Aon Risk Solutions
Financial Services Group

Client Alert: Risk Management Considerations for Distributed Ledger Technology

Distributed ledger technology is a promising innovation in how information is captured and communicated. Cryptocurrencies, such as bitcoin, rely on their underlying DLT platform to offer a decentralized means to conduct transactions. Initial coin offerings, which use a blockchain platform, have grown exponentially, with over $4.2 billion raised in 2017[1]. Along with this promise and potential, however, come many questions, including insurance and risk management implications.

Blockchain

Blockchain is the technology that forms the backbone of digital currencies including Bitcoin, however, a broader adoption of the technology is anticipated across varying industry sectors with a material impact expected by most executives in 5+ years[2]. Understanding the risks associated with blockchain, and how to address such risks, requires an understanding of how the technology works.

Unlike standard databases, which use a centralized server to host data, blockchain utilizes a de-centralized, distributed digital ledger that is used to record transactions across many computers. New data is added to the distributed ledger with the approval or acceptance of all parties. For example, in the context of a payment or financial transaction, the transaction request is broadcast to the network of nodes which house the data. The network of nodes validates the transaction and, following verification, the transaction is combined with other transactions to create a new block of data to be included on the ledger. The new block is added to the blockchain and the transaction is completed. A record in the blockchain ledger cannot be altered retroactively without the alteration of all subsequent blocks and the collusion of the network, providing significant data integrity benefits to using blockchain.

Broader adoption of blockchain beyond cryptocurrency appears to arise from the benefits of the core decentralized and distributed nature of the technology. For example, payment processors have sought to patent systems offering instantaneous guaranteed payments and eliminating credit card verification delays. The technology can also benefit supply chain management to the extent blockchain can hold the complete details of a component from manufacture to delivery.

The benefits of blockchain do not come without risks of course, including regulatory risks and privacy-based concerns. Addressing such risks through risk transfer requires a blockchain-centric analysis of key cyber insurance policy terms and definitions that may have been drafted well before blockchain technology existed. Among such key considerations is whether a cyber policy's definition of "Computer Systems" includes a decentralized peer-to-peer network. Aon continues to address such considerations with our clients and with the markets to address appropriate insurance solutions for these emerging risks.

We're here to empower results

If you have questions about your specific coverage or want more information, please contact your Aon broker.

www.aon.com

1 *2014-2017 ICO Category Breakdown and Funding. Retrieved from https://next.autonomous.com/insights/2017/8/2/2014-2017-ico-category-breakdown-and-funding. Accessed 9 February 2018.*

2 *2017 Blockchain Technology in the Insurance Sector. Retrieved from Quarterly meeting of the Federal Advisory Committee on Insurance (FACI)*

Empower Results®

Cryptocurrency

Cryptocurrency is a digital or virtual currency that uses cryptography (i.e. mathematical encryption) for security, explained in the prior section. Cryptocurrencies, such as bitcoin, can be broken down into two components: the "token" which represents digital ownership; and the "distributed network" (i.e. blockchain). Bitcoin is the most well-known and valuable, but there are over two thousand cryptocurrencies with varying features, purposes and legitimacy. An important characteristic of a cryptocurrency, such as bitcoin, is that it is decentralized. It is not issued by any central government authority and no single institution controls the network. Payments occur between users without using an intermediary such as a bank. This aspect facilitates cross-border transactions. Another characteristic is "pseudonymity" as users don't need to identify themselves when transacting.

There are no physical bitcoins – they are produced and held electronically by computers around the world using software. Ownership is represented by public and private "keys" which can be held in an owner's "wallet".

While there are certainly many examples of illegal uses for cryptocurrencies, many legitimate uses also exist and they are only growing. Several well-known "traditional" companies accept payment with bitcoin, including Expedia, Microsoft, Overstock, and PricewaterhouseCoopers. Many start-up blockchain-related companies have been raising capital via Initial Coin Offerings (see below). Cryptocurrencies are playing an increasing role in the gaming and eSports industry as a means to place wagers and for "in app" purchases. All of this leads to concerns with how these assets are being stored and protected. Are these currencies stored on-line (warm storage) or off-line (cold storage)? This determines how vulnerable they may be to hackers.

With exposures to cryptocurrencies on the rise, companies have been prudently seeking insurance solutions as a mechanism to transfer a portion of the risk. The fact is, most "off-the-shelf" Crime Insurance (a.k.a. Fidelity Insurance) policies do not cover cryptocurrency exposures as these policies were originally designed to address valuable physical property like cash, securities, and precious metals. Furthermore, certain nuances that are unique to cryptocurrencies are not addressed, such as public and private keys and the distinction of cryptocurrency held in "warm storage" and "cold storage."

