The State of Crypto Insurance

Q2 2026 Special Issue

The DAO Hack: A Decade Later

June 17, 2026 marks ten years since The DAO was exploited for approximately $60 million in ETH, triggering a hard fork that (literally) split Ethereum and forced the industry to confront some difficult questions. What does trust mean in a trustless system? Who bears the cost when code fails? What does resilience actually look like?

For this special issue, we talked to the people who've spent the last decade trying to answer those questions. **Griff Green**, one of The DAO's curators, is now directing TheDAO Security Fund, which is using the unclaimed ETH to fund Ethereum security grants. **Hugh Karp** was inspired to found Nexus Mutual in direct response to the gap the hack exposed. We'll also hear from two DeFi-native funds, **Dialectic** and **M1 Capital,** who share how the evolving threat landscape has forced them to rethink risk management.

Published by Nexus Mutual

LEGAL

Disclaimer & Attribution

This report and the Onchain Risk Map (together, the Materials) are published by Nexus Mutual and OpenCover for general informational and educational purposes only. The Materials present a high-level taxonomy and analysis of onchain risk based on publicly available information, historical events, and the authors' research, analysis and interpretation as at the date of publication. The Materials are not intended to be exhaustive and do not purport to identify all risks, threats, failure modes, or vulnerabilities that may be relevant in any given context.

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

The Materials are 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 Materials may be shared and referenced for non-misleading informational purposes, provided that clear and prominent attribution is given to Nexus Mutual and OpenCover. The Materials 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 and OpenCover. 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 Materials at the time of publication, no representation or warranty (express or implied) is made as to their completeness, accuracy, timeliness, or ongoing applicability. Onchain systems, market conditions, threat vectors and risk profiles evolve rapidly, and the Materials may become outdated or incomplete without notice.

Nexus Mutual and OpenCover accept no responsibility or liability for any use or, reliance on, the Materials by any third party. All intellectual property rights in the Materials 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.

01 · RETROSPECTIVE

Ten Years After The DAO

On June 17, 2016, a smart contract holding 3.6 million ETH was drained in a reentrancy attack. The resulting $60 million loss triggered a hard fork that split Ethereum in two and left a question hanging over the entire industry: if the code is law, what do you do when the law is broken?

The community fractured over how to respond. The Ethereum Foundation first attempted a soft fork to freeze the stolen funds, but abandoned it after developers found it opened a denial-of-service vector. A coin-weighted vote (Carbonvote) showed most of the community favored intervention, and on July 20, 2016, at block 1,920,000, the network executed a hard fork: a one-off "irregular state change" that moved the drained ETH into a recovery contract from which DAO token holders could reclaim their funds. A vocal minority rejected this, arguing that immutability was non-negotiable and that rewriting the ledger undermined the premise of a trustless system. They kept mining the original, unaltered chain, which lived on as Ethereum Classic. The forked chain continued as the Ethereum we know today.

The DAO's aftermath reshaped how the industry approached security. Smart contract audits went from rare to expected, and a dedicated audit industry grew up around them, later joined by bug bounties, formal verification, and onchain monitoring. Cover markets emerged to absorb the risk that remained: Nexus Mutual launched in 2019, three years after The DAO, as a direct response to the protection gap the hack had exposed.

> If the code is law, what do you do when the law is broken?

