The Fidelity Law Journal

published by
The Fidelity Law Association

Volume XXIV, November 2018

The Fidelity Law Journal

published by

The Fidelity Law Association

Volume XXIV, November 2018

Cite as XXIV FID. L.J. ___ (2018)

The Fidelity Law Journal is published annually. Additional copies may be purchased by writing to: The Fidelity Law Association, c/o Chiesa Shahinian & Giantomasi PC, One Boland Drive, West Orange, New Jersey 07052.

TALES FROM THE CRYPT: CRYPTOCURRENCY IS HERE—HOW WILL CRIME INSURERS RESPOND?

Mark J. Krone
Emily M. Lukes
Chris McKibbin

"*The swarm is headed towards us*."
– Satoshi Nakamoto,
the "Inventor" of Bitcoin

I.
INTRODUCTION

As Blockchain technology and cryptocurrency continue to mature and proliferate, an understanding of what they are and how they transfer value becomes essential for the fidelity professional. In this article, the authors first explore the fundamentals of cryptocurrencies, how their usage has evolved from initial goals, and how regulators have attempted to regulate the cryptocurrency realm. The article then canvasses potential loss scenarios involving cryptocurrency, and how some carriers have already attempted to address cryptocurrency risks. The article concludes by analyzing some of the potential coverage and valuation issues which may arise in a cryptocurrency loss, and by discussing some of the unique challenges a cryptocurrency loss can pose.

Mark J. Krone is an associate with Anderson, McPharlin & Conners, LLP in Los Angeles. Emily M. Lukes is Claim Counsel with Travelers Bond & Specialty Insurance in Chicago. Chris McKibbin is a partner with Blaney McMurtry LLP in Toronto.

II.
CRYPTOCURRENCY AND BLOCKCHAIN TECHNOLOGY

A. Cryptocurrency Compared with Traditional Currency

In general parlance, "money" is defined as something that is generally accepted as a medium of exchange, a measure of value, or a means of payment, such as an officially coined or stamped metal currency.[1] Until recently, nearly all money was coined and controlled by national governments. Alternative currencies that competed with the U.S. Dollar were deemed unlawful[2] and have even led to criminal prosecutions.[3] This traditional model, however, has been upset by the rise of cryptocurrencies, which as of the date of this article, exceed 1,400 in number.[4]

In order to understand and analyze whether and to what extent a cryptocurrency loss is potentially covered under a commercial crime policy, it is first necessary to understand how cryptocurrencies differ from the traditional notion of money. As discussed below, cryptocurrencies differ from traditional currency in that they (1) are decentralized, (2) are issued in a limited supply, (3) have no physical form or coinage, (4) accommodate pseudonymous—and often anonymous—transactions, (5) are non-reversible transactions, and (6) are not legal tender.

---

[1] Money. (n.d.). Retrieved March 31, 2018, from https://www.merriam-webster.com/dictionary/money (last accessed June 13, 2018).

[2] Veazie Bank v. Fenno, 75 U.S. 533, 549 (1869). See also Press Release, U.S. Mint, Liberty Dollars Not Legal Tender, Sept. 14, 2006, http://www.usmint.gov/pressroom/index.cfm?%20flash=yes&action=press_release&id=710 (last accessed June 3, 2015).

[3] *See*, *e.g.*, Press Release, F.B.I., Defendant Convicted of Minting His Own Currency, Mar. 18, 2011, http://www.fbi.gov/charlotte/press-releases/2011/defendant-convicted-of-minting-his-own-currency (last accessed June 13, 2018).

[4] Digital Shadows, *The New Gold Rush: Cryptocurrencies are the New Frontier of Fraud*, February 1, 2018 at 2. https://info.digitalshadows.com/TheNewGoldRush-CryptocurrencyResearch-Press.html (last accessed June 13, 2018).

1. Cryptocurrencies Are Decentralized

Traditional fiat currencies are controlled and monitored by a national bank. For example, the central bank of the United States, the Federal Reserve System, largely controls the supply of the United States dollar. In contrast, one of the overriding features of cryptocurrencies is that the overwhelming majority of the currencies are decentralized. That is, no single institution controls the cryptocurrency network. In the case of Bitcoin,[5] the network is maintained by a group of volunteer coders, and run by an open network of dedicated computers worldwide.[6] In the same way, Bitcoin software is not developed by one person or institution. Rather, there exists an open-source reference client developed and maintained by a group of core developers who have access to a public software code repository on the web-based hosting service GitHub.[7]

2. Limited Supply and Extreme Divisibility

Fiat currencies, such as dollars and euros, have a potentially unlimited supply. Central banks have the ability to issue as much of their national currency as they want. They do so in order to control the value of the currency relative to other currencies. Most cryptocurrencies, however, are designed to have a limited supply. In the case of Bitcoin, the algorithm is designed so that there will never be more than 21 million bitcoins in circulation. In theory, the limited supply makes bitcoin more attractive. That is, if demand grows but supply remains capped, the value will increase.[8]

The flipside of limited supply is that the currencies are designed to be extremely divisible. For example, smallest unit of a bitcoin is a satoshi, and it is one hundred millionth of a bitcoin (0.00000001).

---

[5] A word on nomenclature: When referring to the currency as a whole, it is capitalized. When referring to a unit of the currency, lowercase is used.

[6] https://www.coindesk.com/information/what-is-bitcoin/ (last accessed June 13, 2018).

[7] The Bitcoin repository on GitHub is located at https://github.com/bitcoin/bitcoin.

[8] https://www.coindesk.com/information/what-is-bitcoin/ (last accessed June 13, 2018).

Conceivably such divisibility can enable online microtransactions that fiat currency cannot.[9]

3. No Physical Counterpart

Fiat currency exists in both physical and electronic form. In the physical realm, a twenty dollar bill may be obtained from a bank's automated teller machine and used to purchase goods. The recipient of the bill may use it to make another purchase, and so on. This same process is not possible with cryptocurrency because the currency exists only in digital form. Even if the necessary private key data were inscribed onto a physical thing, such as a token, the value would be the information on the token, not the token itself. The token would cease to have any value as soon as the private key was used in a transaction and a new block in the public ledger was generated.[10]

4. Pseudonymous Transactions

Online transactions using fiat currency lack anonymity because both the sender and recipient require an account with the third party intermediary handling the transfer. If Arthur used PayPal to send funds to Bette, PayPal will have a record of the transaction and the participants. Considering that both Arthur and Bette have likely linked their PayPal accounts to their credit card or bank accounts, their identities are known.

In cryptocurrency transactions, such as Bitcoin, the sender and the recipient are identified by keys or addresses, which is an identifier of 26 to 35 case-sensitive alphanumeric characters, and may resemble a string such as "1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2."[11] The keys are the only information used to define who the participants to the transaction were, and where the cryptocurrency was sent. Inasmuch as the keys can be generated as often as the user desires, they allow for a degree of anonymity that is not available in online transactions using fiat currencies.

---

[9] https://www.coindesk.com/information/what-is-bitcoin/ (last accessed June 13, 2018).

[10] Bitcoin.org, How does Bitcoin work?, https://bitcoin.org/en/how-it-works (last accessed June 13, 2018).

[11] https://en.bitcoin.it/wiki/Address (last accessed June 13, 2018).

This anonymity, however, is incomplete. Every transaction is recorded in the public ledger, thus it is not a difficult feat to determine all of the transactions associated with an address.[12] Since users usually have to reveal their identity in order to receive services or goods, Bitcoin addresses cannot remain fully anonymous.[13] While there are methods to maximize a user's level of anonymity, such as creating new addresses or bitcoin mixing, such measures are no guarantee of complete anonymity.

Additionally, Blockchain analytics have been remarkably successful in gleaning identities based on nothing more than the ledger itself. Blockchain analytics were used to trace transactions to identify and prosecute Ross Ulbricht, who was involved in the infamous Silk Road.[14] More recently, similar tactics were used to trace and identify two federal agents working on the Silk Road investigation, who themselves stole over two hundred thousand dollars of bitcoin.[15]

5. Non-reversible Transactions

Once the Blockchain reflects a new transaction, the transaction is irreversible and it can only be refunded by the recipient. That is, when a new block is added to the Blockchain, the public ledger is also updated

[12] https://bitcoin.org/en/protect-your-privacy (last accessed June 13, 2018).

[13] Andy Greenberg, *Follow The Bitcoins: How We Got Busted Buying Drugs On Silk Road's Black Market*, FORBES, Sept. 5, 2013 http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/ (last accessed June 13, 2018).

[14] Jason Weinstein, *How Can Law Enforcement Leverage The Blockchain In Investigations*?, COIN CENTER, May 12, 2015, https://coincenter.org/2015/05/how-can-law-enforcement-leverage-the-blockchain-in-investigations.

[15] Charlie Richards, *US Secret Agents Charged with Silk Road Bitcoin Theft, Extortion of Dread Pirate Roberts*, COINTELEGRAPH, March 31, 2015 https://cointelegraph.com/news/us-secret-agents-charged-with-silk-road-bitcoin-theft-extortion-of-dread-pirate-roberts (last accessed June 13, 2018).

for all users of the cryptocurrency. As a result, merchants have no chargeback liability, which reduces transactions costs.[16]

6. Cryptocurrencies Are Not Legal Tender

As yet, cryptocurrency's status as legal tender is dubious.[17] With the exception of the Venezuelan Petro, whose status as a viable cryptocurrency is not established, cryptocurrency is not issued by any government, nor is it guaranteed by any jurisdiction. Cryptocurrencies have value only because users of the currency agree among themselves that the currency has value. Unless the parties agreed prior to the time that the debt arose, a creditor is under no obligation to accept cryptocurrency in satisfaction of the debt.[18] According to FinCEN, cryptocurrency is a medium of exchange, but it lacks all the attributes of real currency. Although cryptocurrency can operate like a currency in some environments, cryptocurrencies lack the status of legal tender in all jurisdictions.[19]

However, cryptocurrency does function as a sort of alternative means of exchange, with different countries providing limited recognition of cryptocurrency in different contexts.[20] In Germany, bitcoins are recognized as "private money"[21] and Bitcoin exchanges are considered financial service companies which must meet specific regulatory requirements.[22] In Brazil, Article 6-VI of Law No. 12,865, permits the creation of "e-money," that is, money stored in devices or

---

[16] Bitcoin.org, You Need to Know, <https://bitcoin.org/en/you-need-to-know> (last accessed June 13, 2018).

[17] *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearings Before the S. Comm. on Homeland Sec. & Gov't Affairs*, 113th Cong. (2013) (statement of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network, U.S. Dept. Treas.) [hereinafter FinCEN Statement].

[18] *Id.*

[19] *Id* at 2.

[20] Oleg Stratiev, *Cryptocurrency and Blockchain: How to Regulate Something We Do Not Understand* 33 BUS. & FIN. L. REV. 173, 198-199 (2018).

