HACKEN

Quarterly report · Q3 2026

Q3 2026 Security & Compliance Report

Continuous security & compliance assurance. How point-in-time evidence is giving way to ongoing reviews and regular verification.

Contributing Partners

Bluechip GOSAI LAW Stellar Chainlink Labs EUROPEUM



hacken.io

Contents

00 Executive summary 03

01 Q3 losses: amount and composition 04

02 Attack paths and loss mechanisms 08

03 Compliance: supervision, licensing and enforcement 16

04 Conclusions 22

Executive summary

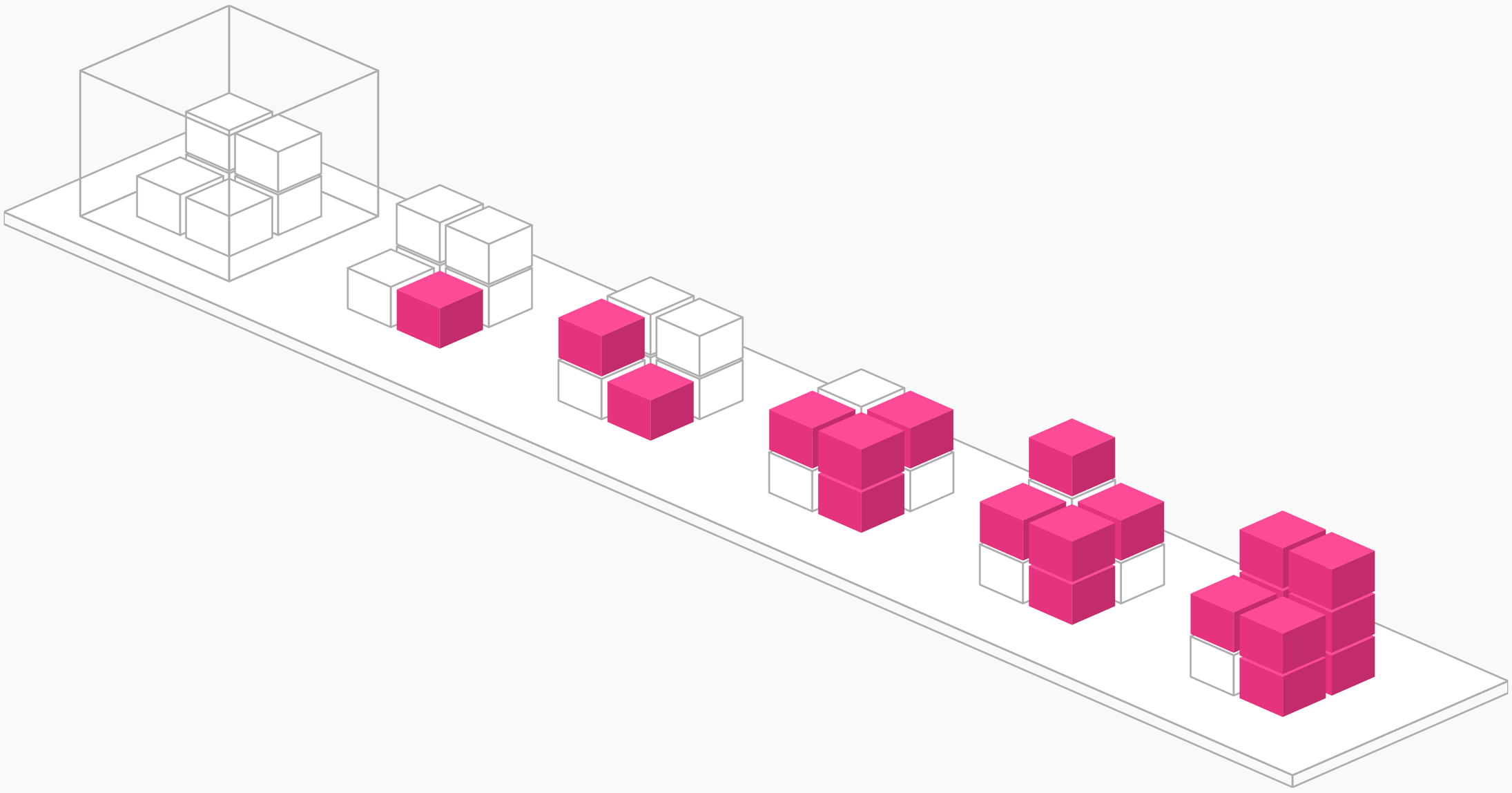
Security and compliance assurance are moving from point-in-time evidence toward evidence that follows change, authority and operational reality.

- **Loss severity concentrated in infrastructure.** Hacken recorded $1,180.8M in losses across 107 incidents between 1 July and 28 September 2026, 55% more in value than in Q2. Application smart contracts accounted for 71 of 107 incidents but only $228.2M, 19% of losses. Most of the value was extracted through chain-level code, suppliers, custody and wallets.

- **The largest attack paths crossed the boundary of the last review.** 77% of losses, $906.8M, came through a compromised supplier or developer tool, a public fix not yet deployed, or a component outside the most recent security review.

- **Known defect classes recur across unrelated codebases.** Six classes, from non-canonical serialization to governance without an effective delay, appeared in independent codebases written in different languages.

- **Regulators are testing controls under continuous operation.** ESMA began reviewing the custody controls of authorized firms on 8 July. Of 24 fines totaling about $229M, 11 addressed failures of monitoring and screening controls. Digital asset firms received five fines totaling approximately $450K, for licensing, disclosure, anti-money-laundering and market-abuse breaches.



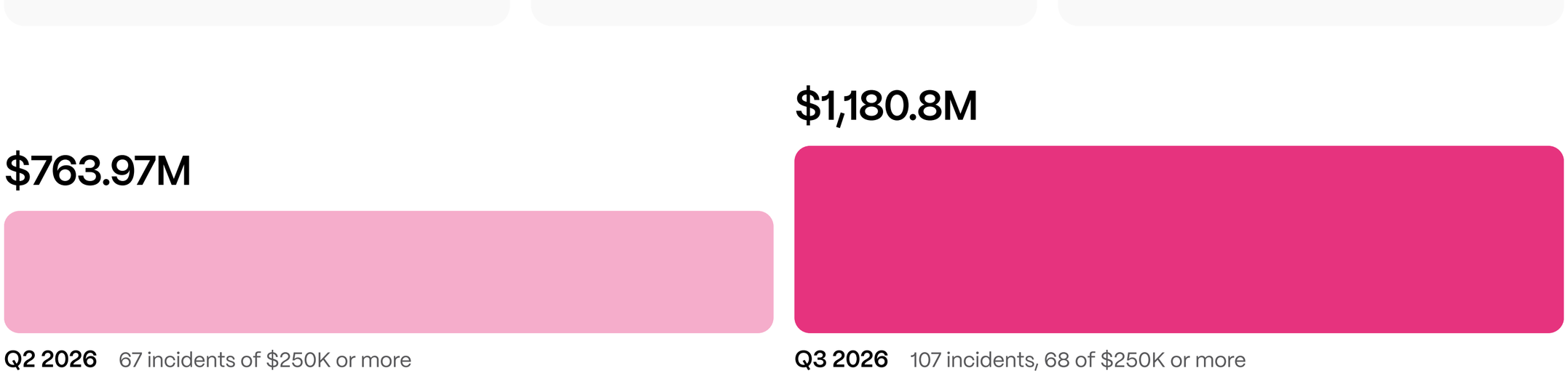
Chapter 1. Q3 losses: amount and composition

Q3 losses rose 55% on Q2, driven by few major incidents

$1.18B
Total loss, 1 Jul to 30 Sep 2026

107
Total incidents

+55%
Change in losses on Q2

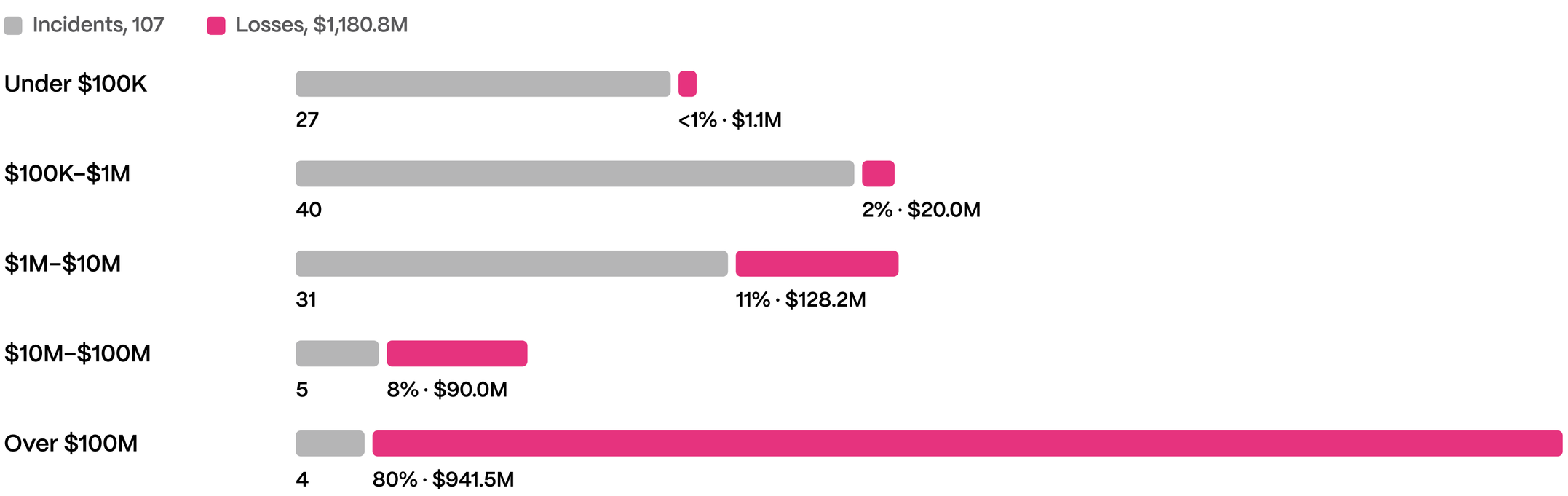


Source: Hacken Q2 2026 report, Hacken Q3 incident dataset, DefiLlama hacks data

Q3 changed where losses concentrated: many small smart contract incidents drove frequency, while a few supplier, custody, wallet and chain-level failures drove severity. By value, Q3 2026 is the largest quarter since the Bybit incident in Q1 2025. Smart contract and protocol code was exploited more often than any other target and mostly for smaller sums: 71 incidents averaging $3.2M, or $1.6M excluding Tectonic

98 incidents recorded a loss below $10M and together lost $149.3M, 13% of the quarter's total. Of these, 67 incidents lost less than $1M each, totaling $21.1M. The median loss across all 107 incidents was $0.67M.