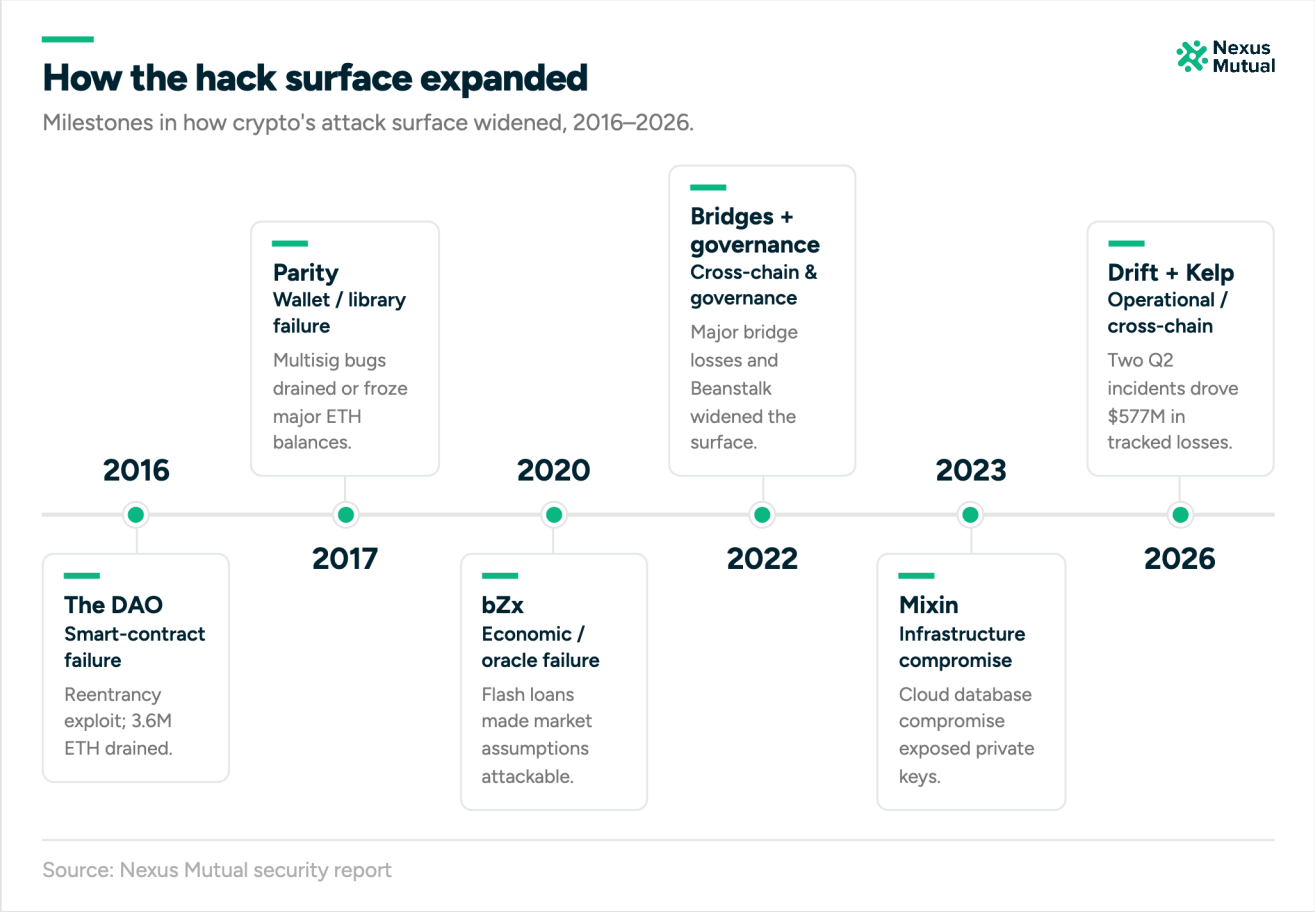
02 · THREAT LANDSCAPE

How the hacks evolved

In the early days of DeFi, the risks were primarily smart contract related, like the reentrancy vulnerability that drained The DAO. Another major loss event, the Parity wallet bugs of 2017 - a 150,000 ETH loss in July, followed by $150 million permanently frozen in November - reinforced the case for rigorous smart contract review.

In 2020, bZx was exploited twice in five days. Attackers used flash loans, uncollateralized capital borrowed and repaid in a single transaction, to manipulate oracle prices and extract profit. This marked the first time flash loans were used as an attack vector in production, and it triggered Nexus Mutual's first-ever claims payout.

Bridges became hackers' main target from 2021 onward. In 2022 alone, Ronin Network lost $625 million; Wormhole lost $320 million; and Nomad lost $190 million. At their peak, bridge exploits accounted for 73% of all DeFi losses[1].



