

The State of Crypto Insurance

Q3 2026

Onchain losses have already reached \$1.9 billion in 2026, and this year still has a quarter to go. That's the highest total since 2022, and we're not out of the woods yet with Q3 alone adding \$987 million.

If you're allocating capital to DeFi, it's crucial to have the right risk management in place:

- What are the latest risk trends?
- Which of those risks are you exposed to?
- Are you protected against them?

Published by



Disclaimer & Attribution

This report, The State of Crypto Insurance, Q3 2026 (the Report), is published by Nexus Mutual for general informational and educational purposes only. The loss figures in the Report come from Nexus Mutual's loss data; other public trackers use different methods and report different totals. The Report presents a high-level analysis of onchain losses, risk trends and crypto insurance based on that data, publicly available information, historical events, and the authors' research, analysis and interpretation as at the date of publication. The Report is not intended to be exhaustive and does not purport to identify all risks, threats, failure modes, or vulnerabilities that may be relevant in any given context.

Nothing in the Report constitutes, or should be construed as, financial, investment, legal, or other professional advice. The Report does not constitute a recommendation, endorsement, solicitation, or guidance in relation to any specific transaction, strategy, or risk management decision.

The Report is intended solely to support independent research and informed discussion. Users are expected to conduct their own research (DYOR) and seek independent professional advice before making financial or operational decisions involving digital assets, onchain protocols, or related systems.

The Report may be shared and referenced for non-misleading informational purposes, provided that clear and prominent attribution is given to Nexus Mutual. The Report may not be modified, adapted, re-branded, or redistributed as a derivative work, nor presented in a way that implies authorship, endorsement, or validation by any party other than Nexus Mutual. Where excerpts, charts, or figures are reused, they must be reproduced accurately and not presented in a misleading or out-of-context manner.

While reasonable efforts have been made to ensure accuracy of the Report at the time of publication, no representation or warranty (express or implied) is made as to its completeness, accuracy, timeliness, or ongoing applicability. Onchain systems, market conditions, threat vectors and risk profiles evolve rapidly, and the Report may become outdated or incomplete without notice.

Nexus Mutual accepts no responsibility or liability for any use of, or reliance on, the Report by any third party. All intellectual property rights in the Report are reserved except to the limited extent expressly permitted in this disclaimer.

* "Crypto insurance" is a generic term covering protection against non-economic crypto losses, such as theft or inability to withdraw from a custodian or exchange, smart contract exploits, staking slashing, or digital asset depegs. It encompasses two distinct types of protection: traditional regulated insurance (underwritten by licensed insurers), and discretionary mutuals (such as Nexus Mutual), which operate onchain and are not regulated.

In This Edition

NO.	SECTION	PAGE
01	YTD Onchain Losses	04
02	Check Your Opsec	04
03	April Fools (for DeFi)	05
04	3 Quarters, 6 Reports	06
05	Are Oracle Attacks Making a Comeback?	07
	Why a Price Feed Fails	08
	New RWAs, Old Risk	09
06	Sitting Down with Adam Wickens	09
07	Onchain Risk Review: Q3 2026	11

Year-to-Date Onchain Losses

This year's onchain losses have nearly caught up to the last three years combined. Annual losses were only \$809 million in 2023, \$530 million in 2024, and \$680 million in 2025 (these figures don't include centralized exchange losses).