Most Q3 incidents were small, and four carried 80% of the loss

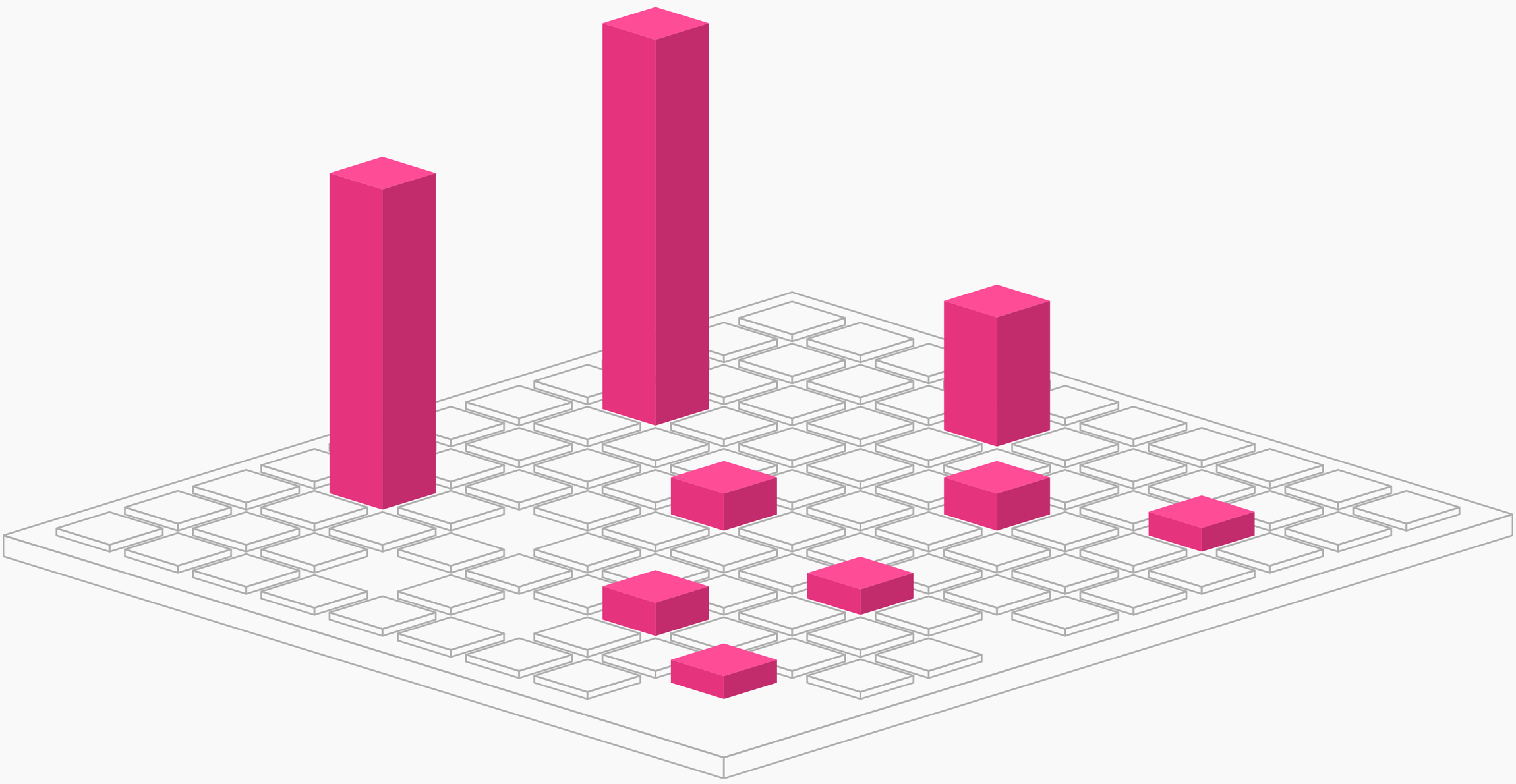


1.1 Largest incidents by value stolen

The 10 largest incidents carried 88% of Q3 losses

The 10 total $1,040.8M, and the other 97 incidents $140.0M

Date	Platform	Vector	Loss
24 Sep	Bitget	Third-party security product flaw. Forged withdrawals bypassed internal risk controls	$387.5M
6 Sep	Liquid Network	Range-proof cache-key collision	$319M
30 Aug	Tectonic / Cronos	TONIC price manipulation against thin liquidity	$120M
30 Jul–6 Aug	Coldcard	Firmware fell back to a deterministic generator	$115M
22 Jul	AFX Trade	Bridge validator keys via a poisoned Git repository	$24M
15 Jul	Ostium	Oracle signer and keeper forwarder compromise	$24M
6 Jul	BonkDAO	Governance takeover, zero-second timelock	$20M
24–26 Jul	Triple-A	Hot wallet compromise	$12M
20 Jul	Wanchain bridge	Non-injective message encoding in Plutus	$10M
22 Sep	Neutron (Astroport, Drop)	Governance proposal passed for ~$20K of NTRN	$9.3M



1.2 Losses by ecosystem and product type

Ethereum, its L2s and BNB Chain had 55% of incidents and 9% of losses

Q3 loss by ecosystem, with incident count

Ecosystem	Incidents	Loss	Share of Q3 losses	Largest mechanisms
Bitcoin and Bitcoin layers	5	$436.9M	37%	Cross-chain verification (Liquid Network, $319M). Wallet key generation (Coldcard, RRWallet, $117M)
Exchanges, custodians and wallet apps, multi-chain	5	$421.1M	36%	Supplier compromise (Bitget, $387.5M). Hot-wallet keys (Triple-A, Duelbits, $19M)
Cosmos SDK chains	10	$144.1M	12%	Spot-price oracle on Cronos (Tectonic, $120M). Governance (Neutron). Cosmos EVM accounting. Bridges
Ethereum and EVM L2s	41	$88.4M	7%	Key compromise (AFX Trade, Ostium, $48M). Share accounting, governance and permission flaws
Other chains	21	$47.2M	4%	Cross-chain verification (Wanchain, Verus, Harmony). Oracles (Bonzo Lend, Nostra)
Solana	7	$29.8M	3%	Governance (BonkDAO, $20M). Bridge (Across)
BNB Chain	18	$13.3M	1%	Missing permission checks (Crypto DAO, $8.2M). Spot-price oracles
Total	107	$1.18B	100%	

Source: Hacken classification of the Q3 incident dataset, DefiLlama chain data

Losses shifted to Bitcoin layers, custody and chain infrastructure

Ethereum, its L2s and BNB Chain had 59 of the 107 incidents, 55%, and $101.7M of losses, 9%. Their incidents were numerous and small: share accounting, permission checks, spot-price oracles and logic flaws in Solidity applications. The larger losses occurred in Bitcoin-layer code written in C++, wallet firmware written in C, in the off-chain infrastructure of multi-chain custodians and in chain-level modules of Cosmos SDK networks.

1.3 Recovery rate

Some $387M was returned or reversed, about 33% of gross losses, through three mechanisms that work differently.

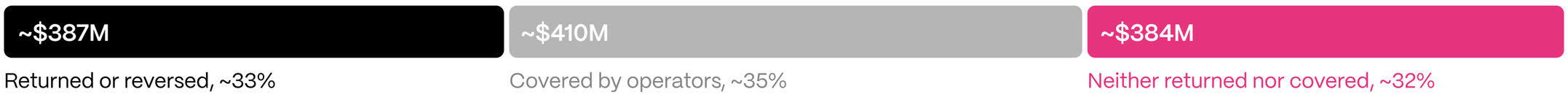
- Attacker return depends on the attacker.
- Chain-state intervention depends on validators changing the ledger.
- Issuer freeze depends on the token issuer, as with Circle and Tether after the Bitget theft.

Mechanism	Value	Events
Attacker return	$272M	Liquid Network, 85% of the $319M taken
Chain-state intervention	~$116M	Cronos rollback of 114 minutes of settled history ($111.2M of the $120.4M borrowed), BounceBit snapshot restore, Cosmos Hub sweep of $2.1M in ATOM from the Neutron attacker
Issuer freeze	~$0.34M	Circle and Tether, from the Bitget theft
Returned or reversed	**~$387M**	**Total**

Operators covered about $410M for users from their own funds: Bitget's User Protection Fund $387.5M, and Triple-A, Coinsbuy and TAC about $22M together. These users were made whole, while the stolen assets remained with the attackers. About $384M, about 32% of gross losses, was neither returned nor covered.

Operators covered more value than was returned or reversed

Gross loss of $1,180.8M by outcome



Source: Hacken Q3 incident dataset, project post-mortems, Cosmos Hub forum

Industry perspective: What happens legally after a protocol loses user funds?

"The litigation runs against three groups, in this order. First, the attacker, rarely identified at the outset, so proceedings are brought against persons unknown, seeking a proprietary injunction, a worldwide freezing order and disclosure orders against the exchanges the assets passed through. Second, the intermediaries. Exchanges and stablecoin issuers are joined to compel KYC and freeze assets, though substantive claims against them are hard to make out.

