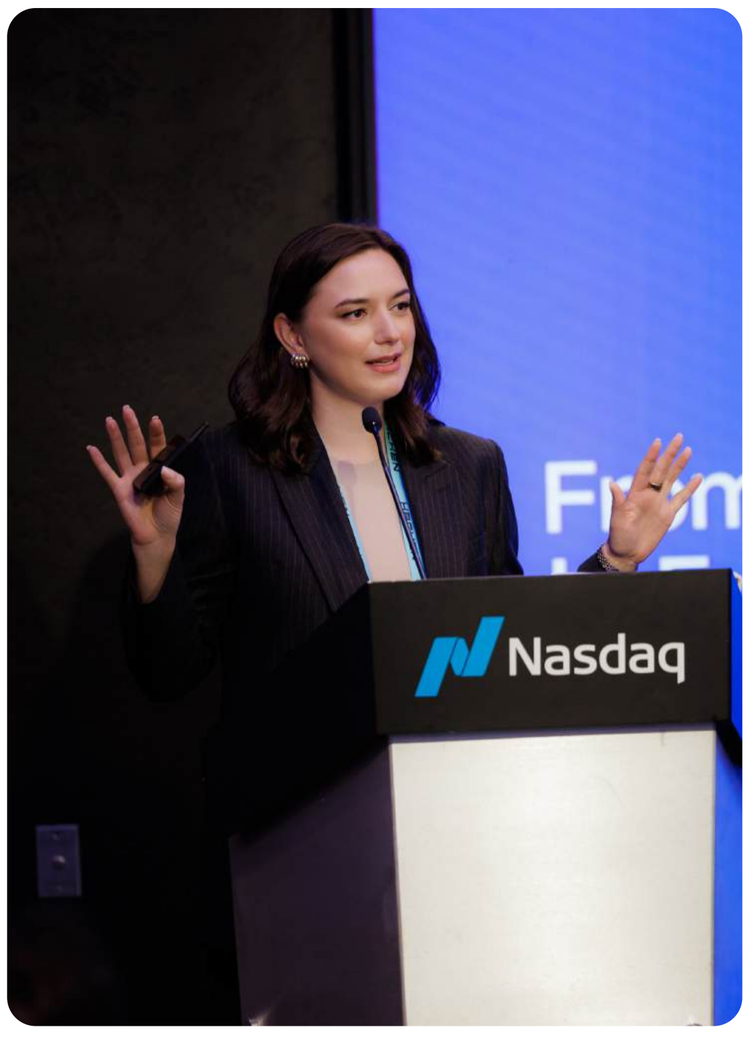
HACKEN

November 2025

The Hacken 2025 Yearly Security Report

We Make Web3
A Safer Place

hacken.io



"Over $4 billion was lost in 2025. The message is clear: cybersecurity must be addressed continuously, not solved by a single product.

In this report, we show how failures emerged across code, infrastructure, operations, governance, and human processes, reinforcing one conclusion: every layer of critical infrastructure must be protected. Only verifiable security can enable new institutional capital to enter decentralized systems."

Yev Broshevan
CEO & Co-Founder, Hacken

Executive Summary

The scale and nature of Web3 security incidents in 2025 highlight a shift from isolated code flaws toward systemic operational risk. This report examines the year's major incidents and incorporates insights from the Hacken Trust Summit 2025 to outline how the industry is responding to these challenges.

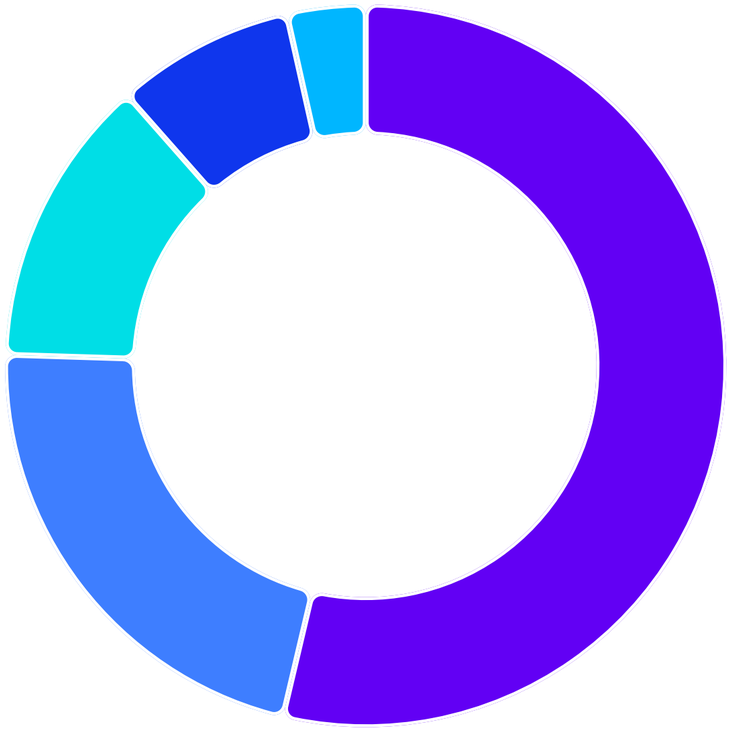
Web3 Security Highlights:

- $4 billion lost in 2025 across all Web3 platforms.
- North Korea is responsible for nearly 52% of the total Web3 losses.
- Operational Security remains the weakest spot with $2.1B hacked.
- DeFi saw massive exploits in the second half of 2025.

Total 2025 loss $4,004,090,000

Distribution of Crypto Losses by Attack Type (2025)

	Total loss including phishing	% of total
Access control exploits	$2,123,633,000	53.0%
Phishing scams	$951,577,000	23.8%
Smart contract vulnerabilities	$512,028,000	12.8%
Rug pulls	$316,852,000	7.9%
Other	$100,000,000	2.5%



Quarterly Crypto Losses (2024–2025)

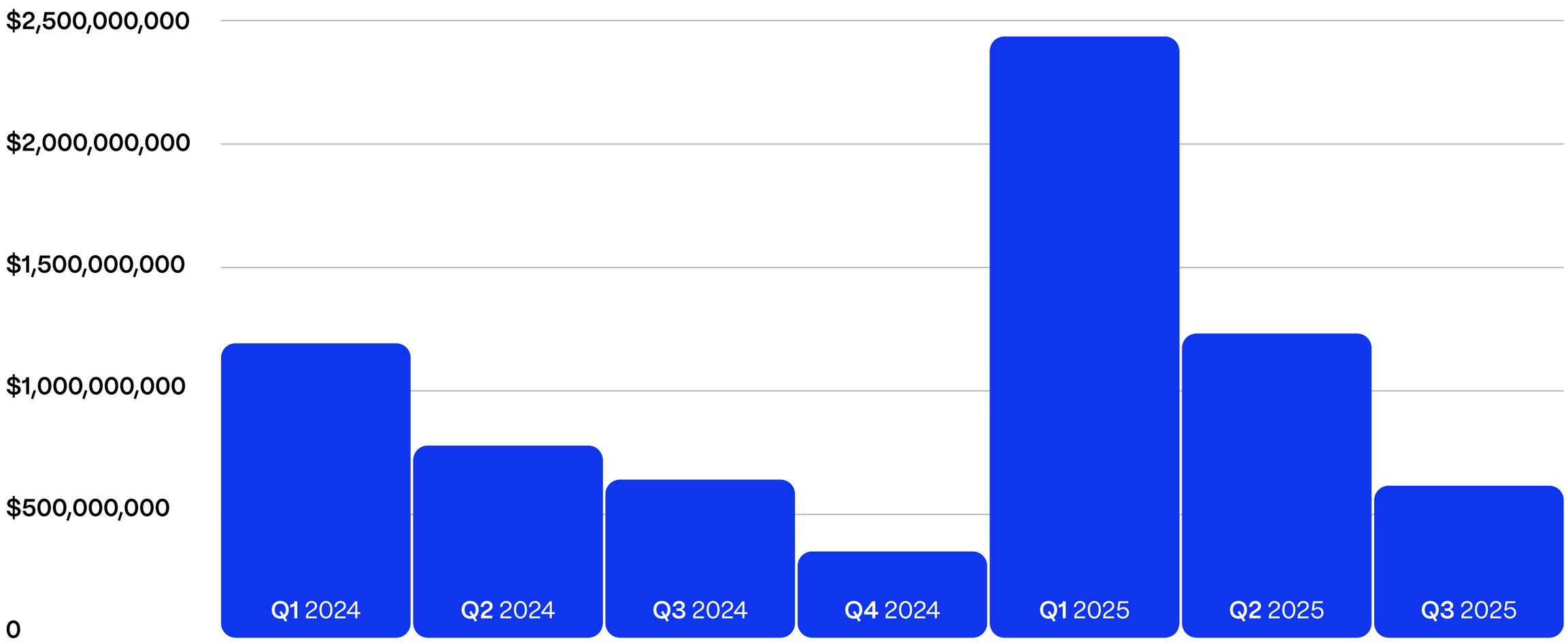


Table of Contents

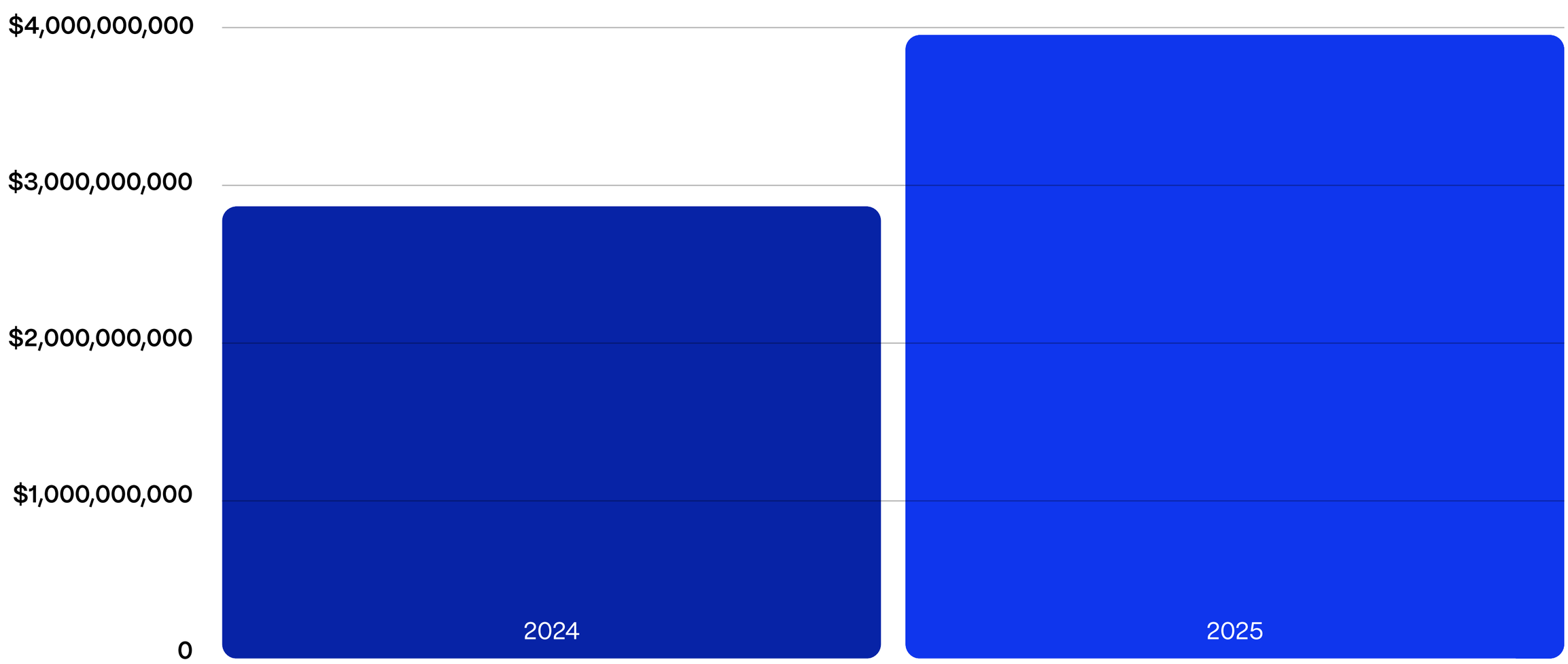
Introduction

In this year we've seen over $4 billion in losses from smart contract vulnerabilities, access control oversights, rug pulls as well as thefts due to phishing and social engineering.