[21] Emily Spaven, "Germany Officially Recognizes Bitcoin as 'Private Currency'" COINDESK, August 19, 2013, http://www.coindesk.com/germany-official-recognises-bitcoin-as-private-money (last accessed June 13, 2018).

[22] Stratiev, *supra* note 20 at 198-199.

electronic systems which allows the user to perform payment transactions.[23]

B. Blockchain Technology Replaces Traditional Authentication Procedures

Decentralization manifests itself in another way as well. In an online transaction between two persons, a third party intermediary is necessary to complete the transaction. If Arthur wants to send money to Bette via the Internet, he must rely on a third party service such as PayPal. Such intermediaries maintain a ledger of the account holders' balances and can verify the transfer of funds. When Arthur sends the funds, PayPal deducts the money from Arthur's account and adds it to Bette's account.

In a decentralized model, transactions are not processed through a third party. Instead, the transactions move directly from person to person.[24] The issue that a cryptocurrency transfer must address is how to confirm—without reliance on a third party administrator—that ownership has been transferred to Bette and that Arthur did not previously transfer the same funds to Charles. This is known as the "double-spend" problem.

Cryptocurrencies accomplish this by use of a public ledger, which is distributed through a peer-to-peer network among all the users of the of currency system. New crypto transactions are validated with a collective consensus algorithm known as Proof-of-Work across the peer-to-peer network.[25] Validated transactions are recorded on a decentralized public ledger called a Blockchain that is visible to the world.[26]

At any given moment, there could be thousands of users logged onto the network and confirming transactions against the Blockchain. In our hypothetical, Arthur's transfer of cryptocurrency would be checked

---

[23] *Law 12,865 of October 9, 2013*, Art. 6-VI.

[24] FinCEN Statement, *supra* note 17, at 3-4.

[25] Andreas M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies 188 (2014).

[26] Bitcoin.org, FAQ, <https://bitcoin.org/en/faq#what-is-bitcoin> (last accessed June 13, 2018).

against the Blockchain to ensure that the coins have not been spent. The transfer is completed when a sufficient number of users have confirmed that Arthur owns the cryptocurrency that he seeks to transfer and a new Blockchain entry is generated. The distributed ledger is then updated to reflect that Bette now owns the cryptocurrency that Arthur transferred. At this point, the currency is irrevocably transferred to Bette.

C. The "Crypto" in Cryptocurrency

The integrity of decentralized cryptocurrencies relies on cryptography. The idea to use cryptography was originated by Satoshi Nakamoto in a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System".[27] Satoshi Nakamoto is a pseudonym; whether Satoshi Nakamoto refers to a single person or a group of people remains the source of much speculation.[28]

In addition to the public Blockchain, each bitcoin has a private key that the owner stores. The public key is used to encrypt plaintext or to verify a digital signature, whereas the private key is used to create a digital signature. The private key and Blockchain are mathematically linked, and their combination proves whether the putative holder owns the cryptocurrency and is permitted to spend it.[29] Every bitcoin transaction requires an addition to the Blockchain that must include the solution to a difficult mathematical problem, which is costly to create in terms of computer resources, electricity and time. Although the problem is difficult to solve, the solution is easy to verify. Additionally, the problem is not arbitrary, but instead is linked to the verification of transactions. While it is theoretically possible to create a Blockchain that

[27] *Id.* Hereinafter the Nakamoto Paper.

[28] Matthew Sparks, *Who is the reclusive billionaire creator of Bitcoin?*, THE TELEGRAPH, Mar. 4, 2014, http://www.telegraph.co.uk/technology/10673546/Who-is-the-reclusive-billionaire-creator-of-Bitcoin.html (last accessed June 13, 2018).

[29] David Meyer, *Yes, you should care about Bitcoin, and here's why*, GIGAOM.COM, Apr. 4, 2013, https://gigaom.com/2013/04/04/yes-you-should-care-about-bitcoin-and-heres-why (last accessed June 13, 2018).

branches from a valid transaction, the necessary resources and time constraints make that possibility vanishingly small.[30]

D. Cryptocurrency Transactions & Mining

1. Procedure to Complete Transaction

In order to use bitcoins, a user must first obtain a "wallet," which is software installed on a phone or computer. The wallet contains the user's private key(s), proving that the user is the owner of the bitcoins allocated to him or her in the Blockchain. The private key also prevents the transaction from being altered by anybody once it has been issued. The Bitcoin wallet can show the total balance of all bitcoins it controls and lets the user pay a specific amount to a specific person.[31] Although a Bitcoin wallet is roughly analogous to a physical wallet, it is more appropriately thought of as storage for the digital credentials for the user's bitcoin holdings. Wallets can be maintained online and are capable of linking to the Internet (also known as "hot" storage), or they can be separate from the Internet and maintained on hard drives or other storage devices (also known as "cold" storage). Although coins in an offline wallet cannot be spent, they also cannot be stolen until they are moved to an online wallet.

When parties transact in bitcoins, the transaction is broadcast to the network. The only information provided on the network is the coin identifier and the transaction amount. The broadcast of transaction information commences the confirmation process, which takes about ten minutes, and is referred to as mining or cryptomining.

2. Mining

Mining is described as a distributed consensus system that is used to confirm pending transactions by including them in the Blockchain. For a transaction to be confirmed, it is packed in a block, i.e., a segment of the Blockchain, according to strict cryptographic rules

[30] François R. Velde, *Bitcoin: A primer*, CHICAGO FED LETTER NO. 317, December 2013.

[31] Bitcoin.org, How does Bitcoin work?, https://bitcoin.org/en/how-it-works (last accessed June 13, 2018).

that will be verified by the mining network. In essence, the servers compare the Blockchain on record with the Blockchain of the transaction. If they match, the seller knows that the buyer is using bitcoins. Each new transaction adds a new block in the Blockchain. The composition of the block is not a simple statement of "X paid Y," but the result of extremely complicated cryptographic algorithms. The algorithm requires the mining computers to keep inputting possible solutions until a correct result is returned.

Once the solution is found, it adds another block to the Blockchain. With each new transaction added to the Blockchain, the complexity of the solution grows exponentially. The cryptographic rules prevent malicious users from modifying previous blocks in the chain, because doing so would invalidate all following blocks. Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively in the Blockchain. This way, no individual can control what is included in the Blockchain or replace parts of the Blockchain to roll back their own transactions. As a result, the mining process enforces a chronological order in the Blockchain, protects the neutrality of the network, and allows different computers to agree on the state of the system.[32]

For example, if payer X wants to send Y bitcoins to payee Z, payer X broadcasts the transaction to the peer-to-peer network of Bitcoin servers using the wallet application on X's smartphone and the wallet application on Z's desktop computer. The wallet applications carry out the transaction, by broadcasting a message to a large network of nodes on the Internet, announcing the proposed transfer of Y bitcoins from X's wallet to Z's wallet. Every ten minutes, the nodes, i.e., "miners," collect the proposed transactions that were recently broadcast. Nodes check that the transaction funds exist, and that they have been correctly signed for. Miners then collect transactions, and include them in blocks, which function as a ledger of bitcoin transactions, i.e., the Blockchain. When a transaction appears in a valid block, the transaction is considered to be confirmed. Confirmation means that a transaction has been processed by the network and is highly unlikely to be reversed. Transactions receive a

[32] *Id.*

confirmation when they are included in a block, and for each subsequent block.[33]

The mining process invites an obvious question. If there are no transaction fees, what is the incentive to participate in mining? The answer is that successful miners are rewarded with newly-created bitcoins for validated transactions. Bitcoin's architecture is structured so that there will never be more than 21 million bitcoins in circulation. Whoever finds the puzzle piece wins a certain number of bitcoins, and the process starts all over again. Aside from the initial 50 bitcoins created by Satoshi Nakamoto through the "genesis block" of the Blockchain,[34] all bitcoins in circulation (17,091,725 as of June 12, 2018)[35] have come into existence as a result of miners' efforts.

Mining, however, involves a huge amount of processing power. Early in the history of Bitcoin, users built specialized mining computers that chained together multiple graphics cards in order to use the graphical processing units to quickly confirm transaction. As the complexity of the algorithm has increased with each addition to the Blockchain, the feasibility of being a profitable single-user miner is no longer cost-effective. Considering the processing demands required for mining, users now band together in "pools" to find the solution and to earn bitcoins more regularly.[36]

The payoff for winning the mining race can be very lucrative and miners have every incentive to harness as much computing power as possible. This has led to unexpected results, including acute shortages of graphics cards, which have graphical processing units ("GPUs") capable

[33] Velde, *supra* note 30.

[34] Stratiev, *supra* note 20 at 190.

[35] Blockchain Luxembourg S.A., Bitcoins in Circulation, https://blockchain.info/charts/total-bitcoins (last accessed June 14, 2018).

[36] Adam Pasick, *Malware Turns Hacked Computers into Slaves that "Mine" New Digital Currency*, QUARTZ, Apr. 8, 2014, http://qz.com/71813/malware-turns-hacked-computers-into-slaves-that-mine-new-digital-currency (last accessed June 13, 2018).

of processing transactions more quickly than the CPU residing on the mother board.[37]

E. Efforts to Regulate Cryptocurrency

1. Securities and Exchange Commission

The United States Securities and Exchange Commission (the "SEC") is an independent federal agency charged with overseeing and regulating securities markets while simultaneously protecting investors against fraudulent and manipulative market practices. Created by Congress in 1934 following the stock market collapse of 1929, the SEC's primary purpose was to ensure that companies provided accurate statements about their business and that securities institutions were fair and honest when dealing with investors. Pursuant to such purpose, the SEC has established an extensive array of rules and regulations applicable to organizations and individuals involved in the securities markets. Generally speaking, any issuer of a security offered in interstate commerce and any entity that sells or trades securities, including, for example, securities exchanges, brokers, dealers, investment advisors, assessment managers and mutual funds must register with the SEC and be subject to its rules and regulations. The SEC has been granted various investigative and enforcement powers in order to fulfill its purpose in promoting stability in the markets and ensuring investors are adequately protected. Although it serves as the primary regulator of the United States securities markets, the SEC works in close collaboration with several other institutions and agencies, including Congress, other federal departments, and state securities regulators, as will be explored further below.

Traditionally, to determine whether an item qualifies as a "security" subject to SEC regulation, one applies the long-standing *Howey* test, as derived from the Supreme Court's 1946 decision.[38] In *Howey*, the Supreme Court held that the investment contracts at issue were securities, which "for purposes of the Securities Act means a

[37] Chris Baraniuk, *Crypto-currency Craze 'Hinders Search for Alien Life'*, BBC NEWS, February 14, 2018, http://www.bbc.com/news/technology-43056744 (last accessed June 13, 2018).

