UNCHAINED AND DECRYPTED: COVERAGE ISSUES CONCERNING BLOCKCHAIN AND CRYPTOCURRENCIES EXPLAINED

Michael S. Levine, Daniel Hentschel, Hunton Andrews Kurth
Rikke Dierssen-Morice, Faegre Baker Daniels
and Thomas Srail, Willis Towers Watson

October 2019

Natural catastrophes shift in the political spectrum, and data breaches on the world's largest social media platforms stole headlines in 2018. Yet another subject also made headlines in 2018 but rarely was it seen "above the fold": Blockchain technology and cryptocurrency. Whether on the internet, in a newspaper or magazine article, or in daily conversation, the new technology undoubtedly appeared in the media with increasing frequency. From major corporations, including the top online retailers, to financial institutions, the implementation of blockchain technology and immersion of cryptocurrencies has arrived.[1]

The same features that make blockchain technology effective in securing cryptocurrency and other sensitive transactions has allowed corporations to transact business in ways centralized banking and data management systems will not allow. Cryptocurrencies also offer a low cost, and

[1]Toshendra Sharma, *Top 10 Companies That Have Already Adopted Blockchain*, (July 2018), https://www.blockchain-council.org/blockchain/top-10-companies-that-have-already-adopted-blockchain/

This paper was first presented and published by ABA Litigation Section, Insurance Coverage Litigation Committee meeting *How Could That (Not) Be Covered? Truthiness and Coverage for False Claims Act Liability* (Tucson, Arizona—March 1, 2019)

fast means of transferring value and information around the globe anonymously. These technologies present an attractive alternative to the established banking, money and data transfer systems. Unfortunately, with all of the benefits that the revolutionizing technology offers, come numerous risks. Insurance companies are actively pursuing ways to insure these risks and the companies that are utilizing blockchain technology and cryptocurrency. However, as discussed in this paper, when it comes to blockchain and cryptocurrency, the industry's insurance policy arsenal is still in its infancy, placing much of the current claim load onto legacy policies that may be ill-equipped to squarely handle blockchain and cryptocurrency-related losses.

Insurance Law Essentials Deep Dives is published in association with *Insurance Law Essentials.* For subscription questions or problems, contact IRMI customer service at (800) 827–4242.

Published by IRMI:
International Risk Management Institute, Inc.
Jack P. Gibson, Publisher
Bonnie Rogers, IRMI Editor
12222 Merit Drive, Suite 1600
Dallas, TX 75251 • (972) 960–7693
www.IRMI.com

The Risks

Blockchain technology and cryptocurrencies focus on changing commercial transactions by purportedly making the transactions safer and more efficient. Due to its decentralized feature, blockchain technology is said to be less susceptible to hacking than the traditional centralized database. However, no technology is perfect. Blockchain and the cryptocurrencies that utilize that platform are computer based technological platforms, meaning they rely on innovative and varied software platforms and hardware, which exposes the technology to data loss and corruption, hardware disruption and cyber breach, among other things.

Several companies already have fallen victim to fraudulent schemes and cyber hacks causing monumental losses. For instance, Bitfinex, the second largest cryptocurrency exchange, suffered a platform breach just last year that resulted in the loss of $72 million in users' cryptocurrency.[2] On January 26, 2018, Coincheck, a cryptocurrency exchange based in Tokyo, suffered a $534 million loss after 500 million cryptocurrency coins disappeared, making it one of the largest hacks in history.[3] In fact, CipherTrace, a blockchain security firm, reported that almost $1 billion worth

[2] *See* Clare Baldwin, *Bitcoin worth 72 million stolen from Bitifinex exchange in Hong Kong*, (Aug. 2016), https://www.reuters.com/article/us-bitfinex-hacked-hongkong/bitcoin-worth-72-million-stolen-from-bitfinex-exchange-in-hong-kong-idUSKCN10E0KP.

