# The State of Crypto Insurance

## Q1 2026*

Crypto is officially in its institutional era, and vaults are the infrastructure of choice. The total value locked (TVL) in DeFi is in the $90 to 100 billion range (depending on which way the wind is blowing today for ETH...)

The threat landscape is expanding on two fronts. Physical attacks on crypto holders hit an unprecedented level in 2025, with more documented incidents than any year prior. Additionally, despite advances in blockchain security, onchain exploits continue at scale.

This report dives into how these threats have evolved and how the crypto cover market is responding.

Published by Nexus Mutual

# Table of contents

**01** The Threat Landscape

**02** Introducing: Crypto Kidnap & Ransom Cover

**03** The Next Infrastructure Layer: Embedded Coverage

**04** Onchain Risk Review: Q1 2026 Hacks & Claims

*With contributions from the Nexus Mutual team and ecosystem partners.*



** "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.*

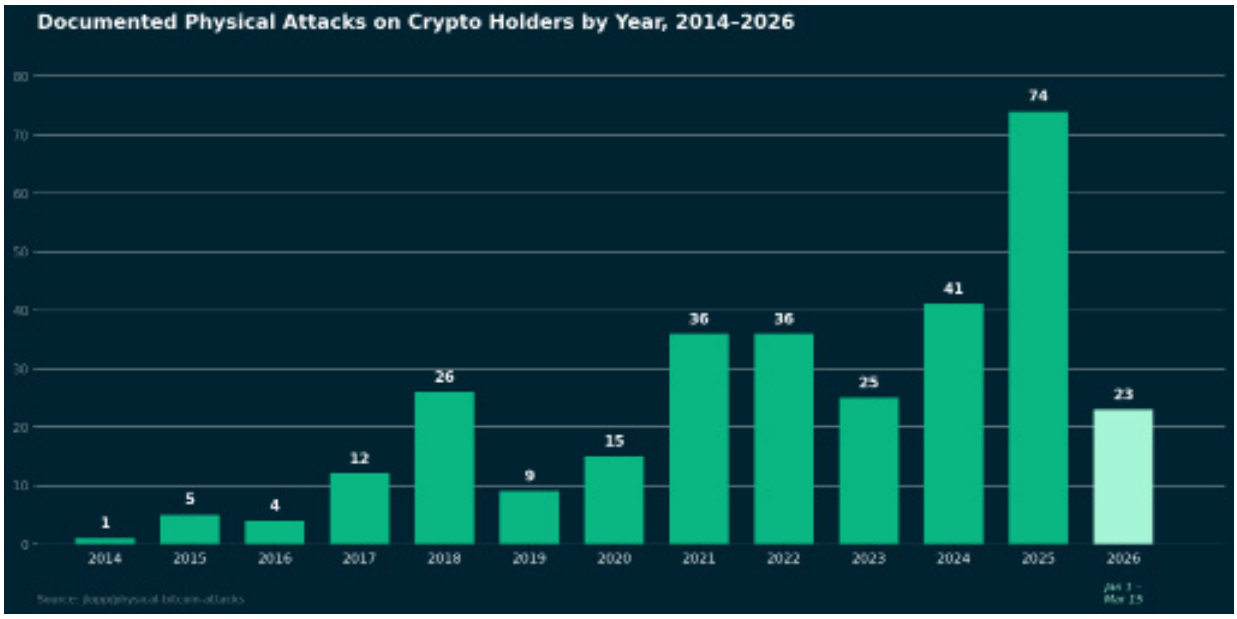
## The Threat Landscape

Starting off on shaky footing this year, market volatility pulled DeFi TVL down 30%; however, long-term capital stayed active in lending, staking, and liquidity protocols. At the same time, the risks of public crypto wealth became painfully clear.

In Q1 2026, crypto holders faced threats on two fronts: an accelerating wave of physical attacks — including kidnappings, home invasions, and extortion targeting investors and their families — and continued onchain exploits. Neither threat is new, but the speed and severity of both have brought them into the mainstream discussion.