The loss-per-quarter shows a descending trend in 2025, very similar to 2024. However, the total amount hacked in 2025 is already $1.15 billion bigger than in 2024. North Korea hackers responsible for 52% of the total stolen amount (as for Hacken's attribution).

For two years straight, the vast majority of losses happened in the first quarter, so we urge blockchain adopters to straighten their security practices right now!

Total Crypto Losses by Year (2024–2025)



This report presents a categorized breakdown of the 2025's incidents, identifies trends, and highlights a growing need for operational maturity across DeFi protocols and CeFi platforms.

The incident patterns observed throughout 2025 are increasingly mirrored in how institutions, regulators, and infrastructure providers are rethinking security, custody, and compliance. To understand where the industry is heading next, this report incorporates executive insights from the Hacken Trust Summit 2025.

Key Trends In Crypto Hacks

HACKED

Reported crypto losses in 2025 reached approximately $4B, a 40% increase since 2024. Losses peaked in Q1 at just over $2B and declined sequentially through the year to around $350M by Q4.

The Bybit incident, nearly $1.5 billion, was the largest single theft on record and a major driver of 2025 losses. North Korea (DPRK) threat actors drive the majority of the damage (about 52%) this year by our attribution. Smart contract side contributed $512 million in losses due to code logic errors. We recorded notable cases with highly audited projects getting hacked and a pattern of old (battle-tested) codebase exploited.

GMX | Balancer | Yearn Finance

In the GMX v1 hack, most funds were later recovered. The so-called white-hat resolution was because on-chain activity is transparent and traceable, and the project actively leveraged this transparency to push the attacker toward a white-hat deal in a negotiated bounty.

In our previous report, we highlighted that losses caused by logic flaws are more likely to allow for engagement and potential fund recovery, whereas incidents stemming from access control failures, particularly those linked to North Korea, rarely result in recovery. This distinction remains broadly valid, but outcomes vary by incident. In other high-profile smart contract exploits, including Balancer and Yearn, no white-hat resolution was achieved, and the majority of stolen funds were laundered through Tornado Cash.

2024 vs 2025

While access control exploits remained the largest source of losses, their relative share declined, as smart contract vulnerabilities, phishing, and rug pulls made up a larger share of incidents. This suggests attackers are exploiting a broader range of weaknesses across the ecosystem.

Change in Loss Distribution by Attack Type (2024 vs 2025)

Attack Type	2024 Share	2025 Share	Change (pp)	Direction
Access control exploits	60.3%	53.0%	−7.3 pp	↓
Smart contract vulnerabilities	10.8%	12.8%	+2.0 pp	↑
Phishing scams	21.3%	23.8%	+2.5 pp	↑
Rug pulls	6.8%	7.9%	+1.1 pp	↑

Main trends shifts in 2025 compared to 2024 were more sophisticated attacks on DeFi protocols (mostly exploiting rounding vulnerabilities) and increased number of DPRK-orchestrated breaches of various protocols and individuals.

Most of the "access control" exploits you see in news come from North Korea. They don't hack smart contracts, they hack operational processes and weak endpoint security.

Also, this year we witnessed $1.15 billion more stolen funds than in 2024 overall. DPRK-TraderTraitor is responsible for about 40% of the total stolen funds across 2024 and 2025, with all losses coming from centralized exchanges hacks.

Access Control Exploits

ACCESS BREACHED

The primary way digital assets were stolen this year was through pure operational security failures across the Web3 ecosystem. The pattern we see over and over is weak access control practices. The biggest heists occurred at centralized exchanges:

BYBIT | BtcTurk | WOOX | PHEMEX | SwissBorg | BigONE

Who Is Targeting Crypto Exchanges?

All of these breaches align with the TraderTraitor playbook and are attributed to the same North Korea's cluster based on consistent access vectors, including malware and supply chain compromise, as well as post-theft fund movement patterns and reuse of addresses linked to prior cases.

However, access control incidents at centralized exchanges are not uniformly attributable to North Korea. For example, the CoinDCX breach involved a supply chain compromise but shows no indicators consistent with DPRK-linked activity. Similarly, other major exchange incidents, including Nobitex and Upbit, could not be attributed to North Korea based on available evidence. Notably, while Upbit was previously breached on the same calendar day four years earlier in an incident attributed to North Korea, the characteristics of the new attack differed materially and do not support the same attribution.

Largest Centralized Exchange Hacks of 2025 With Threat Actor Attribution

Project	Total loss	Was it North Korea?
ByBit	$1.465B	Yes – TraiderTraitor
Nobitex	$90M	No
Phemex	$85M	Yes – TraiderTraitor
BTC Turk	$55M	Yes – TraiderTraitor
CoinDCX	$44M	No
SwissBorg	$41.5M	Yes – TraiderTraitor
UpBit	$36M	No (supposedly)

The Limits of Multi-Sig Security

Compromised signers represent a systemic risk to multi-signature security.

Throughout 2024 and into early 2025, the industry experienced a spike in multi-signature incidents where the signing process itself was compromised. The industry learned the hard way: multi-sig is not a magic shield if the signers live on everyday laptops or when vendors can nudge what is ultimately signed.

Q2 2025 saw a temporary lull in large-scale multi-sig compromises. However, the issue resurfaced later in the year on the DeFi side with the UXLINK incident. In this case, compromised signers allowed attackers to take control of administrative functions, drain multi-sig-protected assets, mint trillions of UXLINK tokens, and dump them on the open market.

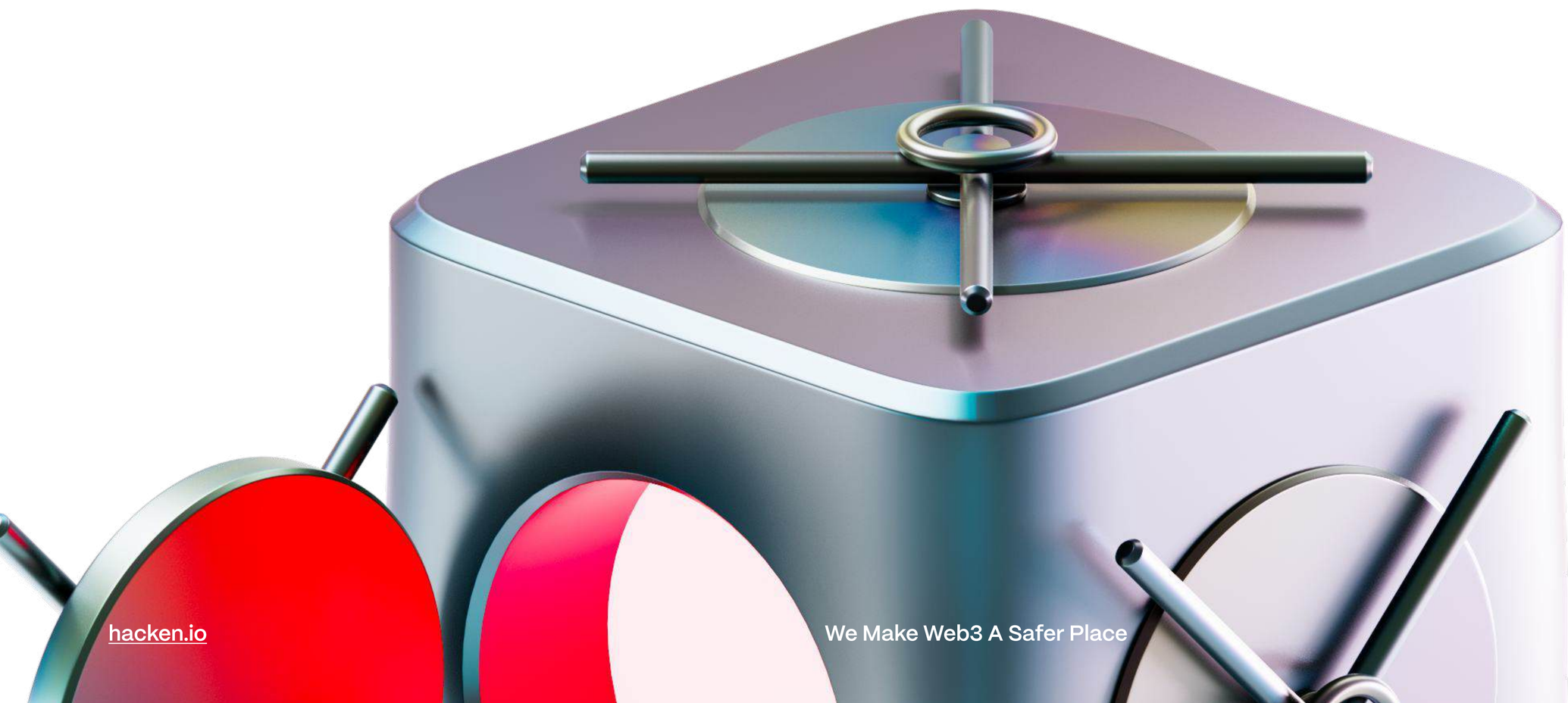
Security Recommendations

Access control is where the largest, least recoverable losses happen, and most of those losses come from a small set of repeatable tactics that teams can actually defend against.

Q2 2025 saw a temporary lull in large-scale multi-sig compromises. However, the issue resurfaced later in the year on the DeFi side with the UXLINK incident. In this case, compromised signers allowed attackers to take control of administrative functions, drain multi-sig-protected assets, mint trillions of UXLINK tokens, and dump them on the open market.