[3] *See* BBC, *Coincheck: World's biggest ever digital currency 'theft'*, (Jan. 2018), https://www.bbc.com/news/world-asia-42845505.

of cryptocurrencies were stolen from cryptocurrency-exchanges during the first nine months of 2018 alone.[4] Recognizing the substantial need for insurance protection, insurance companies have begun to leap to insure businesses utilizing blockchain and cryptocurrencies, but many have done so with plainly inadequate coverage.[5]

In addition to testing the limits of legacy insurance products and forcing the insurance industry to develop new products, the increasing use of blockchain and cryptocurrencies has forced securities and insurance regulators to take notice of the emerging technology. How and by whom will the offering and trading of cryptocurrencies be regulated continues to be undetermined in the United States and beyond. China and South Korea have taken the "zero tolerance" approach and have banned Initial Coin Offerings ("ICO").[6] Whether their approach will be successful remains to be seen. In contrast, the United States District Court for the Eastern District of New York recently held that ICOs may be subjected to the same rules and regulations as equity market offerings.[7] The holding contradicts several findings among various jurisdictions and contributes to the uncertainty regarding insuring corporations utilizing the technology. Despite the inconsistency among regulators, however, the massive boom surrounding this technology is forcing insurance companies to meet their policyholders' needs or risk losing market share.

Seeking Coverage

Identifying the coverage issues likely to arise with claims involving blockchain and the use of cryptocurrency is paramount to understanding whether a company is properly insured for those risks. Companies utilizing blockchain technology and/or cryptocurrency should assess the extent of coverage provided by their current insurance policies as the risks associated with these new technologies, if left uninsured, can lead to dire consequence. Indeed, as the technologies become more ubiquitous, it would behoove all commercial policyholders to assess and continually reassess both the extent of their exposure via blockchain and crypto-assets and the extent to which their insurance might respond to a loss involving those technologies.

[4] *See* Gertrude Chavez-Dryfuss, *Cryptocurrency theft hits nearly $1 billion in first nine months*, report (Oct. 2018), https://www.reuters.com/article/us-crypto-currency-crime/cryptocurrency-theft-hits-nearly-1-billion-in-first-nine-months-report-idUSKCN1MK1J2.

[5] *See* Delton Rhodes, *Bitcoin Insurance Policies – What They Are and Do You Need Them*, https://coincentral.com/bitcoin-insurance-policies/ (noting that "Bithumb was insured by Hyundai Marine & Fire Insurance and Heungkuk Fire & Marine Insurance Co. before a hack that took place in June 2018. Even though the hack resulted in the loss of around $31 million in funds, the insurance coverage only provided $5.39 million in coverage").

[6] *See, e.g.*, https://techcrunch.com/2017/09/28/south-korea-has-banned-icos/; https://www.reuters.com/article/us-china-finance-digital-ico-analysis/crypto-currency-chaos-as-china-cracks-down-on-icos-idUSKCN1BN33R; https://www.cnbc.com/2019/01/07/bitcoin-security-token-and-sto-explained.html.

[7] *See United States v. Zaslavskiy*, No. 17-CR-647 (E.D.N.Y. 2018).

This article discusses some of the risks, gaps, and challenges that may arise when facing claims arising from the implementation of blockchain and cryptocurrency. To address these issues in context, we have constructed a hypothetical fact pattern against which the emerging issues will be discussed.

Hypothetical

Imagine you are a multi-office health provider that recently transitioned its medical file management system to a decentralized storage system utilizing blockchain technology. This new system stores patient records across all office locations. The storage system is operated by a third party cloud provider that allows you to access records and information from computers at your place of business and elsewhere. The system also allows for the sharing of health records with other entities with access to the blockchain, thereby enhancing communication between patients and their providers and reducing waiting times.

In addition, your practice accepts the most common form of cryptocurrency, Bitcoin, as a method of payment for services and prescriptions. Moreover, you have begun accepting payment from your patients and their insurers, and paying your medical suppliers in Bitcoin in order to ensure the payments get processed instantaneously. Your virtual coins are stored in a standard crypto-wallet.

Several months into your journey, you learn that the blockchain ledger storing your patients' information has been hacked. Based on the information provided by authorities, some of the patients' personal identifying information and medical record information have been stolen and are now being sold on the dark web. To make matters worse, the hackers successfully diverted 100 bitcoins, valued at $10,000 each, from your cyrpto-wallet into a third party offshore bank account. The hijacked funds were intended for a medical supplier in fulfillment of a one million dollar order of medical supplies. Consequently, your practice has lost a million dollars' worth of Bitcoin and still owes the medical supplier for the supplies that you received previously and have been using for several months.

You sit on the board of directors as the Chief Operating Officer along with four colleagues. As demands from attorneys begin to trickle in, both on behalf of the patients and your supplier, you direct your general counsel and risk manager to notify your insurers and obtain coverage. You fully expect that one of your four very costly insurance policies will provide coverage for the incidents.