### Physical Attacks: A Crisis Accelerating in Real Time

The most comprehensive public record of physical attacks against crypto holders is Jameson Lopp's open-source repository (available on GitHub at https://github.com/jlopp/physical-bitcoin-attacks), which documents incidents back to 2014. The data tells a clear story: what was once a rare occurrence has become a persistent, global, and increasingly violent phenomenon. In 2025, the repository documented 74 attacks, nearly double the 41 incidents in 2024 and more than triple the count from 2023. The first few months of 2026 suggest no slowdown: at the time of writing this report, 23 attacks have already been documented.



### France: The Epicenter

No country illustrates the severity of the physical threat landscape more than France. In 2025, there were 20 known attacks targeting crypto holders on French soil, ranging from street-level extortion to professional operations involving surveillance, GPS tracking, and coordinated multi-person assault teams.

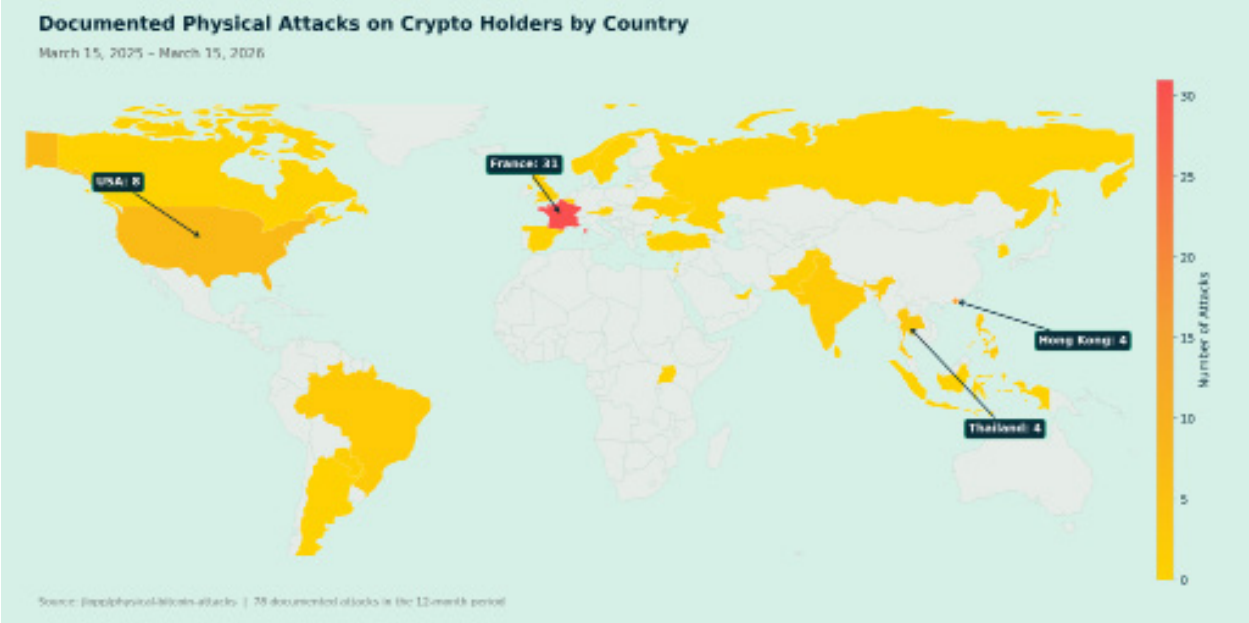
Several cases are notable in Jameson Lopp's repository. In January 2025, the co-founder of hardware wallet manufacturer Ledger was kidnapped with his wife; his finger was severed before France's elite GIGN tactical unit rescued them. In May, the daughter of a crypto exchange CEO was targeted for abduction in broad daylight in Paris, bravely defended by her partner and bystanders who fought off the attackers. That same month, police arrested five suspects after discovering a GPS tracker on a crypto entrepreneur's car in Normandy, preventing a planned kidnapping.