Third, the project: the operating entity, foundation, founders and DAO participants, pleaded in negligence and misrepresentation. Within twelve months, cross-border matters rarely pass tracing, service, jurisdiction and interim relief. Final judgment is unusual, and most recoveries come from outside the courtroom. Speed decides: assets reaching a compellable intermediary before mixing or bridging are recoverable; otherwise they usually are not."

— Krish Gosai, Gosai Law

Chapter 2. Attack paths and loss mechanisms

2.1 Losses attributed by root cause and mechanism

Code overtook access control and operations as the largest share of losses

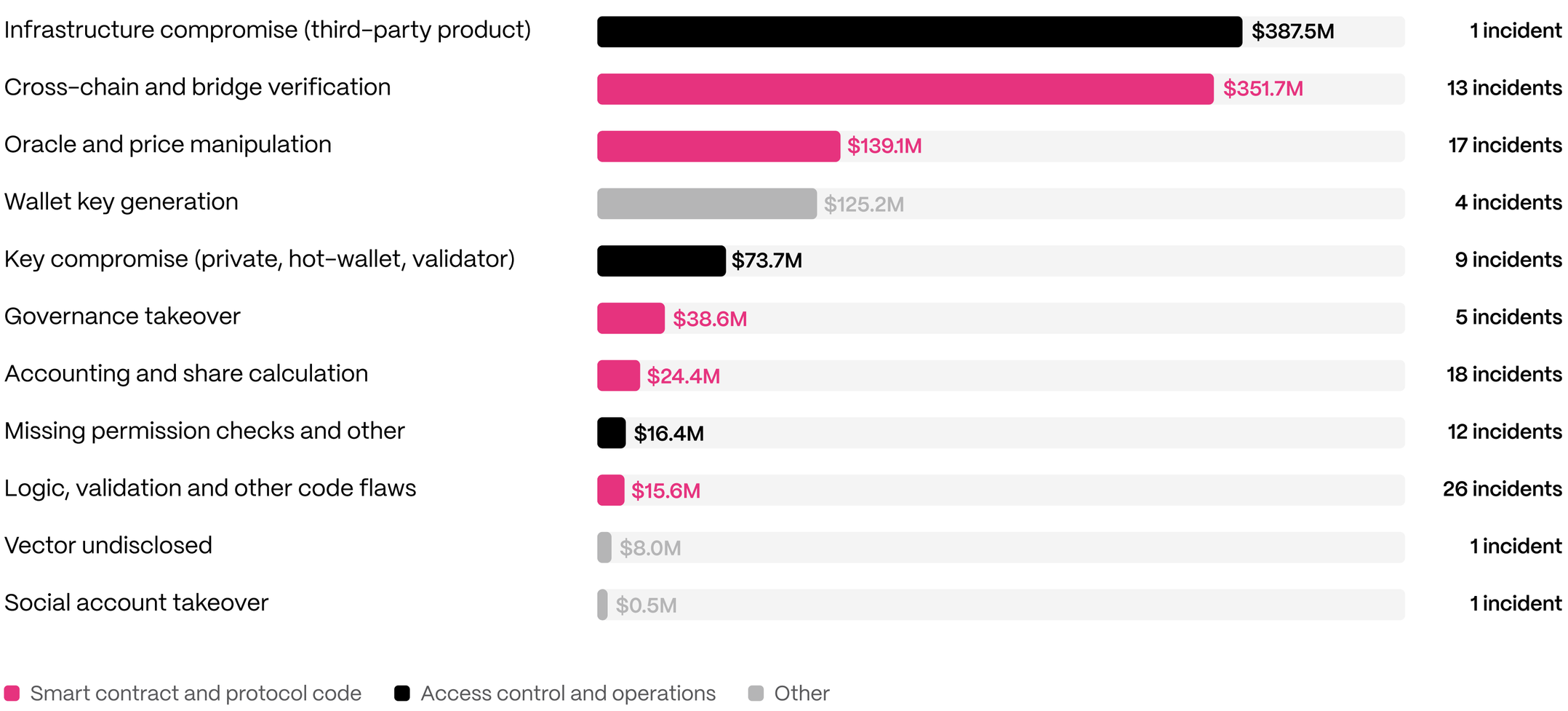
Root cause	Q3 loss	Q3 share	Q3 incidents	Q2 loss	Q2 share	Q2 incidents	Change in share
Smart contract and protocol code	$569.5M	48.2%	79	$87.7M	11.5%	44	+36.8 pp
Access control and operations	$477.6M	40.4%	22	$674.9M	88.3%	21	−47.9 pp
Other	$133.7M	11.3%	6	$1.4M	0.2%	2	+11.1 pp
Total	**$1.18B**	**100%**	**107**	**$763.97M**	**100%**	**67**	

Source: Hacken classification of the Q3 incident dataset, Hacken Q2 2026 report
*Q2 data includes only incidents above $250k of loss

Code defects were the most frequent root cause, at 79 of 107 incidents, and most were small. The 26 logic and validation flaws, the most frequent mechanism, total $15.6M of losses.

The breakdown illustrates what requires protection in digital assets, and why. Losses are divided fairly evenly between the two main categories, but their profiles differ. On-chain exploits of smart contract code occur frequently and for smaller sums, with an average loss of $7.2M. Access control incidents are fewer but carry a higher average loss mostly because of Bitget, $21.7M, or $4.3M excluding Bitget.

Root causes by loss and frequency

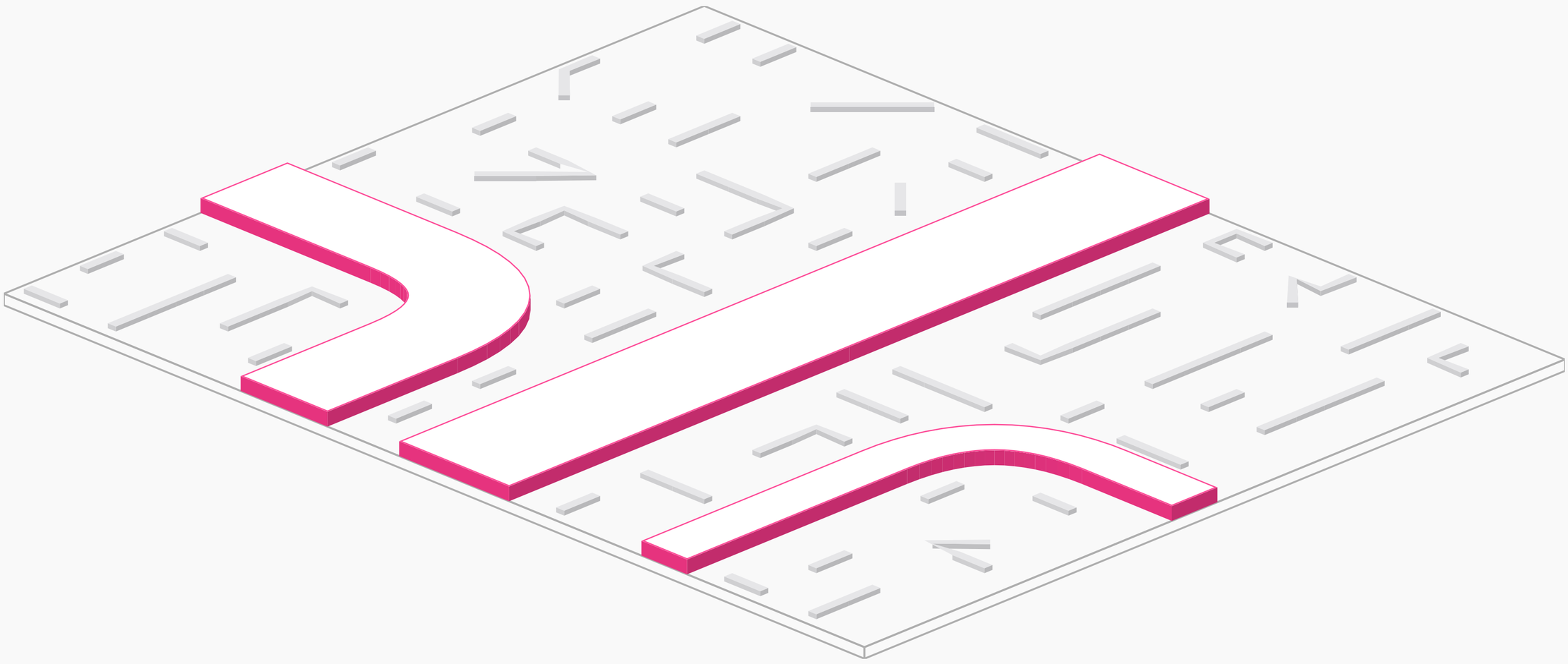


2.2 Three attack paths not included in security reviews concentrated most losses

Two supplier incidents alone exceed the 96 other incidents combined, $411.5M against $274.0M.

Three routes carried 77% of Q3 losses in 11 incidents

Route	Loss	Incidents	Share	Cases
Supplier or developer tooling	$411.5M	2	35%	Bitget (third-party security product), AFX Trade (poisoned Git repository)
Public fix exploited before deployment	$324.8M	4	28%	Liquid Network, Cosmos EVM chains (KiiChain, TAC, Nesa)
Component outside the most recent review	$170.5M	5	14%	Tectonic, Ostium, Bonzo Lend / Supra, Moonwell, Term Labs
All other incidents	$274.0M	96	23%	



2.3 Suppliers and developer tools on attackers' target list

Bitget. The theft of $387.5M on 24 September spanned 11 blockchains, including Ethereum, the XRP Ledger, TRON, Arbitrum, Base and BNB Chain. XRP was the largest single asset taken, at roughly $158M. According to Bitget CEO Gracy Chen, neither private keys nor cold wallets were compromised.

Reports by SlowMist and Mandiant, released by Bitget on 30 September, trace the entry point to a zero-day vulnerability in a third-party security product, with the earliest malicious activity in the available logs dating to 31 August. The attackers used it to obtain high-level internal credentials and to reach the wallet backend.