Commercial Property Insurance

How cryptocurrencies are viewed by courts can be determinative when seeking coverage for a cryptocurrency-related loss. As illustrated above, the loss and theft of virtual currencies has plagued the cryptocurrency market all over the world. Thus, businesses engaged in the use, holding and/or trading of cryptocurrencies must have adequate insurance coverage. Many busi-

nesses affected by losses involving cryptocurrency have turned, in the first instance, to their commercial property insurance policies. Whether cryptocurrency losses are covered under these legacy policies raises a host of issues, only some of which have been touched on by the courts. These issues include, among many others:

- Whether cryptocurrency constitutes "Covered Property";
- Whether the loss of cryptocurrency constitutes "Direct Physical Loss";
- Whether cryptocurrency constitutes "Money" or "Securities"; and
- How (and when) to value cryptocurrency.

Commercial property insurance policies typically provide coverage for "direct physical loss of or damage to Covered Property at the premises described in the Declarations caused by or resulting from any Covered Cause of Loss."[8] "Covered Property" under a traditional commercial property insurance policy is addressed in three subparts: (1) Building; (2) Business Personal property; and (3) Personal Property of others.

Covered property falling under the subpart for Building usually includes: Foundations of buildings, structures, machinery, completed additions to the building or structure, machinery and equipment and outdoor property. Id. Thus, on its face it appears improbable that the Bitcoin stolen in the hypothetical would constitute covered property as virtual coins are not the type of property to be considered a "building." In addition, since the Bitcoin in the hypothetical belonged to the policyholder, not a customer or employee, it would not be considered "personal property of others."

As it relates to finding coverage under the subpart for "Business Personal Property," it may appear that a business involved in the exchange of cryptocurrencies, like the medical provider in the hypothetical, should be entitled to coverage for losses relating to virtual currencies. A business owner like the one in the hypothetical may surmise that the stolen Bitcoin had been stored in the businesses' crypto-wallet, which is property that is owned and used by the business.

But fitting the stolen cryptocurrency into one form of "property" is not the end of the inquiry. To trigger coverage, the covered property must suffer a "direct physical loss" or "damage." Courts have held that an insured did not sustain a "direct physical loss" to its property under its business property insurance policy for losses resulting from fraudulent securities schemes.[9] In those circumstances, the policyholder sustained economic losses arising

[8] ABA Insurance Services, Specimen Policies and Endorsements, Property form ECP 00 560 08 16, http://abais.com/Data/Sites/1/media/specimen/pnc/property.pdf.

[9] *Schmidt v. Travelers Indem. Co. of America*, 101 F.Supp.3d 768 (S.D. Ohio 2015); *Florists' Mut. Ins. Co. v. Ludy Greenhouse Mfg. Corp.*, 521 F.Supp.2d 661, 680 (S.D. Ohio 2007); *see also Tschimperle v. Aetna Cas. & Sur. Co.*, 529 N.W.2d 421, 425 (Minn. 1995) ("loss of [an] investment does not constitute damage to tangible property").

out of the use of fraudulent checks. Id. The courts in those cases reasoned that the funds in question did not have a physical existence and, thus, were not susceptible to physical loss or damage, unlike situations where a check might be destroyed by a fire.[10] Similarly, it is arguable that cryptocurrency is not a tangible item. Indeed, one of the main advantages provided by this technology is that the currency is virtual in nature. Insurers may rely on absence of any "direct physical loss" as a means to avoid coverage under a commercial property policy.

Even if a business owner, like the medical provider from our hypothetical, were able to trigger coverage under its commercial property insurance, there still are coverage limitations that must be overcome. For instance, traditional commercial property insurance policies typically contain the following coverage limitation:

> **Property Not Covered**
>
> Covered Property does not include:
>
> > Accounts, bills, currency, food stamps or other evidences of debt, "money", notes or "securities", except as provided under the Coverage Extensions or Flex Additional Coverage for Accounts Receivable. Lottery tickets held for sale are not securities;

Id.

This provision is ripe with issues that arise in the context of a cryptocurrency loss. "Money," for example, is typically defined in a commercial property policy as "currency, coins and bank notes in current use and having a face value and Travelers checks, register checks and money orders held for sale to the public." Id. The term "Securities" traditionally means negotiable and non-negotiable instruments or contracts representing either "money" or property but not "money." Id. Thus, in the context of our hypothetical, it becomes necessary to determine as a threshold matter whether cryptocurrency is "money" or "securities" within the context of a business's commercial property insurance policy? As is usually the case in law, however, the answers to these questions are not clear.