There is a common misconception that a cyber insurance policy would respond if assets are stolen as a result of a "hack." While most cyber policies cover both first-party and third-party aspects, such as forensics investigations, notifications, and liability, most cyber policies also exclude coverage for the loss or transfer of funds. As such, cyber policies would generally not protect the face value of cryptocurrency.

In recognition of the growing exposures and limitations of traditional insurance, Aon has been working with insurers to develop innovative risk transfer solutions for companies that transact in and own cryptocurrencies. There have been many reports of large losses resulting from hacks of cryptocurrency owners and insurers are conservative in underwriting these risks. Important risk factors that underwriters will study include: management team experience and expertise; security protocols; financial crime concerns (e.g. Anti-Money Laundering); relationships with legal counsel, accountants and banking partners; regulatory focus; and others.

Initial Coin Offerings – Regulatory Environment

Any company considering an initial coin offering, and those engaged in advising them, would be well-served to note recent comments from SEC Chairman Jay Clayton at the January 28, 2018 Securities Regulation institute. Among a range of comments, Chairman Clayton opened his remarks underscoring his and, by extension, the SEC's expectations of securities "gatekeepers," such as securities accountants, attorneys, dealers, and underwriters, and the potential consequences of running afoul of those expectations[3]:

> My first message is simple and a bit stern. Market professionals, especially gatekeepers, need to act responsibly and hold themselves to high standards. To be blunt, from what I have seen recently, particularly in the initial coin offering ("ICO") space, they can do better.

Chairman Clayton goes on to say:

> ...First, and most disturbing to me, there are ICOs where the lawyers involved appear to be, on the one hand, assisting promoters in structuring offerings of products that have many of the key features of a securities offering, but call it an "ICO," which sounds pretty close to an "IPO." On the other hand, those lawyers claim the products are not securities, and the promoters proceed without compliance with the securities laws, which deprives investors of the substantive and procedural investor protection requirements of our securities laws.
>
> Second are ICOs where the lawyers appear to have taken a step back from the key issues – including whether the "coin" is a security and whether the offering qualifies for an exemption from registration – even in circumstances where registration would likely be warranted. These lawyers appear to provide the "it depends" equivocal advice, rather than counseling their clients that the product they are promoting likely is a security...
>
> With respect to these two scenarios, I have instructed the SEC staff to be on high alert for approaches to ICOs that may be contrary to the spirit of our securities laws and the professional obligations of the U.S. securities bar.

For companies contemplating an ICO, the unique technological risk combined with unproven business models and intense regulatory scrutiny will combine to make the procurement of directors' & officers' liability ("D&O") insurance very difficult. What can companies contemplating ICOs anticipate with regard to D&O insurance?

- Markets: Very few traditional insurers are actively considering companies with ICO exposure. For many companies, non-traditional markets are the most likely option.
- Coverage terms: Coverage is less favorable than seasoned classes of business. Insureds are well-advised to focus on key coverage provisions, including adequate non-indemnifiable coverage and avoiding regulatory exclusions.
- Limits / retention / pricing: Insurers considering ICO submissions are closely managing limits exposed, conservatively sizing retentions, and aggressively pushing rates on line.

Suffice it to say, the potential D&O exposure for clients with any measure of ICO exposure is significant, and the D&O marketplace is taking a commensurately cautious approach to them.

Conclusion

Since the days of Alexander Hamilton, fiat currency has posed risks of speculation, asset bubbles, and fraud. However, the convergence of the digital economy with digital currency has created an environment where the pace of change rivals that of the federal monetary system in the late 1700's, and the exposures for our clients are developing in accordance with that pace. As evidenced above, the age of blockchain, cryptocurrencies, and ICOs is upon us. Aon is working to proactively create solutions to meet our clients' needs, and insureds are encouraged to collaborate with their broker to map their unique, emerging exposures relative to the insurance programs in place. Aon will continue to monitor developments in this sector, collaborate with the insurance market to create solutions and inform our clients accordingly.

About Aon's Financial Services Group

Aon's Financial Services Group (FSG) is the premier team of executive liability brokerage professionals, with extensive experience in representing buyers of complex insurance products including directors' and officers' liability, employment practices liability, fiduciary liability, fidelity, and professional liability insurance. FSG's global platform assists clients in addressing their executive liability exposures across their worldwide operations. Aon's Financial Services Group manages more than $2.2 billion in annual premiums, assists with annual claim settlements in excess of $1 billion, and uses its unmatched data to support the diverse business goals of its clients.

3 *Opening Remarks at the Securities Regulation Institute. Retrieved from https://www.sec.gov/news/speech/speech-clayton-012218. Accessed 9 February 2018.*