[38] S.E.C. v. W.J. Howey Co., 328 U.S. 293 (1946).

contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party."[39] The *Howey* test consists of a four-pronged analysis that defines a security as an investment contract in which a person (1) invests their money, (2) in a common enterprise, (3) with an expectation of profits, and (4) based on the efforts of the promoter or a third party.[40]

Historically, the courts and the SEC have taken an extremely broad view of whether any kind of investment is a security.[41] The definition of "security" is expansive and intended to be flexible enough to apply to new investments that share the characteristics of stocks and bonds.[42] For instance, in a seminal decision on prime bank notes, the Seventh Circuit rejected the note purveyors' argument that the prime bank notes were not securities because they were entirely fictional.[43] Instead, in referencing the *Howey* test and illustrating the sweeping definition of security, the Seventh Circuit held that the securities did not need to actually exist as long as the investment as described shared the characteristics of a security.[44]

With respect to cryptocurrencies, the SEC has thus far refused to state categorically whether cryptocurrencies are securities. Instead, the SEC has repeatedly expressed its position that each cryptocurrency must be considered on its own to evaluate whether it meets the definition of a security as laid out in the *Howey* test.[45] The SEC has distinguished cryptocurrencies that are used as a medium of exchange from digital

[39] *Id.*

[40] *Id.*; *see also* John Reed Stark, *Ten Crypto-Caveats Floyd Mayweather and DJ Khaled Should Have Heard from their Lawyers,* THE D&O DIARY, April 16, 2018, https://www.dandodiary.com/2018/04/articles/cyber-liability/guest-post-ten-crypto-caveats-floyd-mayweather-dj-khaled-heard-lawyers/ (last accessed June 13, 2018).

[41] *Id*.

[42] *Id.*

[43] S.E.C. v. Lauer, 52 F.3d 667 (7th Cir. 1995).

[44] Stark, *supra* note 40.

[45] PUBLIC STATEMENT OF SEC CHAIRMAN JAY CLAYTON ON CRYPTOCURRENCIES AND INITIAL COIN OFFERINGS, December 11, 2017, https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11 (hereinafter "SEC December Statement").

coins being offered in the course of an initial coin offering or "ICO." Drawing its name from an initial public offering or "IPO" on the U.S. stock market, an ICO involves companies or individuals offering a new virtual coin or token in exchange for legal tender or cryptocurrencies such as Bitcoin or Ethereum to raise funds and grow the offered business or project.[46] While the former category, which includes well-known cryptocurrencies used as a medium of exchange such as Bitcoin, would likely not qualify as a security, the latter category involving coins offered in ICOs would almost certainly meet the definition of a security, as such coins involve both a person or group that sponsored the creation and sale of the asset, and third parties who invested with the expectation of a return.[47] In fact, in April and June 2018, SEC leaders stated during hearings and at seminars that Bitcoin and Ether respectively would likely not satisfy the definition of a security because those cryptocurrencies have become sufficiently decentralized.[48] In contrast, tokens or coins offered during ICOs do not share such decentralization and as such, would very likely qualify as a security and be subject to SEC regulation.[49]

Consequently, the SEC appears primarily focused on ICOs. In July 2017, the SEC completed an investigation into the offer and sale of DAO tokens during an ICO taking place between April 30, 2016 and May 28, 2016.[50] The DAO ICO raised 12 million ether, a virtual currency used on the Ethereum Blockchain, which at the time was valued at USD $150 million.[51] The July 2017 Investigation Report concluded that the offered DAO tokens qualified as securities and that the offering should have been made in compliance with United States federal

[46] *Id*.

[47] Bob Pisani, *Bitcoin and Ethereum are Not Securities, but Some Initial Coin Offerings May Be, SEC Official Says*, CNBC, June 14, 2018, https://www.cnbc.com/2018/06/14/bitcoin-and-ethereum-are-not-securities-but-some-cryptocurrencies-may-be-sec-official-says.html.

[48] Louise Matsakis, *Rest Easy, Cryptocurrency Fans: Ether and Bitcoin Aren't Securities*, WIRED, June 14, 2018, https://www.wired.com/story/sec-ether-bitcoin-not-securities/.

[49] Pisani, *supra* note 47.

[50] REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: The DAO, SEC Release No. 81207, (July 25, 2017).

[51] *Id.*

securities laws.[52] The SEC ultimately declined to pursue an enforcement action against the DAO founders.

In a December 2017 public statement on Cryptocurrencies and Initial Coin Offerings, SEC Chairman, Jay Clayton, described ICOs as:

> Along with the extensive growth in cryptocurrencies, start-up companies and individuals increasingly have been using ICOs to raise funds for their businesses and projects. The offerings can take many different forms, and the rights and interests a coin is purported to provide the holder can vary widely. The tokens also rise and fall in value and can be bought and sold, giving them characteristics of unregulated securities.[53]

The December statement also reiterated the SEC's view that ICOs offering tokens or coins based on Blockchain technology would likely qualify as securities offerings, and should be registered with the SEC and subject to its rules and regulations. Notably, the statement was directed not just to market professionals such as broker-dealers, investment advisers and exchanges, but also to lawyers and accountants who are counseling clients regarding cryptocurrency and related regulation.[54]

On March 7, 2018, the SEC issued a public statement addressing the regulation of online trading platforms, or exchanges, on which investors have bought and sold digital assets, including coins or tokens sold in ICOs.[55] The SEC again opined that many of the coins sold in an ICO meet the definition of a "security" and, consequently, trading platforms on which ICO tokens trade should register with the SEC as a national securities exchange or alternative trading system, unless exempt

[52] *Id.*

[53] SEC December Statement, *supra* note 45.

[54] *Id*.

[55] SEC Public Statement on Potentially Unlawful Online Platforms for Trading Digital Assets, March 7, 2018, https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading (hereinafter "SEC March Statement").

from registration.[56] The SEC expressed its concern that many of these trading platforms may appear to investors as SEC-regulated exchanges, but are not, and do not meet the regulatory and listing standards of a registered exchange.[57] SEC Chairman Clayton revealed that no ICOs had registered with the commission as of February 6, 2018, despite the rapidly increasing prevalence of ICOs in recent months.[58]

In April 2018, the SEC flexed its enforcement muscle and accused two co-founders of Centra Tech, Inc. ("Centra"), a purported financial services start-up firm, of orchestrating a fraudulent ICO which had been able to secure the promotional efforts of boxer Floyd Mayweather and to raise more than $32 million from thousands of investors. The Centra founders allegedly claimed that funds raised in its ICO would help build a suite of financial products. For instance, they claimed to have partnered with Visa and MasterCard to offer a debit card that would allow users to instantly convert hard-to-spend cryptocurrencies into U.S. dollars or other legal tender. In reality, however, Centra had no such relationship with Visa or MasterCard. The SEC worked in conjunction with the U.S. Justice Department, which separately brought criminal charges against the Centra founders.[59]

In addition to trading platforms and ICOs, the SEC's statement also focused on companies offering "digital wallet services" for holding or storing digital assets. "These and other services offered by platforms may trigger other registration requirements under the federal securities laws, including broker-dealer, transfer agent, or clearing agency registration, among other things," the statement said.[60]

---

[56] *Id.*

[57] Marc Press and Joseph B. Doll, *Blockchain and Cryptocurrency: Recent Legal and Regulatory Developments*, LEXOLOGY, Mar. 14, 2018, https://www.lexology.com/library/detail.aspx?g=46b71855-ead3-4dfe-98f4-6574b7416d61 (last accessed June 19, 2018).

[58] Shannon Liao, *The SEC Is Probing Cryptocurrency Companies with Initial Coin Offerings*, THE VERGE, Mar. 1, 2018, https://www.theverge.com/2018/3/1/17066828/sec-cryptocurrency-companies-icos-initial-coin-offerings-regulation (last accessed June 13, 2018).

[59] Stark, *supra* note 40.

[60] Evelyn Cheng, *The SEC Just Made it Clearer that Securities Laws Apply to Most Cryptocurrencies and Exchanges Trading Them*, CNBC, Mar. 7,

The SEC has also used its investigative powers to evaluate various hedge funds established to invest in cryptocurrencies and initial coin offerings. Currently, there are estimated to be about 220 crypto-focused hedge funds that reportedly manage at least $3.5 billion combined. The SEC reportedly has sent information requests and issued subpoenas to crypto-focused firms inquiring about the valuation process used to price digital investments as well as the firms' compliance with rules and safeguards aimed at preventing theft and keeping investors' assets safe. In fact, certain crypto-focused funds have received subpoenas from the Enforcement Division of the SEC, which is responsible for investigating potential misconduct and enforcing punishments in the case of wrongdoing.[61]

Throughout all its public statements, the SEC has consistently warned the public that ICOs are particularly susceptible to fraud and manipulation,[62] as will be explored in greater detail below, and have substantially less investor protection than traditional securities markets.[63]

2. Commodity Futures Trading Commission

The U.S. Commodity Futures Trading Commission ("CFTC") is the federal regulatory body focused on overseeing commodity futures and the markets in which they trade.[64] A "future" is a contract to purchase or sell a commodity at a specified price in the future.[65]

2018, https://www.cnbc.com/2018/03/07/the-sec-made-it-clearer-that-securities-laws-apply-to-cryptocurrencies.html (last accessed June 13, 2018).

[61] Benjamin Bain, Olga Kharif and Matt Robinson, *Hedge Funds Draw SEC Scrutiny in Crypto Coin Review*, BLOOMBERG, Mar. 14, 2018, https://www.bloomberg.com/news/articles/2018-03-14/hedge-funds-are-said-to-draw-sec-scrutiny-in-crackdown-on-crypto (last accessed June 13, 2018).

[62] Matt Robinson and Christie Smith, *Floyd Mayweather-Backed Coin Promoters Hit With Criminal Charges*, BLOOMBERG, Apr. 2, 2018, https://www.bloomberg.com/news/articles/2018-04-02/floyd-mayweather-backed-coin-promoters-hit-with-criminal-charges (last accessed June 13, 2018).

[63] SEC December Statement, *supra* note 45.

[64] Jerry Brito & Andrea Castillo, Bitcoin: A Primer For Policymakers 55 at 56 (Mercatus Center 2016).

[65] Daniel Shane, *Bitcoin Futures Trading Just Got a Lot Bigger*, CNN, Dec. 18, 2017, http://money.cnn.com/2017/12/18/investing/bitcoin-cme-futures/index.html?iid=EL (last accessed June 13, 2018).

Investors and financial institutions have been trading in Bitcoin futures for several years. In 2017, even greater interest in Bitcoin futures trading developed, owing in part to Bitcoin's prolific rise from below $1,000 per coin in January 2017 to nearly $20,000 per coin in December 2017.[66]

As far back as 2015, the CFTC has defined cryptocurrencies as commodities and regulated cryptocurrency derivatives under its authority to oversee commodity futures trading.[67] Bear in mind that the CFTC is not regulating cryptocurrencies, but regulating the futures market, which are tradable contracts to purchase or sell at a certain date for a certain price.[68] The CFTC has used its authority to investigate cryptocurrency businesses that it views as hoaxing investors. For instance, in September 2015, the CFTC resolved charges against Coinflip Inc. for facilitating options transactions involving cryptocurrencies.[69]

In March 2018, the CFTC's position was affirmed when a federal district court in New York ruled that cryptocurrencies can be regulated by CFTC as a commodity in *CFTC v. McDonnell*.[70] The CFTC brought charges against defendant McDonnell alleging that he and his company, Coin Drop Markets, were operating a fraudulent cryptocurrency scheme in violation of the Commodity Exchange Act ("CEA"). Specifically, the CFTC alleged that the defendants fraudulently induced customers to send money and cryptocurrencies in exchange for purported cryptocurrency trading advice and for cryptocurrency trades on their behalf. After securing payments from several customers, the defendants allegedly ceased communications with the customers and disappeared from the Internet.