Currently, there is little continuity among jurisdictions and regulators when it comes to characterizing cryptocurrency. Whether or not cryptocurrency is "money", "securities" or "property" has been subjected to heavy debate. While some courts have found cryptocurrency to be money, others disagree and have held that cryptocurrencies shall be treated like securities.[11] To add to the confusion, the Commodity Futures Trading Commission has determined that virtual currencies are, in fact, "commodities," and thereby sub-

[10] *Schmidt*, 101 F.Supp.3d 768 at 781 ("This is *not* an instance in which, for example, cashier's checks were destroyed and lost in a fire.").

[11] *Compare U.S. v. Murgio*, 209 F.Supp.3d 698, 707–10 (S.D.N.Y., 2016) (finding that bitcoins are "funds" not "money") under 18 U.S.C. § 1960 *with U.S. v. Ulbricht*, No. 14-CR-68 KBF, 2014 WL 3362059 (S.D.N.Y. 2014) (concluding that Bitcoin is money within the context of the federal anti-money laundering statute).

ject to regulation by the Commodity Futures Trading Commission.[12]

One court has weighed in on the debate, however, and provided guidance (or some may argue confusion) in the context of insurance coverage. An Ohio Court in *Kimmelman v. Wayne Ins. Group*, 18-CV-1041 (Court of Common Pleas, Franklin County, Ohio Sept. 25, 2018), ruled that stolen Bitcoin qualified as "property" and not "money" under an insured's homeowners' policy.[13] The Court relied upon the IRS's acting policy in relation to virtual currencies when making its determination. Specifically, the Court decided that because virtual currencies are recognized as property for "federal tax purposes, virtual currency is treated as property."[14] The issue before the court in *Kimmelman* was whether a specific sublimit limiting the recovery of lost "money" applied to the theft of Bitcoin. Though *Kimmelman* was decided outside the context of a commercial property policy, the Court's characterization of the virtual currency at issue and its reliance on outside sources can be applied to similar contexts and provides guidance to policyholders facing similar claims.

Assuming, however, that our hypothetical cryptocurrency loss is covered, hypothetical, how should that loss be valued, and when? As Bitcoin became increasingly popular, the price of the coin surged to up to $20,000 in December of 2017, but closed 2018 with a value of only $3,747.[15] These values demonstrate the extreme volatility of cryptocurrencies. A review of the valuation methods contained in standard commercial property policies suggest that those policies do not contemplate the types of rapid and substantial changes in value seen with cryptocurrencies.

Commercial property policies typically have valuation provisions that set forth the manner by which the value of a loss is to be calculated using either the lost or damaged property's "Replacement Cost Value" as of the time of loss or damage or the property's depreciated "Actual Cash Value."[16] Replacement cost "is measured by what it would cost to replace the damaged property" whereas actual cash value is generally defined as "fair market value" or

[12] *See Commodity Futures Trading Commission v. McDonnell*, 287 F. Supp.3d 213 (E.D.N.Y. 2018) (stating that "Virtual currencies are 'commodities' subject to regulation by the Commodity Futures Trading Commission").

[13] *Kimmelman v. Wayne Ins. Group*, 18-CV-1041 (Court of Common Pleas, Franklin County, Ohio Sept. 25, 2018).

[14] *Kimmelman*, 18-CV-1041 ("Accordingly, the only authority the Court can rely on in determining the status of Bitcoin is the Internal Revenue Service Notice 2014-21. Under Notice 2014-21, the IRS states, 'For federal tax purposes, virtual currency is treated as property.' Accordingly, the Court finds Bitcoin, although termed 'virtual currency,' is recognized as property by the IRS and shall be recognized as such by this Court.").

[15] Sam Ouimet, *Down More than 70% in 2018, Bitcoin closes Its Worst Year on Record*, (January 2019) https://www.coindesk.com/down-more-than-70-in-2018-bitcoin-closes-its-worst-year-on-record.

[16] ABA Insurance Services, Specimen Policies and Endorsements, Property form ECP 00 560 08 16, http://abais.com/Data/Sites/1/media/specimen/pnc/property.pdf.

"[r]eplacement cost minus normal depreciation," where depreciation is defined as a "decline in an asset's value because of use, wear, obsolescence, or age." Applying these valuation methods to a cryptocurrency loss can prove to be unworkable.