[1] Source: The Ecosystem Vulnerability Scoreboard - Immunefi

In addition to bridge hacks, 2022 saw a new threat: governance attacks. In April, Beanstalk Farms lost $182 million when an attacker took a flash loan large enough to acquire a supermajority of governance tokens and passed a malicious proposal to transfer all protocol funds to an attacker-controlled wallet. Total crypto losses from hacks reached $3.7 billion in 2022, setting a new record at the time[2].

In 2023, losses fell to $1.7 billion, a 54% decline. The year's largest single loss came from a new angle: Mixin Network lost $200 million when attackers accessed the cloud database of its infrastructure provider and obtained private keys directly.

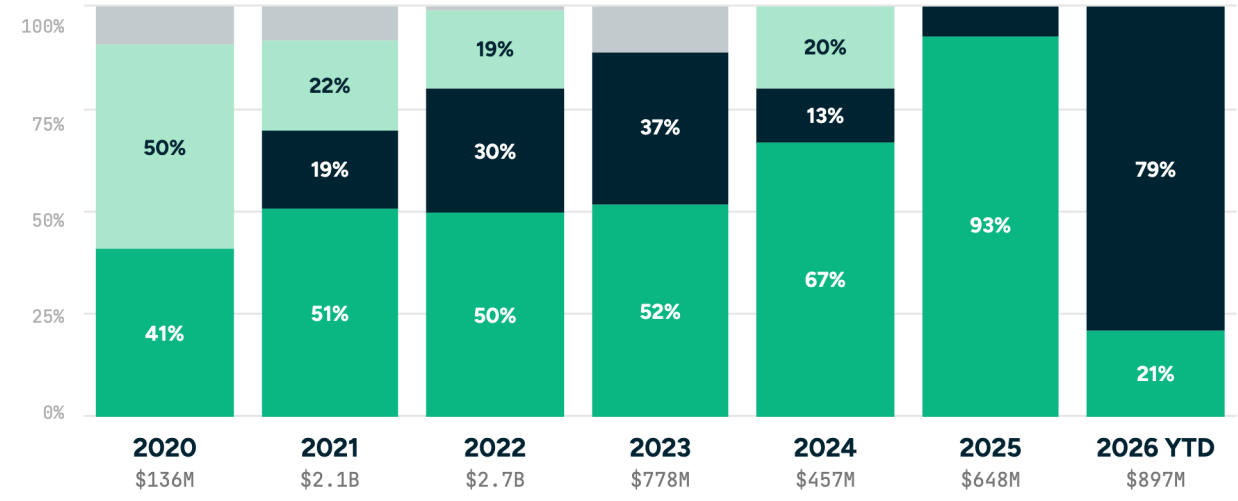
The trend reversed in 2024, when losses climbed back to around $2.2 billion. The targets shifted too: the largest thefts were no longer contract exploits but compromises of keys and operational infrastructure. DMM Bitcoin lost roughly $305 million in May after its signing process was compromised, and WazirX lost about $230 million in July through a breached multisig wallet. North Korea–linked groups alone accounted for an estimated $1.3 billion in losses across nearly 50 incidents.

Attack methods changed

Annual share of DeFi Protocol hack losses (USD), by classification. Centralized exchange losses not included.

2026 YTD
Losses flip back toward infrastructure-driven attacks.

Nexus Mutual



Source: DeFiLlama DeFi Protocol hack records, grouped by classification. 2026 is year-to-date at time of pull.

[2] Source: 2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen - Chainalysis

2025 set a new record at roughly $3.4 billion, almost half of it from a single event: the $1.5 billion Bybit hack in February, the largest crypto theft to date. Lazarus Group had compromised the exchange's multisig signing flow during a routine transfer.

2026 saw one of the worst stretches on record. Drift Protocol lost $285 million on April 1, and Kelp DAO lost $292 million on April 18. Both are attributed to North Korea's Lazarus Group: both the result of compromised operations infrastructure.

