

2026

Insuring Digital Assets:

How Companies Navigate Theft, Cyber, & Custody Risks

LOCKTON®

EY Parthenon
Shape the future with confidence

Key takeaways

- Digital asset operational risk is driven by custody design, key management, wallet architecture, vendors, and human controls.
- The leading loss driver is compromise of privileged people and engineering systems. Signing pipelines can be abused even when keys stay secure.
- No single policy fully addresses digital asset exposure; programs usually combine specie/custody, crime, cyber, tech E&O, and other lines.
- Coverage gaps can often emerge where theft, technology failure, and social engineering, particularly organized long-term campaigns, intersect.
- Design limits based on probable loss scenarios and risk-based modeling, not total assets under custody.
- Prepare for underwriting early: Strong governance and documented controls can improve insurability and pricing.

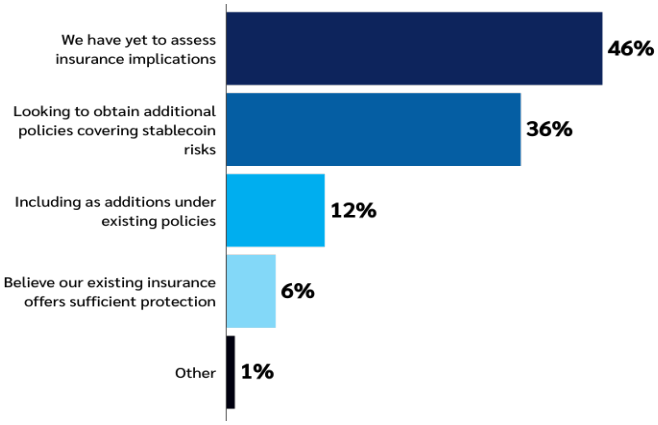
In recent years, digital asset companies have fallen victim to more sophisticated theft schemes and network security exploitations, with different attack vectors being targeted.

The methods of attack vary from case to case, but broadly speaking, attackers tend to target hot wallets by gaining access through impersonation or social engineering schemes, control failures, or by exploiting compromised vendors. Losses range from several million to more than $3 billion. Analysts reported that $3.4 billion in cryptocurrency was stolen in 2025.

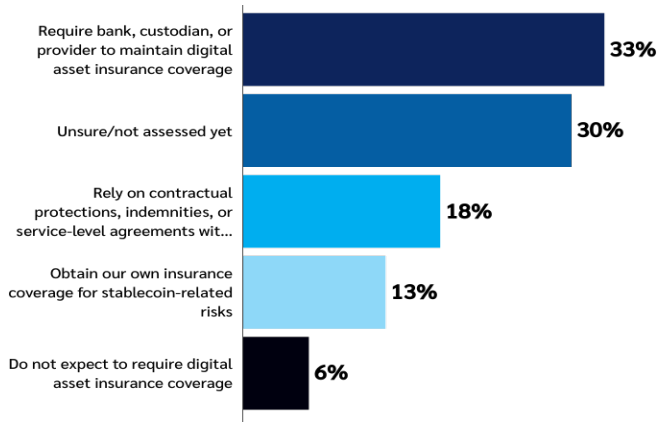
The continued risk of attacks on digital wallets in recent years remains a difficult problem for financial institutions and others handling digital assets to confront. For these companies, a thoughtful approach to security and risk management is critical.

The adoption of digital assets means institutions need stronger custody controls, internal processes, cybersecurity protocols, and appropriate insurance and risk-transfer solutions. But given that no system is impenetrable, digital asset holders need to be mindful of significant insurance blind spots.

A 2026 EY-Parthenon survey found **nearly half** of the 127 financial institutions surveyed had not yet assessed insurance as part of their stablecoin enablement and custody strategies.



That said, a similar EY-Parthenon survey showed increasing recognition of security concerns. Among asset owners, 79% expressed concern about digital asset custody and security in 2026, up 35% from the year before.