On 24 September, a custom withdrawal tool forged risk-control parameters, constructed withdrawal requests and submitted them to Bitget's own withdrawal process, which approved them. Bitget considers North Korean involvement very likely, citing IP behavior.

Bitget's incident timeline

$387.5M	2h 52m	~$0.34M
Loss, revised 25 September	First transfer to last outflow	Frozen by Circle and Tether

31 Aug	Vendor zero-day first exploited (30 September update)
24 Sep 18:31	First unauthorized transfers
19:01	First burst of outflows
19:05	Bitget reconciliation alert
19:16	Second burst of outflows
20:40	Transfers of remaining hot-wallet funds to cold storage begin
21:23	Last outflow

Source: Bitget incident page and notices, Bitquery, Mandiant, SlowMist.

AFX Trade. The bridge lost $24M on 22 July after attackers gained signing control over five of its seven validators. The entry point was a malicious Git repository sent to one of the firm's developers by an attacker posing as a recruiter from Oddium Lab. From 9 July, the attacker persuaded the developer to clone the repository, whose hidden configuration executed a payload during a routine Git operation.

The attacker then moved through internal development systems, placed a malicious plugin in the firm's JFrog artifact repository and drained the bridge 13 days after first contact. This incident is being attributed to DPRK-linked group UNC4899, also tracked as TraderTraitor.

2.4 Public fixes on adversaries' side

Cosmos EVM. Six chains were exploited for $5.72M after attackers used a publicly disclosed vulnerability in Cosmos EVM. The flaw allowed vesting accounts to spend locked tokens. When the EVM layer reconciled the resulting balance with Cosmos accounting, an underflow produced a value near 2^{256}, which let the attacker overwrite another account and withdraw its real tokens.

A bug-bounty report reached Cosmos Labs on 25 April, and a fix merged into the public repository on 15 May. However, the release tags that dependent chains needed did not follow until 19 August, leaving a 96-day gap between the public fix and the updated releases. On 20 August at 07:16, a downstream fork published the exploit path based on the public commit. The first known attack began at 19:06, less than 12 hours later. The vulnerability had been fixed in the code, but the delay in releasing that fix left chains exposed.

Cosmos EVM exploit timeline

25 Apr	Bug-bounty report reaches Cosmos Labs, which judges known production configurations safe
15 May	Fix merged to the public main branch
19 Aug	Backported release tags ship, after research shows every Cosmos EVM chain exposed
20 Aug 07:16	A downstream fork's pull request describes the vulnerability, exploit path and affected releases
20 Aug 19:06	First known attack begins

Source: Cosmos Labs post-mortem

Industry perspective: How does Europeum-EDIC prevent an incident like Cosmos EVM's?

"We start the clock when a security fix is merged upstream, not when it's released. Europeum tracks upstream security commits and node operators have contractually agreed patch deadlines, for example 8 hours for critical fixes. We roll upgrades out in waves so the network never loses consensus quorum, and we check every node's version centrally. A node that misses the deadline is escalated and in the end suspended. If it's needed, we can also trigger a coordinated emergency upgrade that we've rehearsed in advance."

What would Europeum recommend to other public-sector operators?

"Put patch deadlines and consequences into the node operator agreements. Have one release authority that produces signed builds. Keep an inventory of every software dependency and sign up to receive upstream security disclosures. Monitor which version every node runs. Rehearse emergency upgrades every year. And share threat intelligence with other public networks and with national cybersecurity teams, so that the next warning reaches everyone on the same day."

Which lessons matter most for permissioned networks?

"First, once a fix is merged publicly, the vulnerability is effectively disclosed, so the time between merge and release is the real exposure window. Second, when every operator runs the same code, a single bug hits all of them at once. Third, operators run independently, but that doesn't make them ready: each one needs on-call staff and the authority to upgrade fast."

— Iulian Nita, Service Operations Manager at Europeum-EDIC (operator of EBSI) EUROPEUM

Liquid Network. On 6 September, an attacker exploited an ambiguity in Elements' range-proof verification cache to mint 3,998.5 L-BTC without the corresponding BTC reserves. Elements caches successful range-proof checks because verification is computationally expensive. Its cache key did not encode transaction fields unambiguously, allowing a proof validated for one asset and context to be reused in another.

A partial fix, which added transaction context to the cache key, had been public in the Elements repository since 1 September. It left the encoding ambiguous, and the attacker exploited the remaining flaw. A peg-out of about 4,000 BTC subsequently confirmed on Bitcoin.

On 7 September, the attacker, describing themselves as a white hat, returned about 3,400 BTC ($272M) on condition that the flaw be patched. They retained 598.5 BTC, worth about $47M, as a self-assigned bounty.

Liquid Network exploit timeline

1 Sep	Partial fix, adding transaction context to the cache key, public in the Elements repository
6 Sep	Exploit: 3,998.5 L-BTC minted with no BTC behind them
6 Sep, later	Peg-out of about 4,000 BTC confirmed on Bitcoin
7 Sep	Attacker returns about 3,400 BTC ($272M) and keeps 598.5 BTC, about $47M
8 Sep	Complete fix merged
9 Sep	Fix ships as Elements 23.3.4

Source: Elements repository (PR #1600) and release notes, TRM

Industry perspective: What controls does a licensed issuer require from the network?

"When institutions move regulated assets onchain, security cannot be evaluated as an afterthought around the edges of the system. It has to be part of the infrastructure itself. The Stellar network has been designed with compliance in mind since the beginning. It is a public, auditable settlement network with configurable, protocol-level controls for authorization, freezing and clawbacks.
For example, U.S. Bank's recent live USBDC pilot on Stellar tested minting, redemption, freezing and clawback functions while integrating the blockchain with the bank's existing finance, risk, compliance and operations infrastructure. The point is not to make institutions choose between the openness of a public network and the controls required to operate in a regulated environment. Stellar was designed to give them both."

— Tomer Weller, Chief Product Officer, Stellar Development Foundation

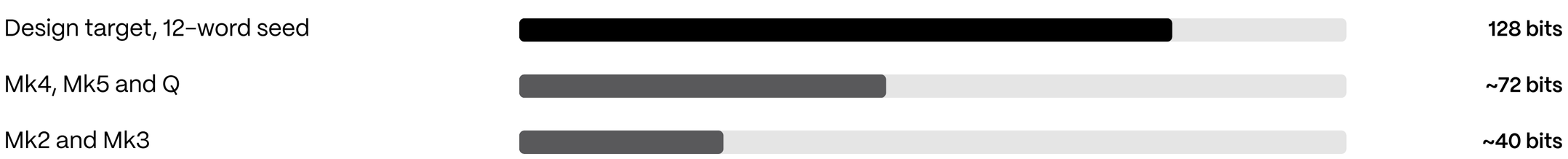
2.5 Earlier reviews missed the conditions behind two Q3 exploits

Coldcard. The incident involved Bitcoin seeds generated with substantially less entropy than intended, resulting in approximately $115M in losses. A firmware change introduced in March 2021 added a build guard that checked whether a hardware-randomness setting existed rather than whether it was enabled. Hardware randomness dropped out of the build, and seed generation fell back to a software pseudorandom generator.

A 12-word Bitcoin seed is designed to provide 128 bits of entropy. Coinkite estimates that affected seeds carried about 40 bits on Mk2 and Mk3 devices and about 72 bits on Mk4, Mk5 and Q. This reduced the search space enough for attackers to generate candidate seeds, derive their addresses and match them against funded addresses on the blockchain. Galaxy Research attributes 1,789.28 BTC across 8,865 addresses to the incident, worth about $114.7M at the time of theft. A paid review in March 2022 covered entropy hardening but did not identify the build condition.

Affected Coldcard seeds carried a fraction of the intended entropy

Effective entropy per seed, bits



Each bit doubles the search space: 40 bits is 2^{88} times smaller than the 128-bit target, and 72 bits 2^{56} times smaller.

Source: Coinkite

Tectonic. The attacker targeted TONIC, Tectonic's own token. They pushed its price up against thin DEX liquidity over about 11 minutes, and Tectonic accepted the inflated price as collateral value. Reported correctly, a price can still be unusable at that value. Three controls that would have caught it were missing at Tectonic:

- a liquidity-depth limit, asking whether that much TONIC could actually be sold at the reported price
- a velocity limit on how fast borrowing power could follow the spot price
- a working borrow cap: Tectonic's published parameters list a borrow cap of 0 for every market, including TONIC, and in its Compound-derived code a zero cap means no cap

According to the Cronos post-mortem, one transaction then borrowed $120.4M across nine markets against the inflated collateral. Four audits had reviewed Tectonic's code, one of them the core lending logic. Checking that a lending contract calculates collateral correctly does not establish that the parameters for one collateral asset are safe in its real market.

In the end, Cronos and its validators halted the chain and restored it to the last block before the attack, reversing about $111.2M, 92% of the $120.4M borrowed.

2.6 The authority path to funds extended beyond the reviewed component in most documented cases

Five of six exploited privileged components were outside the most recent review

Incident	Most recent review covered	Exploited component	What the component could reach
Ostium	Latest listed review: Pashov, January 2026. Zellic noted in writing in November 2025 that forwarders could cancel any order, as a design assumption	Keeper forwarder and price signer. Compromised keepers excluded from the Immunefi bounty	Forged, future-dated prices settled against the OLP vault
Bonzo Lend / Supra	Supra's Move contracts on Aptos	EVM verifier contract on Hedera, live about 2 years	A BLS identity-element bypass accepted forged oracle data
Term Labs	Core protocol, audits including Certora	Custom governance wrapper (Aragon TokenVoting, Zodiac Delay), no published audit found	An empty electorate was taken over and the Zodiac delay set to zero
Moonwell	One strategy contract, one engineer, one day	MAMO market	Exchange-rate inflation by direct donation, then price manipulation
Tectonic	Contract code, four audits	Risk parameters	$120.4M borrowed in one transaction
Coldcard	Entropy hardening, March 2022	Entropy source	Seed generation on every affected device; in scope, build condition missed

In five exploit cases of Q3, the exploited code component was not included in the reviewed scope, yet each held a role that reached client funds: it could sign prices, verify cross-chain messages, execute governance, price a market or set borrowing limits.