By the end of 2025, attackers were more commonly targeting crypto holders' families directly. In October, a woman and her two children were threatened in an attempt to blackmail her husband. In December, attackers invaded a home in La Rochelle, tied up the family, and forced multiple crypto transfers; unconfirmed reports put the loss at $10 million.

This unfortunate pattern continued into 2026. The majority of Q1 attacks occurred in France: a young man kidnapped in Dijon, a woman held captive in Manosque, a couple and their three children taken hostage in La Chapelle-Saint-Aubin, and a 43-year-old man kidnapped in Saint-Léger-sous-Cholet.

"Some products you buy and hope you never have to use. With the recent increase in crypto-targeted kidnappings, we had to act. By teaming up with Merrill Herzog, InShare, and Samphire, we're able to provide aworld-class security solution to address this."

—**Hugh Karp** (Founder, Nexus Mutual)




While France leads in publicly known incidents, significant clusters exist in Thailand, Brazil, Hong Kong, the UAE, and the United States, with major incidents also reported in San Francisco, Oslo, and Istanbul.

Three patterns emerge from the data:

1. Attackers are **increasingly targeting family members** rather than the crypto holders themselves
2. Operations have become more **sophisticated**: surveillance, impersonation of police or delivery workers, and pre-planned ambushes are more common
3. Violence has **escalated**; multiple incidents in 2025 involved torture, mutilation, and in at least five tragic cases, murder

For allocators deploying capital into crypto, physical security risk has reached a critical threshold. Fund managers, protocol founders, exchange operators, and their families are being specifically identified and targeted based on publicly available data, social media activity, and industry visibility.

## Introducing: Crypto Kidnap & Ransom Cover

Securing a wallet doesn't secure the person holding it. Physical coercion is a threat that conventional cyber and custody cover were never designed to address.

In February 2026, Nexus Mutual launched Crypto Kidnap & Ransom Cover along with crisis response firm Merrill Herzog and specialist underwriters InShare and Samphire Risk. This product provides 24/7 access to a global response team of former special forces and intelligence operators and ransom reimbursement payable in crypto . Cover can extend to spouses, children, and other close family members.

Confidentiality of coverage is key. No publicly available information connects the cover to any individual. Premiums range from 0.75% to 2%+ of the covered amount per year; the exact fee is based on coverage limits, residency, travel patterns, and public visibility.

To request a confidential quote, contact the Nexus Mutual team at **nexusmutual.io/contact**.

"Our solution brings together alternative capacity, specialist underwriting and proven crisis response capability to deliver a world first in K&R protection that is credible, discreet and fit for the realities of the crypto world."

—**Graeme Thurgood**
(Chief Underwriting Officer, InShare)

## The Next Infrastructure Layer: Embedded Coverage

Vaults have become the defining infrastructure of institutional DeFi. From the early days of Yearn Finance to today's ERC-4626 standard, vaults have evolved from a simple yield aggregator into a comprehensive finance engine: pooling capital, executing complex strategies, and serving as the primary interface through which institutional investors access onchain markets.

Protocols like Morpho, Euler Finance, Veda, and Midas provide vault issuance infrastructure, and professional curators such as Gauntlet and Steakhouse Financial manage risk parameters. Real-world assets are increasingly flowing through vault structures, bridging DeFi with traditional finance.

But there's a conspicuous gap in this maturing stack.

### Cover Is the Missing Layer

Billions in TVL sit in vault infrastructure with no systemic protection layer. Vaults pool capital from multiple depositors and deploy it across complex, interconnected strategies. A single exploit or misconfiguration can affect every depositor simultaneously. For most vault deployments, cover remains something investors source separately, if at all.

For institutions with fiduciary obligations, that gap is increasingly difficult to ignore.