Corporate buyers showed a similar gap

- Among the 383 decision-makers at non-financial institutions, **nearly one-third** were unsure of or had not assessed stablecoin custody, wallet, or transaction risks.
- At the same time, **one-third** expected banks or custodians to maintain digital asset insurance.
- **This mismatch points to a readiness gap** between corporate expectations and financial institutions' insurance programs.

Digital asset holders should understand where losses can occur, which insurance products are well suited to provide coverage, and how to build a coordinated insurance program to meet their novel and heightened exposures. Businesses leveraging third-party custodians should validate that appropriate controls are in place.



Mitigating loss scenarios

Digital asset companies face familiar risks, including cyber attacks, phishing schemes, compromised vendors, and internal theft or misconduct. Digital asset losses can occur quickly and may be challenging to recover.

Blockchain immutability means transactions often cannot be reversed. While blockchains can provide better transparency, in some cases, pseudonymity and AI-enabled laundering schemes can hinder investigations. Policies on recourse after a loss are disparate and undertaken firm by firm and event by event. (For example, bank depositors enjoy limited protection against loss from the Federal Deposit Insurance Corporation.)

Similar to fiat currency, attackers can also harness artificial intelligence to craft more convincing social engineering ploys and accelerate and to automate their attacks at scale.

Major security risk areas

01 Transaction governance

Digital asset holders need controlled systems to approve and sign transactions, authorizations, and any messages. These protocols are designed to prevent employee theft and external manipulation. But attackers can infiltrate a financial institution's systems through a compromised third- or fourth-party vendor or via social engineering, phishing, or other means of deception. From there, an attacker can manipulate transaction instructions or spoof approvals, helping them make off with ill-gotten assets.

Reducing the probability of loss: *Digital asset holders should assess potential weaknesses across their transaction systems and vendor network. Hardware security modules and distributed signing technologies such as multiparty computation can help protect key material and reduce reliance on a single signer or system. These safeguards should be complemented by controls such as those that validate transaction instructions, destinations, and policy compliance before signing, including transaction decoding or simulation to validate the transaction being authorized. Each signing request should be tied to its underlying approval and the exact transaction being approved. Digital asset holders should also maintain and test response and recovery procedures for suspected compromise of key material, credentials or transaction systems, including the ability to suspend transactions, revoke access, rotate affected credentials or key material, preserve evidence, and securely transfer assets when necessary.*

02 Custody structure

How firms store and manage private keys is a critical decision. Concentration of funds in too few wallets or, specifically, in hot wallets, can lead to severe loss scenarios.

Reducing the probability of loss: *Most assets should be maintained in offline or otherwise highly protected storage, consistent with the institution's liquidity and operational requirements. Assets maintained in online wallets should be segmented and subject to risk-based limits, independent authorization, transaction monitoring, and controls designed to prevent a single compromised user, system, or service provider from enabling an unauthorized transfer.*

03 Vendors

A common vector for external attackers is vendors with weak cybersecurity and network security practices.

Reducing the probability of loss: *Vendor due diligence should include an examination of their cybersecurity practices, financial strength, incident response readiness, transaction workflows, system and organization control (SOC) reports, other fourth-party relationships and technology, and key management standards if handling private keys.*

04 Privileged access & personnel security

Employees with privileged access to wallet, signing and production systems can be targeted through phishing, social engineering, or other means of deception. A compromised employee or endpoint can provide attackers access to sensitive systems or facilitate unauthorized transactions.

Reducing the probability of loss: *Digital asset holders should apply least-privilege access, phishing-resistant multifactor authentication, separation of duties, and hardened workstations for privileged activities. These controls should be supported by role-specific security training, personnel screening, and procedures to quickly escalate suspicious activity or potential compromise.*



Types of digital asset insurance

Even with risk mitigation measures in place, institutions remain susceptible to attacks. When attacks occur, insurance plays a crucial role in digital asset risk management.

Global banks and large financial institutions have become increasingly sophisticated buyers of digital asset insurance, but digital natives and startups frequently grapple with the cost-benefit of spending capital on insurance versus deploying capital to harden security, enhance operations, and support company growth.