---

[66] Kate Rooney, Much of Bitcoin's 2017 Boom Was Market Manipulation, Research Says, CNBC, June 13, 2018, https://www.cnbc.com/2018/06/13/much-of-bitcoins-2017-boom-was-market-manipulation-researcher-says.html (last accessed June 13, 2018).

[67] *Id.*

[68] Matt Robinson & Tom Schoenberg, *Bitcoin Price Manipulation Probe Launched by Justice Department*, BLOOMBERG, May 24, 2018, https://www.bloomberg.com/news/articles/2018-05-24/bitcoin-manipulation-is-said-to-be-focus-of-u-s-criminal-probe (last accessed June 13, 2018).

[69] Wolfie Zhao, *Cryptos Are Commodities, Rules US Judge in CFTC Case*, COINDESK, Mar. 7, 2018 https://www.coindesk.com/us-judge-rules-cryptocurrencies-are-commodities-in-cftc-case/ (last accessed June 13, 2018).

[70] 287 F.Supp.3d 213 (E.D.N.Y. 2018).

The District Court, after discussing the definition of a commodity under the CEA and relying, in part, on a 2015 CFTC administrative ruling that cryptocurrencies were commodities, held that "virtual currencies can be regulated by CFTC as a commodity," and that, in the absence of federal rules, the CEA permitted the CFTC in a fraud case to exercise its jurisdiction over cryptocurrencies that did not directly involve the sale of futures or derivative contracts.[71] "Virtual currencies are 'goods' exchanged in a market for a uniform quality and value. . . . They fall well within the common definition of 'commodity'," the Court held. As such, the Court entered a preliminary injunction against the defendants and allowed the case to proceed.

"The CFTC has previously specified that it views its jurisdiction as extending both to matters involving cryptocurrency derivatives and to fraud and manipulation in cryptocurrency spot markets (seemingly including for cryptocurrencies that have not yet developed futures markets)."[72] The *McDonnell* case is just one of several recent cases brought by the CFTC. The district court's decision in *McDonnell* further expands regulatory authority over cryptocurrency and related products and services.

In May 2018, the CFTC was reported as working with federal prosecutors at the U.S. Justice Department investigating whether traders are illegally manipulating the price of Bitcoin and other cryptocurrencies.[73] The Chairman of the CFTC was recently quoted as stating: "One thing is certain: ignoring virtual currency trading will not make it go away. Nor is it a responsible regulatory strategy. The CFTC has an important role to play."[74]

---

[71] Press & Doll, *supra* note 57.

[72] Michael J. Gilbert *et al*, *Federal Court Ruling Recognizes CFTC Jurisdiction over Cryptocurrencies as Commodities*, LEXOLOGY, Mar. 26, 2018, https://www.lexology.com/library/detail.aspx?g=1bea098f-5306-41bd-9e85-ad779ec8502e (last accessed June 13, 2018).

[73] Robinson & Schoenberg, *supra* note 68.

[74] Benjamin B. Coulter, *CFTC Can Regulate Cryptocurrencies as Commodities*, LEXOLOGY, March 20, 2018, https://www.lexology.com/library/detail.aspx?g=f9ab791d-6e06-4290-8b70-50135665c950 (last accessed June 13, 2018).

3. Financial Crimes Enforcement Network

FinCEN, a bureau of the U.S. Department of the Treasury, was the first federal agency to address convertible cryptocurrency regulation. FinCEN is tasked with issuing, implementing, and administering regulations pursuant to the Bank Secrecy Act ("BSA") mandate. Roughly speaking, the BSA is a compilation of statutory provisions designed to prevent money laundering.[75] The BSA was enacted in 1970 to deter the use of banks and other financial institutions for money laundering.[76] To this end, the BSA requires that financial institutions disclose the identities of parties to transactions exceeding $10,000.[77] Additionally, the BSA requires financial institutions to file Suspicious Activity Reports for suspected-illegal transactions and implement anti-money-laundering programs.[78]

Included in this framework are the regulations pertaining to money service businesses ("MSB"), which are defined as a "person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in one or more of the capacities listed in paragraphs (ff)(1) through (ff)(7) of this section."[79] Among those capacities is "money transmitter," which is a "person that provides money transmission services . . . mean[ing] the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[80] This extends to persons who transmit money or other value that substitutes for currency.[81] This definition is broad enough to encompass cryptocurrency

[75] 31 U.S.C. §§ 5311-5332.

[76] Kavid Singh, *The New Wild West: Preventing Money Laundering in the Bitcoin Network*, 13 N.W.. J. TECH. & INTELL. PROP. 37, 45 (2015).

[77] 31 U.S.C. § 5313(a) (2012); 31 C.F.R. § 1010.311 (2011).

[78] *Id.* § 5318(g)(1), (h) (2012).

[79] 31 C.F.R. 1010.100(ff).

[80] *Id.* § 1010.100(ff)(5)(i).

[81] *Id.* § 1010.100(ff)(5)(A) (Lexis Advance through the May 2, 2018 issue of the Federal Register. Title 3 is current through May 4, 2018).

exchangers and administrators.[82] Cryptocurrency users, i.e., persons who obtain cryptocurrency and use it to purchase real or virtual goods or services, are not MSBs under FinCEN's regulations. Money transmitters are required to register with FinCEN,[83] file certain reports,[84] keep specific records,[85] and implement anti-money-laundering programs.[86] Under the USA Patriot Act of 2001,[87] the operation of an unlicensed money-transmission business is a felony.[88]

The requirement for exchangers and administrators to register with FinCEN and to monitor and report suspicious activity does not exist in the abstract. FinCEN has fined non-compliant cryptocurrency MSBs for their failure to adhere to the BSA. On May 5, 2015, FinCEN announced that it fined Ripple Labs, Inc. and its subsidiary, XRP II, LLC, $700,000.[89] Ripple Labs built a payment transfer platform that people can use to move real or virtual money, and the company maintains its own cryptocurrency, called XRP II, which loosely compares to Bitcoin. Unlike Bitcoin, XRP was fully generated before it went on the market, so an equivalent to Bitcoin miners doesn't exist in XRP. Ripple, however, failed to register as a MSB while selling XRP and failed to establish an adequate anti-money laundering program.[90]

---

[82] FinCEN, FIN-2013-G001, *Application Of FinCEN's Regulations To Persons Administering, Exchanging, Or Using Virtual Currencies*, Mar. 18, 2013, http://fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.

[83] 31 U.S.C. § 5330(a)(1).

[84] 31 C.F.R. § 1010.306.

[85] *Id.* § 1010.410.

[86] *Id.* § 1010.310; 31 C.F.R. §§ 1022.320, 1022.210(a).

[87] 115 Stat. 272 (2001).

[88] Andrew Schouten, *Unlicensed Money Transmitting Businesses and Mens Rea Under the USA Patriot Act*, 39 MCGEORGE L. REV. 1099, 1100 (2008).

[89] Press Release, Financial Crimes Enforcement Network, FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger, May 5, 2015, http://www.fincen.gov/news_room/nr/pdf/20150505.pdf.

[90] Megan Geuss, *Cryptocurrency Maker Ripple Labs Fined $700K For Flouting Financial Regs*, ARSTECHNICA, May 5, 2015, http://arstechnica.com/tech-policy/2015/05/cryptocurrency-maker-ripple-labs-fined-700k-for-flouting-financial-regs (last accessed June 13, 2018).

In July 2017, FinCEN assessed a civil money penalty in excess of $110 million against BTC-e a/k/a Canton Business Corporation for willfully violating anti-money laundering laws. Additionally, FinCEN assessed a $12 million penalty against Russian national Alexander Vinnik, one of the operators, for his role in the violations:

> Among other violations, BTC-e failed to obtain required information from customers beyond a username, a password, and an e-mail address. Instead of acting to prevent money laundering, BTC-e and its operators embraced the pervasive criminal activity conducted at the exchange. Users openly and explicitly discussed criminal activity on BTC-e's user chat. BTC-e's customer service representatives offered advice on how to process and access money obtained from illegal drug sales on dark net markets like Silk Road, Hansa Market, and AlphaBay.[91]

4. Internal Revenue Service

The IRS has confirmed that cryptocurrencies will be taxed as property, rather than currency.[92] Thus they are taxed at capital gains rates. The classification also means that owners of cryptocurrency potentially owe tax any time that they use the currency, whether in a sale or a trade. The IRS classification is not surprising. The applicable statute limits "currency" to the "coin and currency of the United States, or of any other country."[93] Because no country issues a cryptocurrency that is recognized by the United States,[94] they cannot be considered "currency" under U.S. tax laws.

The IRS is also actively seeking users of cryptocurrency who are not reporting gains from transactions. In 2016, the IRS served an

[91] Press Release, FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales, July 27, 2017, https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware (last accessed June 13, 2018).

[92] Brito & Castillo, *supra* note 64.

[93] *Id.*

[94] See discussion of the Venezuelan Petro, *infra*.

administrative summons on Coinbase, Inc., the largest Bitcoin exchange in the U.S., seeking information for accounts with at least the equivalent of $20,000 in any one transaction. The IRS sought account registration records, know-your-customer due diligence, documents regarding third-party access, transaction logs, records of payments processed, and account or invoice statements.[95] Following Coinbase's refusal to comply with the subpoena, the Court ruled that Coinbase must honor the subpoena. The Court was persuaded that there was evidence that Coinbase users were underreporting gains from Bitcoin transaction. There were 8.9 million Coinbase transactions and 14,355 Coinbase account holders, but only 800 to 900 taxpayers reported gains related to bitcoin in each of the relevant years, notwithstanding that more than 14,000 Coinbase users either bought, sold, sent or received at least $20,000 worth of bitcoin in a given year.[96] This decision suggests that, regardless of how the IRS categorizes cryptocurrency, it intends to collect the taxes due.

5. State Efforts at Regulation

a. New York

Several states have worked to implement rules to address cryptocurrencies. On June 24, 2015, the New York Department of Financial Services issued its final BitLicense regulations with respect to Bitcoin and other virtual currencies.[97] The regulations require all persons engaging in a virtual currency business to apply and obtain a BitLicense, and to maintain certain minimum standards and programs to help ensure customer protection, cyber-security and anti-money laundering compliance.[98]

---

[95] U.S. v. Coinbase, Inc., Case No. 17-cv-01431-JSC, 2017 U.S. Dist. LEXIS 196306, 5-6 (N.D. Cal. 2017).

