MARSH

DIGITAL ASSET RISK TRANSFER (DART) TEAM

Blockchain Technology and Digital Assets: Top 10 Reasons Why Insurance Matters

Around the world, companies of different sizes and in different industries are investing hundreds of millions of dollars to capitalize on new blockchain technology and digital asset opportunities that offer the potential to create groundbreaking new business models, and can also help address intractable challenges like cybersecurity, privacy, control of confidential data, supply chain management, and quality assurance. But blockchain and digital assets are a new and fast-growing technology and asset class functioning within an increasingly complex operating environment and facing an uncertain regulatory future. Organizations operating with blockchain and digital assets should therefore understand and manage key exposures, some of which are specific to companies in the blockchain space, which can make finding the right insurance protection even more challenging.

The Top 10 List:

1. Protecting Your Customer's Assets and Helping Retain Customer Trust
2. Protecting Directors' and Officers' Personal Assets and Attracting Top Talent
3. Protecting Your Company's Balance Sheet
4. Protecting Key Individuals
5. Complying with Regulatory Requirements
6. Insuring Against Business Interruption and Other Breach Repercussions
7. Covering Financial Losses Arising Out of an Error or Omission in the Delivery of Professional Services
8. Transferring Exposure for Technology-Related Errors
9. Managing Employment-Related Liability Exposures
10. Supporting Growth and Innovation

1 Protecting Your Customers' Assets and Helping Retain Customer Trust

Companies in the blockchain space may suffer direct financial loss due to the theft, disappearance, or destruction of property that they own or are holding for a third party. Given the prevalence of hacks and thefts of digital assets, crime/fidelity coverage is especially relevant.

Crime insurance provides coverage for direct financial losses due to the theft, disappearance, or destruction of covered property. It can be structured to protect assets in cold, warm, or hot storage. Cold storage-specific insurance provides coverage for loss of digital assets from internal and external theft, damage, or destruction of private keys.

2 Protecting Directors' and Officers' Personal Assets and Attracting Top Talent

We live in a litigious world. And the significant amount of regulatory activity in the blockchain and digital asset space creates a huge pocket of exposure for directors and officers. In particular, they can face exposure arising from claims brought by investors, shareholders, limited partners, and regulators associated with potential securities violations, breach of duties, and regulatory investigations or proceedings. Directors and officers liability (D&O) insurance becomes critical where a company is unable or simply refuses to indemnify its directors and officers.

D&O coverage protects directors and officers in the event they are accused of wrongdoing in the performance of their management duties. D&O insurance is often referred to as the best form of personal asset protection and can thus be used to attract top talent to a company's board and management team.

3 Protecting Your Company's Balance Sheet

Aside from protecting your directors and officers, D&O insurance also provides coverage for a company's own acts. For example, should a company make some type of offering — whether an initial public offering, an initial coin offering, or a security token offering — and is sued for purportedly failing to properly register its currency or making misrepresentations during the offering process, D&O insurance could protect the entity by paying its defense costs and potentially a settlement or judgment. In addition, D&O coverage could protect the company against certain regulatory investigations or proceedings. And it also reimburses the company for the indemnity provided to its directors and officers.

D&O insurance provides balance sheet protection and can protect the company in the event of corporate misconduct allegations.

4 Protecting Key Individuals

Companies in the blockchain space tend to have a select group of individuals who hold the private keys or information that controls access to digital assets. In addition, given the amount of wealth associated with working with digital assets, the kidnapping of such key individuals and potential for ransom demands in exchange for their release are major risks.

Kidnap and ransom (K&R) insurance provides affordable first-party coverage as well as access to threat response and corporate and personal security experts in the event of a ransom, kidnap, or other triggering event.

5 Complying with Regulatory Requirements

As the application of these new technologies continues to grow, governments are encouraging innovation while at the same time looking to protect investors and the broader market. Regulatory scrutiny varies depending on the nature of the business, but certain companies such as broker dealers or trusts, must comply with a range of regulatory requirements, including the purchase of bonds.

Financial institutions, ERISA, and surety bonds are examples of bonds that could be required by regulatory agencies.

6 Insuring Against Business Interruption and Other Breach Repercussions

Because blockchain technology could involve the collection and storage of customers' personal identifying information, companies in this arena are at particular risk of a cyber breach or privacy incident. In the event of such a breach, these companies may incur substantial notification and business interruption costs if they are unable to operate while they investigate and address the incident. The company may also be pursued by a regulatory body in the event of a breach.

