Blockaid

BLOCKAID THREAT INTELLIGENCE

2025 Web3 Security Wrapped

Blockaid

Table of contents

Blockaid

2025 at a glance

Total Losses

2025

$2.58B

Incidents by funds lost →

#1 BYBIT FEB 21

$1.5B

#2 CETUS MAY 22

$223M

#3 Balancer NOV 3

$128M

Key findings

- In 2025, we tracked **63 incidents** totaling **$2.58B** in losses.
- **Infrastructure exploits** —led by Bybit's $1.5B multisig breach —caused 61% of 2025's losses despite not being the most common attack vector.
- **Price manipulation and code logic** were the most frequent vulnerabilities, accounting for 43% of incidents, yet representing only 21% of funds lost.
- **2025 losses were concentrated in Q1,** driven by the Bybit and Phemex breaches. **Ethereum** remained the most affected network, followed by Arbitrum.

Frequency ≠ Financial Impact

Vulnerability type	Total loss	# of incidents
Infrastructure exploit	$1.58B	7 incidents
Private key compromise	$331M	9 incidents
Price manipulation	$295M	16 incidents
Code vulnerability	$257M	11 incidents
Phishing/blind signing	$50M	1 incidents
Reentrancy	$42M	2 incidents
Unchecked/unsafe external calls	$7.56M	9 incidents
Access control issues	$5.78M	4 incidents
Proxy/upgrade exploits	$1.36M	4 incidents