[96] *Id.* at 12.

[97] N.Y. COMP. CODES R. & REGS. tit. 23, §§ 200.1 et seq. (2015).

[98] Guy C. Dempsey, Jr. & Gary De Waal, *New York BitLicense Regulations Virtually Certain to Significantly Impact Transactions in Virtual Currencies*, NAT'L. L. REV., Jul. 9, 2015, http://www.natlawreview.com/article/ new-york-bitlicense-regulations-virtually-certain-to-significantly-impact-transactio (last accessed June 19, 2018).

According to the legislation, anyone involved in any of the following activities in the state of New York is required to obtain a business license from the Department of Financial Services:

- Transmission or receipt of virtual currency, except when undertaken for non-financial purposes and for nominal amounts;
- Storing, holding, or maintaining custody or control of virtual currency on behalf of others;
- Buying and selling virtual currency as a customer business;
- Performing exchange services as a customer business; and,
- Controlling, administering, or issuing a virtual currency.[99]

The BitLicense regulations require licensees to maintain capital in an amount and form as the superintendent determines is sufficient to ensure the financial integrity of the licensee, which amount depends on the licensee's total assets, including the position, size, liquidity, risk exposure, and price volatility of each type of asset, as well as other factors.[100] Moreover, the licensee is required to maintain surety bonds for the benefit of its customers.[101] Not surprisingly, the BitLicense regulations require licensees to implement and maintain anti-money laundering programs and cyber security programs.[102]

The BitLicense process is generally seen as prohibitively arduous, and as a result few applications have been submitted and fewer

[99] N.Y. COMP. CODES R. & REGS. tit. 23, §§ 200.2-200.3.
[100] *Id.* § 200.8.
[101] *Id.* § 200.9.
[102] *Id.* § 200.15-200.16.

still have been approved.[103] As of November 28, 2017, the New York State Department of Financial Services has approved the applications for virtual currency licenses for just six entities: bitFlyer USA, Inc., Coinbase Inc., XRP II and Circle Internet Financial, Gemini Trust Company, and itBit Trust Company.[104] The consensus

b. California

As of the date of this article, California has not yet enacted legislation to regulate cryptocurrency. The most recent attempt to regulate cryptocurrency in California was Assembly Bill 1123,[105] which would have built on the BitLicense model from New York. The bill however was heavily opposed and died pursuant to Art. IV, Sec. 10(c) of the California Constitution. There does not currently appear to be pending alternative legislation.

More specific to Blockchain, assembly member Ian Calderon submitted Assembly Bill 2658,[106] which expands the definition of electronic records and signatures—contained in the Uniform Electronic Transactions Act—to include records and signatures on the Blockchain, providing, "A record that is secured through Blockchain technology is an electronic record." The current law, provides that a "record or signature may not be denied legal effect or enforceability solely because it is in electronic form."[107] The proposed legislation would make a signature on a Blockchain legally enforceable.

---

[103] Jen Wieczner, *Inside New York's BitLicense Bottleneck: An 'Absolute Failure?'*, FORTUNE, May 25, 2018, http://fortune.com/2018/05/25/bitcoin-cryptocurrency-new-york-bitlicense/ (last accessed September 15, 2018).

[104] Press Release, DFS Grants Virtual Currency License to bitFlyer USA, Inc., Nov. 28, 2017 https://www.dfs.ny.gov/about/press/pr1711281.htm (last accessed June 13, 2018).

[105] *See generally* Cal. Assembly Bill 1123, https://legiscan.com/CA/bill/AB1123/2017 (last accessed June 13, 2018).

[106] *See generally* Cal. Assembly Bill 2658, https://legiscan.com/CA/text/AB2658/2017 (last accessed June 13, 2018).

[107] CAL. CIV. CODE § 1633.7.

c. Florida

Effective July 1, 2017, Florida's Money Laundering Act was expanded to expressly prohibit the laundering of virtual currency, which is defined as "a medium of exchange in electronic or digital format that is not a coin or currency of the United States or any other country."[108] The recent change is widely seen as a legislative response to a criminal decision of the Eleventh Judicial Circuit Court of Florida in a case entitled *Florida v. Espinoza*,[109] where the Court held that that bitcoin does not constitute a form of money within the confines of Florida's legal system.[110]

d. Washington

Although cryptocurrency is not an official medium of exchange, the State of Washington added virtual currencies, such as Bitcoin, to the definition of "Money Transmission."[111] As a result, all currencies and virtual currencies in Washington are subject to the Uniform Money Services Act.[112] Thus transmitters of virtual currency are required to be licensed in Washington.[113] Washington's Uniform Money Services Act has a number of exclusions to licensing. For example, governments, banks, and credit unions are generally not subject to the Act. Also excluded are certain payment processors, and designated contract market boards of trade and registered futures commission merchants under the CEA, among others.[114]

---

[108] FLA. STAT. ANN. § 896.101 (LexisNexis).

[109] *See* Order Granting Defendant's Motion to Dismiss the Information, Case No. F14-2923 (July 22, 2016).

[110] Stan Higgins, *In Rejecting Bitcoin as Money, Florida Court Sets Likely Precedent*, COINDESK, July 25, 2016, https://www.coindesk.com/court-reject-bitcoin-money-florida-espinoza-trial (last accessed June 13, 2018).

[111] WASH. REV. CODE ANN. § 19.230.010 (LexisNexis, Lexis Advance through 2018 c 6).

[112] *Id.*

[113] *Id.* § 19.230.005-19.230.905.

[114] *Id.* § 19.230.020.

e. The Uniform Regulation of Virtual-Currency Businesses Act

In 2017, the Uniform Law Commission completed the Uniform Regulation of Virtual-Currency Businesses Act (the "Uniform Act"), which provides a statutory framework for the regulation of companies engaging in "virtual-currency business activity." That is, exchanging, transferring, or storing virtual currency; holding electronic precious metals or certificates of electronic precious metals; or exchanging digital representations of value within online games for virtual currency or legal tender.[115]

The Uniform Act provides a three-tiered structure. Tier one is for persons that are exempt from regulation under the Act. Tier two is for providers that must register with the state. As the business successfully matures, reaching virtual-currency business activity levels greater than $35,000 annually, it would migrate to the third tier. The goal of the three-tier system is to provide a "regulatory sandbox" whereby companies' early stage of business development are allowed to focus on innovation and experimentation. The Uniform Act also exempts some forms of businesses already regulated by the federal government or by individual states. As well, the Uniform Act only regulates companies that assume control of a client's virtual currency. The term "control" is defined so businesses that do not have the requisite power over virtual currency are not required to obtain a license under the Uniform Act.[116]

The Uniform Act is designed to assure consumers of the safety and security of their virtual currency. For example, Section 501 of the Uniform Act sets forth the disclosures which licensees and provisional registrants must issue to potential customers to inform them about fees, any insurance coverage for the product or service, etc.[117] In addition, all virtual-currency businesses regulated by the Uniform Act must establish specific policies and compliance programs to guard against fraud, cyberthreats and terrorist activity.[118]

---

[115] Uniform Act § 102(25).
[116] *Id.* § 102(3).
[117] *Id.* § 501.
[118] *Id.* § 601.

The Uniform Act has been introduced in Connecticut,[119] Hawaii[120] and Nebraska.[121] As of the date of this article, no state has enacted the Uniform Act.

6. Outside the U.S.

a. Canada

In some ways, Canada has been at the forefront of international efforts to regulate cryptocurrency. To set the context, it is helpful to provide a brief description of Canada's legal system. Like the United States, Canada has a federal system of government, with subject-matter jurisdiction divided between the federal government and the governments of each of ten provinces. Nine of Canada's provinces use the English common law system for private law, while the Province of Québec uses a Civil Code system similar to that in effect in Louisiana.[122]

As outlined in the Constitution Act, 1867, the federal government has jurisdiction over the regulation of trade and commerce;[123] currency and coinage;[124] bills of exchange and promissory notes;[125] and legal tender.[126] The issuance of paper currency is handled by the Bank of Canada, which is Canada's central bank and which has many responsibilities similar to the U.S. Federal Reserve System. Each province has jurisdiction over property and civil rights in the province,[127] as well as "all matters of a merely local or private nature in the province."[128] Provincial jurisdiction over property and civil rights is broad. For example, the regulation of securities falls within provincial

[119] Uniform Regulation of Virtual-Currency Business Act, 2018 Bill Text CT H.B. 5496, 2005 Bill Text CT H.B. 549.

[120] 2017 Bill Text HI S.B. 2129.

[121] Uniform Regulation of Virtual-Currency Businesses Act., 2017 Bill Text NE L.B. 987.

[122] Canada also has a federal court system, but its jurisdiction is relatively narrow and is focused on matters such as taxation and admiralty law.

[123] CONSTITUTION ACT, 1867, 30 & 31 Vict., c. 3 (U.K.), s. 91(2).

[124] *Id.* at 91(14).

[125] *Id.* at 91(18).

[126] *Id.* at 91(20).

[127] *Id.* at 92(13).

[128] *Id.* at 92(16).

jurisdiction. Each province has its own securities regulator, and there is no federal securities regulator equivalent to the SEC.

Thus, it is apparent that different aspects of cryptocurrency can potentially fall into federal or provincial regulatory jurisdiction. To date, most regulatory efforts relating to cryptocurrency have been taken at the federal level. However, there has been no comprehensive approach. The response has been a somewhat *ad hoc* combination of cryptocurrency-specific measures, as described below, and attempts to analogize to existing statute law, much of which dates from the 19th century.

The issue of whether cryptocurrency is "money" is currently unclear in Canada, although it is possible to speculate based on existing sources of law.[129] For example, the issue of whether cryptocurrency is legal tender would be governed by the federal *Currency Act*.[130] While the *Act* does not define "money" (presumably because no one thought it necessary to do so when the predecessor legislation was drafted in 1870), it does provide that a payment of money is legal tender only if made in Bank of Canada notes or current coins. This strongly suggests that payment in cryptocurrency would not be considered legal tender.

The *Currency Act* also provides that contracts "relating to money" must be denominated in the currency of Canada or the currency of a country other than Canada.[131] Cryptocurrency is not issued by any country, which supports the view that it would not be considered "money" for the purposes of the *Currency Act*. However, a contract denominated in cryptocurrency, or for the purchase or sale of cryptocurrency, would seemingly still be an enforceable contract—just not a contract "relating to money." There is an element of circularity here which demonstrates that, in some ways, the existing legislative framework does not fit conceptually with cryptocurrency.

[129] For an excellent analysis of the issue of whether cryptocurrency is "money" in Canadian law, *see* S. Hoegner and J. Friedman "Canada" in S. Hoegner, Ed., THE LAW OF BITCOIN (Bloomington, Indiana: iUniverse, 2015).

