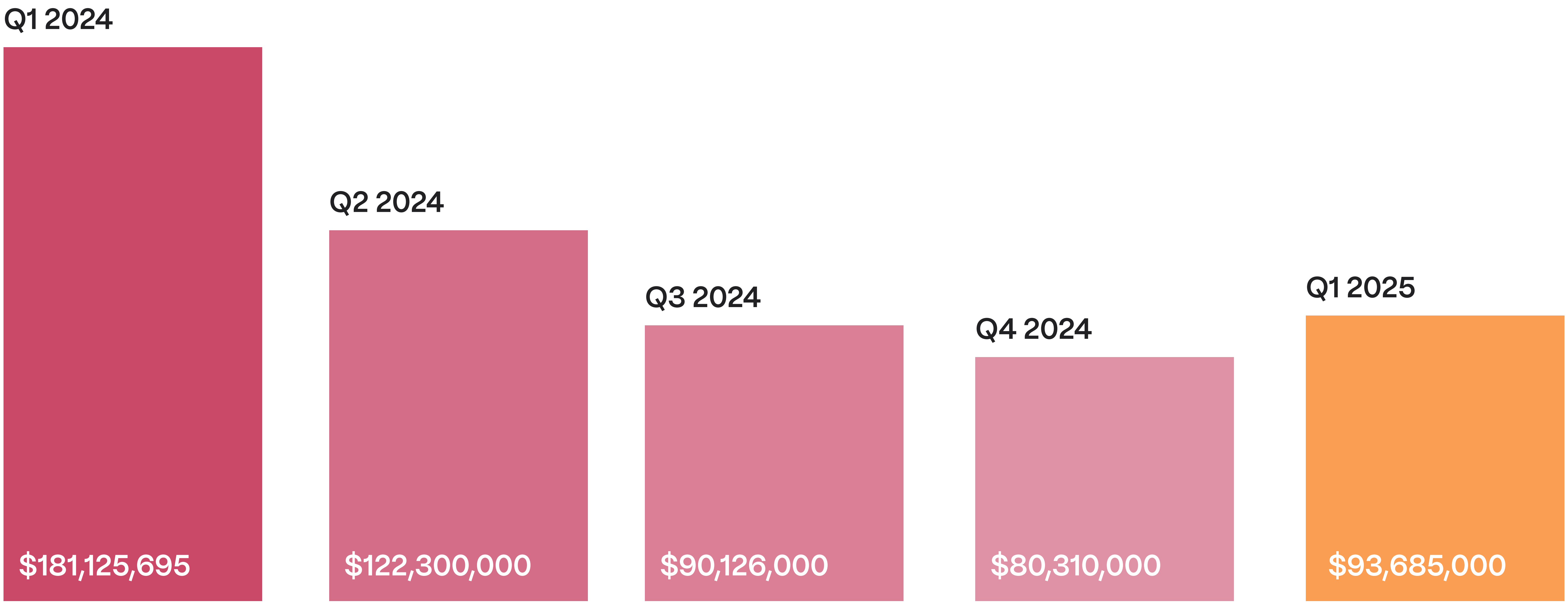
Hacken Extractor steps up with a robust defense tailored to smart contract vulnerabilities.

Attack Detector zeroes in on suspicious actors, identifying wallets tied to mixers like Tornado Cash or other red-flag funding sources as they interact with smart contracts, while also tracking suspicious activities on chain in real time.

Advanced Monitoring takes it a step further – spotting attack preparation patterns, like unusual transaction spikes or anomalous calldata, before damage strikes.

Extractor doesn't just watch – it acts, flagging malicious addresses early to prevent harm and even initiating real-time limitations on vulnerable contract functions to halt exploits mid-flight.