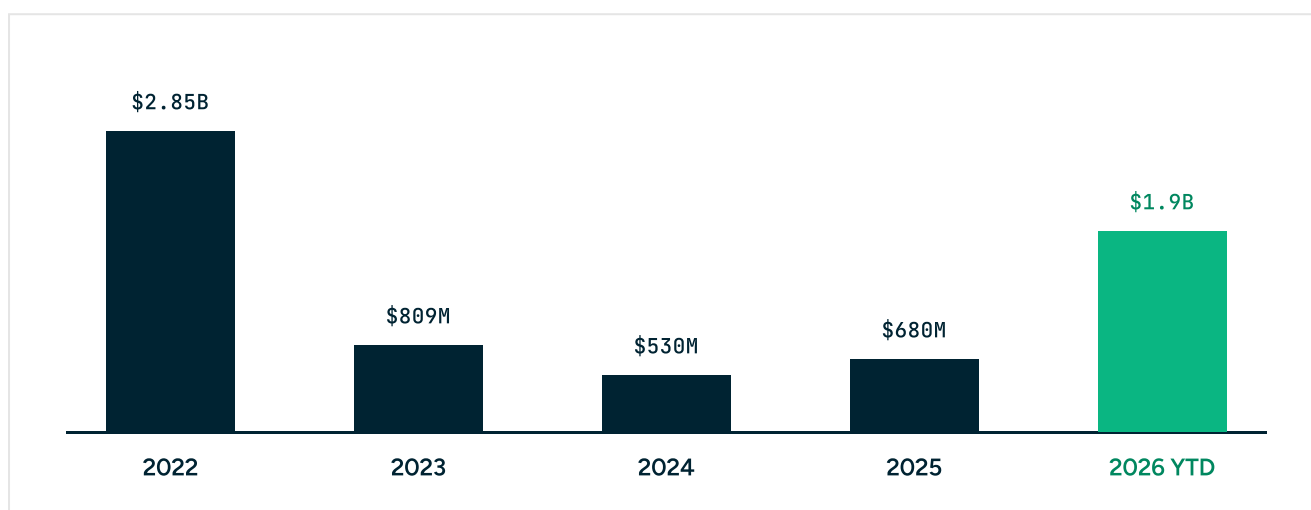


FIG. 01 – Onchain losses by year (USD), 2022 to 2026 YTD (excluding centralized exchange losses).

Check Your Opsec

Onchain risk is more than just smart contract exploits. Digital assets can also be exposed to depeg, custodial, and operational (opsec) risk. Opsec onchain losses saw a dramatic increase this year, going from \$78.3 million in 2025 to \$642 million YTD.

Compromised keys and social engineering are the main opsec failure points. Drift lost \$285 million on April 1st, after a six-month social-engineering campaign. Attackers eventually persuaded two of the five signers on its Security Council multisig to pre-sign transactions that hid admin authorizations.

Drift said the intrusion may have involved malware on contributors' devices. TRM Labs and QuillAudits both concluded that the exploit did not depend on a smart contract bug, and our [Drift Protocol incident report](#) goes into more detail.



"Most allocators don't see how layered their exposure is until we rebuild it for them. A client says, I'm allocating to these three vaults, here are the addresses. We look underneath and it's five protocols and ten assets. We go back and ask, are you aware you're exposed to this? Often the answer is no, I didn't know that was in there."

Hugh Karp
FOUNDER & CEO, NEXUS MUTUAL

April Fools (for DeFi)

Two of the year's largest losses hit in April. Drift (ironically) on April 1st. KelpDAO and LayerZero followed on April 18th, when attackers compromised the infrastructure behind a 1-of-1 Decentralized Verifier Network configuration, so a single verifier approved a forged bridge message. The message released 116,500 rsETH (\$292 million). Read our [KelpDAO and LayerZero incident report](#) for a full breakdown.

In the aftermath of the exploit, capital allocators pulled their funds across DeFi. Just two days after the KelpDAO event, DeFi TVL fell by \$13.4 billion with Aave alone accounting for \$8.45 billion of the drop.