[130] CURRENCY ACT, R.S.C. 1985, c. C-52.

[131] *Id.* at 13(1).

This circularity is also illustrated by the federal *Bills of Exchange Act*,[132] which governs negotiable instruments in Canada, and which has many similarities to Article 3 of the UCC. A bill of exchange is defined as an unconditional order in writing, addressed by one person to another, signed by the person giving it, requiring the person to whom it is addressed to pay a sum certain in money to order or to bearer.[133]

Again, there is no neat "fit" with cryptocurrency; a Bitcoin transaction does not involve a "promise to pay," as a Bitcoin transaction is simultaneously the instruction to pay; the payment; and the record of the payment made. Theoretically, a check or other instrument could be drawn payable in Bitcoin, but the issue would then be whether the Bitcoin amount was "a sum certain in money"; if Bitcoin is not money, then the instrument is not a bill of exchange.[134] Without a concrete definition of money, the existing legislative framework only goes so far in helping us to understand the legal and regulatory environment in Canada.

Case law is of similarly limited guidance. There are, as of June 2018, no Canadian case law specifically addressing the legal status of cryptocurrency.[135] Some commentators have pointed to obiter comments in the Supreme Court of Canada's 1938 *Alberta Reference*[136] as support for the proposition that cryptocurrency could be considered "money" in

[132] BILLS OF EXCHANGE ACT, R.S.C. 1985, c. B-4.

[133] *Id.* at 16(1).

[134] *Id.* at 16(2).

[135] There are some cases involving cryptocurrencies. For example, in *Arend v. Boehm*, 2017 ONSC 3424 (CanLII), the respondents to an application for an oppression remedy under the BUSINESS CORPORATIONS ACT unsuccessfully moved on the basis of forum non conveniens that Austria was a more appropriate forum to hear the disputes regarding their cryptocurrency business. The court held that, although the business was worldwide in scope, there was a real and substantial connection to Ontario so as to justify the court taking jurisdiction.

[136] Reference re Alberta Legislation, S.C.R. 100 (1983), *aff'd* (1939) A.C.117 (J.C.P.C.).

Canadian common law, despite not being legal tender, but that conclusion is questionable.[137]

With these points in mind, it is important to note that both the federal government and certain provinces have addressed cryptocurrency in the context of specific problems and concerns, such as anti-money laundering (AML) efforts and taxation. Canada was at the forefront of AML efforts involving cryptocurrency, and its AML measures directed at cryptocurrencies are considered by some to be the first national cryptocurrency law of any kind.[138] The federal government operates the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), which has a mandate broadly similar to FinCEN. FINTRAC assists in the detection, prevention and deterrence of money laundering and the financing of terrorist activities pursuant to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.[139]

In 2014, the federal government amended the *PCA* to extend its application to persons and entities that deal in virtual currencies.[140] Such persons and entities will (once certain further regulations are implemented)[141] be considered money services businesses[142] and will have to register with FINTRAC, implement compliance programs, keep and retain prescribed records, report suspicious or terrorist-related

[137] This contention is based on obiter comments of Duff, C.J., writing for two of the six justices on this point, observing that "Any medium which by practice fulfils the function of money and which everybody will accept in payment of a debt is money in the ordinary sense of the words even although it may not be legal tender" (*Id.* at 116).

[138] C. Duhaime, "Canada implements world's first national digital currency law; regulates new financial technology transactions" June 22, 2014 https://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/ (last accessed June 13, 2018).

[139] PROCEEDS OF CRIME (MONEY LAUNDERING) AND TERRORIST FINANCING ACT, S.C. 2000, c. 17 [hereinafter PCA].

[140] ECONOMIC ACTION PLAN 2014 ACT, NO. 1, S.C. 2014, c. 20.

[141] Though the law has received Royal Assent, the specific provisions dealing with it is not yet in force. The amendments will not come into force until subordinate regulations and guidance on the amendments and the regulations are issued.

[142] ECONOMIC ACTION PLAN 2014 ACT, NO. 1, *supra* note 140, s. 256(2).

property transactions, and determine if any of their customers are "politically exposed persons."[143] The law will also apply to virtual currency exchanges operating outside of Canada "who direct services at persons or entities in Canada."[144] The new amendments also prohibit banks from opening and maintaining accounts or having a "correspondent banking relationship" with companies dealing in virtual currencies, unless that person or entity is registered with FINTRAC.[145]

Similar to the IRS, the Canada Revenue Agency (CRA) issued an advisory stating that it views "digital currency" not as money, but as a commodity. Where digital currency is used to pay for goods or services, the rules for barter transactions apply. A barter transaction occurs when any two entities agree to exchange goods or services and carry out that exchange without using legal currency. The amount to be included would be the value of the goods or services in Canadian dollars. The tax rules relating to barter transactions apply to transactions involving digital currency.[146] The characterization of digital currency as a commodity also entails that any resulting gains or losses can be taxable income, or capital gains/losses, for the taxpayer.[147] If an employee receives digital currency as payment for salary or wages, the amount (in Canadian dollars) will be included in the employee's income for tax purposes.[148] Federal and provincial value-added taxes also apply to the fair market value of any goods or services purchased using digital currency.[149]

b. Québec and Bitcoin ATMs

Canada's constitutional division of powers confers regulation of property and civil rights within a province onto the provincial

---

[143] Duhaime, *supra* note 138.

[144] ECONOMIC ACTION PLAN 2014 ACT, NO. 1, *supra* note 140, s. 255(2).

[145] *Id.* at 258.

[146] https://www.canada.ca/en/revenue-agency/news/newsroom/fact-sheets/fact-sheets-2015/what-you-should-know-about-digital-currency.html (last accessed June 13, 2018).

[147] *Id.*

[148] INCOME TAX ACT, R.S.C., 1985, c. 1 (5th Supp.), s. 5(1).

[149] https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html (last accessed June 13, 2018).

legislature.[150] Under Québec's *Money-Services Businesses Act*,[151] businesses that provide money services for remuneration, which includes the operation of an automated teller machine, must hold a license issued by the Autorité des Marchés Financiers (AMF). On February 12, 2015, the AMF amended the Policy Statement to the *MSBA* to bring cryptocurrency ATMs and trading platforms within the ambit of the *MSBA*. As a result, businesses that operate a cryptocurrency ATM or trading platform will now be required to obtain a license from the AMF and comply with the verification, reporting and other requirements of the *MSBA*.[152]

c. Self-Regulation: the United Kingdom

While the United Kingdom's Financial Conduct Authority has issued consumer warnings in connection with ICOs (and reserves the right to regulate aspects of ICOs insofar as they involve arranging, dealing or advising on regulated financial investments), cryptocurrencies are currently unregulated in the UK.[153]

In February 2018, the formation of the UK's first trade association of cryptocurrency companies—CryptoUK—was announced, seeking to introduce self-regulation through a code of conduct. It is not yet clear what the FCA's response to self-regulation will be.[154]

---

[150] CONSTITUTION ACT, 1867 (Canada), *supra*, s. 92(13) [hereinafter MSBA].

[151] LOI SUR LES ENTREPRISES DE SERVICES MONÉTAIRES, LRQ 2010, c. 40, ann. I.

[152] A. Hodhod and P. Côté, *Operators of Virtual Currency ATMs and Trading Platforms in Québec must be Licensed*, April 16, 2015, http://blg.com/en/News-And-Publications/Publication_4086 (last accessed June 13, 2018).

[153] Financial Conduct Authority, STATEMENT: INITIAL COIN OFFERINGS, September 12, 2017, https://www.fca.org.uk/news/statements/initial-coin-offerings (last accessed June 13, 2018) [hereinafter FCA].

[154] J. Boldon, B. Loechner and K. Derrick, "Cryptocurrency: is UK regulation on the horizon?" THOUGHT LEADERSHIP, March 5, 2018, https://www.kennedyslaw.com/thought-leadership/article/cryptocurrency-is-uk-regulation-on-the-horizon (last accessed June 13, 2018).

Her Majesty's Treasury has announced plans to regulate traders of cryptocurrencies, forcing them to disclose their identities and to report suspicious activities. There have also been discussions at the EU level regarding amending Anti-Money Laundering and Terrorist Financing regulations to extend these to virtual currencies in 2018.[155] On February 22, 2018, the House of Commons Treasury Committee announced an inquiry into cryptocurrencies and Blockchain technology, due to "market volatility, money laundering and cybercrime."[156] This will likely serve as a foundation for future government regulation; the Governor of the Bank of England, Mark Carney, foreshadowed as much in a March 2018 speech to the Scottish Economics Conference.[157]

d. Narrow Regulatory Regime (Anti-Money Laundering): the Example of Australia

In April 2018, the Commonwealth of Australia introduced its own regulatory regime respecting cryptocurrency exchanges. Under amendments to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*,[158] which bear some similarity to the Canadian enactments, a "digital currency" is defined as:

> (a) a digital representation of value that:
>
> (i) functions as a medium of exchange, a store of economic value, or a unit of account; and
>
> (ii) is not issued by or under the authority of a government body; and

[155] *Id.*
[156] *Id.*
[157] B. Chu, "Cryptocurrency exchanges to face regulatory clampdown, says Bank of England's Mark Carney" THE INDEPENDENT, March 2, 2018 https://www.independent.co.uk/news/business/news/url-cryptocurrency-bitcoin-regulation-trading-uk-mark-carney-bank-of-england-clampdown-a8236066.html (last accessed June 13, 2018).
[158] ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING ACT 2006 (Australia), C2006A00169, as amended and in force 29 May 2018 (C2018C00194) [hereinafter AML/CTF Act].

(iii) is interchangeable with money (including through the crediting of an account) and may be used as consideration for the supply of goods or services; and

(iv) is generally available to members of the public without any restriction on its use as consideration; or

(b) a means of exchange or digital process or crediting declared to be digital currency by the AML/CTF Rules [legislative instruments promulgated under the *AML/CTF Act*[159]];

but does not include any right or thing that, under the AML/CTF Rules, is taken not to be digital currency for the purposes of the *AML/CTF Act*.[160]

The *AML/CTF Act* also provides for the Digital Currency Exchange Register, maintained by the Australian Transaction Reports and Analysis Centre (AUSTRAC).[161] Any entity which exchanges digital currency for money (whether Australian or not), or vice-versa, where the exchange is provided in the course of carrying on a digital currency exchange business,[162] must be registered with AUSTRAC[163] and must comply with the AML/CTF Rules. These include requirements that cryptocurrency exchanges "collect information to establish a customer's identity, monitor transactional activity, and report to AUSTRAC transactions or activity that is suspicious or involves large amounts of cash over $10,000" in Australian funds.[164]

[159] *Id.* at 229(2).
[160] *Id.* at 5.
[161] *Id.* at 76B(1).
[162] *Id.* at 6, Table 1, item 50A.
[163] *Id.* at 76A(1).
[164] Jessica Yun, "AUSTRAC begins oversight of cryptocurrency" INVESTOR DAILY, April 12, 2018, https://www.investordaily.com.au/regulation/

e. Broader Regulatory Regime (Consumer Protection): the Example of Japan

In April 2017, Japan enacted amendments to its *Payment Services Act*[165] which introduced a fairly comprehensive regulatory regime for cryptocurrency. Under the amendments, businesses dealing in "Virtual Currency Exchange Services" (VCE Services) must register with Japan's Financial Services Agency (FSA). VCE Services include:

(i) Purchase and sale of cryptocurrencies, or exchange for other cryptocurrencies;

(ii) Intermediary, brokerage or agency for (i); and,

(iii) Management of cash or cryptocurrencies in relation to (i) and (ii).[166]

VCE Service providers must comply with operational rules made pursuant to the *Payment Services Act*, which include the following:

- The VCE Service provider must segregate customers' cash from its own by placing customers' cash into a separate bank account or a trust;
- The VCE Service provider must segregate customers' cryptocurrency from its own, such that customers' cryptocurrency is immediately identifiable;
- The above segregation of cash and cryptocurrency must be audited by a certified accountant or auditing firm at least once per year;

42839-crypto-exchanges-now-regulated-by-austrac (last accessed June 13, 2018).