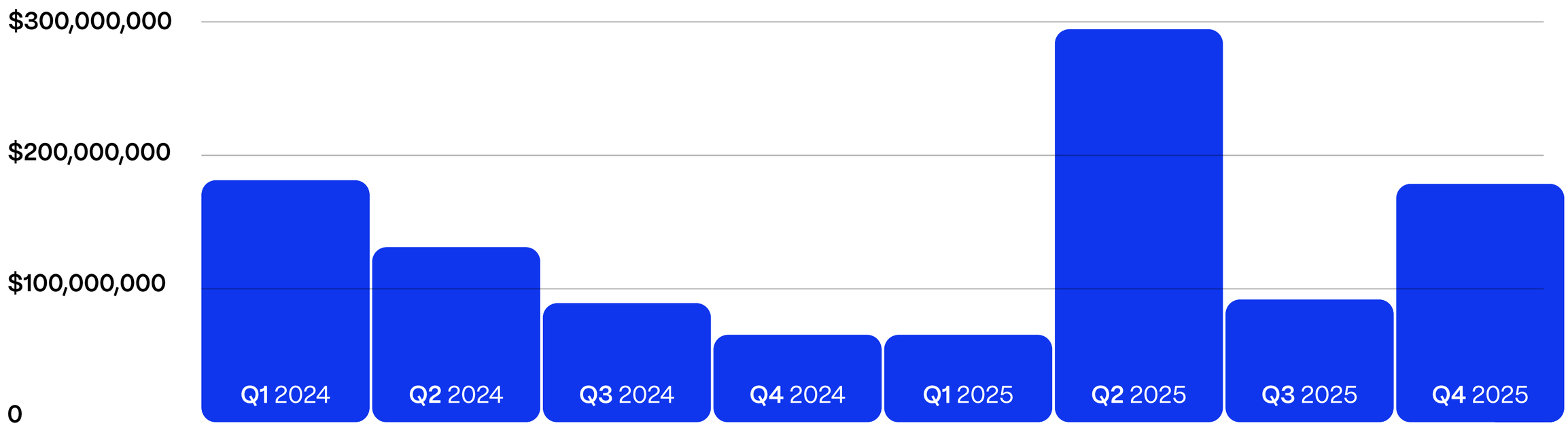
Our Advice

Use hardware wallets. But also very important is not using your daily driver laptop when signing transactions with that hardware wallet. Users have to use an alternative device for signing (e.g., an IPhone or an IPad) and not to message from there, not to use GitHub from there, not to read emails there. Have to keep it isolated.



DeFi Hacks

DeFi Losses by Quarter (2024–2025)



In 2025 to date, DeFi losses reached approximately $512M, driven mainly by smart contract vulnerabilities and, to a lesser extent, by operational security compromises involving developer key theft. Several of the largest DeFi exploits occurred despite projects having undergone multiple security audits, including incidents affecting otherwise battle-tested protocols.

Balancer

Root cause: Mathematical rounding error in Composable Stable Pools

Stolen: $128M

Attackers found a subtle rounding issue in Balancer v2 Composable Stable Pools. By pushing certain pools into very thin liquidity and hammering them with batchSwap calls, they managed to turn minor mathematical rounding differences into significant price distortions.

This allowed them to push the BPT price down and systematically pull value out of the affected pools across multiple chains, resulting in losses exceeding $100 million.

GMX

Root cause: Reentrancy vulnerability in order execution logic

Stolen: $42M

Attackers exploited a reentrancy vulnerability in the executeDecreaseOrder function. They deployed a malicious contract that reentered the protocol mid-transaction during the refund process, causing accounting inconsistencies in global short positions and assets under management (AUM).

This led to GLP being mispriced, allowing attackers to redeem significantly more assets than they had deposited. Approximately $42 million was extracted, though around 90% of the funds were later returned following a negotiated bounty agreement with the GMX team.

Yearn Finance

Root cause: yETH StableSwap "infinite mint" bug

Stolen: $9M

Yearn's old yETH StableSwap setup had a serious accounting mistake that effectively let the attacker mint yETH almost without limit. The attackers minted hundreds of trillions of yETH tokens and used the inflated balances to exploit a custom yETH StableSwap pool, draining approximately $8 million in liquid staking tokens (LSTs).

They also drew roughly another $1M from a yETH/WETH Curve pool, putting total losses at $9 million.

Why Uniswap v4 Requires Specialized Security

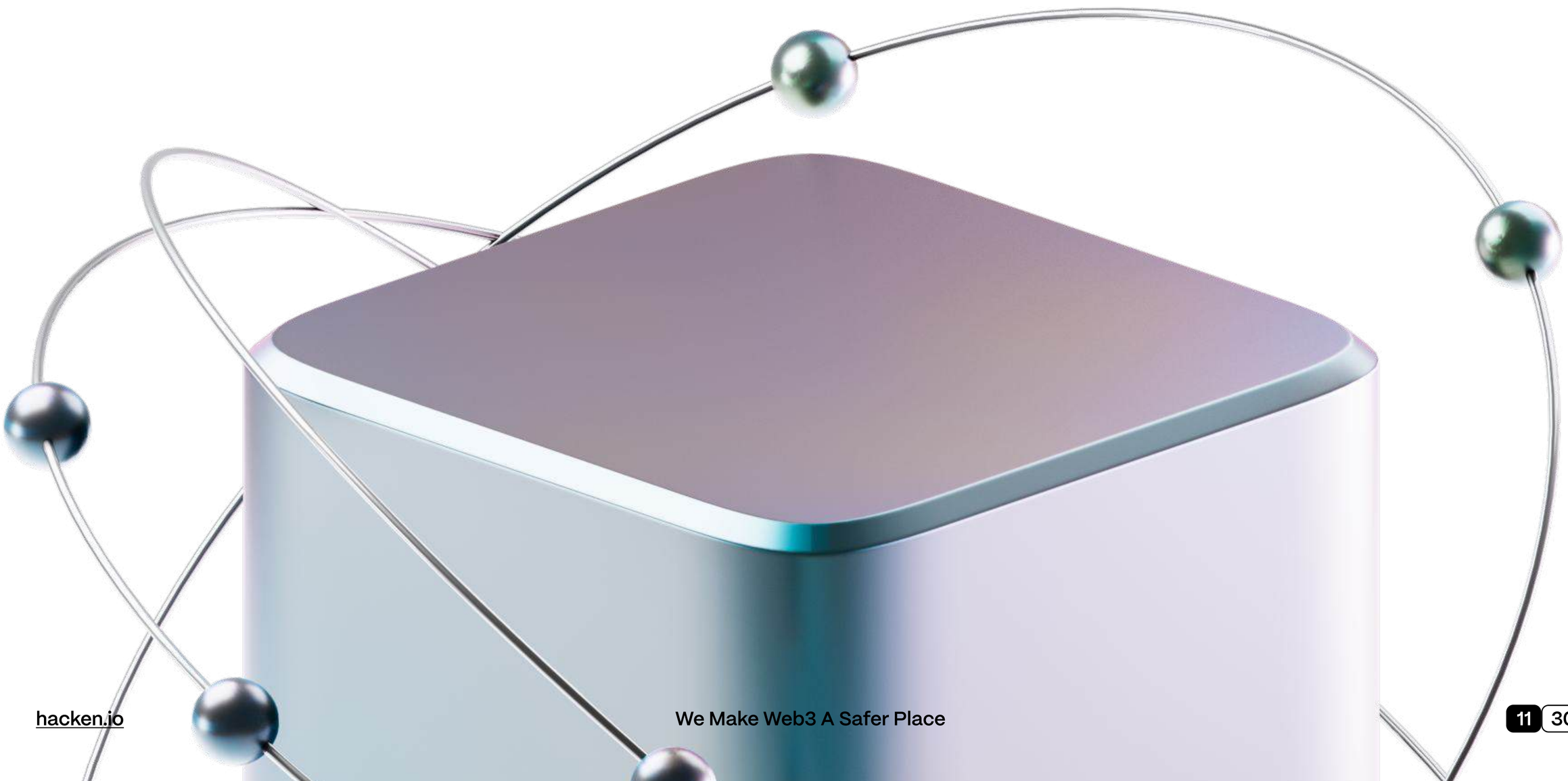
Several newly launched projects were compromised despite having undergone audits, including Bunni, Arcadia Finance, and Nemo. Bunni alone lost approximately $8.2 million in a sophisticated smart contract exploit, becoming the first major hack on Unichain. The protocol was built on top of Uniswap v4 using hook-based architecture and was shut down in early Q4 following the incident.

Uniswap v4 represents one of the most recent and complex developments in decentralized exchange design, introducing new primitives such as hooks and transient storage that materially expand the attack surface. Securing protocols built on Uniswap v4 therefore requires specialized expertise and deep understanding of these mechanisms. Hacken is among the very few security providers with deep expertise auditing v4 hooks and related components.

Further reading, open-source tools and technical analysis:

↗ Open-Source Uniswap v4 Hook Testing Framework
↗ Auditing Uniswap v4 Hooks
↗ Uniswap v4 & Transient Storage Security
↗ Uniswap v4 Truncated Oracle: Risks & Considerations
↗ Uniswap v2 Core Contracts Security

These incidents reinforce that audit quality and methodology materially affect security outcomes. Moreover, layered defense models that extend beyond standard code review provide stronger risk reduction. Hacken's DualDefense combines a primary smart contract audit with an additional crowdsourced review, providing an added security layer that can materially improve outcomes in unfortunate cases where a standalone audit falls short.



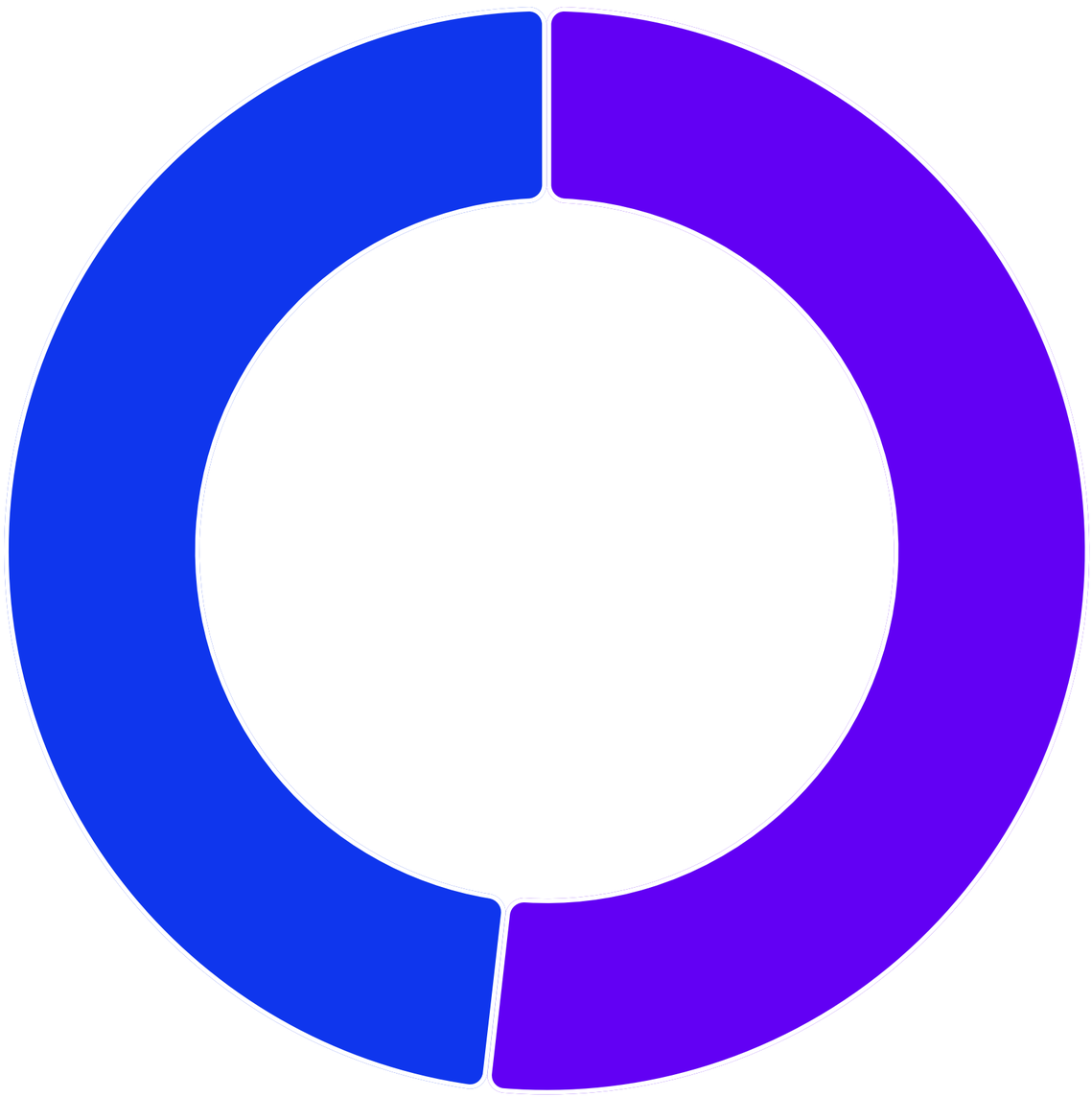
North Korea-Linked Hacks

North Korean cyber operations have become the dominant force behind cryptocurrency theft. Based on current tracking, approximately nine in ten dollars lost through access control exploits trace back to DPRK threat actors, representing over half of all stolen funds this year approaching $2 billion. The cluster known as TraderTraitor has been particularly devastating, executing massive exchange breaches including ByBit and several other platforms, extracting roughly $1.85 billion.