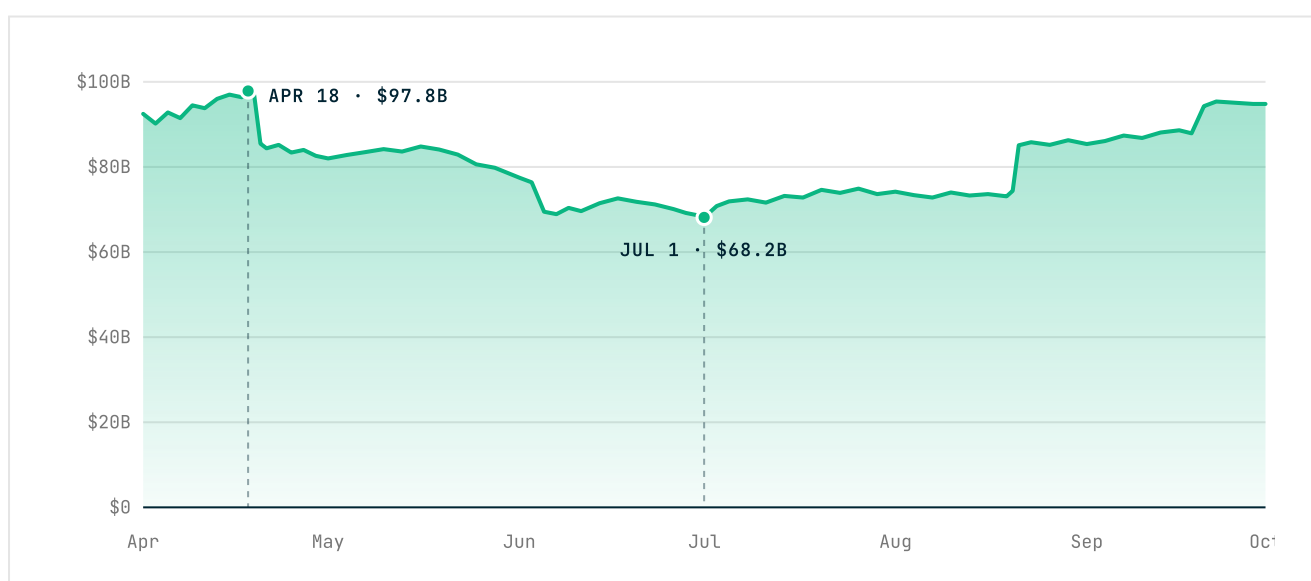


FIG. 02 — DeFi total value locked (USD), April 1 to October 1, 2022.

Source: DefiLlama.

3 Quarters, 6 Reports

Nexus Mutual published six incident reports through the end of Q3, drawing on our unique experience and insight from underwriting onchain risk.

\$23M-\$24.5M

March 22

Resolv

An attacker obtained a privileged minting key held in Resolv's AWS Key Management Service environment and used it to mint unbacked USR. Halborn put direct losses at \$23 million and The Record at \$24.5 million. Bad debt flowed to lenders that accepted USR, and we identified \$7.77 million of Morpho lending exposure locked in markets with no available liquidity. [Read the report.](#)

\$285M

April 1

Drift

A six-month social-engineering campaign enabled attackers to get pre-signed approvals on two of the five Security Council multisig signers, draining \$285 million. [Read the report.](#)

\$292M

April 18

KelpDAO and LayerZero

Attackers compromised the RPC infrastructure behind LayerZero Labs' verifier, the only one on Kelp's 1-of-1 route, and a forged bridge message released 116,500 rsETH (\$292 million). [Read the report.](#)

\$57.4M LIQUIDATED

July 27

XYZ and SK Hynix on Hyperliquid

At the open of pre-market trading on the Nextrade venue, a single one-share trade at the lower price limit became the oracle reference price for Trade.xyz's SK Hynix perpetual, and 960 long accounts holding \$57.4 million in positions were liquidated. Trade.xyz did not disclose realized losses (estimated \$17.3 million) and announced a one-time discretionary compensation. [Read the report.](#)

\$8.47M

August 23

Term Finance

Few depositors had wrapped their vault shares to vote, so 0.5 ETH worth of deposits gave the attacker 90.7% of the ETH Meta Vault's votes. The attacker then set the vaults' withdrawal delay to zero and drained them for \$8.47 million. [Read the report.](#)

\$319M

September 6

Liquid Network

To increase efficiency, Elements nodes cached range-proof checks without capturing all the data that makes a proof valid. A doctored transaction reused an earlier valid result and skipped full verification. The attacker created 3,998.5 unbacked L-BTC and drained \$319 million in BTC from the federation's reserve. The attacker returned 3,400 BTC (\$268 million), leaving 598.5 BTC (\$48 million) outstanding. Network function was restored and no user loss had been announced. [Read the report.](#)

Are Oracle Attacks Making a Comeback?

At Nexus Mutual, we know oracle risk. We began covering it back in 2021 with claims starting to get paid that same year, nearly \$400k in the aftermath of CREAM.