DeFi Q1 Losses: Trends and Key Highlights



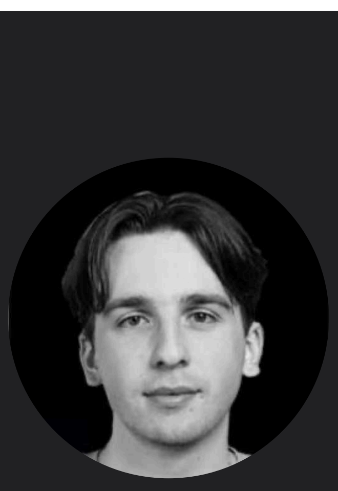
Total DeFi losses in Q1 2025 were $94M, continuing the downward trend, comparing to all the quarters of 2024

The biggest DeFi exploit this quarter was Infini ($50M) due to access control. In Ionic (12.3m), hackers used social engineering to trick protocol owners to approve malicious collateral, which allowed the funds to be drained. Other notable cases, such as zkLend, 1inch and a few others (less notable) were due to smart contract vulnerabilities.

The sector held steady overall, with no systemic exploits or protocol-wide collapses – a good sign of maturing protocol design, though governance and operational processes still need improvement.

INFINI
IONIC
zkLend
1inch

Hackers Employ New Money Laundering Techniques



Yehor Rudytsia
Hacken Security Researcher

X linkedIn

"We are observing evolving money laundering tactics — instead of traditional mixers, attackers increasingly turn to trading platforms, especially perpetual exchanges like Hyperliquid, to clean or reposition stolen funds with fewer traces. Strengthening CeFi and DeFi monitoring is essential to counter these schemes."

1. High-Leverage Trading on Perpetual Exchanges

In January, ZachXBT traced multiple wallets tied to UK national William Parker – a known cybercrime offender – who had built up over $20 million across Hyperliquid and GMX. The initial capital was sourced from phishing scams and online casino exploits.

The funds were pushed into high-leverage trading strategies, turning illicit assets into legitimate-looking trading PnL. Because these platforms lack onboarding friction and the trading volume is real, the resulting balances are difficult to distinguish from organic profit.

Laundering strategy through perpetuals platforms like Hyperliquid may be the following:

- Use stolen funds to open a large leveraged short or long.
- Hedge that position elsewhere using clean capital.
- Let the leveraged position get liquidated.
- The profit remains on the clean side, while the stolen funds are wiped from the system.

By sacrificing the origin wallet and creating a loss event on-chain, the attacker distances themselves from the stolen capital while retaining its economic value. This method exploits how liquidation engines behave under extreme leverage and price movement.

2. Intentional Sandwich Attacks

Bad actors are now also imitating sandwich attacks, intentionally losing funds to clean illicit assets under the guise of MEV bot activity. On March 12, 750K USDC was "sandwiched" in 6 trades across just 35 Ethereum blocks.

- 6 sandwich attacks in 5 minutes
- All sandwiches executed in blocks built by the same builder
- Funds were funneled through Aave, Compound & Uniswap before getting sandwiched

This technique potentially reframes stolen or flagged assets as MEV profit. By embedding the funds within what looks like normal DeFi arbitrage, attackers may bypass traditional detection models used by exchanges and compliance systems.

zkLend Money Laundering Saga

Some privacy-preserving tools can successfully filter suspicious transactions – a vital AML step. In the zkLend smart contract exploit, hackers' efforts to clean the stolen money quickly went wrong.

Railgun Attempt

After the hack, the attackers deposited 706 ETH into Railgun, hoping its privacy features would hide the funds. However, Railgun's filtering mechanism stopped the transaction.

The hackers then had to withdraw the ETH – an awkward and costly setback. As @VitalikButerin noted, this shows how privacy pools can stop illicit transactions without extra surveillance.

Tornado Cash Attempt

About 1.5 months later, on March 31, the attackers tried to use Tornado Cash to launder the funds again. This time, the stolen funds were deposited into a phishing website posing as Tornado Cash.

According to @officer_cia:

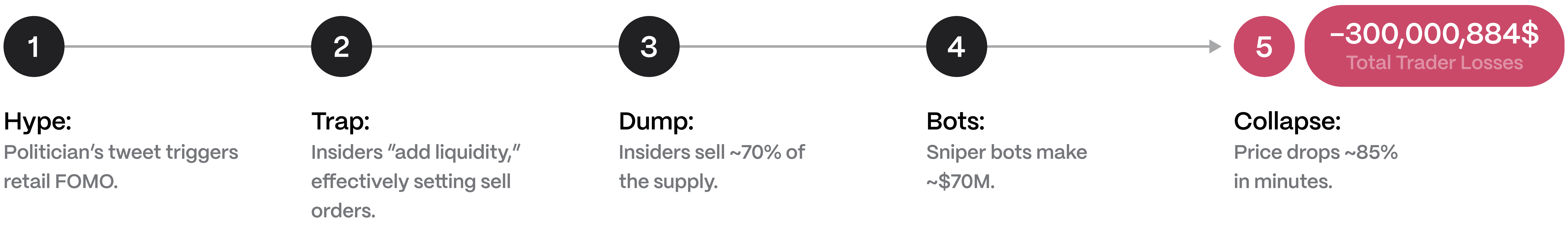
> "It seems that the 2,930 ETH stolen from @zkLend was deposited into a phishing website imitating TornadoCash and was immediately taken away by the phishing website's operators."

The on-chain message from zkLend attackers confirmed that the attackers lost almost all of the stolen ETH. It remains unclear who is behind the phishing website.

Rug Pulls & Politically-Backed Scams

Javier Milei

$LIBRA: The Presidential Rug Pull



1 **Hype:** Politician's tweet triggers retail FOMO.

2 **Trap:** Insiders "add liquidity," effectively setting sell orders.

3 **Dump:** Insiders sell ~70% of the supply.

4 **Bots:** Sniper bots make ~$70M.

5 **Collapse:** Price drops ~85% in minutes.

-300,000,884$ Total Trader Losses

On February 14, 2025, Argentina's President Javier Milei tweeted promotion of a new meme coin, $LIBRA, claiming it would fund small businesses and boost Argentina's economy. Within minutes of launch, $LIBRA's price rocketed from nothing to $5.20, pushing its market cap to about $4.6 billion.

However, behind the scenes, insiders controlled approximately 70–82% of the supply and quickly added "liquidity" — effectively placing large sell orders — before dumping their tokens en masse.

🚩🚩🚩

No due diligence at all | Tokenomics not public | Website was new | Google form | Massive bundle of initial holders

Dyma Budorin
Hacken Co-Founder & CEO

X linkedIn

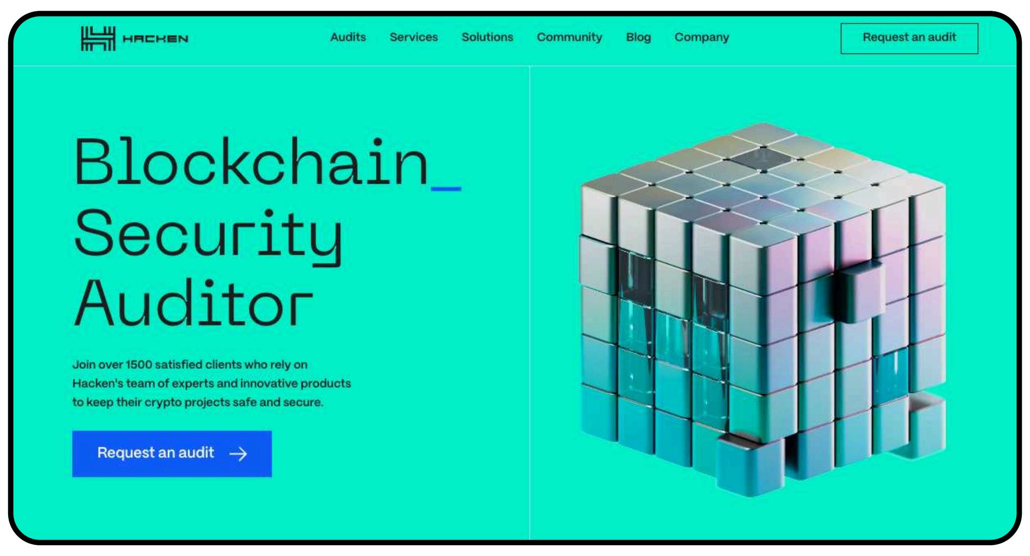
"$LIBRA added new concentrated liquidity. For newbies, it sounds as if they added value to the coin. In fact, this is a selling order that transforms tokens into cash when the price goes up... Never invest in anything like that. This kills our industry and turns it into a circus"

Read the full post

Insiders withdrew over $100 million from liquidity pools (mostly in SOL and USDC), cashing out around $87 million within the first three hours. This triggered an immediate collapse — $LIBRA lost ~85% of its value in minutes and fell by over 95% within hours.