[165] PAYMENT SERVICES ACT, Act No. 59 of June 24, 2009, as amended April 1, 2017.

[166] Masahiko Ishida, Edward Mears and Ryutaro Takeda, "Japan Regulatory Update on Virtual Currency Business" FINANCIAL REGULATORY ALERT, December 29, 2017, https://www.dlapiper.com/en/japan/insights/publications/2017/12/japan-regulatory-update-on-virtual-currency-business/ (last accessed June 13, 2018).

- The VCE Service provider must notify the customer that his or her cryptocurrency is not considered Japanese or foreign currency and that a risk of loss that may result from fluctuations in cryptocurrency value;

- Before a customer conducts a transaction or enters into an agreement for VCE Services, the VCE Service provider must disclose information to the customer concerning its corporate registration, the substance of the transaction(s), information regarding each cryptocurrency handled by the VCE Service provider, and information regarding how the VCE Service provider segregates customers' cash and cryptocurrency from its own; and,

- The VCE Service provider must also provide the FSA with periodic reports regarding its VCE Services, and comply with KYC requirements.[167]

f. State Fiat Cryptocurrencies: Venezuela and (possibly) Russia

The Republic of Venezuela has taken a different approach, by introducing the Petro (short for *Petromoneda*), a cryptocurrency that is: (i) issued by a central authority (*i.e.*, the government itself); and, (ii) explicitly backed by the country's oil reserves. Venezuela's socialist economy has declined significantly over the last several years, and the value of its government-issued fiat currency has been eroded by hyperinflation. In December 2017, the government introduced the Petro as the world's first "fiat cryptocurrency," built on the Ethereum Blockchain, and set an ICO to begin in March 2018.[168] In theory, one

[167] *Id.*

[168] Jon Markman, "This Is Why The Venezuela Cryptocurrency Matters" *Forbes*, March 20, 2018, https://www.forbes.com/sites/jonmarkman/2018/03/20/this-is-why-the-venezuela-cryptocurrency-matters/ (last accessed June 13, 2018).

Petro coin was backed by one barrel of crude from Venezuela's Orinoco oil belt.[169]

In introducing the Petro, Venezuelan president Nicolas Maduro claimed that it could "take on Superman."[170] But not, it seems, U.S. President Donald Trump, who issued an Executive Order on March 19, 2018 which prohibits U.S. citizens from owning or transacting in the Petro, on the basis that these acts violate existing U.S. sanctions on Venezuela.[171]

Venezuela is not the only nation to pursue a government-issued cryptocurrency. The Russian Federation, also the subject of U.S. sanctions, is developing its own fiat-digital coin, the CryptoRuble.[172] In January 2018, the *Financial Times* reported that Sergei Glazyev, Vladimir Putin's chief financial adviser, had told a government meeting that such a cryptocurrency would allow the Russian government to make and receive payments with counterparties worldwide, irrespective of sanctions,[173] a conclusion which may no longer follow in view of President Trump's Executive Order in respect of the Petro.

It remains to be seen whether fiat cryptocurrencies will gain traction; one of the perceived benefits of open-source cryptocurrencies has been the lack of any central regulatory authority, which is perceived to offer anonymity while also preventing price or supply manipulation by a central bank or similar entity.

g. Banning Cryptocurrencies, ICOs and Cryptomining: the Example of China

In February 2018, western media outlets reported that the People's Republic of China was poised to increase regulations banning ICOs and cryptocurrency exchanges, and that steps were being taken to

---

[169] *Id.*

[170] *Id.*

[171] TAKING ADDITIONAL STEPS TO ADDRESS THE SITUATION IN VENEZUELA (Executive Order 13827), 83 FR 12469 (FR Doc. Number: 2018-05916).

[172] Markman, *supra* at 168.

[173] *Id.*

end all cryptocurrency trading entirely.[174] China also blocked Internet access to cryptocurrency exchange and ICO websites,[175] and went so far as to ask local governments to make an "orderly exit" from the Bitcoin mining industry.[176] Huobi and OKEX, formerly two of the largest cryptocurrency exchanges in the Chinese market, promptly relocated to Hong Kong and continued operations.[177]

III.
CRYPTOCURRENCY—SPECIFIC RISKS & LOSS SCENARIOS

Cryptocurrencies are not immune to loss. Bitcoin owners have sustained losses, primarily through the theft and fraudulent use of private keys, but also though numerous other forms as described below. They will continue to sustain losses so long as the currency has value. It is not always the actual cryptocurrency software or platform that is insecure; the vulnerabilities lie in the layers of software that are built on top of the platform. Fraudsters hack into the system using various methods and steal cryptocurrencies, often cleaning out a company's accounts and customers' coins. Cryptocurrency theft represents an extensive and significant threat, with approximately $1.36 billion lost to scammers during the first two months of 2018.[178] Some of the more prevalent ways in which cryptocurrency losses arise are discussed below.

---

[174] Sara Hsu, "China Serious About Ending ICOs, Cryptocurrency Exchanges" *Forbes*, February 7, 2018, https://www.forbes.com/sites/sarahsu/2018/02/07/china-serious-about-ending-icos-cryptocurrency-exchanges/ (last accessed June 13, 2018).

[175] David Meyer "China Enlists Its 'Great Firewall' to Block Bitcoin Websites" *Fortune*, February 5, 2018, http://fortune.com/2018/02/05/bitcoin-china-website-ico-block-ban-firewall/ (last accessed June 13, 2018).

[176] Hsu, *supra* note 174.

[177] Joseph Young, "Despite Crackdown on Trading, Crypto and Blockchain in China Are Alive" *CoinTelegraph,* March 7, 2018, https://cointelegraph.com/news/despite-crackdown-on-trading-crypto-and-blockchain-in-china-are-alive (last accessed June 13, 2018).

[178] Kai Sedgwick. $9 million a Day is Lost in Cryptocurrency Scams, March 2, 2018, https://news.bitcoin.com/9-million-day-lost-cryptocurrency-scams/ (last accessed June 13, 2018).

A. Wallet Vulnerabilities

Bitcoin wallets are simply a means of storing Bitcoin keys. The wallets can be stored offline and kept separate from the Internet, or they can be stored online. When the wallet exists online, the security of Bitcoin is only as good as the security of the online wallet service. Wallets are frequently the target of hacking attacks. In some cases, wallets have been compromised through computer intrusions.

A combination of Bitcoin's price hike and increased speculation in cryptocurrencies means that there are more online accounts available with a lot more value in them. This makes customer accounts on exchanges and trading platforms particularly attractive targets. Bad actors are selling access to these accounts online, including on criminal forums and on paste sites. How do they gain customer account details? Through phishing and credential stuffing—techniques that have served them well in other criminal activity.[179] Unlike banking institutions that can provide FDIC insurance on deposits up to $250,000, there are no such safeguards provided to digital wallets.[180]

1. Phishing

Industry experts estimate that over $225 million in cryptocurrencies were lost to phishing in 2017. The goal in a phishing attack is to gain access to a user's cryptocurrency wallet credentials, which will then allow the attacker to steal the cryptocurrency available in the wallet in a matter of seconds.[181] In the case of phishing, attackers send fraudulent emails to users that may include a link to a scam page

[179] Alastair Paterson, *Cryptocurrency Fraud: In the Midst of a Gold Rush, Beware of Scammers*, February 22, 2018, https://www.securityweek.com/cryptocurrency-fraud-midst-gold-rush-beware-scammers (last accessed June 13, 2018).

[180] Kevin LaCroix, *Why the Crypto-Enforcement Onslaught by U.S. Regulators Has Just Begun*, THE D&O DIARY, June 3, 2018, https://www.dandodiary.com/2018/06/articles/cyber-liability/guest-post-crypto-enforcement-onslaught-u-s-regulators-just-begun/ (last accessed June 13, 2018).

[181] Comodo, *Bitcoin Under Attack: Comodo Stops Cunning Spear-Phishing Attack on a Cryptowallet Owner*, February 6, 2018, https://blog.comodo.com/comodo-news/bitcoin-phishing-attack-on-cryptowallet-owner/ (last accessed June 13, 2018).

that asks them to input their user name and password before redirecting them to the actual site. They may also use typosquatting to imitate the official domain, or spoof pages on social media to capture their credentials.[182]

One particular phishing scam involved leading users to websites impersonating blockchain.info, a popular online wallet service. Security experts reported in February 2018 that the group behind this specific attack stole $50 million in cryptocurrency over a three-year period.[183]

Another phishing scam involved myetherwallet.com, an online wallet service used for storing the cryptocurrency Ethereum. This phishing email directed recipients to follow a link in order to install an alleged new update for the site. In reality, the link took users to a spoofed website that appeared to be the legitimate page. The phishing site used a typosquatting technique to imitate the official website by replacing the "t" with a (ț)—a letter from the Romanian alphabet. After users entered their credentials on the impersonated site, the criminals would use those credentials to access the users' wallets and steal their Ethereum coins.[184] In addition to email methods, fraudsters also use social media to create spoofed profiles that imitate cryptocurrency exchanges, hoping to trick users into providing their account credentials associated with the legitimate site.[185]

In other instances, wallets are compromised through social engineering attacks. In the case of Inputs.io, a company that used to store bitcoins in digital wallets for people across the globe, the fraudster posed as someone else using email and gained access to the website's systems

[182] *Cryptocurrency Fraud: In the Midst of a Gold Rush, Beware of Scammers*, February 22, 2018, https://www.securityweek.com/cryptocurrency-fraud-midst-gold-rush-beware-scammers (last accessed June 13, 2018).

[183] Stan Higgins, *Cisco: Bitcoin Phishing Scam Bagged $50 Million Over 3 Years*, COINDESK, February 15, 2018, https://www.coindesk.com/cisco-50-million-bitcoin-phishing-scam-mimicked-blockchain-web-wallet/ (last accessed June 13, 2018).