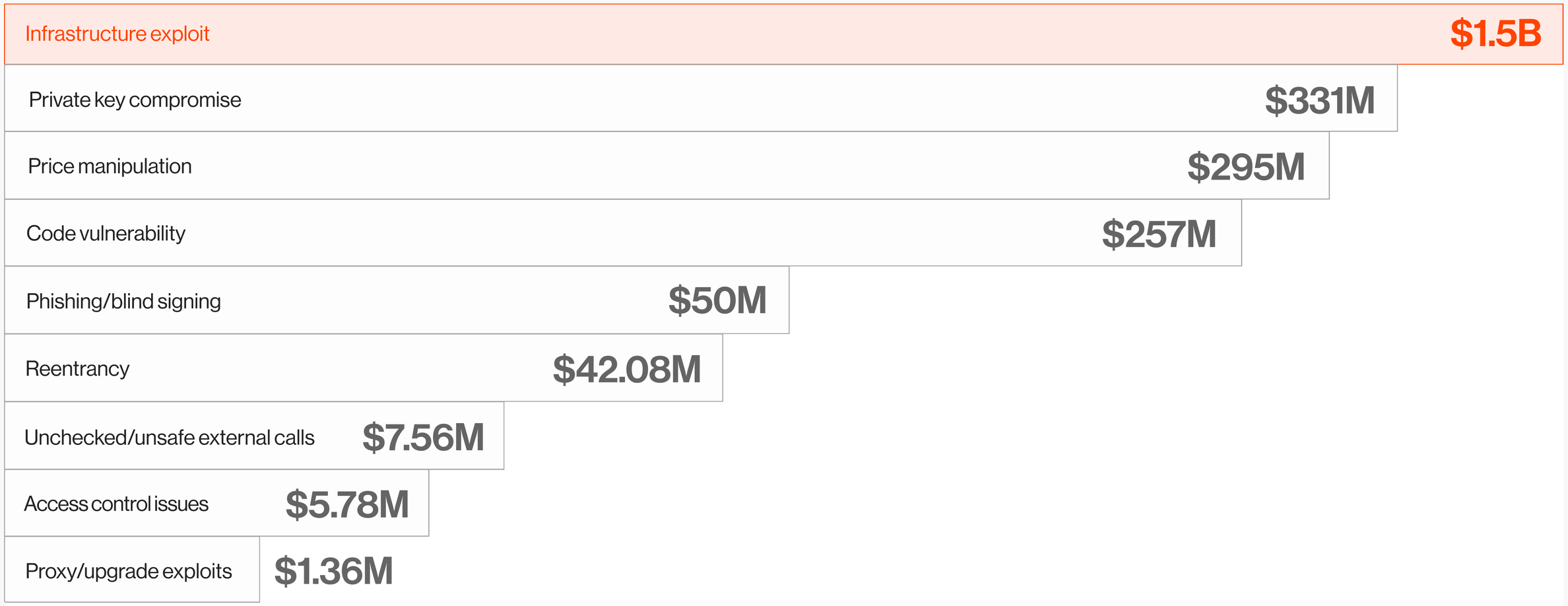
Blockaid

Top 10 incidents

Business	Date	Amount lost	Chains	Vulnerability type	Attack type
BYBIT	Feb 21, 2025	$1.5B		Infrastructure exploit	Nation-state APT
CETUS	May 22, 2025	$223M		Code vulnerability	Unknown
Balancer	Nov 3, 2025	$128M		Price manipulation	Nation-state APT speculation
Bitget	Apr 20, 2025	$100M		Price manipulation	Unscrupulous traders
phemex	Jan 23, 2025	$85M		Private key compromise	Nation-state APT
NOBITEX	Jun 18, 2025	$80M		Private key compromise	Nation-state APT
US-based individual	Dec 20, 2025	$50M		Phishing, blind signing	Financially-motivated actor
INFINI	Feb 24, 2025	$49.5M		Private key compromise	Former developer
BtcTurk	Aug 14, 2025	$48M		Private key compromise	Financially-motivated actor
CoinDCX	July 18, 2025	$44M		Private key compromise	Nation-state APT

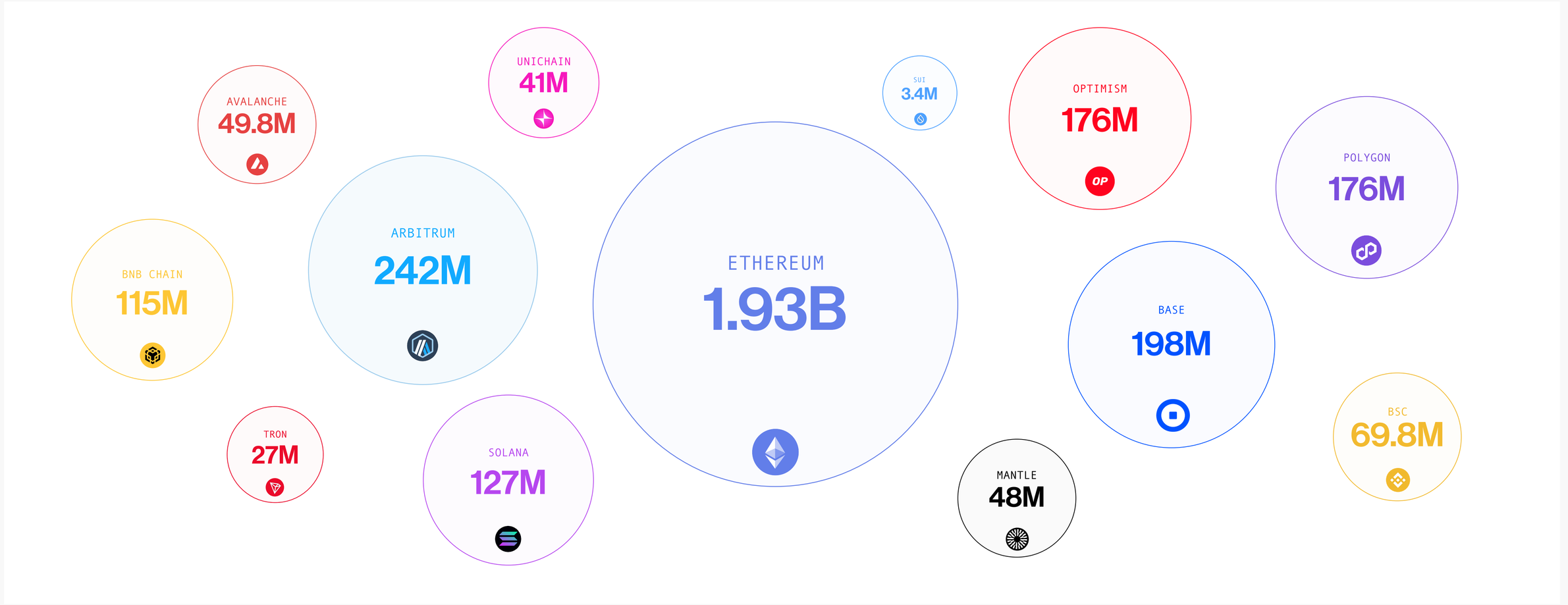
Blockaid

Losses by attack type



Blockaid

Losses by chain network



2026 SECURITY IMPERATIVES

Shift from an ad hoc to continuous, preventive security model

Lesson learned

Every surface and interaction needs to be treated as a potential threat. In 2025, infrastructure exploits accounted for just 11% of incidents but caused 61% of the losses. Bybit alone drove $1.5B in losses because of a compromised UI from a wallet provider. BigONE also occurred because of the compromised backend of a third party. SwissBorg was due to the compromise of a third party API.