DeFi TVL went from under $700 million at the start of 2020 through a peak of $255 billion in November 2021, settling around $75 billion today. While the amount at risk has varied, the attack surface has never stopped growing.

03 · INTERVIEWS

Hear from the Builders

We talked to the people who've spent the decade since The DAO hack building risk management infrastructure, and deploying capital across DeFi.

Hugh Karp

FOUNDER, NEXUS MUTUAL

Hugh Karp was an early participant in the Ethereum ecosystem. Inspired by The DAO Hack, he officially founded Nexus Mutual three years later, building the first blockchain-native discretionary cover protocol.

"In 2016, you couldn't simulate a transaction before running it. You crossed your fingers and hoped the code did what you thought it did.

Audit firms as we know them today didn't exist. There were a handful of early Solidity developers offering their services individually, and most protocols shipped without any audit at all. Token contracts weren't standardized; every project wrote its own version. SafeMath wasn't in common use, and integer overflows were a routine issue."

Griff Green

CO-FOUNDER, THEDAO SECURITY FUND & GIVETH

Griff Green worked for Slock.it and launched The DAO. When the hack happened in June 2016, he co-led the White Hat Group, a counter-exploit effort that drained the remaining DAO funds before the attacker could reach them, and became a Curator to facilitate fund recovery efforts. He's since co-founded Giveth, DAppNode, and Commons Stack, and is now directing TheDAO Security Fund, which is deploying the unclaimed ETH from the original hack toward Ethereum security grants.

You've said the hack kickstarted Ethereum's security industry. Ten years on, have we focused on building the right things?

Mostly, yes. The industry focused heavily on smart contract security, and that was probably the most important thing it could have done. We now have audits, bug bounties, formal verification, monitoring systems, and a rich ecosystem dedicated to protecting smart contracts. The progress has been extraordinary.

But I think we became too narrowly focused on smart contracts and underinvested in operational security, user safety, and shared security infrastructure.

Ethereum today is like an apartment building where every project has installed a vault door, cameras, and a guy with a shotgun outside its own apartment. Meanwhile, the building itself has no doorman, no cameras in the hallways, and doesn't do fire drills.

Every protocol spends enormous amounts independently securing itself, but the ecosystem hasn't taken full advantage of the economies of scale available when securing shared infrastructure. The Ethereum Foundation has done strong work at the network level, but the wider community hasn't coordinated nearly enough around systems that make Ethereum safer for everyone.

We focused on the right problem. We haven't always focused our resources in the most effective way.

What surprised you most about how the industry has evolved?

What surprises and disappoints me most is that in 2026, I still can't give my mom a non-custodial wallet and walk away knowing she'll be okay. Even last night I spent 30 minutes on the phone with my brother so he could buy a gift card with crypto safely.

The safest consumer crypto products are often custodial products from centralized exchanges or traditional financial companies. If I onboard someone to a non-custodial wallet, I have to explain seed phrases, token approvals, phishing, address poisoning, networks, bridges. I've been onboarding nonprofits to crypto through Giveth for years, and I've watched them lose money in almost every way imaginable.

What's an important lesson from The DAO hack that the industry hasn't fully acted on?

We need to control the configuration space.

The DAO raised too much money. It feels strange to describe raising too much money as a design failure, but the system allowed an enormous amount of capital to accumulate without sufficiently constraining the possible outcomes. We saw the same problem years later with Fei/TribeDAO.

When the public can interact permissionlessly with a system, designers need to constrain both the upper and lower boundaries of what can happen: fundraising caps, withdrawal limits, circuit breakers, rate limits, and delays for unusually large or abnormal transactions.

If someone wants to bridge $100 million, it's acceptable for that to take a day or more. If someone wants to move $10 million, it may be reasonable to require dividing it into smaller transactions with time between them. These constraints could dramatically limit losses from hacks and give defenders time to respond.

Permissionlessness doesn't require making every possible action instantaneous and unlimited.

You spent the last decade building coordination infrastructure that didn't exist in 2016. What's meaningfully different now about how protocols manage shared resources and risk?