The previous year (2024) saw similar devastation with DMM Bitcoin and WazirX falling victim to exchange heists executed by TraderTraitor. Multiple DPRK groups operate independently but share a unified objective: **exploiting anyone with access to cryptocurrency.**

Who Are the Threat Actors Behind Crypto Losses

2025 DPRK	$2,035,060,000
other	$1,969,030,000



In recent years, 100% of crypto thefts attributed to North Korean actors have relied on social engineering and advanced phishing rather than smart contract exploitation. Observed operational playbooks include fake IT workers, fraudulent job interviews, malicious video calls, and supply-chain attacks.

Contagious Interview Playbook

One persistent threat cluster, tracked since late 2022, specializes in weaponizing the hiring process itself. They approach targets (typically anyone working in crypto) with job offers at recognizable companies like Coinbase or Kraken. Victims receive LinkedIn messages from polished Western recruiter personas advertising remote positions with generous compensation. The profiles look legitimate at first glance but reveal red flags: recently created accounts, sparse connections, AI-generated or scripted responses, and vague job descriptions.

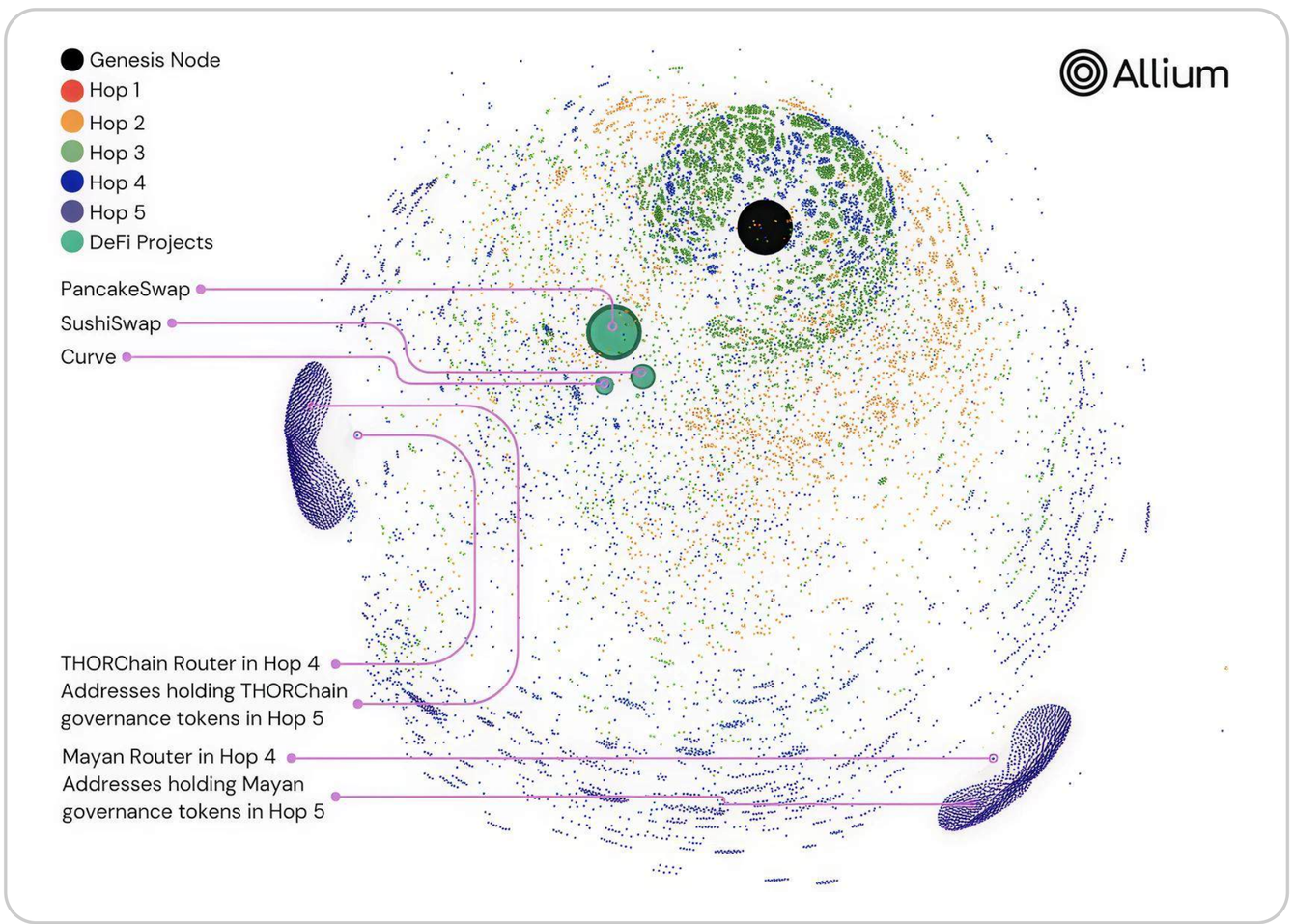
Once engaged, victims are asked to complete "skills assessments" or freelance tasks requiring them to run code delivered via GitHub, Bitbucket, or zip files. This code deploys infostealers like BeaverTail, which immediately drains any browser or desktop wallets on the infected machine. BeaverTail also loads InvisibleFerret, a backdoor enabling persistent access for future payloads. Attackers then harvest private keys, explore the compromised environment extensively.

Dangerous Password and the Fake VC Call

Another cluster, active since around 2018 and linked to the broader Lazarus umbrella, targets high-value individuals (CEOs, CFOs, founders) through spearphishing emails, LinkedIn outreach, and Telegram messages from hacked partner accounts. Their signature move: impersonating venture capitalists proposing collaboration on new products. Victims are invited to video calls where "audio issues" prompt them to install malicious software disguised as fixes. This group has already extracted nearly $200 million this year alone and operates under numerous aliases including SnatchCrypto, CryptoMimic, and BlueNoroff.

Laundering the Proceeds

DPRK threat actors primarily launder stolen funds through DeFi protocols, mixers, and centralized exchanges. DeFi protocols are particularly useful for laundering because they don't require KYC verification. Attackers can interact directly with smart contracts without linking their addresses to verified identities.



In the Bybit hack, Allium's cross-chain analysis of Ethereum transactions found that approximately $386 million was routed through DeFi aggregators, which automatically split transactions across multiple decentralized exchanges.

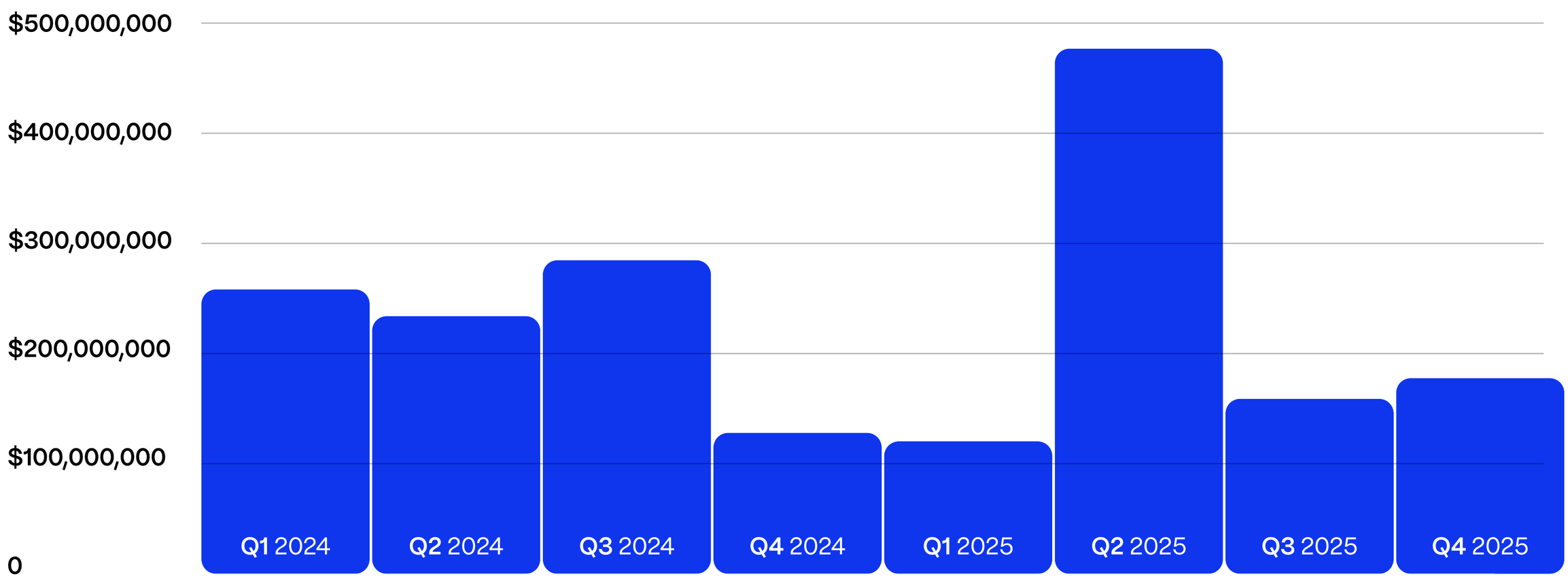
PancakeSwap alone processed $263 million, roughly one-fifth of the total stolen funds. This dispersion across multiple assets and liquidity pools complicates tracing of the stolen funds and recovery efforts.

DeFi laundering paths in the Bybit hack, based on Allium's cross-chain analysis of Ethereum transactions. Allium ↗

Phishing and Social Engineering

Phishing, social engineering, and physical attacks on a rise across 2025:

Phishing and Social Engineering Losses by Quarter (2024–2025)



Phishing / Social Engineering accounted for more than $950 million in industry losses this year. It comes from on-chain phishing as well as social engineering of the victims. We have already discussed that most of the phishing attempts come from the DPRK, but there are threat actors lurking all around the globe trying to steal the crypto. Some of the infamous cases we have seen in this year:

The single biggest social engineering hit was a $330 million Bitcoin theft from an elderly US holder, where complex social-engineering tactics convinced them to hand over wallet access. The attacker peeled the BTC through hundreds of wallets, mixed it into Monero (pushing its price up 50%), bridged some funds into Ethereum, and only a fraction of the stolen coins were ever frozen.