For example, in our hypothetical, the stolen Bitcoin was valued at $10,000 per coin at the time that it was stolen for a total value of $1,000,000.; however, what if the Bitcoin was worth $3,000,000 on the date the loss was actually discovered? Does the insurer owe you the $1,000,000 based on the value at the time of theft, or $300,000,000 based on the value of the asset when the theft was discovered? Or, adding a third wrinkle; what if the value of the asset had decreased following the date of discovery to $1.5 million as of the date of loss adjustment?

The difficulties here turn on the fact that traditional commercial property policies may not contain a valuation mechanism designed to address rapidly fluctuating values.[17] The lack of clear guidance lends itself to arguments favoring either side. For instance, utilizing a replacement cost valuation, a policyholder might reasonably argue that he/she should be entitled to at least $1,000,000, since that was the value of the property at the time of the loss. Using an actual cash value method, on the other hand, a policyholder might reasonably argue that it should receive more than $1,000,000, since the actual value of the asset had increased following the fire. Conversely, if the asset had lost value during that period, the insurer would undoubtedly argue in favor of a lower valuation. Ultimately, however, the proper manner for valuing a crypto asset, like any other insured property, will come down to the policy's explicit valuation terms.

Cyber Liability Insurance

Companies utilizing blockchain technology and cryptocurrency are subject to hacking and data breaches that have the potential to impact their ability to access blockchain information or crypto assets. Even worse, these exposures have the potential to result in permanent loss of assets and confidential information. Numerous jurisdictions have recognized that a duty of care exists when it comes to protecting a customer's confidential information.[18] In

[17] *Trinidad v. Florida Peninsula Ins. Co.*, 121 So.3d 433 (Fla. 2013).

[18] *In re Sony Gaming Networks and Customer Data Breach Security Litig.*, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) (holding "the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity … [is] well supported by both common sense and [applicable state] law"); *In re: The Home Depot, Inc., Customer Data Security Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *3 (N.D. Ga. May 18, 2016) ("A retailer's actions and inactions, such as disabling security features and ignoring warning signs of a data breach, are sufficient to show that the retailer caused foreseeable harm to a plaintiff and therefore owed a duty in tort."); *In re Target Corp. Customer Data Security Breach Litig.*, 64 F. Supp. 3d 1304, 1308 (D. Minn. 2014) ("[G]eneral negligence law imposes a general duty of reasonable care when the defendant's own conduct creates a foreseeable risk of injury to a foreseeable plaintiff."); *Resnick v. AvMed, Inc.*, 693 F.3d 1317, at 1326-28 (11th Cir. 2012) (finding health care provider had a duty to secure customers' information).

addition, courts have held that cyber policies may provide coverage in situations where confidential information is disclosed to third parties.[19] Unsurprisingly, therefore, policyholders will look to their cyber liability insurance policies when faced with claims resulting from hacks and cyber breaches.

Many of the cyber liability insurance policies available in today's insurance market are confined and their coverages are varied. These differing policies give rise to a host of issues in the context of blockchain and cryptocurrency losses just as they do in the context of other cyber and privacy breaches and incidents. Common among these issues are the following:

- Does the release of blockchain data trigger coverage under a cyber policy?

- Who has "custody or control" of information stored on a blockchain?

Cyber liability insurance is intended to address first-party losses and third-party liability as a result of data security incidents, the disclosure of or failure to protect private information, and privacy law violations. In the hypothetical presented above, the hackers penetrated the blockchain that stored the insured's patients' confidential information and sold that information to third parties. In that situation, the medical provider may look to its cyber liability policy in an effort to obtain coverage for claims asserted against it by the patients as well as the breach response costs that the practice incurs as it complies with the various and rigorous breach notification laws and regulations that may be triggered by such an incident.

Cyber policies typically provide coverage for data breach liability. An insuring agreement might contain language stating that "[t]he Insurer will indemnify the Insured for Loss resulting from Claims for Wrongful Privacy and Security Acts made against the Insured if such Claims are first made during the Policy Period or the Discovery Period."[20] The policy might define "Wrongful Privacy and Security Acts" as:

> Any actual or alleged error, omission, misstatement, act of negligence, or breach of duty committed by the Insured or a Service Provider in connection with a Privacy and Security Act that results in the unauthorized access to Confidential Information in the custody or control of the Insured, an Electronic Data Processor, or a Service Provider.

Id.

