Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Is Your Insurance Ready For Blockchain Technology?

Law360, New York (June 3, 2016, 12:01 PM ET) --


Matthew J. Schlesinger


R. Gregory Rubio


Tara A. Brennan

From its obscure beginnings in late 2008, today bitcoin, the most widely used cryptocurrency, has received increasing attention and adoption from mainstream companies, including market-leading online retailers, banks and financial institutions. Likewise, the blockchain or distributed ledger technology on which bitcoin is based appears ready to expand into wider adoption across a broad array of commercial contexts. As just one example, the governor of Delaware recently announced the "Delaware Blockchain Initiative," a coordinated effort to develop and provide a legal and regulatory framework to encourage the development of distributed ledger technologies across a wide spectrum of financial and commercial services, including by bringing the power of blockchain to securities transactions through "digital ledger shares."

As both bitcoin (and other cryptocurrencies) and distributed ledger technology grow and evolve in commercial relevance, there is increased focus on the risks of loss. The 2014 collapse of Mt. Gox — then the world's largest bitcoin exchange — following the theft or disappearance of nearly $500 million in bitcoin, is a conspicuous example of such risk. The insurance industry has responded with new policy language, incorporating both exclusions and specific coverage grants. Financial institutions and other actors wishing to participate in cryptocurrency markets or to take advantage of distributed ledger technologies are well advised to consider carefully how their insurance coverage programs, including crime policies, address any risks associated with cryptocurrencies, distributed ledgers and related new technologies.

The Bitcoin and Blockchain Technology

Bitcoin is an internet-based, open source, public payment system that renders a central authority unnecessary through peer-to-peer technology. Individual transactions are conducted using a few fundamental tools and then are verified, recorded and secured on the public bitcoin blockchain. Specifically, each participant has a "wallet," a digital account that stores and can transfer the user's bitcoin. Each wallet is associated with two digital "keys," a public key that functions as an address for the wallet, and a private key that is known only to the user and functions as a password. Users conduct transactions by recording the public key wallet addresses of both parties to the transaction, the amount of the transaction in bitcoins and the user's own private key as verification of the transaction's authenticity. The information for the transaction is added digitally to a "block" along with "blocks" for other prior transactions in the "chain." Once a block is verified, it

becomes a permanent part of the bitcoin blockchain ledger that provides an authoritative public record of each verified transaction.

The same features that make the blockchain effective in effecting and securing bitcoin transactions make it a highly promising technology for a wide variety of other commercial transactions. Startups and established financial giants alike have taken notice. Most major banks and many other financial institutions are researching and investing in the development of distributed ledgers to automate and streamline everything from recording sales of real property or the details and history of precious stones, to the sale and transfer of commercial securities, or even to the use of so-called "smart contracts" that implement themselves when certain conditions are satisfied.

Chatter About Potential Risks

Although cryptocurrencies and distributed ledger technology aim not only to make transactions more efficient, but safer, this technology remains in its relative infancy. Thus, mistakes and glitches likely are inevitable, and those with less-than-benevolent intent are sure to test the technology. Like all computer-based technologies, cryptocurrencies and distributed ledgers (both the bitcoin blockchain and other distributed ledger systems) necessarily rely on computer systems and software that can be hacked or otherwise compromised. Already, terms like "51 percent attack" and "Sybil attack" and "fork" have entered the lexicon. An evolving and fractured regulatory response from jurisdictions domestic and international, including increased enforcement activity, also present risk, including for the many emerging distributed ledger applications. Accordingly, potential loss or liability stemming from mistakes, fraud and corporate governance all should be considered and mitigated to the extent possible, including through the use of appropriate insurance.

Finding Coverage

Any entity involved in using or developing cryptocurrencies and/or distributed ledger technology should assess the full range of insurance policies available to it including: cyberliability; commercial crime; professional services; directors and officers; and commercial general liability. There are potential pitfalls. Crime policies, for example, often define "money" as currencies that have been "authorized or adopted by a domestic or foreign government as part of its currency" — which may not include bitcoin and other cryptocurrencies. The Insurance Services Office created both a new virtual currency exclusion and an endorsement providing certain coverage for scheduled cryptocurrencies.

Interestingly, the definition of "money" in Bitpay Inc.'s crime policy had been amended to include bitcoin, but Bitpay still found itself in a coverage dispute after suffering a $1.85 million bitcoin loss resulting from a "phishing" attack. See Bitpay Inc. vs. Massachusetts Bay Insurance Co., Case No. 1:15-cv-3238 (N.D. Ga. 2015). Bitpay's CFO was the target, and the hacker used the information obtained to induce Bitpay to transfer bitcoins to a "customer" wallet the hacker controlled. Bitpay sought coverage for the loss under its crime and fidelity policy, but Massachusetts Bay Insurance Co. (MBIC) denied the claim, asserting that (1) the loss was "indirect" because the executive willingly provided the information the hacker sought; and (2) the stolen bitcoins were not taken from within BitPay's physical location as, MBIC asserted, was required for coverage. Based on recent public court filings, it appears a settlement of this matter has been reached.

Errors and omissions policies, which provide coverage for loss arising from the policyholder's negligence or mistakes in the rendering of professional services, also are likely to be implicated. Fintech and other companies involved in developing cryptocurrency, distributed ledger technology or providing related

services should look carefully at their E&O policies to ensure, for example, that any definition of professional services is broad enough to cover such activities. Similarly, as the risk of governmental investigations or actions increases and potential liability creeps into the board room, companies should review their D&O policies for any potential gaps that could affect coverage for cryptocurrency or distributed ledger related matters. As just one example, companies should understand whether their D&O policies contain any professional services exclusion and seek to narrow or remove it if possible. Finally, some insurers have developed limited cryptocurrency specific coverage, which should be carefully evaluated.

With the continued growth and commercial acceptance of cryptocurrency and the rapid emergence of distributed ledger technologies across the commercial spectrum, it is clear that these technologies will be a part of the digital economy going forward. As with any other new technology, the risks associated with cryptocurrencies and blockchain technologies are sure to come into sharper focus as these industries continue to expand. For companies engaged in these industries, however, the need to stay ahead of this risk and to develop adequate tools, including insurance policies, to deal with the risks is real. A creative and careful evaluation of the policyholder's existing program and their options for additional coverage will ensure that such tools are in place.

—By Matthew J. Schlesinger, R. Gregory Rubio and Tara A. Brennan, Covington & Burling LLP

Matthew Schlesinger is a partner and Greg Rubio and Tara Brennan are associates in Covington & Burling's Washington, D.C., office.