At the end of the year, a user lost $50 million in a single transaction, falling victim to an address poisoning attack. Address poisoning is when scammers "mine" an address where the first and last few characters (4-6) look identical to addresses you've been interacting with. The scammers hope you mistakenly copy-paste the address from transaction history and send your funds there. This is exactly what happened in this theft. The scammer sent 0.005 USDT to the victim, then the victim sent 49,999,950 USDT to the scam address. Just devastating. The screenshot of victim transaction (txn above) and scammer's transactions (txn below):

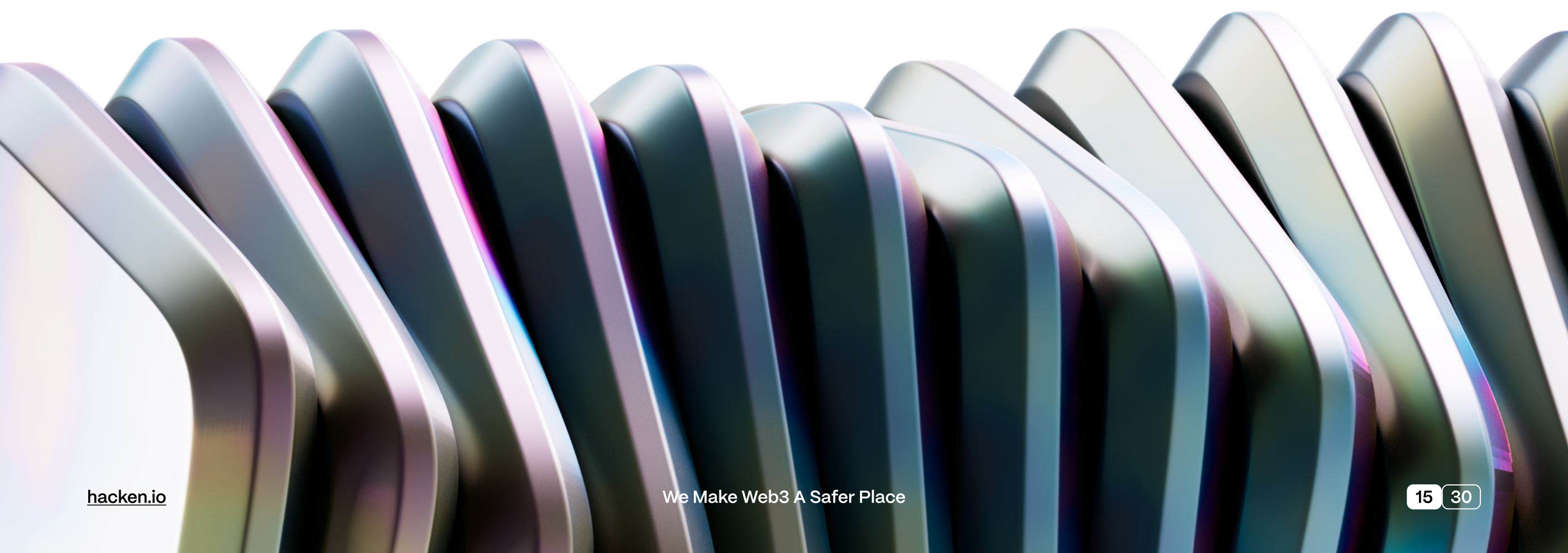
2025-12-19 15:32:59	0xcB80784e...859600819	OUT	Fake_Phishing1691332	49,999,950	Tether USD (USDT)
2025-12-19 15:20:35	Fake_Phishing1691332	IN	0xcB80784e...859600819	0.005	Tether USD (USDT)

The mitigation is straightforward: use an address book. Ensure a single source of truth for recipient addresses. Transaction history is not a place to copy from.

At the same time, high-net-worth Coinbase users have been hit by phishing, vishing, and social engineering following a data breach that unfolded over many months. Callers posing as "Coinbase support" quoted real balances to gain trust and trick victims into revealing keys or passcodes, stealing over $100 million before laundering the funds via mixers, OTC desks and DeFi.

The advices for users to not become a victim of a phishing / social engineering attack:

1. Never pick up phone calls claiming to be support from your exchange
2. Avoid clicking links in branded SMS or chat messages
3. Open your exchange app or website directly to check alerts
4. Inspect email headers to confirm the sender's domain
5. Only accept help from people you already know and trust
6. Use an authenticator app or hardware key instead of SMS for 2FA
7. Store large balances in vaults or cold wallets, not in hot wallets
8. Keep your recovery phrases and keys out of plain files and folders



AI Agents, MCP, and Security Failures

In 2025, AI agents and Anthropic's Model Context Protocol (MCP) expanded from experimental pilots into broader production use across Web2 systems and early-stage Web3 deployments.

This expansion coincided with the first well-documented wave of AI-native security failures (primarily prompt and tool injection) with real-world impact, primarily emerging once agents were connected to privileged tools and execution surfaces (e.g., filesystems, shells, CI/CD pipelines, SaaS APIs, IDE automation).

AI & MCP Adoption Across Web3 and Web2 in 2025

In Web3, AI adoption in 2025 remained early-stage and focused on wallets, treasuries, and on-chain decision support. Agents use MCP to read on-chain state, ingest off-chain signals, and craft transactions, either signing directly or generating unsigned transactions for wallet or multisig approval.

Industry guidance favors transaction-crafter models due to the risks of agent-held keys. Early deployments show persistent weaknesses, including implicit trust in connectors, limited modeling of prompt injection, and key custody as the dominant risk factor.

In Web2, AI and MCP adoption advanced more rapidly across enterprise SaaS, developer tools, browsers, and CI/CD systems. While platforms relied on controls such as OAuth and audit logging, our research showed that AI-augmented tooling can expose execution surfaces when prompt injection intersects with automation. These cases consistently demonstrate that once AI agents connect to enterprise tools, traditional trust boundaries collapse and must be treated as high-risk execution surfaces.

How secure is the AI-generated code? Independent research indicates that AI-generated code frequently introduces security weaknesses: Veracode found that 45% of tested AI-generated code samples failed security checks, often introducing OWASP Top 10-class issues. Complementing this, Aikido suggests that roughly one in five breaches or incidents were attributed by respondents to AI-generated code deployed in production.

AI Security in 2025

AI / MCP Security Incidents in 2025

EchoLeak

Zero-click indirect prompt injection leading to enterprise data exfiltration.

↗ Microsoft Security Response Center – CVE-2025-32711

Copilot / Visual Studio

Local command injection enabling local code execution with user interaction.

↗ Microsoft Security Response Center – CVE-2025-53773

Claude MCP

Unauthorized local tool invocation from browser-originated connections.

↗ Datadog Security Labs – CVE-2025-52882

MCP Inspector

Remote code execution caused by missing authentication between Inspector components.

↗ Oligo Security – CVE-2025-49596

WordPress AI Engine

Authorization failures and token exposure enabling privilege escalation.

↗ Wordfence – CVE-2025-5071 / CVE-2025-11749

Perplexity Comet (disputed)

High-risk browser-to-local execution design pattern with contested exploitability.

↗ TechRadar – Vendor Response

Agentic FoF / BasisOS

Reported financial loss of approximately $531k and operational pause; technical attribution unresolved.

↗ BasisOS Public Disclosure

Key AI Security Failure Patterns Observed in 2025

- Indirect prompt injection across trust boundaries.
- Insecure local transports ("localhost is not a boundary").
- Insecure defaults and over-trust in tools.
- MCP servers as a new plugin-style supply chain.
- AI-generated code acting as a vulnerability multiplier.
- Developer workstations and CI pipelines as high-leverage targets.

+ Web3-specific observations

- High-quality technical postmortems for AI-agent-caused losses remain rare.
- Public guidance already anticipates the main failure modes (key custody, ambiguous intent, misconfiguration).
- Given reporting gaps, risk may be under-reported rather than absent.

AI Security Recommendations for 2026

Web3

- Prefer transaction-crafter models.
- Treat MCP servers as untrusted.
- Require explicit human approval for fund-moving actions.
- Use on-chain guardrails and monitoring.

Web2

- Model prompt injection as an architectural threat.
- Lock down local transports.
- Apply least privilege to agents and tools.
- Harden defaults in AI integrations.
- Treat MCP servers as a supply chain.

Platform & Infra

- Secure-by-default transports.
- Explicit warnings for high-risk tools.
- Comprehensive agent threat modeling.
- Strong auditability and telemetry.

Security Teams

- Update AppSec playbooks for AI-native risks.
- Track AI-involved incidents explicitly.
- Train developers on AI tool trust boundaries.

Crypto Regulation: Security as a New Baseline

Across the U.S., EU, and other major jurisdictions, crypto regulation in 2025 shows clear convergence around security, custody, and operational resilience.

What do regulators actually care about? Despite jurisdictional differences, regulatory expectations, whether operating under a U.S. state license, UK FCA registration, or EU MiCA authorization, consistently cluster around five core areas:

01 Governance and accountability.

02 Custody and key management.

03 Operational and cyber resilience.

04 Third-party and outsourcing risk.

05 Independent assurance.

Security as a Licensing Prerequisite

The incident patterns observed in 2024–2025 reinforce why regulators emphasize operational security. Many of the largest losses occurred in environments where formal compliance existed, but access control, key management, or third-party risk practices were insufficient. As a result, security is increasingly treated as a prerequisite for licensing and continued operation rather than a one-time compliance exercise.

The United States

Jurisdiction / Regime	Core Security Governance & Policies	Technical & Operational Security Controls	Independent Testing / Audits & Assurance
FinCEN MSB (Crypto Money Transmitter) Federal	• Written AML/BSA program with internal controls, risk assessment, and CVC procedures. • Designated BSA/AML Officer. • Policies for KYC, sanctions, recordkeeping, SAR/CTR filing.	• Secure handling of customer & transaction data (RBAC, logging). • Crypto-specific transaction monitoring (mixers, chain-hopping). • Secure onboarding & IDV workflows.	• Independent AML/BSA review (internal or external). • Transaction-monitoring model/rules validation. • Remediation tracking following exams or partner reviews.
SEC Broker-Dealer / ATS (Digital Asset Securities) Federal	• Written Supervisory Procedures (WSPs) covering cyber risk. • Compliance with Reg S-P and, where applicable, Reg SCI. • Governance over system resilience and change management.	• SCI controls for capacity, integrity, availability & security. • Strong access control and segregation of duties. • Logging, surveillance, encryption, vendor controls.	• Annual pen testing & SCI reviews (for covered entities). • SEC / FINRA exams. • Regular internal compliance and cyber testing.
Digital Asset Trust Bank / Custodian Federal / State	• Board-approved bank-level info-sec and operational risk frameworks. • Policies on safekeeping, segregation, and client disclosures. • Formal third-party risk management.	• Institutional-grade custody stack (HSMs, MPC/multi-sig, cold storage). • Continuous monitoring and anomaly detection. • Robust data protection and BCP/DR.	• Recurring banking / trust examinations. • External financial & IT audits (often SOC 1 / SOC 2). • Regular pen tests, incident simulations, and custody control reviews.
Money Transmitter Licenses (Crypto) State	• State-approved compliance & info-security program. • Governance over safeguarding customer funds & data. • BCP/DR and vendor risk management.	• Baseline information security program (access control, encryption, SDLC). • Wallet controls (hot/cold segregation, key management). • Incident detection, escalation, and notification processes.	• Independent financial & controls audits (often SOC 1 / SOC 2). • Periodic regulatory exams. • Common expectation of pen testing & vulnerability scans.
New York – BitLicense State	• Board-approved cybersecurity program aligned with risk profile. • Appointed CISO. • Formal enterprise risk assessment. • Custody and segregation policies.	• Controls aligned to 23 NYCRR Part 500 (MFA, logging, SDLC). • Strong key management (HSMs, multi-sig, cold storage). • Network security, monitoring, BCP/DR, vendor oversight.	• Annual penetration testing & vulnerability assessments. • Independent cyber risk assessments and internal audit. • NYDFS exams and formal remediation tracking.
New York – Limited Purpose Trust Company (Digital Assets) State	• Bank-level governance and three lines of defense. • Board-approved info-sec and custody frameworks. • Detailed asset segregation and approval policies.	• Bank-grade security controls (MFA, network segmentation). • Highly controlled custody operations (HSMs, air-gapped cold storage). • Real-time monitoring and tested BCP/DR.	• Regular internal IT & cyber audits. • Independent pen tests and SOC reports. • Recurring NYDFS safety, soundness & cyber exams.
Louisiana – Virtual Currency Business License State	• Documented info-security and compliance program. • Safeguarding policies for keys and customer data. • AML/BSA procedures tailored to virtual currency.	• Secure wallet architecture and role-based access. • Authentication, logging, encryption where appropriate. • Incident response and BCP/DR coverage.	• State regulatory examinations. • Increasing expectation of third-party security assessments (pen tests / infra audits).
Wyoming – SPDI (Digital Asset Bank) State	• Bank-style ERM framework with cyber & custody risk. • Written digital asset custody and key-management policies. • Board-level oversight of cyber risk.	• Hardened custody architecture (multi-sig, HSMs, cold storage). • Strong network security and secure SDLC. • Comprehensive BCP/DR with on-chain recovery testing.	• Regular IT and safety & soundness exams. • Independent cybersecurity audits and pen testing. • Ongoing validation of custody and recovery procedures.