[19] *Smith v. Triad of Alabama*, LLC, No. 1:14-CV-324-WKW, 2015 WL 5793318, at *9 (M.D. Ala. Sept. 29, 2015) (finding that plaintiffs in a data breach case established injury in fact where they alleged identity theft and fraudulent tax returns were filed in their names); *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *26 (N.D. Cal. May 27, 2016) (finding that plaintiffs' allegations of using their own time to monitor their credit in the aftermath of a data breach was injury in fact sufficient to confer standing).

[20] ABA Insurance Services, Specimen Policies and Endorsements, Cyber Cover form EEO 40 997 (02 15).

As discussed above, a distinct feature of blockchain technology is its decentralized aspect, which functions via peer-to-peer transactions. As such, a user's "Confidential Information," such as the medical provider's patients' records, is not held by a single Service Provider at a single location. Rather blockchain technology keeps data in an encrypted ledger, which is distributed across synchronized, replicated databases.[21] Access to or breach of data stored on a blockchain likely involves accessing information owned or maintained not only by the insured, but by many other entities as well. This raises several unique questions with respect to insuring an unauthorized dissemination of that information. For instance, does each user of the blockchain have "custody and control" of the confidential data that resides on that chain such that the disclosure of data on a blockchain triggers coverage under cyber liability insurance held by each user of the blockchain? Or, does it trigger coverage under only the policy held by the entity to whom the confidential information was initially entrusted?

Ultimately, the answer may turn on determining which entity or entities actually had "custody or control" of the sensitive information within the blockchain. Though there is no case law interpreting the language as it relates to blockchain technology, an insurer might argue that use of blockchain technology essentially inhibits a corporation's ability to retain exclusive "custody or control" of the sensitive information, although such an argument would effectively render the coverage illusory. Conversely, policyholders may be able to argue that liability should be shared—and coverage thereby is triggered—among each user of the blockchain, since each user had equal "custody and control" of the confidential information.

Commercial Crime Insurance

Theft and the fraudulent transfer of virtual currencies by third-party actors is a concern for businesses engaged in the use of cryptocurrency. Companies facing cryptocurrency losses may seek coverage under their commercial crime policies. As with other lines of coverage, claims for blockchain and cryptocurrency-related losses raise a number of coverage issues under commercial crime insurance policies, including:

- Does the theft of cryptocurrency trigger coverage?
- Is cryptocurrency "Other Property" as defined in a commercial crime policy?
- Is cryptocurrency held within an "Insured's Premises"?

[21] HIPPA Journal, *The Benefit of Using Blockchain for Medical Records*, (September 2017), https://www.hipaajournal.com/blockchain-medical-records/ ("Rather than store data in a single location, blockchain keeps data in an encrypted ledger, which is distributed across synchronized, replicated databases. Each block is linked to the previous block by a unique public key with access to data carefully controlled.").

Insuring agreements within commercial crime policies typically provide coverage for a loss that an insured sustains resulting directly from an "occurrence" taking place at any time which is "discovered" by an insured during the policy period.[22] An "occurrence" is usually defined as "(1) An individual act; (2) The combined total of all separate acts whether or not related; or (3) A series of acts whether or not related; committed by a person acting alone or in collusion with other persons, involving one or more instruments, during the Policy Period." Id. Commercial crime policies typically include multiple insuring agreements, which are intended to cover losses similar to the one illustrated in the hypothetical above.

For instance, a majority of commercial crime policies provide coverage for "Computer Fraud," and "Inside the Premises—Theft of Money and Securities." However, coverage under either insuring agreement is limited to certain circumstances.

The "Computer Fraud" insuring agreement typically provides coverage for:

> [L]oss of or damage to "money," "securities" and "other property" resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the "premises" or "banking premises:" (a) To a person (other than a "messenger") outside those "premises;" or (b) To a place outside those "premises."

Id.

The "Inside the Premises—Theft of Money and Securities" insuring agreement provides coverage for:

> [L]oss of "money" and "securities" inside the "premises" or "banking premises": (1) Resulting directly from "theft" committed by a person present inside such "premises" or "banking premises"; or (2) Resulting directly from disappearance or destruction.

In the hypothetical illustrated above, hackers diverted Bitcoins from the policyholder's crypto-wallet into an offshore account. Because cryptocurrency is virtual, the hacker inevitably used a computer in performing his/her actions. The policyholder may therefore reasonably believe that both insuring agreements have been triggered for the criminal loss. Here too, however, the terms of coverage may not squarely fit the facts of a crypto-loss.