Industry perspective: Does having an audit help a project in court?

"An audit is evidence, not a safe harbor. It assists the project where the auditor reviewed the deployed code, the audit was current at the exploit, findings were remediated and verified, and later changes controlled. The same report hurts where any step is missing. A claimant will ask whether the exploited function was in scope, whether the auditor flagged the risk, whether findings were unresolved, whether deployed code differed from what was reviewed, and whether the project kept calling itself 'audited' or 'secure'. Those facts support a misrepresentation claim. A badge on the website carries little weight; a project is best placed where the audit is part of a continuing risk-management process."

— Krish Gosai, Gosai Law GOSAI LAW

2.7 The same technical defects recur across independent codebases

Defect class	What goes wrong	Q3 incidents
Non-canonical serialization	Variable-length fields concatenated without length prefixes, so distinct inputs produce identical bytes and one signature or cache key covers both	Liquid Network (C++), Wanchain (Plutus), Injective (Go), Coreum (Go)
Build and configuration checks by existence	A guard tests whether a flag or value is defined rather than what it is set to. A zero reads as unlimited or as enabled	Coldcard (#ifndef on the RNG flag), Tectonic (borrow cap of zero read as unlimited)
Weak key generation	Wallet software or firmware draws keys from a predictable source, so seeds can be searched	Coldcard, D'CENT, RRWallet, Zilliqa
Balance and share accounting mismatch	The ledger model and the token model disagree on what a balance is, or share prices move on a direct donation	Cosmos EVM (spendable against locked balance, underflow to ~2^{256}), Moonwell, Lazy Summer...
Spot price against thin liquidity	Borrowing or minting priced from a pool that one transaction can move	Tectonic, Nostra, Moonwell, Flamincome...
Governance with no effective delay	A proposal can pass and execute before holders can react	BonkDAO, Term Labs, Neutron...

The Q3 cases show that these issues can recur across different languages, protocols and implementations. A defect identified in one codebase does not automatically become visible to teams working on a different implementation of the same underlying logic.

None of these defect classes is new. Non-canonical serialization is a known source of collisions, including the abi.encodePacked issue in Solidity, while manipulable spot-price oracles have been implicated in lending-market incidents for several years.

We recommend using incident-driven variant analysis. When a major incident exposes a defect class, teams can search their own code and configuration for equivalent conditions rather than limiting the review to the affected implementation. The same principle can be applied through:

- **Variant analysis after every major incident.** Search the codebase for the defect class, whatever the language, rather than only checking whether the affected dependency is used.
- **Defect-class checklists per language**, built from incidents and run in every review and every CI pipeline.
- **Invariants that encode the class.** Canonical encodings with explicit lengths, build flags tested by value, non-zero governance delays, liquidity-depth caps on spot-priced collateral and balance invariants across ledger models.
- **Configuration and parameters as release gates.** A listing, a cap or a build flag gets the same sign-off as a code change.

Variant analysis is also a useful application of AI-assisted code review. The same defect pattern can be searched for across large and heterogeneous codebases, provided the underlying condition is defined precisely enough to distinguish relevant variants from false positives.

Industry perspective: What should a protocol do when a price looks wrong?

"An oracle accurately reporting a distressed or manipulated market is different from an oracle reporting incorrect data. Protocols should assess the asset's liquidity and market integrity, set collateral and borrowing limits accordingly, and use application-specific bounds or suitable independent references to detect anomalies. A lagging time-weighted average or a price from a thinly traded pool is not a reliable basis for overruling a market-wide price."

— Chainlink Labs Chainlink Labs

2.8 Exposure followed change, authority and time

Across Q3, several incidents share a common condition: post-review changes, authority over funds or risk parameters being outside the reviewed scope, or an older defect present in code without reassessment against later findings.

We assume that AI-assisted tools influence the quantity of smart-contract exploits, as these instruments reduce the cost of code analysis and exploit development. While exact AI-influence could not be quantified, the incidents do show several areas where existing exposure can persist between reviews and deployments.

Four exposure points recur in the Q3 evidence:

- **Public commits.** A merged security fix can reveal the underlying defect before the fix is deployed. In at least two cases, attackers acted on information available through public fixes while affected deployments were still exposed.
- **Legacy code.** A previous audit does not establish that a codebase remains secure after new defect classes, attack techniques or implementation changes emerge.
- **Scope and post-review change.** In five of six documented cases, keepers, verifiers, governance wrappers or risk parameters had authority affecting funds outside the reviewed code scope. Parameter and build changes can therefore alter the security properties of a deployment without changing the audited contract code.
- **Fix distribution in shared ecosystems.** A fix merged upstream does not mean that all downstream deployments have adopted it. For Cosmos EVM, 96 days passed between the merged fix and a tagged release.

Industry perspective: An oracle is a shared component for thousands of projects. What failure do you plan for?

"We plan for failures in both the integrity and availability of oracle data, including correlated failures that affect multiple components at once. That means accounting for compromised data sources, node outages, shared software vulnerabilities, and blockchain congestion. Chainlink's defense-in-depth architecture addresses these risks across the full path from data sourcing to onchain delivery.

Chainlink's market price feeds use three layers of aggregation: professional data providers aggregate prices across trading venues, independent node operators aggregate data from multiple providers, and the oracle network aggregates node observations. This combines market-wide coverage with decentralized validation, reducing exposure to manipulated prices on an individual exchange or a compromised data provider. The operators are security-reviewed and Sybil-resistant, with geographically distributed infrastructure spanning cloud providers and bare-metal servers. Monitoring, failover systems, and redundant blockchain connections add protection against infrastructure outages.

Chainlink also uses decentralized oracle networks that deliver price data natively to each supported blockchain. This avoids making price updates across multiple chains dependent on one intermediary blockchain or a bridge relaying those updates. It limits a source of correlated failure, while each feed still depends on the availability of the chain where it publishes data.

Shared software risk requires additional defenses. Chainlink combines regular security audits with continuous monitoring and bug bounty programs. For integrators, using a feed's proxy address allows the underlying aggregator to be upgraded without changing every consuming contract. Teams should also follow feed maintenance notices and verify that any required integration changes have been applied. The lesson from an unapplied patch is that remediation must reach production to protect users.

That defense in depth extends into the application. Protocols need tested freshness checks, circuit breakers, and exposure limits suited to their markets, alongside procedures for pausing and safely resuming affected operations. Secure oracle infrastructure and sound application risk management are both essential to protecting user funds."

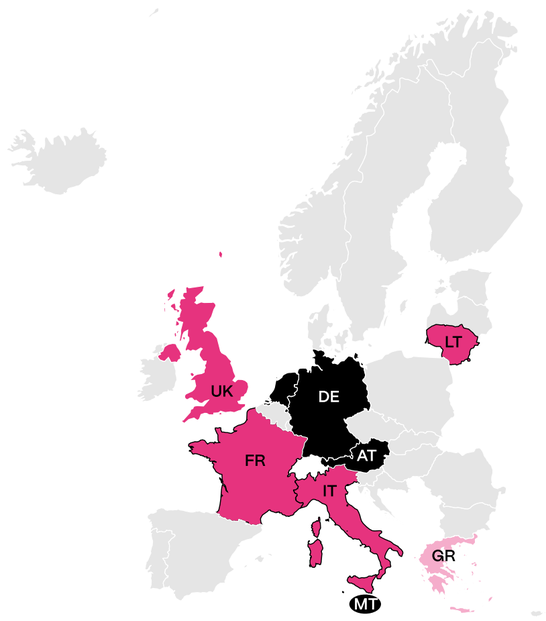
— Chainlink Labs Chainlink Labs

Chapter 3. Compliance: supervision, licensing and enforcement

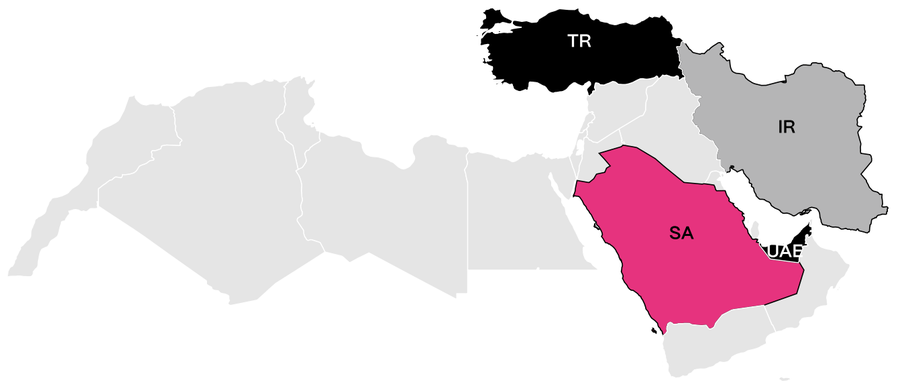
In Q3 2026, supervisory attention shifted to continuous verification of how security controls operate. ESMA launched a custody review of authorized firms on 8 July, and the quarter's largest penalties addressed controls that were documented but did not operate as designed.