The market cap plunged from ~$4.6 billion to under $200 million. While Milei later deleted the promotional tweet and denied involvement, it was one of the largest rug pulls on record sparking public outrage and regulatory investigations.

Empowering Secure Digital Innovation for Web3 Businesses and Crypto Users



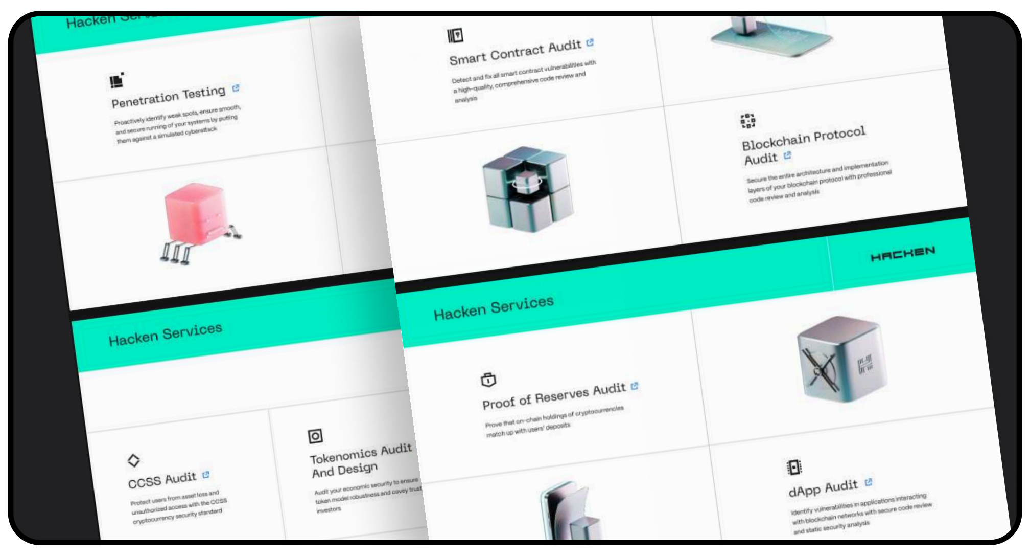
Blockchain_ Security Auditor

Join over 1500 satisfied clients who rely on Hacken's team of experts and innovative products to keep their crypto projects safe and secure.

Discover Security Solutions

Your trusted blockchain security auditor. Learn how you can strengthen resilience, prevent exploits, and build trust with Hacken.