Almost none of today's coordination infrastructure existed in 2016. Ethereum wasn't even a year old when The DAO was hacked. At the time, it felt like one project. Today it feels like thousands of projects, sectors, networks, and competing ecosystems.

We now have stablecoins, mature multisigs, governance tooling, legal entities, onchain voting, insurance protocols, Layer 2 networks, proof-of-stake infrastructure, and established security industries. Stablecoins in particular became essential coordination infrastructure: they made it much easier for distributed organizations to budget, transact, and manage risk without requiring a custodian.

The legal environment has changed enormously too. The DAO had no formal legal entity. In 2016, the relationship between smart contracts and the legal system was extremely awkward to navigate. It's still complicated, but protocols now have far more established tools, structures, and expectations.

One area that gives me real hope is the smart contract security community. Auditors, researchers, and security teams often share information and coordinate remarkably well despite being direct competitors. Some parts of Ethereum have developed a genuine culture of shared defense. The challenge is extending that culture across the wider ecosystem.

TheDAO Security Fund is now putting the unclaimed ETH to work for Ethereum security grants. What's the governing principle behind how you'll deploy it?

The governing principle is competition.

TheDAO Security Fund won't simply choose where the funds go. The goal is to run well-designed competitive processes where the best ideas, projects, and solutions can emerge and receive funding.

We've built a community of 200 Ethereum security experts, represented through ETHSecurity badges, who help evaluate the options. Instead of deciding in advance that one organization or approach should receive funding, we want to set the table with a range of credible proposals and have them compete in the open.

We've already applied this through a quadratic funding round involving 134 security projects. Over time, we expect more rounds structured around specific requests for proposals - a round might contain 10 to 20 competing RFPs, with different budgets and different approaches to a defined security problem. ETHSecurity badge holders and other relevant expert communities evaluate the proposals and direct funding toward the strongest options.

We may move slowly at first while the treasury grows and the process matures, but the long-term goal is recurring rounds, ideally quarterly, using a variety of DAO coordination tools. The principle stays the same: create meaningful competition, draw on distributed expertise, and avoid concentrating funding decisions in a small group.

How can we make Ethereum safer?

Security and safety aren't the same thing.

Ethereum is the most secure blockchain in the world, but it's still not safe for an ordinary person to use. People with good intentions are losing money in countless ways: sending funds to the correct address on the wrong network, clicking phishing links, receiving calls from scammers pretending to be Coinbase support, opening fake DocuSign emails, depositing into protocols that are later hacked or rugged.

We've focused so much on security that we've lost touch with the needs of ordinary people who simply want to hold assets and use decentralized technology without becoming full-time security experts.

Crypto can be safer than the banks. We can adopt the tools banks use to protect consumers: monitoring, transaction controls, recovery mechanisms, cover, and fraud detection. But we have an advantage banks don't: we can build those protections without requiring a custodian to control the user's funds.

There's no wallet today that I consider truly safe for an ordinary person. If we want Ethereum to grow beyond experts and gamblers, safety needs to become the industry's highest priority.

Steven Wisbrun

MANAGING PARTNER, CIO, M1 CAPITAL

M1 Capital is an Amsterdam-based digital asset hedge fund focussed on market-neutral strategies.

What's the biggest structural risk in DeFi that the industry is still underestimating?

Composability is one of the unique selling points of DeFi, and it is also DeFi's main risk vector. With everything built on top of everything else, every investment comes with a dependency risk. The average DeFi user still typically doesn't price this risk with their investment. When one thing breaks, it doesn't break alone; everything stacked on top inherits the damage.

What's the gap between DeFi's risk management infrastructure today and what institutional allocators actually need?

The user base is still largely retail, and it reacts to headline APY, not risk management. So we often observe protocols optimize for the number on the front page, not the soundness behind it.

It's a market that rewards the loudest yield rather than the safest one, and the incentives flow downhill from there. Until the capital base starts demanding real risk disclosure, protocols won't build it, because nobody's paying them to.

The biggest losses in 2025 and 2026 were OpSec failures. Does that change how you manage operations and risk at M1?