Enforcement reached every region

Monetary penalty · Supervisory or perimeter action · Open case · Sanctions target · No enforcement in Q3 recorded



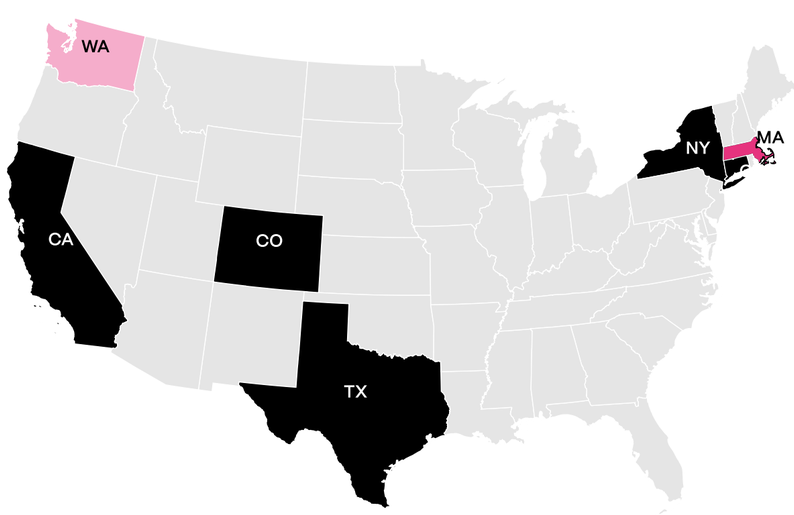
EEA & UK



Turkey and MENA



Asia-Pacific



United States

3.1 Supervision now requires operating evidence from authorized entities

In our assessment, Q3 showed three shifts in supervisory practice:

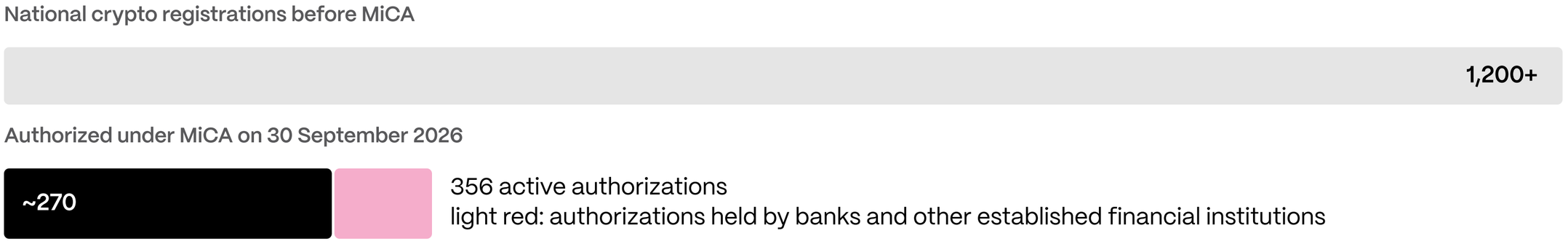
- **Authorization is becoming the start of continuous supervision.** ESMA's Common Supervisory Action (launched on 8 July 2026) reviews authorized CASPs across six areas, including key management and third-party dependencies, through mid-2027. This changes the model for authorized entities from achieving point-in-time evidence to meeting security obligations over an extended period under supervision.
- **Supervisors increasingly expect evidence that controls operate in practice.** On 31 July, the European Supervisory Authorities stated that annual penetration tests and compliance audits may be insufficient in an environment of AI-accelerated exploitation, and encouraged continuous vulnerability scanning and dependency monitoring. The direction is clear: documented policies are weaker evidence where firms cannot demonstrate that controls operate across the systems and activities they run.
- **Responsibility is moving to individuals and connected parties.** Hong Kong's SFC said on 9 July that it will hold firms accountable for client losses from inadequate authentication controls, and that senior management are responsible for overseeing the change. At the same time, Korea's amended Specified Financial Transaction Information Act, in force from 20 August, extended fitness review to major shareholders of exchanges. We expect these trends fully or partially to be adopted across other major jurisdictions. Due diligence therefore has to extend to who controls critical functions and whom a counterparty serves.

The US remains on a different timeline. Q3 produced more movement in supervisory enforcement and sanctions than in rulemaking: the CLARITY Act did not advance, while the GENIUS Act still lacks clearly defined rules. Federal action against crypto firms in Q3 was concentrated in sanctions designations rather than operating-control supervision.

3.2 MiCA has consolidated the EEA market

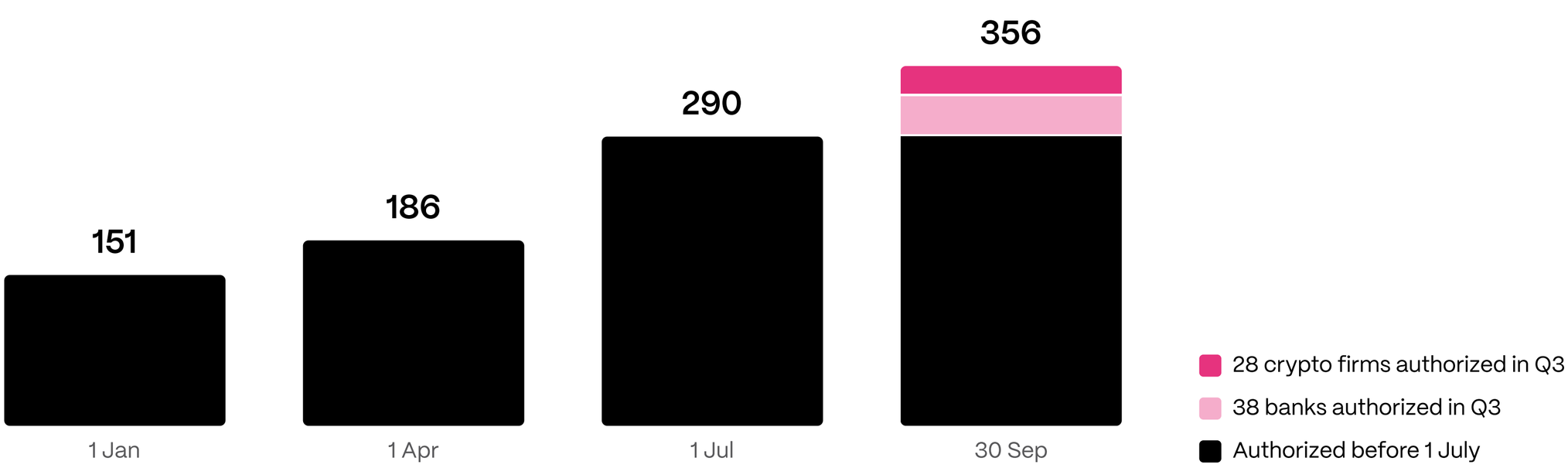
By our estimate, MiCA has reduced the number of firms authorized to serve EEA clients by more than two thirds and shifted the market toward banks and larger exchanges. More than 1,200 firms held national crypto registrations before MiCA, according to KPMG. ESMA's register lists 356 firms authorized as of 30 September 2026.

Pre-MiCA national registrations compared with MiCA authorized CASPs in 2026



Source: ESMA interim MiCA register (file updated 6 October 2026), entries dated to 30 September 2026; pre-MiCA baseline from KPMG.

The MiCA register more than doubled in 2026



Source: ESMA interim MiCA register (file updated 6 October 2026), entries dated to 30 September 2026, CASPs by authorization date.

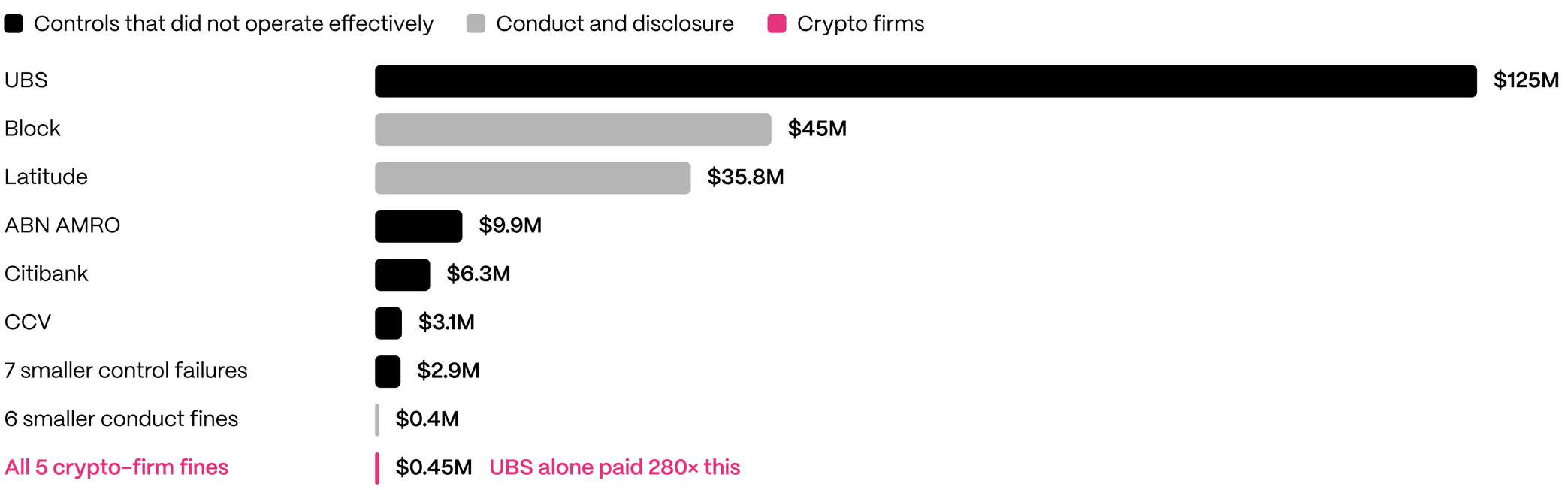
- **Higher market concentration.** Authorizations peaked at 75 in June 2026, ahead of the end of the transitional period, and licensed venues accounted for approximately 83% of European trading volume that month, according to Kaiko Research (20 July 2026). In our assessment, greater concentration increases the potential client impact of a custody or key-management failure at any single authorized firm.
- **Banks and financial institutions as distributors of crypto services.** 38 of the 66 register entries dated between 1 July and 30 September went to banks, mainly German cooperative banks notifying under Article 60.
- **MiCA is tightening access, but enforcement of the boundary is still being tested.** When the transitional period ended, Binance France's legacy registration lapsed on 2 July, together with those of 53 other French providers that had not obtained MiCA authorization. After withdrawing its Greek MiCA application, Binance stopped new EU registrations and restricted services from 1 July. Press reports after the quarter say it continued serving some EU clients through Abu Dhabi entities under MiCA's reverse-solicitation exemption. That exemption is narrow: the client must initiate the relationship, the firm cannot solicit clients in the EU, and it cannot be used to market new types of crypto-asset services. In October, ESMA and several national authorities were reported to be reviewing whether that activity stays within those limits.