Cyber insurance protects a company in the event of a data breach, privacy-related issue, or another cyber event by providing coverage for first-party losses (including business interruption and breach notification costs) and third-party liability and regulatory liability associated with network security, data privacy, and system failure events.

7 Covering Financial Losses Arising Out of an Error or Omission in the Delivery of Professional Services

Protection against errors and omissions (E&O) associated with a blockchain company's delivery of professional services is especially important. An example of potential exposure relates to companies that provide advisory services; if your client sues you because the advice you provided was wrong or insufficient, your E&O insurance could provide coverage for your defense. If your company enters into a contract to provide some form of custody service to a bank, and this is found to be deficient and your company is sued, E&O insurance could apply.

And these are just a few examples of where E&O exposures could exist for companies operating in this space. Additionally, E&O insurance is often required by certain contracts, including those with outside vendors, business partners, and clients, which are instrumental in growing your business. These reasons make E&O coverage an essential protection for companies in the blockchain space.

Professional liability/E&O insurance provides coverage for defense costs, settlements, and judgments for negligent acts or omissions in connection with services provided to clients for a fee.

8 Transferring Exposure for Technology-Related Errors

A company operating in the blockchain or digital asset arena could face significant liability if a client suffers a financial loss because of a technology-related error or omission in a product or service provided by that company. As technology investments accelerate, the number of such claims will also increase.

Technology errors and omissions insurance (tech E&O) transfers the risk of exposure for technology-related issues off a blockchain company's balance sheet.

9 Managing Employment-Related Liability Exposures

The heightened focus on employment practices liability, especially exposures triggered by the #MeToo movement, persists and continues to be a challenge for many companies, including those using blockchain technology and digital assets. These companies, too, must proactively manage and respond to the potential allegations of employment-related sexual harassment, discrimination, and retaliation.

In addition, startup companies — which are among the most frequent users of blockchain technology — may not yet have human resources departments and may not have made large investments in employment-related policies. Newer companies also have smaller balance sheets, increasing the need to transfer their employment-related exposures and liabilities off their books.

The risk of workplace discrimination claims is heightened by the ease with which such claims can be filed with the Equal Employment Opportunity Commission (EEOC). While individual claims may be small, the combined cost of multiple claims can be substantial.

Employment practices liability (EPL) insurance can help manage these exposures by providing coverage for allegations of wrongful employment conduct, such as discrimination, workplace harassment (sexual or otherwise), wrongful termination, and retaliation.

10 Supporting Growth and Innovation

All companies are exposed to various forms of liability based on the services they provide. Insurance supports all industries and helps boost an industry's brand. In addition, banks and outside investors will see a company as a better investment or partner if it has proper insurance coverage, making it easier to obtain the capital needed to innovate and grow. And, if there is a loss, the company will have a safety net to stay afloat and continue to grow.

Insurance helps by transferring risk away from companies and the individuals involved and lets you focus on what's really important — operating and growing your business.

Insurance is vital to the growth and development of any industry and business. Businesses in the blockchain space are no different and insurance is a crucial element to help them on their journey to continued development and growth.

Why Marsh?

Marsh's DART team is a dedicated group of US-based colleagues (including senior advisors, product leaders, claims specialists, and former attorneys) who can provide trusted advice, thought leadership, and innovative solutions to protect blockchain and digital asset companies' critical assets. We have deep experience in all forms of financial and professional insurance coverage and a proven track record of placing such coverage for blockchain and digital asset clients, including cryptocurrency exchanges and trading platforms, merchant banks, financial services advisors, technology incubators, custodians, and more. Our claims advocacy teams can zealously advocate on your behalf and excel at maximizing insurance recoveries for clients while protecting their relationship with insurers. Working with Marsh colleagues around the world — including London, Bermuda, Canada, and Asia — and others within Marsh & McLennan Companies, we can ensure global coordination and consistency and deliver innovative alternative risk transfer solutions. And, as a global leader in insurance brokering, we are focusing on educating insurers about blockchain technologies and industry-specific risks, helping them stay informed about and confident in insuring your critical risks.

For more information, contact your Marsh representative or:

JACKIE QUINTAL
Managing Director & Digital Asset Leader
US Financial Institutions Practice
+1 917 209 8772
jacqueline.quintal@marsh.com

JACK FLUG
DART Team Co-Leader
Marsh FINPRO
+1 212 345 6493
jack.flug@marsh.com