WHITE PAPER

Insurance for Digital Currencies

What clients need to know

Contents

01 Bringing transparency to insurance for digital currencies

Within the financial services industry, the role of custodian is the safekeeping of physical or electronic assets on behalf of customers. Custodians provide the first line of defense with software, hardware, rigorous security policies and procedures, and physical security measures. These operational practices are necessary for the safekeeping of assets, but not the only ways in which custodians deliver valuable protection. Due to their specialization, sophistication, resources, and scale, custodians also have the ability to procure commercial insurance which acts as a financial backstop and reduces counterparty risk faced by the owner of assets under custody.

Today, the greatest threat posed to institutions holding digital currencies is the theft or loss of private key(s), whether in digital or physical format. As many digital currencies are essentially bearer assets, it can be difficult or impossible to recover funds once a transaction has been approved and added to the blockchain. As a result, many custodians are implementing an additional layer of protection against theft or loss of private key(s) in the form of commercial insurance policies. These risk transfer solutions are tailored to address the unique risks associated with providing financial services to this emerging asset class, but the quality and availability of these solutions is far from standardized.

There are a number of reasons why the quality and availability of insurance for custodians of digital currencies varies materially in the current environment, including but not limited to:

- Nascency of technology and a wide array of implementations means that underwriting “best practices” have not yet been defined
- Concerns around regulatory risk, reputational risk, solvency, and legal exposure potentially faced by the insurance buyer
- Trepidation around regulatory and reputational risk to the insurance company
- Lack of claims data and/or industry track record needed to price risk

- Shortage of quality institutional buyers with the attributes necessary to build a pool of similar risk and thus spread and mitigate aggregation of risk
- High volume of submissions from cryptocurrency companies not able to pay the requisite premiums in order to fund significant losses
- Many existing insurance products are insufficient and do not apply to cryptocurrency or blockchain technology companies thus requiring significant contract amendments in order to be confident they will perform
- General education gap around the technical features and necessary security measures of smart contracts and blockchain technology

As a result, many companies who make public claims about their insurance coverage are not specific or transparent about what the coverage entails. This leads to significant asymmetry in what one company is able to purchase compared to another, and a "buyer beware" environment due to the opacity of policies.

Our intent is to establish a framework for what clients should expect from their custodian; clarity around what is and what is not insured; the value of insurance per incident; how the insurance policy is designed for coverage; and what questions they need to ask any custodian they are considering using.

02 What insurance companies evaluate when deciding whether to write a policy for a cryptocurrency firm

While determining a company's viability for insurance, providers assess custodial compliance, cold storage methods, policies, and procedures.

$100M
Coverage

The quality of these measures will define the company's ability to purchase adequate coverage. In the current insurance environment, custodians obtaining and providing insurance of $100 million have demonstrated a thorough commitment to asset security in cold storage.

Custodians who seek out compliance measures and install robust security controls demonstrate a willingness to be transparent. These measures and controls include:

- Qualified custody certification under the Advisers Act of 1940
- Strong Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) oversight
- SOC 1 and SOC 2 reporting and auditing designations
- CryptoCurrency Security Standard (CCSS) and Financial Services — Information Sharing and Analysis Center (FS-ISAC) membership

---

Security is not based on speed of access to funds. Deep cold storage provides assurances that funds can not be easily transferred, requiring rigorous controls amongst multiple people. A security-first approach includes:

- Protection of digital keys in physical, bank-grade vaults
- Sharding of keys across multiple physical vault locations
- Presence of multiple people to unlock institutional funds

Enacting institutional-quality control environments with rigorous policies and procedures makes it feasible for a custodian or exchange to obtain significant coverage:

- 100% multi-signature technology with multiple people present to withdraw assets
- Reporting of digital assets in and out of cold storage for trading or spending including how transfer requests are initiated, transactions are approved, assets are moved, and how final approval is given

03 Types of insurance that custodians and exchanges should seek

With many possibilities for loss, there are varying types of insurance designed to provide specific coverage. An effective policy will be comprised of multiple types of insurance.

While one category of insurance may directly protect a client's assets, another category may protect the company securing those assets. As a result, both types of insurance are important.

Custodians and exchanges should seek insurance covering a range of possible risks. Policies may include:

Cyber risk insurance, which helps mitigate risk exposure by financially supporting recovery of funds after a cyber-security breach, but does not cover theft of digital currencies.

Commercial crime insurance, which covers computer fraud, funds transfer fraud, forgery or alteration, kidnap ransom or extortion, and theft or loss of money and securities.