We're extremely paranoid about who we work with and what we trust. We realised early that OpSec isn't only a protocol problem, so we brought in specialists like Hypernative and ZeroShadow.

What the last two years changed most is the weight we put on OpSec when doing counterparty diligence. It was always part of the conversation, but it now receives a lot more weight.

How are you thinking about your evolving cover needs?

Cover is getting more important, and we've bought materially more of it this year. The principle is simple: a tail event shouldn't be able to wipe out part of the portfolio, and with this many unknowns in the system, better safe than sorry. The genuinely hard part is pricing it, but luckily that's the job of the smart people at Nexus Mutual, not ours.

Alessandro Buser

CEO, DIALECTIC

Dialectic is an industry-leading DeFi fund and a Nexus Mutual member. They approach DeFi risk less as a binary question of safety, and more as a question of pricing, sizing, monitoring, and return.

The DAO shaped how the industry thinks about risk. How did it shape how you think about it?

The hack of The DAO was the first major smart-contract exploit. It demonstrated, for the first time, how the immutability of smart contracts can be a double-edged sword, and how a small bug in the code can lead to devastating consequences through just a few onchain transactions. While this was understood in principle by anyone working on smart contracts at the time, the deep rift it caused across the ecosystem was a wake-up call around the seriousness of smart-contract risk and security.

What changed most in how you evaluate protocol risk, and what event or moment drove that shift?

Smart-contract hacks have remained the largest category and source of lost funds in DeFi. But over time, more layers of risk have caused serious losses and need to be considered and properly mitigated, including oracle risk, access control and governance risk, bridge risk, and collateral and economic risk. Our view of DeFi risk has become broader and more inclusive of a wider set of categories and vectors, while our ability to monitor and react has also improved significantly. Contrary to common perception, we believe aggregate risk in DeFi is currently at an all-time low, largely because most capital is allocated to a small number of blue-chip, battle-tested protocols that have achieved a high degree of Lindy-ness over the last five years.

What has, or would, make you more confident deploying larger positions into DeFi?

We have developed enough risk management expertise over the years that we feel highly confident in our ability to allocate in DeFi profitably and sustainably at any size.

If return opportunities in DeFi were able to sustain much larger capacity, the current level of risk, when well managed, is already acceptable for large-scale deployments.

How do you evaluate whether a protocol is genuinely resilient versus just unattacked so far?

The risk equation is not binary. We do not categorize a protocol as simply resilient or vulnerable. Instead, we operate on a risk spectrum, where higher-risk opportunities require higher returns to be attractive and, when they are attractive, receive smaller capital allocations. Our approach requires objectively quantifying even the most qualitative risk factors into a risk score, so that each opportunity can be compared against others on a relative basis and produce a real-time risk-to-return efficiency score.

As an allocator, how do you think about the gap between what crypto cover can do today versus what your risk management actually requires?

The largest challenge is efficient pricing. Given the complexity of measuring and pricing risk in DeFi, underwriters are forced to apply large margin-of-safety premiums to each cover in order to account for the wide margin of error and uncertainty inherent in underwriting novel, highly complex, and high-stakes systems. As an allocator, our own ability to quantify and price the risk required to justify returns is not always fully matched by an insurer's ability to absorb that risk into a more diversified portfolio of covers. If this mismatch grows too large, certain opportunities that would be attractive on their own become unattractive once the insurance premium is applied, limiting our ability to allocate efficiently. With Nexus Mutual, we have been able to price covers more dynamically and maintain greater flexibility across our allocations, achieving a better overall risk-adjusted return for our clients.

04 · QUARTERLY REVIEW

Onchain Risk Review: Q2 2026 Hacks & Claims

In Q2 2026, two incidents attributed to North Korea's Lazarus Group account for $577M of the roughly $765M lost across 27 confirmed events. Operational security failures drove the majority of losses. KelpDAO's rsETH bridge was drained after attackers tricked LayerZero's verifier into approving a fake cross-chain message, releasing 116,500 rsETH from escrow. Each of the below events impacted more than $3 million.

