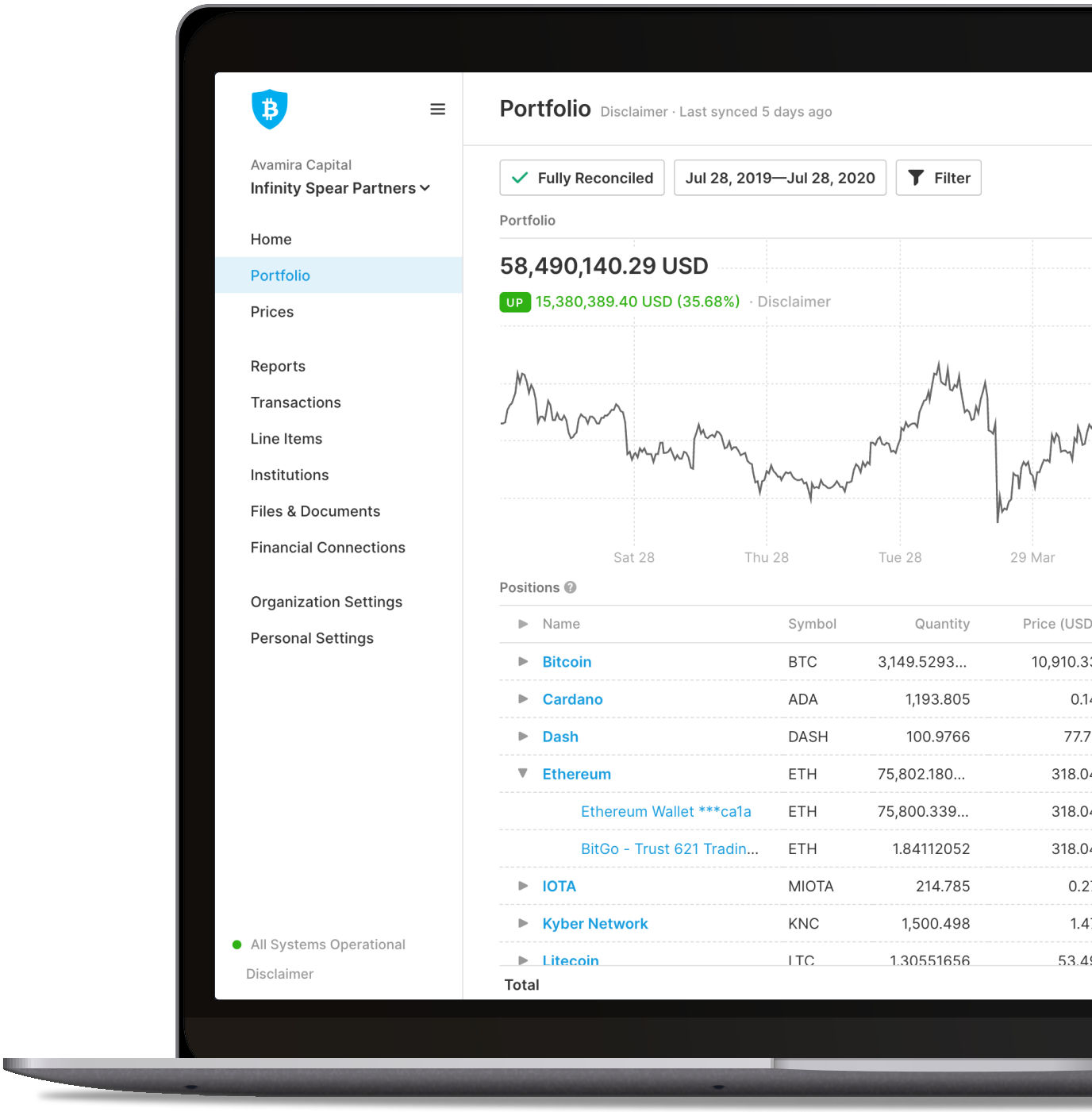
BitGo

Insurance for Digital Currencies: What Clients Need to Know



Insurance for Digital Currencies

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 “best practices” have not yet been defined to underwrite against
- Concerns around regulatory risk, reputational risk, solvency, and legal exposures potentially faced by the insurance buyer
- Concerns around regulatory and reputational risk to the insurance company
- Lack of claims data and/or industry track record needed to price risk
- Lack 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 don’t apply to cryptocurrency or blockchain technology companies, 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

Insurance for Digital Currencies

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.

WHEN EVALUATING CANDIDATES FOR INSURANCE, WHAT DO INSURERS LOOK FOR?

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

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 $250 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; and
- 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 cannot 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; and
- Multiple people must be present 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.

Insurance for Digital Currencies

TYPES OF INSURANCE CUSTODIANS AND EXCHANGES SHOULD SEEK

There are varying types of insurance designed to provide specific coverage for different perils or exposures to Loss. An effective insurance program will comprised of multiple types of insurance.

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

Technology Errors & Omissions/Cyber risk insurance, responds to failure of a technology product or service to perform as designed or expected, breaches in network security or privacy including theft of protected data (not directly private key material). These policies cover first party costs including breach response, forensics, notification and legal costs in addition to liability arising out of failure to secure the custodians network or failure of a technology product to perform.

Commercial Crime/Fidelity insurance, which covers employee theft, computer fraud, funds transfer fraud, forgery or alteration, and theft or burglary of property from a premises or in transit

Specie insurance, insures assets in secure vault environments (cold storage) against theft by employees, robbery or burglary by malicious actor, or physical damage or destruction of digital asset key material.

Directors and Officers insurance (D&O), Protects Directors & Officers of the organization if sued by stakeholders for alleged breach of duty in their capacity as D&Os.

Errors and Omissions insurance (E&O), Protects the organization against alleged breach of duty, acts, errors or omissions related to the provision or failure to provide professional services.

INSURANCE THAT PROTECTS YOU

With relatively nascent history around claims or best practices for analysts and underwriters to draw from, policies today are often bespoke. As such, the scope and quality of 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:

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

Insurance for Digital Currencies

DETERMINING THE TYPE OF INSURANCE A CUSTODIAN OR EXCHANGE OFFERS

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:

What is the aggregate limit of relevant policy carried by the custodian?
The aggregate limit refers to the maximum amount of insurance coverage over a set period of time.

Who are the insurers underwriting the policy? What are the AM Best ratings of carriers backing the policy(s)?
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.

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.

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.

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

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.

What legal entities are covered by the insurance policy?
Does this match legal entity for which customer has entered into a service agreement?

Does the design and structure of the custodian or exchange's insurance 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 or excess protection should the custodian's insurance be exhausted by a loss suffered by a different customer? Have the limitations to a custodian or exchanges insurance been sufficiently described so that you understand what is and what is not insurable under their policy?

Insurance for Digital Currencies

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?
If they do, they should be transparent about what percentage of self-insurance they have so that you can more accurately consider your counterparty exposure with respect to risks they retain in relation to their balance sheet.

The commercial Insurance carried by digital asset providers adds an additional layer of protection in that it provides an additional source of recovery above and beyond their balance sheet should they be responsible for financial damages to you, 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 your 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.