Specie insurance, which insures high value assets while undergoing transfer or in vaulted security, and provides opportunity for the insured business to more easily scale its offering. In addition to digital assets secured in cold storage, specie traditionally applies to fine art, bullion and other precious metals, diamonds, cash, and securities.

Errors and omissions insurance (E&O), which covers professional liability, protecting individuals and companies that provide professional advice and services from carrying the entire financial cost of defending against a negligence claim. However, E&O insurance does not cover theft of digital currencies.

Directors and officers insurance (D&O), which covers liability of a corporation's management, covering the corporation as well as directors and officers of the corporation, but does not cover theft of digital currencies.

Co-insurance, which is a policy that combines self-insurance with an insurer. 80/20 split is common with co-insurance, where the insurer pays 80% after the deductible is covered by the insured party. Important to note, this deductible is in addition to a traditional deductible which applies to the first portion of a loss.

04 Insurance that protects you

With no history of claims or best practices for analysts and underwriters to draw from, policies today are bespoke. As such, coverage will be complex and differ from company to company. In order to protect the client, transparency surrounding depth and availability of coverage is critical.

Standards around security and the insurance market are still developing and clients may find a lack of clarity from custodians regarding how an insurance policy functions in the event of a breach. Specifically, some custodians and exchanges may not opt for coverage that applies to certain security risks like wallet hacks. This kind of approach is insufficient, leaving wide gaps where insurance will not be effective and putting clients at risk.

Here is what you should look for when assessing whether an insurance policy protects you:

1. Coverage for third-party hacks, copying, or theft of private keys
2. Coverage for internal theft by company employees or executives
3. Coverage for loss of keys

If a policy does not cover these items, it is likely that it will not be effective in supporting the security needs of today's threat vectors.

05 Determining what kind of insurance a custodian or exchange has

With regulation around cryptocurrencies still developing, custodians and exchanges will fulfill their compliance obligation at varying degrees. As insurance for digital currencies takes shape, premiums are costly with probability of risk still unknown, and policies will be constructed differently based on the merits of each company's security practices.

These questions will help to determine how comprehensive a company's insurance policy is and serve to guide which custodian or exchange has the best insurance offering for your assets:

Q: **What is the aggregate limit of relevant policies carried by the custodian?**

The aggregate limit refers to the maximum amount of insurance coverage of all relevant policies.

Q: **Who are the insurers underwriting the policy? What are the AM Best ratings of carriers backing the policy(ies)?**

Are the insurance providers and underwriters of the policy A-rated? A-rated insurance firms operate with the highest level of creditworthiness, defined by the financial strength of the firm.

Q: **Does the policy cover theft of digital assets?**

See definition of “Property” to ensure it includes crypto as opposed to fiat or other physical property.

Q: **Does the policy cover loss/destruction of private keys caused by natural disasters?**

This includes fire, lightning, smoke, windstorm, hail, riot, civil commotion, aircraft, vehicles, vandalism, sprinkler leakage, sinkhole collapse, volcanic action, falling objects, weight of snow, ice, or sleet; water damage, flood, and earthquakes.

Q: **Does it cover insider theft?**

Does theft include insider theft by executives or other company employees?

Q: **Is the coverage for cold wallets, hot wallets, both, neither?**

Some programs have partial coverage (aka “sub-limits”) for hot wallets but full limits for cold wallets, so ask for specifics of limit available for each type of wallet.

Q: **What legal entities are covered by the insurance policy?**

Does this match the legal entity for which a customer has entered into a service agreement?

Q: **Does the custodian or exchange allow you to purchase additional insurance of your own?**

Does adding your own insurance affect the custodian or exchanges policy? Can you purchase additional insurance for a key recovery service?

Q: Does the custodian's policy employ "co-insurance" or "self-insurance" in addition to the per loss deductible? What is the amount of the deductible? What is the percentage of the co-insurance?

The custodian should be transparent about what percentage of self-insurance they have because it will partially determine how much risk the company has taken on. When a custodian or exchange opts for a portion of self-insurance, they may not term their coverage to be "fully insured," as a percentage of any single loss would be self-insured.

Insurance for digital assets provides an additional layer of protection against loss, but the extent of that protection depends on the practices and procedures of the custodian seeking to be insured. Clients should expect transparency and clarity from their custodian because these are key indicators of dedication to reliable security.

Asking the right questions will help to determine whether a company's insurance coverage is right for its assets, and whether it will perform as promised. Digital currencies are an emerging asset class offering new investment potential. Make sure your assets are held by a company who is committed to your security.