Oracle-related losses reached \$190.6 million through Q3, already more than 2024 and 2025 combined, with incidents becoming much more frequent.

FIG. 03 — Oracle-related losses, 2024 to 2026



Source: Nexus Mutual loss data, as of September 30, 2026.

One incident drives the majority of the losses this year. Tectonic's \$120.4 million loss is more than six times the size of the largest oracle loss in either of the previous two years.

Table 2. Largest oracle-related losses, 2024 to 2026

YEAR	PROTOCOL	DATE	GROSS LOSS	RECOVERED
2026	Tectonic	Aug 30	\$120.4M	\$111.2M
2026	Ostium	Jul 15	\$23.75M	--
2026	YieldBlox	Feb 22	\$10.2M	--
2026	Bonzo Lend	Jul 11	\$9.05M	--
2025	Resupply	Jun 25 '25	\$9.6M	--
2025	KiloEx	Apr 14 '25	\$7.5M	\$6.75M
2025	LoopScale	Apr 26 '25	\$5.8M	\$5.22M
2024	UwU Lend	Jun 10 '24	\$20.0M	--
2024	Polter Finance	Nov 16 '24	\$12.0M	--
2024	WOOFi Swap	Mar 5 '24	\$8.5M	--

Source: Nexus Mutual loss data. Ostium began as a private key compromise; it is included because the stolen key was used to manipulate an oracle source, which caused the loss.

There are two core inputs that drive the majority of oracle risk: how many independent inputs feed the oracle, and who can push an update. Every 2026 incident below failed on one of those points.

Why a Price Feed Fails

Thin or New Markets

When the market behind a feed is new or illiquid and lacks the proper controls, an attacker can try to move its price for far less than the value of the impacted collateral. On February 22, the USTRY oracle used by Blend V2 and YieldBlox was pushed 100 times higher, causing YieldBlox to lose \$10.2 million. This was followed by the year's largest example, Tectonic: an attacker manipulated the price of the thinly traded TONIC collateral token to steal \$120.4 million.

Configuration Error

This one can happen with no attacker involved. On February 15, a Moonwell governance proposal (MIP-X43) went live with an oracle configuration that priced cbETH using only the cbETH/ETH exchange rate, without multiplying it by the ETH/USD price. The oracle reported cbETH at \$1.12 instead of \$2,200, liquidators seized 1,096.3 cbETH, and Moonwell was left with \$1.78 million in bad debt, according to Anthias Labs' incident summary. Moonwell later proposed \$310,000 from its treasury as a partial repayment to the 181 affected borrowers.

On March 10, a misconfigured Aave CAPO oracle caused 10,938 wstETH in positions to be liquidated across 34 accounts, according to Chaos Labs' post-mortem. Cointelegraph valued the liquidations at \$27.1 million. The Aave DAO refunded affected users 512.2 ETH (\$862,000), and there was no bad debt.

The losses didn't end there. Silo Finance lost \$392,000 to an oracle misconfiguration, and Singularity Finance lost \$413,000 after an invalid Uniswap V3 fee-tier configuration returned a zero price.

Offchain Signing and Verification

As Hugh Karp puts it, "Every oracle configuration can be different, and the risk profile is very different depending on that setup."

On July 11, the Supra price verifier used by Bonzo Lend accepted a zero BLS signature, causing a loss of \$9.05 million. Then on July 15, an attacker used a stolen Ostium oracle-signer key to submit forged price reports, and \$23.75 million in USDC was paid out of Ostium's liquidity vault. The Ostium breach started as a private key compromise, but the key gave the attacker control of an oracle source, and the manipulated prices from that source caused the loss.

New RWAs, Old Risk

Tokenized real-world assets (RWAs) reintroduce oracle centralization risk that DeFi hasn't seen in years. The price pipeline is often bespoke, a single party or multisig may push the net asset value, secondary liquidity may be thin, and the asset's real price sits offchain, where no smart contract can verify it directly.

The XYZ and SK Hynix flash crash on Hyperliquid is a clear example. The price feed for a tokenized stock used a weak price source: a single one-share trade on a thinly traded pre-market venue at its early-morning open. The feed passed that price straight through, and the resulting liquidations caused losses for users.