Both insuring agreements provide coverage for the loss of or damage to "money," and "securities." In fact, unlike the traditional commercial property policy discussed above, the Computer Fraud insuring agreement specifically provides expansive language, which encompasses not only

[22]Brown Stone Agency, Specimen Policies, Commercial Crime Coverage Form (CR 00 20 05 06).

"money" and "securities," but also "other property." As explained above, there appears to be a lack of consistency among jurisdictions when it comes to characterizing cryptocurrency as "money" or "securities."

Regardless whether cryptocurrency constitutes "money" or "securities," coverage may still be available if the crypto-asset meets the policy meaning of "other property." Commercial crime policies typically define the term "other property" as "any tangible property other than 'money' and 'securities' that has intrinsic value but does not include any property excluded under this insurance."[23] This definition would appear to be helpful to an insured in a jurisdiction that finds cryptocurrencies do not meet the definitions of "money" or "securities." However, at least one federal appeals court, applying California law, has found the term "tangible property," in the insurance context, to mean "things that can be touched, seen, and smelled."[24] It may therefore be difficult for a policyholder to argue, at least under California law, that cryptocurrency is "tangible property" since it cannot be touched, seen or smelled and exists solely in virtual form. In such a case, the policyholder must attempt to fit its cryptocurrency into the definitions of either "securities" or "money."[25] Courts that have addressed this issue have reached inconsistent outcomes.[26]

Another issue that may arise under commercial crime policies is whether the theft occurred on or off the premises. Each of the insuring agreements above contains language requiring that the transfer occur from "inside the premises." Given the "virtual" nature of cryptocurrency, however, it is difficult to say that the asset resides inside of a premise. At least one insurance company has argued against coverage for the loss of Bitcoin under a commercial crime policy on the basis that the virtual coins weren't physically in the policyholder's offices.[27] In that instance, the carrier relied on the definition of the term "premises," which was defined as "the interior of that portion of any building you occupy in conducting your business." Id. Specifically, the insurer took the position that because the stolen Bitcoins were stored on digital wallets online and transferred on a blockchain, and were not on the physical premises of the insured, the Bitcoin transactions did not involve a transfer of property from inside the insured's premises to outside the premises. The policyholder

[23] *Supra*, xvi.

[24] *very Dennison Corp. v. Allendale Mut. Ins. Co.*, 310 F.3d 1114 (9th Cir. 2002) (quoting, *Kazi v. State Farm Fire & Cas. Co.*, 24 Cal.4th 871, 880, 103 Cal.Rptr.2d 1, 15 P.3d 223 (2001).

[25] *See, e.g., Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89, 96 (4th Cir. 2003) ("The insurance policy in this case covers liability for 'physical damage to tangible property,' not damage to data and software, i.e., the abstract ideas, logic, instructions, and information.").

[26] *Supra*, xvii.

[27] *See BitPay Inc. v. Massachusetts Bay Insurance Co.*, 1:15-cv-03238, (N.D. Ga. 2015).

responded by claiming that the coverage was illusory, considering the policy contained a specific endorsement adding Bitcoin to the definition of "money," illustrating that there are arguments to be made in favor of coverage. Id. The matter settled before a determination could be rendered.

The location of stolen or otherwise misappropriated cryptocurrency will continue to be an issue in the application of policy wording such as the examples above. However, policyholders utilizing cryptocurrencies can help avoid that issue by endorsing their policies to expressly address the loss or theft of cryptocurrencies.

Directors & Officers Liability Insurance

Directors and Officers Liability insurance policies provide coverage for claims against directors, officers and other insured persons for wrongful acts committed in their official capacity at or on behalf of the insured company. The risk of being hacked and lack of regulation as it relates to the holding and trading of cryptocurrencies can expose directors and officers to liability, including liabilities under federal, state or foreign securities laws. This potential exposure raises a number coverage issues as it relates to blockchain technology and cryptocurrency. For instance,

- Do traditional D&O exclusions clearly apply to blockchain technology?
- Are ICOs within the scope of coverage under D&O policies?

Standard D&O policies provide coverage for "[l]oss resulting from Claims first made during the Policy Period or the Discovery Period against the Insured Persons for Wrongful Acts for which the Insured Persons are legally obligated to pay[.]"[28]

A Wrongful Act is usually defined as:

> Any actual or alleged error, omission, misstatement, misleading statement, neglect or breach of duty by:
>
> (1) any Insured Person in the discharge of their duties while acting solely in the capacity as such;
>
> (2) any Insured Person while acting solely in the capacity as director, officer, or member of the board of trustees of a not-for-profit entity pursuant to Section II (B); or
>
> (3) the Company or any person or entity for which the Company is legally responsible, but only to the extent that coverage is granted to the Company by Insuring Agreement made a part of this Policy.