3.3 Q3 enforcement followed provable control failures, often after incidents

Q3 enforcement did not yet mirror the quarter's security losses. Hacken recorded 24 fines against crypto, fintech and adjacent firms totaling approximately $229M, with 11 fines for monitoring and screening controls that did not operate effectively. Crypto firms received five fines totaling approximately $450K, for licensing, disclosure, anti-money-laundering and market-abuse breaches.

None of the key-management, dependency or configuration failures that drove the major security losses resulted in a fine.

The UBS penalty was 280 times the combined fines on crypto firms



Bar length is proportional to the fine.

Source: regulator notices and press reports; fines published 1 July–28 September 2026.

Control failures were identified after an attack

3

Ransomware attack

Order Express · NYDFS

Academy Mortgage · California DFPI

Luk Fook · SFC

3

Hack or ledger error

Bitkub · Thai SEC

Upbit · Korea FSS

Bithumb · Korea FSS

4

Supervisory examination

UBS · FinCEN

CCV · DNB

CoinFlip · Washington DFI

Midas · SPK

1

Partial self-report

Citibank · OFSI

Source: Hacken Q3 2026 enforcement register.

- **Incidents as the trigger for enforcement.** In six of the eleven control-failure cases we tracked, fined or pending, an incident exposed the weakness: three ransomware attacks, two exchange hacks and one ledger error. In our assessment, the first significant security sanction against a crypto firm will follow an incident; Korea's pending Upbit and Bithumb cases may be first, with a Bithumb decision expected around year-end.
- **Timely reporting does not offset control deficiencies.** Order Express reported its ransomware incident to NYDFS within the required timeframe and was nonetheless fined $250K for deficiencies in its risk assessment and patch management.
- **Accuracy of regulatory reporting.** Thailand's SEC has filed a criminal complaint alleging that Bitkub omitted a hot-wallet loss of approximately $47M from its capital reports for six months. Korea's proceedings against Upbit and Bithumb, opened in July and August, are still pending.

3.4 Cyber resilience requirements anchor independent testing to fixed cycles

Q3 exposed a gap between the speed at which digital-asset systems change and the way regulatory assurance is scheduled. All five frameworks reviewed require recurring testing, and all expect changes to be tested through the firm's own change management. They differ in what a change triggers: some require additional testing, others continuity, recovery or risk reviews.

None makes a dependency or configuration change trigger independent security testing, the kind of change behind Cosmos EVM and Tectonic. This is a finding about the texts reviewed, not legal advice.

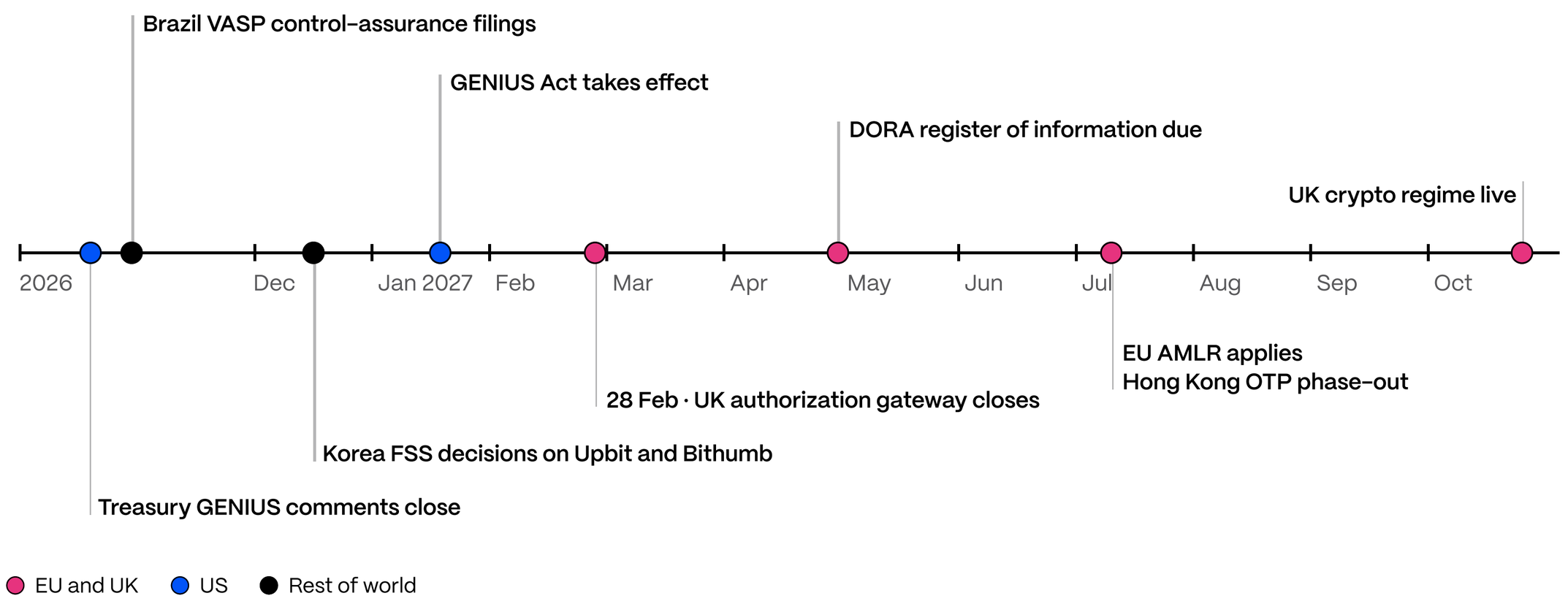
Regime	Periodic testing	Change-triggered requirement	Before a new system goes live	Dependency or configuration change
EU · DORA	● At least annual testing of ICT systems supporting critical or important functions (Art. 24(6))	● Continuity and response/recovery plans after substantive changes (Art. 11(6))	● Testing of ICT systems before use (RTS 2024/1774 Art. 16)	◐ Change testing and open-source library tracking (Art. 9(4)(e); RTS Arts 10, 17); no independent re-test
US · NYDFS Part 500	● Annual penetration testing (500.5(a)(1))	● Vulnerability scans promptly after material system changes (500.5(a)(2))	○ Not found	◐ Scans after material system changes; no dependency trigger
Singapore · MAS TRM Guidelines (non-binding)	● Annual penetration test of internet-facing systems (13.2.4)	● Penetration test after major changes (13.2.4)	● Testing before production (6.1.3, 7.5.3)	◐ Open-source tracking and patch testing (6.1.4, 7.4)
Dubai · VARA	● Independent VAPT at least annually (Rule I.E.1)	● Tests before any production update (Schedule 1 B.11, guidance)	● Independent testing before a new system, application or product (Rule I.E.1)	◐ Production updates and external protocol changes (Sch. 1 B.11; Rule I.B.3(n))
UAE · CMA	● Annual testing of internet-connected systems (Art. 51(16)(b))	● Changes tested before implementation (Art. 51(6)–(7))	◐ Through change management (Art. 51(7))	◐ Change testing and software updates (Art. 51(7)–(9))

● The requirement appears in the text named.
◐ Covered only by the firm's own change or patch testing; no independent test is triggered.
○ Not mentioned in the texts.

- **Change-triggered assurance is not the same as repeating the annual test.** DORA requires continuity and recovery plans to be tested after substantive changes, and its technical standards require changes to be tested before production. NYDFS requires vulnerability scans promptly after material system changes, and MAS expects penetration tests of internet-facing systems after major changes. Only VARA requires an independent test of every new system before it goes live; DORA sets that for central securities depositories and central counterparties only.
- **Dependencies remain a practical assurance problem.** DORA's register of information covers contractual ICT services, and inherited open-source components are usually not contractual. DORA's technical standards do require firms to track the open-source libraries they use and, where feasible, to test that code before deployment, but no text reviewed sets a deadline for applying an upstream fix. The Cosmos EVM fix took 96 days to reach a tagged release.
- **Other assurance gaps remain outside the testing cycle.** Apart from VARA's custody disclosures on forks and finality, the frameworks reviewed do not require firms to show whether settlement on a chain can be reversed, as the Cronos rollback did. None covers devices that clients buy for self-custody; DORA reaches a hardware supplier only when it provides services to a regulated firm. The Coldcard defect went undetected for more than five years.

3.5 Key compliance milestones through October 2027

Compliance milestones, October 2026 to October 2027



Source: ESMA, FCA, US Treasury, Federal Register, Korea FSS reporting, CVM IN 739, SFC circular of 9 July 2026, Supreme Court docket 26-299.

Industry perspective: What do you expect of stablecoin ratings adoption?

"When you hold stablecoins, you're essentially lending your funds to the stablecoin issuer. This means a stablecoin rating is just another form of credit rating, and we expect adoption to follow the same path: first as an input to due diligence, eventually a requirement for licensing. The first step has already begun. Basel's crypto framework already asks banks to rigorously test whether a stablecoin they hold can keep its intended peg.

An independent rating is a natural input to that test. What institutions will need is a rating that stays current. If a bank's treasury policy says 'nothing below B+,' that policy is safe only as long as the rating remains fresh. We expect adoption to favor ratings that combine slow-moving financial evidence, like legal protections and redemption terms, with fast-moving operational evidence, like multisig configuration and admin permissions. When the latter changes, an alert should re-open the rating for an update right away."

— Benjamin Levit, CEO, Bluechip

Chapter 4. Conclusions

01 **Losses were concentrated in infrastructure and access paths.**

Smart contract and protocol code defects accounted for most incidents, but a few large failures in protocol code, suppliers, custody and wallets accounted for most of the $1,180.8M lost in Q3. The loss profile therefore extended beyond the smart contracts and applications that are most commonly subject to security review.