LOSS VALUE	DATE	PROJECT(S)	CHAIN	LOSS EVENT TYPE
$292M	Apr 18	Kelp DAO (rsETH)	Ethereum / LayerZero bridge	Compromised Operations Wallet
DPRK/Lazarus-attributed; attackers compromised LayerZero DVN infrastructure around Kelp's 1-of-1 verifier and forged cross-chain messaging to mint/drain 116,500 rsETH (~$292M) in about 46 minutes				
$285M	Apr 1	Drift Protocol	Solana	Compromised Operations Wallet
DPRK-linked six-month social-engineering campaign; compromised multisig approvals and Solana durable nonces enabled admin takeover, fake collateral/oracle manipulation, and ~$285M drained in ~12 minutes				
$36M+	Jun 8-9	Humanity Protocol / H token	Ethereum, BNB Chain	Compromised Operations Wallet
Employee laptop compromise exposed multiple Gnosis Safe signing keys; attackers took bridge/admin control, drained protocol-linked wallets, and minted additional H on BNB Chain				
$18.4M	Apr 16	Rhea Finance	NEAR	Smart Contract Vulnerability
Attacker used fake tokens/pools and route construction to exploit Rhea's margin-trading parser/slippage/collateral validation; material funds were later frozen/recovered				
$13.7M	Apr 15	Grinex Exchange	Not protocol-specific; funds routed via Tron/Ethereum	Custodian Security Breach
User deposit wallets drained and funds rapidly converted via Tron/SunSwap and Ethereum routes				
$11.6M gross	May 18	Verus-Ethereum Bridge	Verus / Ethereum bridge	Smart Contract Vulnerability
Forged or invalid cross-chain payload; validation gap between source-chain proof/economic backing and EVM-side value binding. 4,052.4 ETH later returned, with 1,350 ETH retained as bounty				
$10.7M	May 15	THORChain	THORChain (Cosmos SDK app-chain)	Smart Contract Vulnerability
Newly churned malicious node exploited a GG20 threshold-signature (TSS) vulnerability, draining one THORChain vault; signing/trading halted during response				

LOSS VALUE	DATE	PROJECT(S)	CHAIN	LOSS EVENT TYPE
$9.5M	**Apr 7-13; reported Apr 14**	**Ledger (fake App Store app)**	**Not chain-specific**	**Phishing Attack**
Counterfeit Ledger Live app on Apple's macOS App Store harvested seed phrases from victims across multiple chains				
$7.3M	**May 29**	**DxSale**	**BNB Chain**	**Misconfiguration**
Legacy v1 lockers drained; external analysis points to ownership/privileged configuration and backdated lock mechanics affecting ~1,400 LP positions				
$5.4M	**May 30**	**Gravity Bridge**	**Cosmos / Ethereum bridge**	**Compromised Operations Wallet (suspected)**
Bridge halted after ~$5.4M drain including ~$4.3M USDC, 274 ETH/WETH, USDT and other assets. Early reports suspected signing-key compromise; later analysis disputes/refines that, so root cause remains caveated pending official postmortem				
$5M+	**Apr 30**	**Wasabi Protocol**	**Ethereum, Base, Blast, Berachain**	**Compromised Operations Wallet**
Compromised deployer/admin EOA granted attacker-controlled contracts privileged roles; vault strategies and pool implementations were upgraded and drained across four EVM chains				
$3.8M-$4.0M	**May 25**	**New Market Trading / third-party SquidRouterModule**	**Ethereum, Base, Arbitrum**	**Smart Contract Vulnerability**
88 victim Safes drained via a confused-deputy flaw: the module decoded the delegate address from attacker-controlled cross-chain payload and used it for Safe permission checks. Not a Squid-core or Safe-core exploit				
$3.5M	**Apr 21**	**Volo Protocol**	**Sui**	**Compromised Operations Wallet**
Admin key compromised via social engineering; WBTC, XAUm, and USDC drained from three vaults				

YOU'RE COVERED WITH NEXUS MUTUAL

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