Hacken helps crypto businesses meet U.S. licensing and supervisory requirements by aligning security maturity with regulatory expectations. We support FinCEN MSB, state MTL, NYDFS BitLicense, and institutional custody regimes through independent security assessments, penetration testing, and custody reviews designed for regulators, banking partners, and auditors.

↗ Learn more – hacken.io/services/advisory

Europe

Jurisdiction / Regime	Core Security Governance & Policies	Technical & Operational Security Controls	Independent Testing / Audits & Assurance
MiCA – Crypto-Asset Service Provider (CASP) Authorisation EU	• Accountable management body for ICT/security • Information-security & risk management framework (cyber, ops, outsourcing) • Outsourcing and access-control policies	• Secure custody & key management (HSMs, multi-sig, wallet segregation) • Transaction monitoring, logging, BCP/DR • Tamper-resistant monitoring of admin and security events	• Internal audit or equivalent assurance • Regular pen tests & vulnerability scans • Third-party assurance on critical outsourcers • Incident post-mortems and regulatory reporting
MiCA – Issuers of Asset-Referenced Tokens (ARTs) EU	• Board-approved reserve & liquidity risk framework • Governance over custodians, redemption, crisis scenarios • Third-party and outsourcing oversight	• Segregated reserve custody & reconciliations • Secure issuance/redemption keys (HSMs, multi-sig) • Treasury controls and on-chain/off-chain supply monitoring	• External reserve audits • Stress testing and scenario analysis • IT/security testing of issuance & admin systems • Assurance over custodians and banks
MiCA – Issuers of E-Money Tokens (EMTs) (via Credit Institution or Electronic Money Institution) EU	• Bank/EMI governance with MiCA & DORA alignment • Enterprise risk management (ICT, payments, liquidity) • Safeguarding and redemption policies	• Bank-grade ICT & payment security • Fund segregation, reconciliations, real-time monitoring • Secure SDLC and change management	• Three-lines-of-defense audits (risk, compliance, IA) • External financial & IT audits • DORA-style resilience and penetration testing • Supervisory reviews and remediation tracking

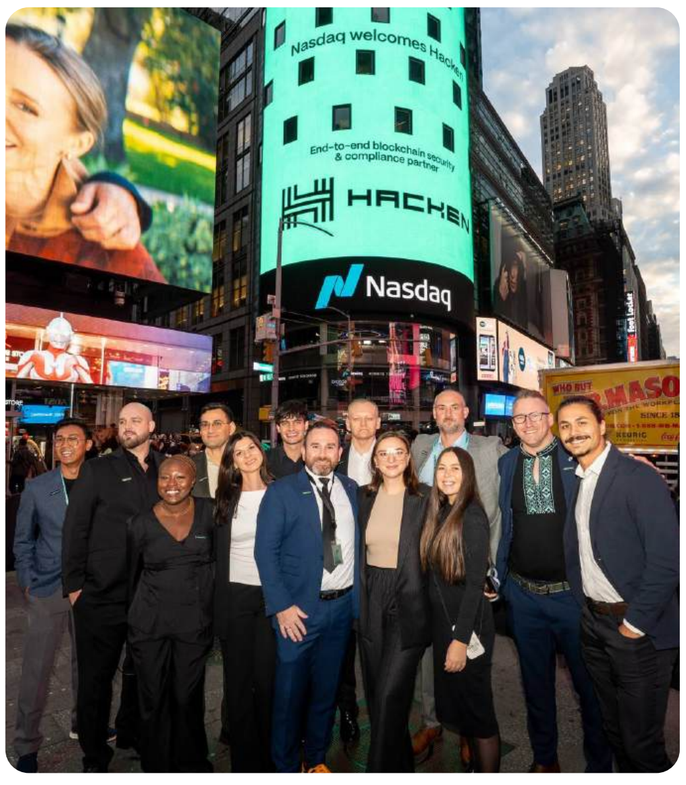
Achieve MiCA Compliance With the Help of Hacken

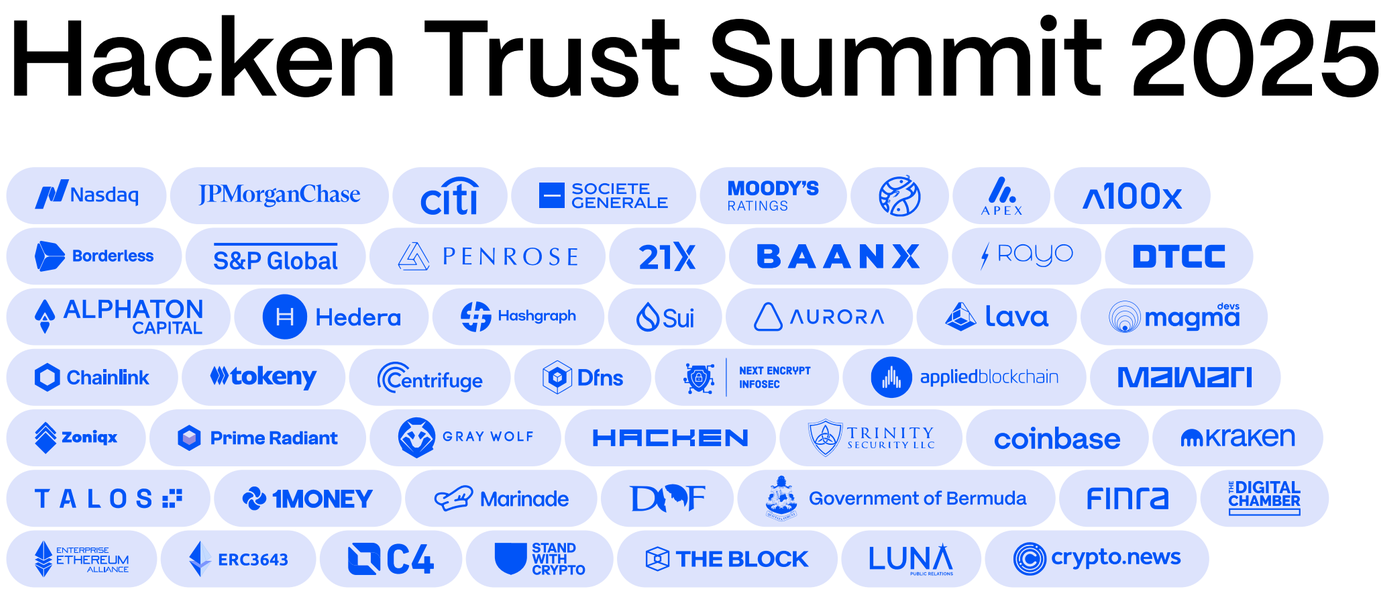
Area	Hacken Services
Governance & Advisory	• vCISO / Fractional CISO• MiCA / DORA gap analysis & roadmap • Policy development (custody, incident response, BCP, outsourcing) • Third-party risk assessments
Technical Security	• Smart contract audits • Penetration testing (infrastructure, web, mobile, APIs) • Wallet & custody security audits • Tokenomics & economic security reviews • Proof of Reserves (PoR) audits
Independent Assurance	• CCSS (Cryptocurrency Security Standard) audits • Bug bounty platform (HackenProof) • Ongoing monitoring (Hacken Extractor) • Incident response retainers • DORA-aligned TLPT (threat-led penetration testing) • Operational resilience & DR testing
Regulatory Readiness	• Documentation packages for NCA applications • Audit reports suitable for regulatory submission • Continuous compliance monitoring & re-certification • Retainer programs for fixed-fee, on-demand support

Hacken delivers end-to-end CASP/VASP compliance beyond the U.S. and Europe, mapping security, governance, and operational requirements across relevant regimes to each client's specific operating model10

Executive Insights From the Hacken Trust Summit 2025

Held at the iconic Nasdaq MarketSite in New York, the inaugural Hacken Trust Summit convened an exclusive assembly of 100 institutional leaders to define the next era of digital assets.





Hacken team at the Nasdaq Tower during Hacken Trust Summit 2025, New York — November 3, 2025.

The consensus was absolute: the "wild west" is officially behind us. With a room representing trillions in assets, including heavyweights like Nasdaq, JPMorgan Chase, Citi, Société Générale, Moody's, and S&P Global, alongside industry titans Coinbase, Kraken, and DTCC, the focus shifted from speculation to objective certainty of cryptographic truth.

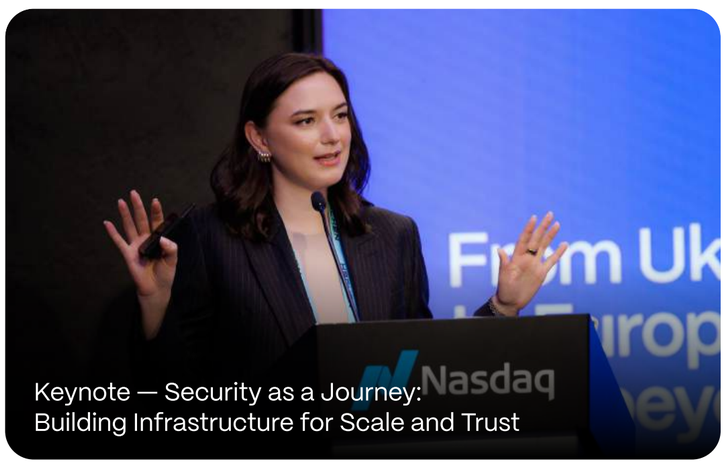
Across 14 high-impact panel discussions, keynotes, fireside chats, over 50 speakers spanning traditional finance, regulatory bodies, and blockchain infrastructure united around a single, urgent objective: **"How do we build digital infrastructure for SCALE and TRUST?"**

The answer lies in four key pillars:

- **Verifiable Assets**
- **Enforceable Rules**
- **Resilient Systems**
- **Responsible Innovation**

"Don't Trust, Verify"

The highlight of the summit was clear: trust in digital assets must be engineered, not assumed. The "strength of the chain" becomes a measurable metric of survival, where cybersecurity must be designed across every layer and independently verified.