In addition to risk transfer, the underwriting process can provide an external perspective on a company's processes, systems, and risk posture. Digital asset insurance is rarely a single product. Programs usually combine several policies, each responding to different loss scenarios.

Some digital asset market participants also retain a portion of their risk through self-insurance, including dedicated safety or reserve funds. This approach can provide additional capacity where commercial insurance is limited, costly or does not fully address a company's potential loss scenarios.

Comparison of digital asset insurance types

Primary risks addressed	Typical buyers	When companies should consider coverage
SPECIE/CUSTODY		
Theft, loss, or damage involving cold-storage media, private keys, or other safeguarded physical assets	Custodians, exchanges, banks, financial institutions, and other companies holding digital assets in custody	Companies taking custody of digital assets. Companies that utilize cold storage, offline signing devices and private keys, or have physical intervention in the signing process.
CRIME		
Employee theft, computer fraud, fraudulent funds transfer, and social engineering losses	Custodians, exchanges, banks, financial institutions, payment service providers, broker/dealers, and companies transacting in digital assets	Companies taking custody of digital assets that utilize cold, warm, or hot wallets, or that use cloud-based signing devices and private keys
CYBER		
Network intrusions, ransomware, data loss, incident response, business interruption, smart contract exploits, and other cyber events	Digital asset platforms, exchanges, custodians, fintech companies, miners, and other technology-dependent organizations	Any company. This coverage responds to network security and privacy events.
TECHNOLOGY ERRORS & OMISSIONS		
Customer losses arising from software, platform, wallet, smart contract, or vendor technology failures	Wallet providers, custody technology vendors, exchanges, blockchain infrastructure providers, and software firms	Companies selling technology products and services, particularly when customers depend on the technology to enable transactions or when disruptions or downtime will cause a customer loss
SLASHING/STAKING RISK		
Losses from validator penalties in proof-of-stake networks, including slashing events tied to operational errors or malicious behavior	Validators, staking providers, and institutions participating in proof-of-stake blockchain networks	Companies that operate validators and staking infrastructure. Companies staking assets with third-party validators can also explore contingent staking risk coverage
KIDNAP & RANSOM		
Physical threats, extortion, kidnapping, ransom demands, burglary, harassment, and security incidents targeting executives or key personnel	Digital asset company executives, founders, senior leaders, and firms with personnel perceived to control access to valuable assets	Any company, particularly those that have high-profile executives whom criminals may target for perceived wealth, or who have access to cold-storage assets and private keys

Overlaps & gaps in digital asset insurance

Like many insurance programs, digital asset insurance can have overlapping coverages and gaps between coverage.



Technology errors & omissions (E&O) policies often exclude theft of funds, meaning stolen or inaccessible assets may not be covered. Some insurers now offer affirmative coverage for the value of lost assets as damages against technology providers when a technology failure occurs.



Crime policies have historically defined money as cash, stocks, bonds, or other tangible assets. Insurers that deal in digital assets have expanded the definition to include digital assets. Traditional financial institutions looking to expand into the space should verify that their existing crime insurance covers digital assets.



Crime policies may not cover theft of confidential information, leaving that exposure to **cyber** policies. Gaps can arise when stolen information enables the theft of covered property if exclusions are not properly carved back. Buying crime, cyber, and tech E&O policies from the same carrier can also help align language and reduce disputes.



Other coverage considerations. Recent digital asset incidents highlight the importance of reviewing policy language around many coverage aspects and definitions. Among those: state-backed attacks and related exclusions, discovery and prior knowledge, aggregation of related losses, asset valuation and recoveries, voluntary customer reimbursements, and emerging attack techniques that may not fit traditional definitions of cyber or smart contract events.

Operational & enterprise-level gaps

Policy structures

Wallet structure, custody design, asset type, trading frequency, and the scale of digital asset activity all shape insurance-buying strategies.