"Insurance infrastructure will be a **make-or-break primitive** for onboarding 100+ billion in RWAs in a composable, DeFi-centric manner.

It's probably the most important part of the mass adoption puzzle to figure out."

—**Misha Putiatin** (Founder, Symbiotic)

## From Bolt-On to Built-In

The trajectory of cover in DeFi is progressing through four distinct phases:

| Protocol Cover | Native Protocol Cover | Embedded Vault Cover | Agentic Coverage (up next) |
|---|---|---|---|
| Investors independently purchase cover for specific protocol deployments.<br><br>This process is manual and requires active oversight. | Protocols integrate cover directly into their products.<br><br>Friction is reduced and awareness increased. | Cover is built into the vault itself.<br><br>Depositors receive protection as part of the vault structure, earning a risk-adjusted yield without additional steps. | Autonomous onchain agents will manage cover dynamically, adjusting limits and responding to risk signals in real time. |

## The Infrastructure Making This Possible

Three developments are driving the industry toward embedded and agentic cover.

1. **Expanding underwriting capital**. Cover can only scale as fast as the capital behind it. In November 2025, Nexus Mutual partnered with Symbiotic to create a composable onchain underwriting layer. Capital allocated through Symbiotic can simultaneously secure proof-of-stake networks and underwrite Nexus cover, expanding capacity to protect against larger and more complex risks without requiring idle reserves.
2. **ERC-4626 standardisation**. The Tokenized Vault Standard has established a common interface across vault deployments, allowing cover to be integrated and applied composably across the ecosystem.
3. **A shared taxonomy of onchain risk**. Embedding cover requires pricing it accurately. The Onchain Risk Map, developed by Nexus Mutual and OpenCover, provides the first comprehensive taxonomy of DeFi risk, from smart contract vulnerabilities to oracle manipulation, governance attacks and more. Standardising how risk is defined is the prerequisite for automating how it's covered.

## Onchain Risk Review: Q1 2026 Hacks & Claims

Q1 2026 saw significant risk-related losses in DeFi despite market volatility decreasing onchain activity. The below loss events each impacted more than $1 million on EVM-compatible networks.

| Date | Project(s) | Loss Event Type | Loss Value |
|---|---|---|---|
| 12 March | Aave | Human Error | $50M |
| 10 March | Aave / Chaos Labs | Oracle Misconfiguration | $27.8M |
| 9 January | Truebit | Smart Contract Vulnerability | $26M |
| 22 March | Resolv Labs | Compromised Operations Wallet | $23M* |
| 4 February | Aperture Finance | Smart Contract Vulnerability | $3.7M |
| 15 March | Venus Protocol | Smart Contract Vulnerability | $3.7M |
| 20 January | Makina | Oracle Manipulation | $4.1M |
| 1 February | CrossCurve | Smart Contract Vulnerability | $3M |
| 5 March | Solv Protocol | Smart Contract Vulnerability | $2.7M |
| 26 February | FOOMCASH | Smart Contract Misconfiguration | $2.3M |
| 18 February | Moonwell | Oracle Misconfiguration | $1.8M |
| 8 January | TMXTribe | Smart Contract Vulnerability | $1.4M |

**Final figure still being reconciled at time of writing.*

## Conclusion

Although crypto crossed the rubicon to institutional adoption, it didn't leave the risk behind. Physical threats have only accelerated, and onchain vulnerabilities remain ever present.

Since 2019, Nexus Mutual has covered more than $6.5 billion in digital assets against onchain risk, paid more than $18.5 million in claims, and continued to build innovative solutions to crypto's biggest threats.

### You're Covered with Nexus Mutual

If your protocol, fund, or project would like to be featured or contribute to future editions of The State of Crypto Insurance, please reach out to us at nexusmutual.io.


**VISIT**
nexusmutual.io

**FOLLOW**
x.com/NexusMutual

**CONTACT**
info@nexusmutual.io