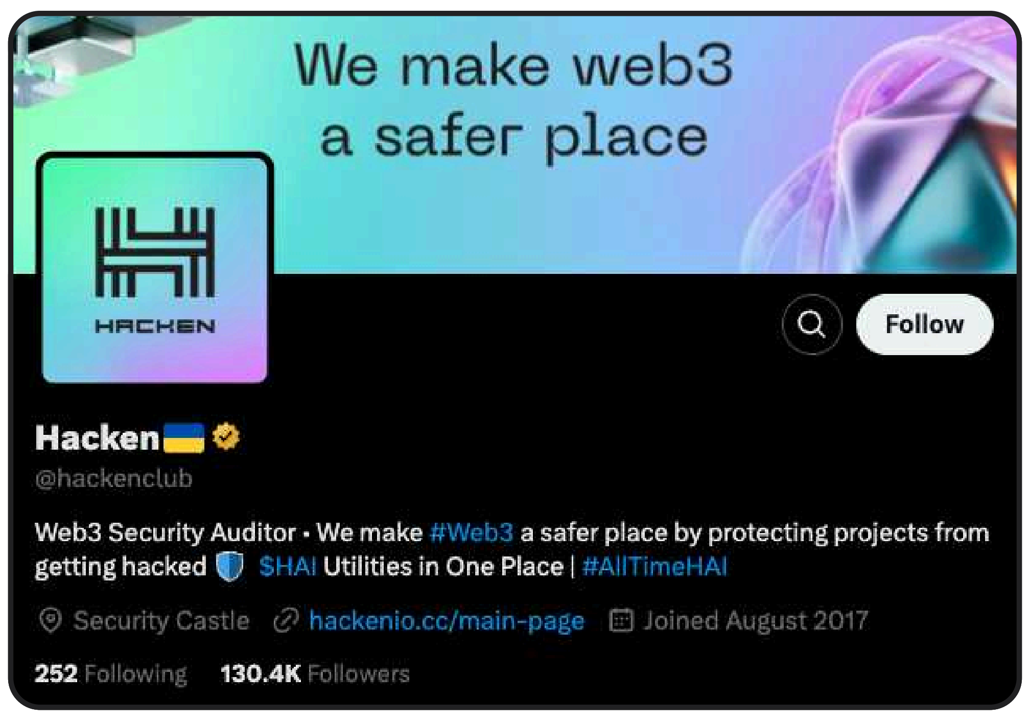
hacken.io



Access Educational Resources

Stay ahead of risks with Hacken's tools and resources—because knowledge is your first line of defense.

hacken.io/research



Hacken 🇺🇦
@hackenclub

Web3 Security Auditor • We make #Web3 a safer place by protecting projects from getting hacked 🛡 $HAI Utilities in One Place | #AllTimeHAI

Security Castle hackenio.cc/main-page Joined August 2017

252 Following 130.4K Followers

Support a Safer Web3

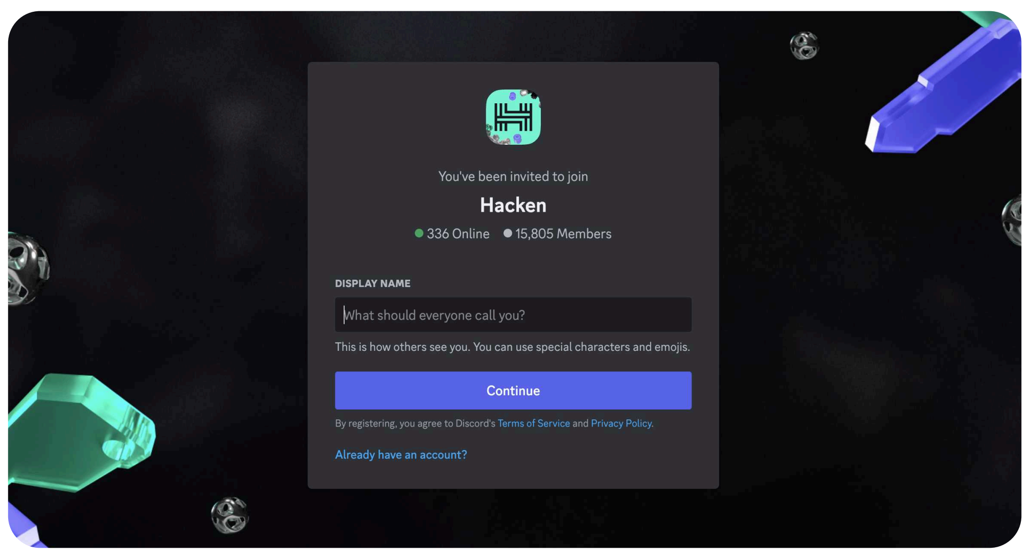
Join Hacken's security community. Stay updated, get involved, and advocate for blockchain security.

x.com/hackenclub

Subscribe to Hacken Digest

Get monthly Web3 security insights, exclusive webinars, and company updates — delivered straight to your email.

hacken.digest



You've been invited to join
Hacken
● 336 Online ● 15,805 Members

DISPLAY NAME
What should everyone call you?
This is how others see you. You can use special characters and emojis.

By registering, you agree to Discord's Terms of Service and Privacy Policy.

Already have an account?

Join HAI Discord Community

Master the art of DYOR and level up your crypto investment game with the strongest security-first community in Web3.

discord.gg/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 Contribution

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.

ethereum foundation BINANCE ebsi European Blockchain CoinGecko NEAR

AURORA RADIX 1inch ADGM BYBIT METIS

For media inquiries

marketing@hacken.io

hacken.io X linkedIn

This material is for informational purposes only and does not constitute legal, financial, tax, or investment advice. Hacken assumes no responsibility for decisions made or actions taken based on this material.

Authors: Rudytsia Y., Malanii O., Sheptytskyi A., Broshevan Y., Budorin D.