[28] ABA Insurance Services, Specimen Policies and Endorsements, Directors & Officers Liability Policy Specimen form (07 09).

Though D&O polices regularly provide coverage regarding a wide range of claims, the policies contain certain exclusions that may impact claims involving blockchain and cryptocurrency-related losses. For instance, a majority of D&O liability policies contain exclusions for privacy risks.[29] These exclusions can be implicated by claims against entities engaged in the use of blockchain and cryptocurrencies where such claims involve the alleged disclosure of confidential information, as occurred in the hypothetical above.

Another issue that is likely to impact claims under D&O policies for loss involving blockchain and cryptocurrency concerns the "securities offering" or the "Brokerage/Advisory Services" exclusion that is often found in D&O policies.[30] These exclusions operate to limit coverage for claims involving certain types of securities transactions and brokerage services. Initial Coin Offerings ("ICOs") and public offerings involving virtual currencies have increased in frequency and scope and that trend can be expected to continue as the technologies continue to proliferate. Whether ICOs and public virtual coin offerings are considered "securities" subject to the same rules and regulations as equity market offerings may impact the applicability of the securities and brokerage exclusions. In fact, a judge in the Eastern District of New York recently held that ICOs may be covered by securities laws in the context of a criminal proceeding. The holding will likely embolden insurers to deny coverage; however, as discussed above, a policyholder may point to recent case law stating that cryptocurrencies are not "securities" or "money."

Change Is Happening

Blockchain technology and cryptocurrencies are in their infancy and the rules and regulations governing those technologies are only beginning to take shape. Even further behind the curve is the insurance industry, which continues to struggle to effectively insure businesses involved in these sectors. Nevertheless, major insurers like Great American Insurance Group, Lloyd's, XL Catlin, Chubb, and Mitsui Sumitomo Insurance have recently introduced insurance products touted as being geared specifically for cryptocurrency and blockchain related technology.[31]

The Insurance Services Office ("ISO") also is now offering ISO forms specifically tailored to cryptocurrency risks.[32] For instance, language found in some of the ISO

[29] *See, e.g., L.A. Lakers, Inc. v. Fed. Ins. Co.*, No. CV 14-7743 DMG (SHx), 2015 WL 2088865, at *5-9 (C.D. Cal. Apr. 17, 2015); *LAC Basketball Club Inc. v. Fed. Ins. Co.*, No. CV 14-00113 GAF (FFMx), 2014 WL 1623704 at *4-5 (C.D. Cal. Feb. 14, 2014).

[30] *Supra*, xxxiv.

[31] Dennis Mangoli, *Cryptocurrency Insurance: More Companies Join The Bandwagon,* (Feb. 2018), https://www.ccn.com/cryptocurrency-insurance-more-companies-join-the-bandwagon/

[32] *See* ISO Form CR 25 46 11 15; ISO Form CR 25 45 11 15; IS Form FI 20 74 10; 16, IS Form CR 00 20 11 15; ISO Form CR 00 25 11 15; IS Form CR 00 11 15; ISO Form CY 00 01 01 18; ISO Form CY 00 11 01 18.

forms explicitly expands the definition of "money" to include "virtual currencies." Other forms contain a broad exclusion for "Loss involving virtual currency of any kind, by whatever name known, whether actual or fictitious, including, but not limited to, digital currency, crypto currency, or any other type of electronic currency." The ISO forms are currently limited to commercial crime, cyber liability, and financial institution coverage, thus, gaps among the coverages offered under these new forms and legacy coverages such as those under commercial property policies, will continue to exist. Though the new ISO forms are far from perfect and currently do not specifically address coverage for blockchain technology, these forms indicate an incremental movement to address the potential pitfalls and coverage issues that arise from the use of these new technologies.

Conclusion

With the unceasing development of technological advances, it has become increasingly clear that blockchain technology and cryptocurrencies will soon revolutionize commercial transactions around the world. As has been the case in the past and will continue to be in the future, with new technology will come new risks. As evidenced above, the current state of insurance policies fail to effectively protect corporations that have ventured into the world of blockchain technology and cryptocurrency. The insurance industry must develop adequate tools and insurance policies that address policyholders' needs. Fully understanding the innovative technology will be a step in the right direction in order to ensure suitable coverage is available.