For established banks, fintechs, and other financial institutions where digital assets are a smaller part of the business, existing carriers may offer digital asset coverage.

Some buyers may prefer a separate program for digital assets to avoid impacting the rest of the business's program or to obtain lower retentions for their digital asset operations.

Companies with significant digital asset exposure should work with carriers that understand the digital asset risk landscape and have experience covering market participants across the ecosystem. They may be more willing to structure appropriate coverage at a reasonable rate.

Thinking about policy limits

An obvious question when considering digital asset insurance is how much coverage to buy. The answer is usually less clear.

A financial institution holding $1 billion in digital assets may assume it needs $1 billion in coverage. But many institutions do not need coverage equal to the total assets under custody.

A sharper question to ask: What are the institution's probable loss scenarios?

Effective custody and operating models can avoid single points of failure by distributing assets, access, and control responsibilities across different systems and personnel. Limits should be tied to probable loss scenarios rather than total asset value.

Approaching the underwriting process

Digital asset underwriting is a detail-oriented process. Executives, security leaders, and cyber teams should expect focused questions from underwriters about cyber-readiness, governance, policy adherence, and operational maturity.

Factors that will likely weigh on an underwriter's analysis of a company include:

- Management experience and willingness to adhere to compliance and regulatory requirements, such as anti-money laundering controls and "know your customer" procedures.
- Security controls demonstrated in third-party audits and assurance reports, such as SOC 1/SOC 2, alignment with National Institute of Standards and Technology frameworks, and International Organization for Standardization 27001 certification.
- Technology governance, operational maturity, and dependency on vendors and cloud providers.
- The degree to which assets are concentrated in particular wallets.
- Financial position.
- Percentage of assets in cold storage.
- Physical security at facilities and vaults.
- Management of keys.

Wallet controls, key life cycle management, hardware security modules, and multiparty computation structures that split keys and reduce single points of failure will likely receive focused attention from knowledgeable underwriters.

They will also examine measures to reduce employee theft, including whether custody infrastructure is built in-house or outsourced, and how transactions are approved.

For privileged activities, controls should also include phishing-resistant multifactor authentication, time-limited access, and hardened developer endpoints.

Larger or higher-risk transactions may require increased approval quorums and approvers from different functions. For example, an institution might require two of three approvals for routine transactions of $100,000 and three of five for higher-risk transactions of $500,000, with thresholds determined by transaction value, asset type, destination, and velocity.

Effective velocity controls should detect unusual activity or rapid-fire transactions and act as circuit breakers to pause or stop suspicious activity.

Preparations for underwriting can lead to a stronger program with reasonable rates.

Getting started

As financial institutions adopt digital assets, they should move quickly to identify risks that are unique to the space. Companies should not wait for underwriting to uncover gaps in governance, controls, or protocols.

With the help of brokers, legal counsel, and specialized advisory partners experienced in digital assets, companies can enter the digital asset market better equipped to limit losses and with an effective insurance program to mitigate damage if and when a loss occurs.

VISIT OUR WEBSITE

CONNECT NOW

Contributors



Miguel Cano
Vice President
U.S. Blockchain & Digital Assets (LEAP) Advisory
Lockton
miguel.cano@lockton.com



Ian Graham
Senior Vice President
U.S. Blockchain & Digital Assets (LEAP) Advisory Leader
Lockton
igraham@lockton.com



Sarah Downey
Executive Vice President
Global Blockchain & Digital Assets (LEAP) Advisory Leader
Lockton
sdowney@lockton.com



Prashant Kher
Digital Assets Strategy and Transactions Leader
EY-Parthenon,
Ernst & Young LLP
prashant.k.kher@parthenon.ey.com



Scott Mickey
Senior Director
EY-Parthenon,
Ernst & Young LLP
scott.mickey@parthenon.ey.com



Bo Rieker
Consultant
Ernst & Young LLP
bo.rieker@ey.com



UNCOMMONLY INDEPENDENT

lockton.com | © 2026 Lockton Companies. All rights reserved.

FS: 9384372