02 **Security reviews did not consistently cover exploited components.**

77% of Q3 losses were associated with a compromised supplier or developer tool, a public fix that had not yet been deployed, or a component outside the most recent review. In five of six documented cases, the exploited component was outside the scope of the latest review, although it could affect prices, messages, governance or borrowing.

03 **Changes between reviews remained a material source of exposure.**

The Q3 incidents at Cosmos EVM, Coldcard and Tectonic involved conditions that arose or remained after earlier assurance work. The cases differed technically, but each involved a change, configuration or deployment condition that was not adequately reflected in the latest evidence.

04 **Supervisory attention is also moving toward operating controls.**

Q3 enforcement focused largely on controls that regulators could establish as ineffective through records, examinations or incident investigations. ESMA's custody review and other supervisory measures indicate a broader focus on how controls operate after authorization, rather than on authorization or documented policies alone.

05 **Counterparty assurance should account for scope, changes and evidence age.**

A security review, certification or attestation describes a defined scope at a defined point in time. For institutional due diligence, its usefulness therefore depends on whether the reviewed scope still corresponds to the production system, its dependencies, its authorities and its current controls.

4.1 Shelf life of security and compliance evidence

Hacken's due-diligence model determines when different types of evidence are sufficient for an assurance decision, when they should be corroborated, and when they should be refreshed. A material change within the scope of the evidence requires reassessment regardless of the evidence's age for certain reviews.

How long evidence remains sufficient for a due-diligence decision



- **Time-bound evidence.** Proof of reserves and vulnerability scans describe conditions that can change rapidly. Their value therefore depends on the recency and frequency of the evidence.
- **Cycle-bound evidence.** Certifications, SOC 2 reports and regulator-mandated audits follow defined observation, certification or testing cycles. Their usefulness for current due diligence depends on whether the relevant cycle remains current and whether required surveillance or bridge documentation is available.
- **Change-bound evidence.** Smart contract, L1 and custody audits describe a defined build, release or set of signing arrangements. Material changes to code, releases, signers or other in-scope components require the evidence to be reassessed regardless of when the original review was issued.

Industry perspective: How quickly can a stablecoin become unsafe without anything changing in its financials?

"A stablecoin can turn unsafe within hours, without anything changing in the issuer's financial statements. In May 2026, MiCA-authorized issuer StablR lost control over one of three keys that could mint its USDR and EURR stablecoins. Since minting required only 1-of-3 signatures, the attacker minted $13.5 million in unbacked stablecoins. Within hours, both pegs broke and redemptions were suspended. Slow-moving financial evidence, like reserve quality and asset segregation, sits mostly offchain. Fast-moving operational evidence, like signature thresholds and minting permissions, sits mostly onchain. These factors can change in a single transaction, and need real-time monitoring to stay refreshed.
The most accurate stablecoin rating will track both kinds of evidence, where changes in fast-moving operational evidence trigger an alert to re-open the rating for an update right away."

— Amey Dandawate, Ratings Director, Bluechip

4.2 Priorities for institutions preparing for 2027

Supervisors are moving from reviewing documentation to testing controls in operation, while enforcement still focuses on breaches that are straightforward to evidence. In our assessment, this gap will narrow during 2027 as ESMA's custody findings, Korea's exchange decisions and the GENIUS Act's supervisory regime take effect.

Firms that can evidence operating controls before then will be better placed in authorization, supervision and counterparty due diligence.

Hacken recommends six priorities, each drawn from a Q3 finding:

- **Monitoring and screening capacity.** Alert handling was the most frequently penalized failure in Q3: backlogs at Citibank and UBS, alerts closed without review at CCV, and a 6–9 month backlog behind the fine proposed against CoinFlip. Firms should size alert review for peak volumes, report queue age as a management metric and test that monitoring covers every customer segment and channel.
- **Sanctions screening at wallet and jurisdiction level.** OFAC now lists individual wallet addresses and, since August, has treated Iran's digital-asset sector as sanctionable. Exchange deposit addresses followed on 30 September. Screening should cover counterparty wallets and exposure to designated jurisdictions and networks, including the A7 network, designated on 1 October.
- **Custody and key-management evidence.** ESMA's review covers keys and storage, transaction controls and third parties, and the OCC's GENIUS Act proposal addresses control of private keys. Firms should maintain a current signer and access matrix, records of key ceremonies and changes, and reconciliation of client positions to on-chain holdings.
- **Change-triggered testing and dependency oversight.** In the regimes reviewed, independent testing runs on annual cycles and change testing is left to firms' own processes, while Q3 losses followed changes made between tests. Firms should maintain an inventory of software dependencies, oracles, bridges and signers, and re-test after security advisories, upgrades and parameter changes.
- **Incident response and accurate disclosure.** Order Express was fined despite timely reporting, and the Bitkub complaint concerns what was omitted from regulatory reports. Firms should rehearse DORA's 4-hour initial notification, document root-cause remediation and ensure that regulatory reporting reflects incidents accurately.
- **Authorization planning by legal entity.** UK firms must apply for authorization by 28 February 2027, and MiCA's reverse-solicitation exemption is narrow. Firms serving EEA or UK clients should confirm the authorization status of each contracting entity and plan applications against these deadlines.

Venue risk pack: where one key can move user funds

$700M+ of user assets at two of the biggest venues sits behind a 3-of-4 key set or admin keys whose holders are not disclosed

We traced upgrade rights, signing authority, price and outcome controls, public audit coverage and applicable licenses using public documentation and direct inspection of blockchain contracts across 12 derivatives exchanges and prediction markets.

Upgrade authority

Who can change the code that holds user money, and how fast

Outcome resolution

Who sets prices or settles markets, and whether results can be challenged

Audit coverage

Whether audits and bug bounties cover the parts that hold this authority

Regulatory exposure

Which license applies, and what a regulated counterparty must show

Who the venue risk pack is for:

- **Risk and due-diligence teams** at banks, brokers, asset managers and custodians deciding whether to trade on, provide liquidity to, connect custody with or list on these venues.
- **Compliance teams** who must show regulators they have checked the venues they rely on (third-party risk under DORA, MiCA or local rules).
- **Venue operators** who want to know what an institutional reviewer will ask, and what to fix first.

Q3 Venue Risk Pack

How 12 prediction and derivatives venues expose institutional users to control, governance and infrastructure risk

4 Critical | 4 High | 1 Unknown | 3 Lower | Send me the pack

Hacken assessed 12 venues against upgrade authority, price and outcome control, audit coverage and regulatory exposure. The full pack contains the venue-by-venue assessment, worst-case exposure, relevant requirements and what each operator should change.

About the research

The findings in this report are drawn from Hacken's own practice areas: exploit and incident data was prepared and analyzed by the Offensive Security Services team, and regulatory analysis by the GRC and security operations teams.

Hacken Track Record

2,168
public security assessments delivered since 2017

16,735
vulnerabilities identified across engagements

$430B+
in assets verified through Proof of Reserves services

ISO 27001
certified information security management

Hacken Practice Areas

The specialists contributing to this report work across the following practices:

Offensive Security

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

Compliance and Advisory

- MiCA and DORA Compliance ↗
- NIS2 Readiness ↗
- SOC 2 Readiness ↗
- ISO 27001 ↗
- ISO 42001 Readiness ↗
- EU AI Act Readiness ↗
- CCSS Audit ↗
- Executive Cybersecurity Training ↗
- Licensing and Advisory ↗

Continuous Security

Extractor ↗
Real-time on-chain risk monitoring and incident response.

CORE3 ↗
Web3 risk infrastructure indexing with monitoring and due diligence reports

DualDefense ↗
Post-audit assurance

Retainer security & compliance ↗
Annual engagement for predictable security costs and assurance cycles

Contributing Partners: Bluechip, GOSAI LAW, Stellar, Chainlink Labs, EUROPEUM

We thank our contributing partners for sharing their expertise and operational perspectives throughout this report.

Authors & Contributors: Anton Sheptytskyi (Design & Visuals), Dmytro Yasmanovych (Compliance), Remilekun Adeopatoye (Regulatory), Dmytro Zaporozhchenko (Copywriting), Maksym Fedchak (Partner outreach), Olesia Bilenka (Smart contract vulnerabilities data), Seher Saylık (Risk data), Oleksandr Iurkin (Strategic oversight).
Evidence staleness contributors: Joaquin Girardi (PoR), Faizan Nehal (Pentest reports), Olesia Bilenka (Smart contract audit reports), Tanuj Soni (L1 Audit Report), Dmytro Yasmanovych (Compliance certificates)

Securing Digital Frontier Since 2017

Hacken is a security and assurance partner for financial institutions and the infrastructure they rely on.

ISO 27001:2022 Certified

“Hacken is praised for its professionalism, thorough audits, and timely delivery.”

Read all reviews on Clutch

Trusted by industry leaders for 9+ years

Tier-1 CEXes

crypto.com	KUCOIN	MEXC	BitMEX	Bitso
BINANCE	BYBIT	OKX	Gate.io	kraken
whitebit	BigONE	Backpack	BYDFi	

Wallets

METAMASK
status

Regulators, Financial Institutions & Banks

	European Commission	VARA شلطة تنظيم الأصول الافتراضية VIRTUAL ASSETS REGULATORY AUTHORITY	BMA BERMUDA MONETARY AUTHORITY
ADGM	ebsi European Blockchain	EUROPEUM	FORGE SOCIETE GENERALE GROUP

L1 / L2 Protocols, Platforms & Foundations

MINA	vechain	AURORA	near	IoTeX
QAN	BASE	Sui	somnia	APTOS

DeFi, RWA, GameFi & Ecosystem Projects

coingecko	tokeny	WEMADE	status	Chainlink	MAVIA
DEXALOT	ADI	1inch"	PANINI	RedStone	Zcash

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 and follow us on social media:

hacken.io LinkedIn X