Sitting Down with Adam Wickens



ADAM WICKENS

Adam Wickens spent 30 years as an underwriter in traditional insurance and is now setting up Nexus Mutual's regulated carrier group.

He watched how oracle cover got dropped. "You'll see exclusionary language like, okay, we'll cover it, but two oracles have to say the wrong information at the same time," he says. "If you don't understand it, you can say you're insuring it but water it back down again. The devil is in the detail."

When asked what he thinks about the recent momentum from traditional finance in DeFi, Adam Wickens replied, "it's bringing Wall Street to Main Street."

The application layer increasingly looks like a bank, with familiar interfaces and compliance language, but the plumbing underneath still carries crypto-native risks: smart contracts, keys, operational security, bridges, oracles, and configuration.

Wickens has seen where the traditional market's appetite ends. "The insurance industry has been very quick to insure the incredibly low-risk areas. Where it starts falling over, and the capacity almost drops off a cliff, is the more complex DeFi space," Wickens says.

Outside cold-storage custody, traditional carriers' appetite drops sharply. Few of them have underwriters who can tell one DeFi risk from another, let alone price it. "The only thing worse than working with no data is to work with bad data," Wickens says. "We have the people at Nexus Mutual who've lived through these things, so we can apply probabilities to the likelihood of an event rather than a historical pattern."

Most teams need only a portion of their risk behind a regulated carrier: the part their process can't accept otherwise. A practical program pairs that portion with the Mutual's discretionary capacity on the same risk.

If you'd like to learn more, you can get in touch with Adam at: adam.wickens@fern-insurance.com

Onchain Risk Review: Q3 2026

Just four incidents account for over 85% of the \$941.65 million lost in Q3: Bitget lost funds due to a zero-day in a third-party security product, Liquid Network with a verification flaw in its consensus software, Tectonic due to a manipulated collateral price, and AFX Trade with validator signing keys that approved a single withdrawal.

LOSS VALUE	DATE	PROJECT(S)	CHAIN	LOSS EVENT TYPE
------------	------	------------	-------	-----------------

\$387.5M	Sep 24	Bitget	Ethereum, BNB Chain, Avalanche, XRP Ledger and other chains	Custodian Security Breach
-----------------	---------------	---------------	--	----------------------------------

Bitget said a zero-day vulnerability in a third-party security product let the attacker reach its internal systems, steal high-privilege credentials and write forged withdrawal commands into its wallet system, moving \$387.5M from twelve hot and warm wallets. Bitget said private keys were not compromised and cold wallets were unaffected.

\$320M	Sep 6	Liquid Network	Liquid / Bitcoin	Protocol Software Vulnerability
---------------	--------------	-----------------------	-------------------------	--

A range-proof verification-cache flaw in Elements, the consensus software behind Liquid, let the attacker create 3,998.5 unbacked L-BTC and redeem it for BTC from the federation's reserve. The attacker returned 3,400 BTC, leaving 598.5 BTC (\$48M) outstanding.

\$120.4M	Aug 30	Tectonic	Cronos	Oracle Manipulation
-----------------	---------------	-----------------	---------------	----------------------------

An attacker manipulated the price of the thinly traded TONIC token used as collateral on Tectonic's Cronos lending market and borrowed liquid assets far beyond what the real collateral supported, after which Cronos validators halted the chain and later resumed it with a rollback through an emergency validator-consensus action. Cronos's post-mortem puts the amount borrowed at \$120.4M. The rollback reversed \$111.2M, and \$9.19M was bridged off the chain before the halt and not recovered.

\$24.15M	Jul 22	AFX Trade	Arbitrum / Ethereum	Compromised Operations Wallet
-----------------	---------------	------------------	----------------------------	--------------------------------------

According to public reporting, enough of the AFX custody bridge's validator signing keys were compromised to meet the withdrawal quorum, and five validator signatures authorized a single 24.15M USDC withdrawal on Arbitrum that was bridged to Ethereum and swapped to ETH, leaving the Arbitrum native bridge unaffected.

YOU'RE COVERED WITH NEXUS MUTUAL



VISIT

nexusmutual.io

FOLLOW

x.com/NexusMutual

CONTACT

info@nexusmutual.io