Keynote — Security as a Journey:
Building Infrastructure for Scale and Trust

"One of our core values is 'Don't trust, verify.' I want everything to be verified by a third party. Everything should be objective as much as possible in this decentralized system."

Yev Broshevan
CEO & Co-Founder, Hacken

I. Security: The Adversarial Mindset

Security remains the industry's largest hurdle. The discussions moved beyond the critical smart contract audits to advanced key management and psychological warfare.

Fireside Chat — Trust by Design:
Security the Most Trusted Exchange in the US

"Always bring an adversarial mindset to your product... Everyone launching a new product should be able to answer the question, 'How would you break it?'"

Jeff Lunglhofer
CISO, Coinbase

The Human Element vs. The Code. While code is maturing, humans remain the primary attack vector.

Jamie Udinson (Senior Director, Head of Crypto Asset Investigations, FINRA), when asked for the biggest threat to secure markets in one word, answered: **"Carelessness."**

Custody and Key Management. The consensus is that Multi-Party Computation (MPC) is the new standard for custody. **Coinbase's CISO Jeff Lunglhofer** explained that Coinbase's "cold storage" relies on MPC where key shards never coexist in one place. A "holistic key" never technically exists to be stolen.

The "Weakest Link." Speakers warned that decentralized systems are often compromised by centralized dependencies.

Yair Cleper (Co-Founder, Magma Devs / Contributor, Lava Network) argued that if the "weakest link is the trust placed in a small number of people, entities, or middlemen," the system is fundamentally insecure.

Panel – Cybersecurity, Compliance & Regulation:
Enforcing Secure Markets


Yair Cleper
Panel — Security & Compliance for the Future Capital Markets

II. Tokenization & Real-World Assets (RWA)

The focus was on how to move trillions of dollars in assets—from US equities to deposits—onto the blockchain without breaking market integrity.

Merging TradFi and DeFi. Nasdaq provided the institutional anchor for the day, outlining how they are bridging the gap between traditional efficiency and digital innovation.

Fireside Chat — The Bedrock of Trust

"Nasdaq is involved in tokenization because we want to see innovation and evolution in the markets while preserving the key benefits of the current market... We have filed with the SEC to permit trading of tokenized securities on Nasdaq."

Chuck Mack

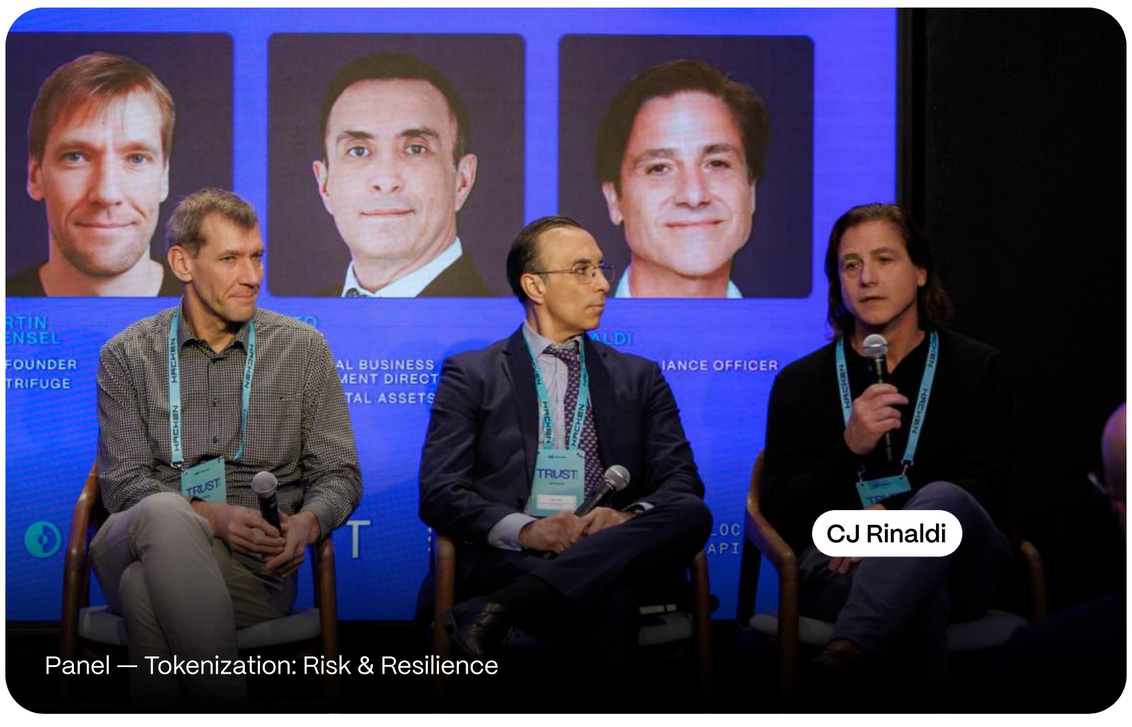
SVP, North American Markets, Nasdaq

Risk & Transparency in RWAs

Martin Quensel (Co-Founder, Centrifuge) highlighted that on-chain products add transparency to risk levels. Tokenization allows investors to see underlying risks (like unpaid invoices in supply chain finance) that are opaque in traditional bundles.

CJ Rinaldi (CCO, Kraken) noted that unlike capital markets, tokenized equities operate **24/7**, creating new arbitrage opportunities that will stress-test system resilience during market meltdowns.

Panel — Tokenization: Risk & Resilience



Panel — Tokenization: Risk & Resilience

III. Stablecoins: The Bridge to Adoption

Stablecoins were positioned not just as trading pairs, but as the future of global payments and settlements.

Transparency of Reserves


Panel — Building Secure Stablecoin Ecosystems

"The main risk is where the cash or reserves sit, and knowing the custodian bank's name is key... Societe Generale keeps cash as a collateral reserve and publishes the names of the custodian banks."

Charles-Antoine Michallet

Director of Digital Assets, Societe Generale

Privacy vs. Verification

Christopher Lalan (Chief Legal Officer, 1Money Co.) argued that privacy and transparency are not mutually exclusive. Technologies like **ZK-KYC (Zero-Knowledge Proofs)** allow a person to prove identity without revealing their specific PII. Simon Jones (Chief Commercial Officer, Baanx) suggested the industry is moving toward "Proof of Actor," verifying who a person is and how they behave, rather than just trusting the transaction.


Christopher Lalan
Panel — Building Secure Stablecoin Ecosystems

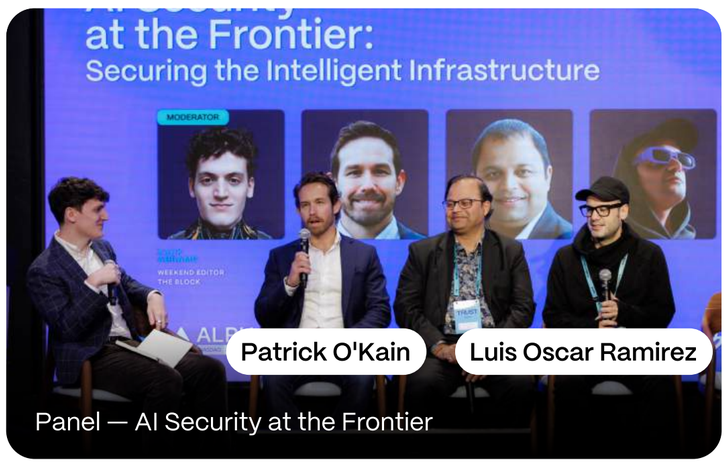
IV. The AI Frontier: Defender and Attacker

Artificial Intelligence is a dual-use technology: a tool for unprecedented efficiency and a weapon for sophisticated fraud. The consensus is that "good AI" will be strictly necessary to combat "nefarious AI" in a perpetual arms race.

The Threat: AI-Powered Social Engineering

Patrick O'Kain (General Partner, Borderless Capital) observed that while complex flash loan attacks have decreased, **social engineering attacks are increasing to almost 50%,** largely driven by AI tools.

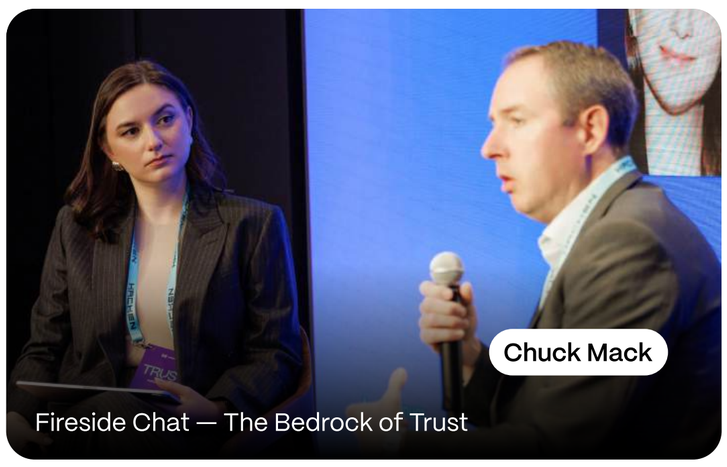
Luis Oscar Ramirez (CEO, Mawari) stated: "Within five years, visual manipulation in XR will be photorealistic and targeted. 'Don't trust—verify' must reach the display stack."



Panel — AI Security at the Frontier

The Solution: AI for Surveillance

Chuck Mack (Nasdaq) detailed how Nasdaq uses AI in "surveillance," making it efficient for analysts to research alerts that were previously manually intensive.