Root cause

What these incidents share: **static security measures that do not asses all the surfaces within the threat environment** at all times. Audits, key management policies, and access controls were all in place, but none could detect malicious intent, in real time.

Forward look

As the self-custody stacks grow more complex—MPC coordinators, policy engines, third-party SDKs, governance layers—the attack surface expands with them. In 2026, expect attackers to target the operational layers around key management, not the keys themselves.

Blockaid

2026 SECURITY IMPERATIVES

Shift from an ad hoc to continuous, preventive security model

Our recommendations:

Monitor your assets and smart contract operations in real-time

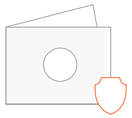
Continuously monitor the performance of wallets, contracts, bridges, oracles and tokens. Metric anomalies and invariant violations help expose vulnerabilities and prevent attack. Scan contracts for code vulnerabilities before deploying or continuously run synthetic tests to verify emergency functions 24/7.

Simulate and validate a transaction before you sign

Never approve a transaction you haven't simulated. Before signing, verify the payload matches expected behavior and that destination addresses are legitimate, even from trusted sources. This is your last line of defense against blind signing.

Enforce behavior-based policy governance

Move beyond static allowlists and role-based permissions. Define policies based on transaction intent and behavioral patterns—flagging actions that are technically authorized but contextually abnormal, like unusual withdrawal timing or atypical counterparties.



Apply “Zero Trust” principles to every interaction

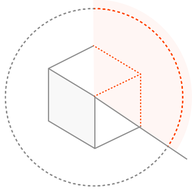
Treat every surface and transaction as a threat, including third-party providers. Composability is a feature of blockchains but security can only be as strong as the weakest link your stack.

Blockaid

Blockaid: Enterprise-grade security for everything onchain

Onchain Monitoring

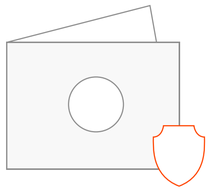
Detect and respond to scams, fraud, exploits, and financial risks.



FOR CHAINS, PROTOCOLS

Cosigner

Secure transactions with automated monitoring & cosigning.



FOR HEDGE FUNDS, TRADING DESKS

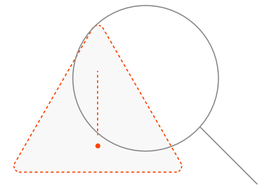
End-User Protection

Protect users from fraud, scams, and hacks.

FOR WALLETS, DAPPS, EXCHANGES

Crypto Fraud Detection

Identify and prevent social engineering scams



FOR EXCHANGES, BANKS, FINTECHS

Blockaid

Reference: attack type definitions

Category	Definition
Phishing/blind signing	Attacks exploiting users signing transactions without understanding the payload; Address poisoning, social engineering to steal funds
Price manipulation	Oracle attacks, flash loan price manipulation, TWAP/AMM exploits, exchange rate manipulation
Proxy/upgrade exploits	Uninitialized proxies, malicious upgrades, storage collisions, implementation takeovers
Code vulnerabilities	Integer overflow/underflow, unchecked inputs, boundary condition flaws, input validation, logic flaw caused exploit
Private key compromise	Private key theft, hot wallet breaches, compromised signers, seed phrase exposure
Access control issues	Attacker calls privileged function that should be restricted but lacks permission checks
Infrastructure exploit	Supply chain attacks, backend compromise, API exploits, cross-chain bridge issues
Unchecked/unsafe external calls	Exploits that manipulate call mechanisms (call, delegatecall, callbacks) to execute unauthorized operations or bypass intended contract logic
Reentrancy	Exploit where attacker recursively calls back into a function before prior execution completes, draining funds via repeated withdrawals
Infinite mint exploits	Flaws allowing unlimited token creation, broken mint logic

Blockaid

Trusted by the best

coinbase · METAMASK · world · Uniswap · zerion

Revolut · Robinhood · Fidelity INVESTMENTS · rainbow · LEDGER

OpenSea · 1inch · Fireblocks · Backpack · anchorage digital

DEX SCREENER · SOLFLARE · ...and 200 more

Follow Blockaid on LinkedIn and X
Request a demo here to explore our proprietary Threat Intel Knowedge Base