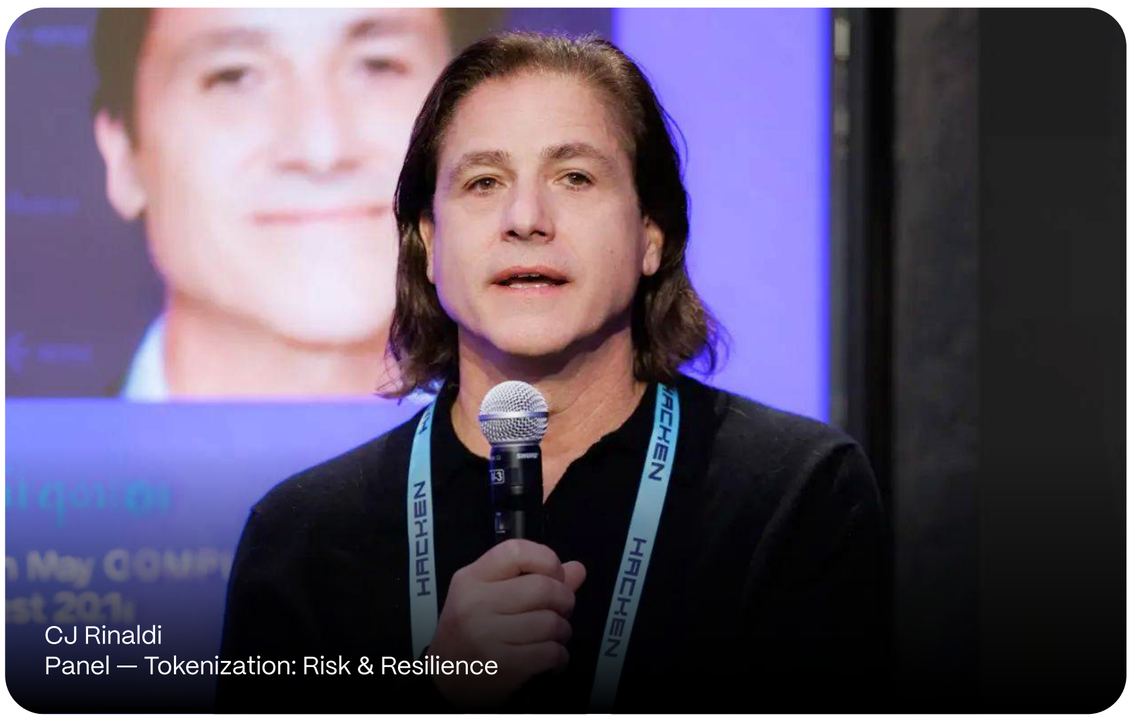
Fireside Chat — The Bedrock of Trust

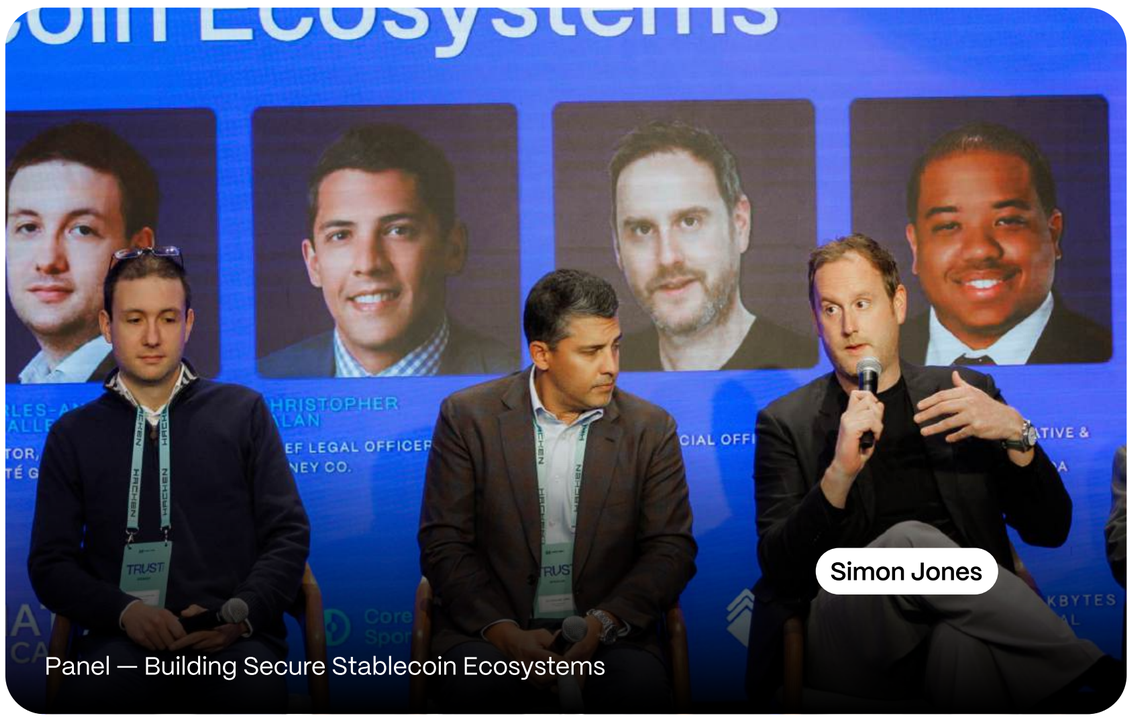
V. Compliance & Regulation

The industry is moving toward "Compliance by Design"—embedding regulatory rules directly into smart contracts and monitoring solutions. However, industry leaders name fragmentation as a top hurdle. In particular, **CJ Rinaldi** (Chief Compliance Officer, Kraken) highlighted the complexity of operating in **25+ global jurisdictions**, necessitating the use of AI to manage differing transactional patterns and laws.

What's the ideal level of regulation?

Incoming Trend: Automated Compliance. Simon Jones (Chief Commercial Officer, Baanx) suggested regulators should allow smart contracts to govern the consumer-merchant relationship, codifying that "code is law" for assured redemption.


CJ Rinaldi
Panel — Tokenization: Risk & Resilience



Panel — Building Secure Stablecoin Ecosystems

Automated Stablecoin Compliance for Bermuda's Financial Regulator

Groundbreaking pilot of the on-chain stablecoin compliance platform for the Bermuda Monetary Authority developed by Hacken, Chainlink, Apex Group, and Bluprynt to give the regulator real-time insight into stablecoin reserves and circulation while automating on-chain compliance and continuous risk monitoring. **Extractor by Hacken** provided real-time compliance and risk monitoring, enabling the BMA to observe on-chain behavior and detect breaches or anomalies instantly rather than weeks or months later.

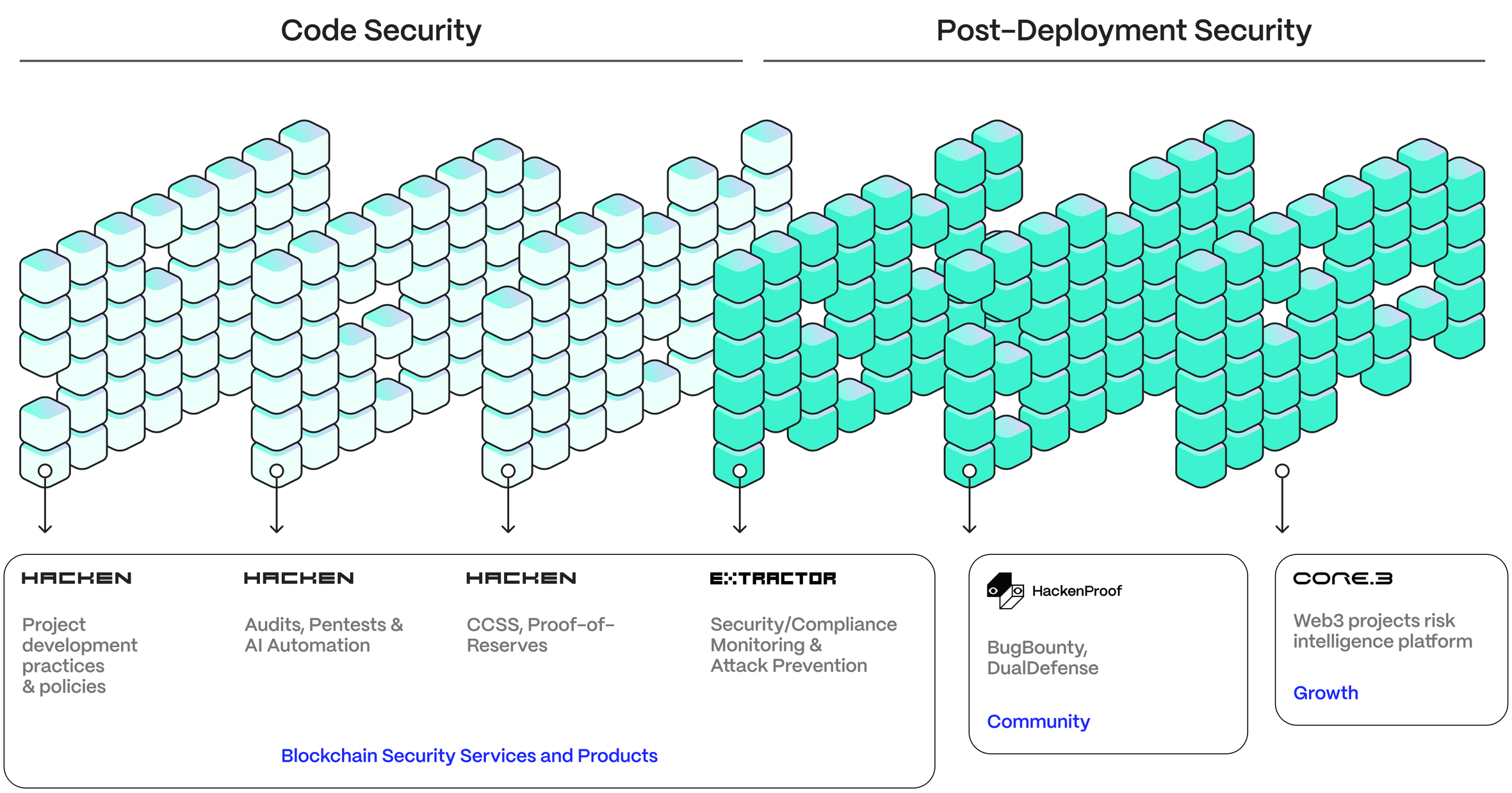
This marks a key 2026 regulatory trend: authorities like the BMA and ADGM are moving oversight live and directly on-chain, with more jurisdictions set to follow.

↗ Learn More

Empowering Secure Innovation for Digital Assets

As digital assets mature, security can no longer stop at pre-deployment audits. Real resilience requires continuous protection across code, infrastructure, operations, and compliance.

Hacken delivers an end-to-end security model that combines deep technical audits, real-time monitoring, crowdsourced validation, and regulatory-grade compliance tooling. Together, these layers address the majority of real-world attack vectors observed across Web3 in 2024–2025.



Hacken covers approximately 95% of observed Web3 incident types through layered security, monitoring, and compliance solutions.

Build Resilient Web3 Infrastructure

Protect your code, operations, and users with layered security and continuous monitoring.

Hacken delivers an end-to-end security model that combines deep technical audits, real-time monitoring, crowdsourced validation, and regulatory-grade compliance tooling. Together, these layers address the majority of real-world attack vectors observed across Web3 in 2024–2025.

↗ Explore Hacken Solutions

Security Services

In-depth assessments across every layer of your blockchain infrastructure

- Smart Contract Audit
- dApp Audit
- Yield Audit
- Blockchain Protocol Audit
- Proof of Reserves Audit
- Cryptography
- Penetration Testing
- Tokenomics Audit & Design
- AI Security Audit

Security Products

Continuous protection with AI-powered solutions and global security researchers

- DualDefense — Post-Audit Assurance
- Extractor — Real-Time Threat Detection and Response
- A3 — White Label Web3 Risks Intelligence for Regulators

Our services are available for all major ecosystems & programming languages

Making Web3 a safer place

Hacken is an end-to-end blockchain security & compliance partner for digital assets

6800+
vulnerabilities found

$430B
on-chain assets verified

1B+
transactions monitored

$15M
paid out in bug bounties

50+
centralized exchanges

30K+
malicious contracts detected

60+
certified security engineers

ISO 27001
certified

Evolving alongside the industry for 8+ years

European Commission · VARA · European Blockchain Sandbox · Enterprise Ethereum Alliance · INATBA · Dubai Blockchain Center · C4 · The Digital Chamber · ERC3643 · Crypto Valley · Qatar Financial Centre · The Millennium Alliance

Trusted by 1500+ digital asset leaders

MetaMask · ethereum foundation · ebsi · ADGM · Forge · Binance · Bybit · crypto.com · OKX · KuCoin · Chainlink · Mawari · nubank · Aurora · Sui

Our Story

Unlike traditional providers, Hacken was born on blockchain, combining deep Web3 expertise with enterprise-grade quality, AI-powered offensive security, and globally recognized certifications. Since 2017, Hacken has been trusted by startups, enterprises, and regulators to secure the new digital frontier.

Learn more: hacken.io

Follow us on social media: linkedIn, X

Authors & Contributors: Yehor Rudytsia (Research & Data Analysis); Oleh Malanii (Editing); Anton Sheptytskyi (Design & Visuals); Valentyna Kondratenko (Legal & Compliance); Stephen Ajayi (AI Security Research); Valeriia Skorik (Production & Coordination); Svitlana Diachenko (Strategic Direction); Yevheniia Broshevan (Executive Oversight).