[184] Digital Shadows, supra note 4 at 6.

[185] *Id.* at 7.

on the cloud-hosting provider. The password was reset by the thief and the bitcoins disappeared.[186]

Fraudsters have gone so far as to create scam wallet services, which lured customers by promising desirable services such as greater transaction anonymity. As long as the deposit remains small, the scammers do not touch the currency, but if the wallet balance increases to a certain threshold, the scammers move the cryptocurrency from the customer's wallet into their own wallet. It has been reported that users of certain wallet services have been targeted by this type of scam.[187]

2. Loss or Destruction of Private Key

Another disadvantage of cryptocurrencies like Bitcoin is that, although the cryptography preventing double spending is robust, the currency is not safe from theft and manipulation through other avenues. Considering that ownership of bitcoins consists of the combination of public and private keys which are stored in wallets, bitcoins can be stolen from compromised wallets. The dubious honor of being the first victim of a hack involving bitcoins goes to a user by the name of "Allinvain." In June 2011, Allinvain claimed that 25,000 bitcoins were stolen from his/her wallet after hackers compromised Allinvain's computer.[188] The thieves responsible for the Coincheck heist, discussed further below, reportedly used private keys to steal the coins from users' wallets.[189]

The fact that Bitcoin and other decentralized cryptocurrencies rely on a private key to prove ownership means that the currency units

---

[186] Adam Stier, *Bitcoin Where Did They All Go?*, LIBERTY VOICE (5 March 2014) http://guardianlv.com/2014/03/bitcoin-where-did-they-all-go/ (last accessed June 13, 2018).

[187] Marie Vasek and Tyler Moore, "There's no free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams" at 9 http://lyle.smu.edu/~tylerm/fc15.pdf (last accessed June 13, 2018).

[188] Alex Hern, *A history of bitcoin hacks*, THE GUARDIAN, March 18, 2014, http://www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency (last accessed June 13, 2018).

[189] Mike Orcutt, *What the Coincheck Hack Means for the Future of Blockchain Security*, MIT TECHNOLOGY REVIEW, February 1, 2018, https://www.technologyreview.com/s/610092/what-the-coincheck-hack-means-for-the-future-of-blockchain-security/ (last accessed June 13, 2018).

can be lost if the private key is lost. For example, in 2010, a user known as "stone man" claimed to have lost his entire Bitcoin savings when he failed to properly back up his wallet. Inasmuch as "stone man" self-reported, his loss and surrounding have not been independently verified. When his wallet was lost, so were the 8,999 bitcoins in his wallet.[190] Similarly, in late 2013, a British man claimed to have thrown out a hard drive that had 7,500 bitcoins on it, worth over $7.5 million at the time. He had purchased the bitcoins for almost nothing in 2009. He says he likely threw out the hard drive sometime over the summer, and only recently remembered that he had stored the coins on his computer.[191]

3. Hardware / Software Vulnerabilities

A hardware wallet designed to store crypto-currencies, and touted by its manufacturer as tamper-proof, was recently hacked by a British 15-year-old. Saleem Rashid said he had written code that gave him a back door into the Ledger Nano S, a $100 device that has sold millions around the world. It would allow a malicious attacker to drain the wallet of funds, he said. The firm behind the wallet said that it had issued a security fix. Hardware wallets store these private keys and can be connected to a PC via a USB port. One significant limitation for the method discovered by the teenager is that the attacker would need physical access to a wallet before it got into the hands of the victim—so, for instance, by buying one, altering it and then selling it on eBay or a similar online site. In this particular case, it was discovered that anyone with physical access could modify the Ledger hardware wallet to gain access to funds. In effect, this would mean that someone selling this hardware wallet would be able to steal funds from their customers. A few weeks later, Ledger confirmed that a separate flaw made its wallets susceptible to another attack in which malware could trick users into unknowingly sending their crypto-currency to hackers.[192]

---

[190] Stier, *supra*, note 186.

[191] *Id.*

[192] BBC Technology, *Teenager Hacks Crypto-currency Wallet*, BBC NEWS, Mar. 21 2018, https://www.bbc.com/news/technology-43489404 (last accessed June 13, 2018). The teen shared the code with the manufacturer.

B. Compromised Exchanges

There have been instances where ventures purporting to be Bitcoin exchanges proved to be simply short-lived scams. These scams, which include BTC Promo, btcQuick, and CoinOpend, lured their victims by offering features that many other exchanges did not offer, such as PayPal/Credit Card processing or attractive exchange rates. Often the exchanges never fully launched. Rather, they existed just long enough to receive funds from the victims, but never delivered the bitcoins to the customers.[193] As cryptocurrencies have matured and customers have grown in sophistication, fraudulent exchange services have become less common.

In place of fraudulent exchange services, a new concern regarding the security of online wallets and cryptocurrency exchanges has arisen. The following examples illustrate how exchanges often lack basic security measures and are susceptible to attacks. This ultimately calls into question the purported security underlying cryptocurrency as a whole.[194]

1. Exchange Hacks—Mt. Gox, Coincheck

Cryptocurrency exchanges are routinely targeted by cyber criminals, a trend expected to intensify as cryptocurrencies rise in value. The largest theft to date involved Coincheck, a Japanese cryptocurrency exchange that lost $534 million of virtual coins to hackers in January 2018. On January 28, 2018 at 2:57 a.m. local time in Tokyo, attackers hacked into Coincheck's digital wallet and withdrew over $530 million of NEM coins.[195] The technical details as to how Coincheck's site was infiltrated remain unclear, but it is likely due to the "hot" nature of the

[193] Ben Doernberg, *Why Are There So Many Bitcoin Scams?*, COIN CENTER, June 9, 2015, https://coincenter.org/2015/06/why-are-there-so-many-bitcoin-scams/ (last accessed June 13, 2018).

[194] Orcutt, *supra* note 189.

[195] Yuji Nakamura & Andrea Tan, *Massive Cryptocurrency Heist Spurs Call for More Regulation*, BLOOMBERG, Jan. 28, 2018, https://www.bloomberg.com/news/articles/2018-01-28/massive-cryptocurrency-heist-puts-spotlight-on-exchange-security (last accessed June 13, 2018).

users' accounts.[196] Coincheck managed users' funds in a "hot wallet" (i.e., connected to, and accessible through, the internet).[197] Having funds in a hot wallet allowed for much faster transfers in comparison to funds stored in a "cold wallet" (i.e., offline storage). In the course of its marketing efforts, Coincheck focused on the convenience, speed and usability of its platform.[198] Commentators have asserted that Coincheck failed to implement basic security measures, and attribute the breach to this deficiency.[199]

Since the attack in January 2018, Coincheck has reportedly cut back on the use of hot wallets and now keeps more users' funds in cold wallets.[200] Coincheck resumed operations and reportedly refunded $430 million to the affected users.[201] Additionally, in March 2018, Coincheck came under new ownership and has reportedly devoted a large amount of

[196] *The Coincheck Hack and the Issue with Crypto Assets on Centralized Exchanges*, REUTERS, Jan. 29, 2018, https://www.reuters.com/article/us-japan-cryptocurrency-q-a/the-coincheck-hack-and-the-issue-with-crypto-assets-on-centralized-exchanges-idUSKBN1FI0K4 (last accessed June 13, 2018).

[197] *Coincheck Cryptocurrency Hack: Everything you Need to Know*, REUTERS, Jan. 29, 2018, http://fortune.com/2018/01/29/coincheck-japan-nem-hack/ (last accessed June 13, 2018).

[198] Elaine Ramirez, *Is Japan Still Asia's Crypto Haven After Coincheck Heist? Probably Not*, FORBES, May 10, 2018, https://www.forbes.com/sites/elaineramirez/2018/05/10/is-japan-still-asias-crypto-haven-after-coincheck-heist-probably-not/#37fc2986258e (last accessed June 13, 2018).

[199] Orcutt, *supra* note 189.

[200] Taiga Uranaka & Thomas Wilson *Japan Punishes Seven Cryptocurrency Exchanges over Regulatory Lapses*, REUTERS, Mar. 7, 2018, https://www.reuters.com/article/us-crypto-currencies-japan-announcement/japan-punishes-seven-cryptocurrency-exchanges-over-regulatory-lapses-idUSKCN1GK05Y (last accessed June 13, 2018).

[201] Ramirez, *supra* note 198.

capital to improve security.[202] In May 2018, Coincheck was reported to be planning its comeback, including expansion to the United States.[203]

Another recent instance of a compromised cryptocurrency exchange involves Bitfinex. In August 2016, Bitfinex reported that almost 120,000 bitcoins were stolen from users' accounts, which at the time equated to $72 million and today would come close to $1 billion.[204] Notably, the impacted user accounts at Bitfinex were protected with multi-signature authentication, widely considered a valuable security measure, and one missing in the case of Coincheck.[205] Fraudsters were nonetheless able to gain access to the authentication keys and drain bitcoin from users' accounts to an unknown address.[206]

Mt. Gox represents one of the earliest and perhaps most infamous example of a targeted exchange hack. Mt. Gox previously held the title of being the largest Bitcoin exchange in the world. In 2011, a hacker compromised a user's account on the site and then effected a massive sale of bitcoins, which at the time, caused the price of Bitcoin to plunge from $32 per coin to mere pennies per coin. In total, the attacker allegedly stole over 800,000 bitcoins during a prolonged attack that spanned years.[207]At the time, the stolen bitcoin were valued around $460 million. Mt. Gox initially rebound from the incident but, by February 2014, Mt. Gox had filed for bankruptcy protection. Mt. Gox's CEO reportedly stated that technical issues had opened the door for the fraudulent withdrawals.

---

[202] Yuji Nakamura et al, *Biggest Hacking Victim Plots a U.S. Comeback*, BLOOMBERG, May 17, 2018, https://www.bloomberg.com/news/articles/2018-05-17/crypto-s-biggest-hacking-victim-plots-a-comeback-in-u-s-japan (last accessed June 13, 2018).

[203] *Japanese Cryptocurrency Exchange Coincheck Is Plotting Its Comeback*, BLOOMBERG, May 18, 2018, http://fortune.com/2018/05/18/japan-coincheck-matsumoto/ (last accessed June 13, 2018).

[204] Sean Williams, *The Biggest Cryptocurrency Hacks in History*, MOTLEY FOOL, May 9, 2018, https://www.fool.com/investing/2018/05/09/the-biggest-cryptocurrency-hacks-in-history.aspx (last accessed June 13, 2018).

[205] Orcutt, *supra* note 189.

[206] Williams, *supra* note 204.

[207] *Id.*

Threats to exchanges continue to persist. As recently as April 2018, Japanese exchange Binance was forced to issue a statement reassuring users that their accounts were secure amidst rumors of a compromise.[208] Additionally, in June 2018, a cryptocurrency exchange based in South Korea, Coinrail, reported that it suffered a security breach which resulted in hackers stealing roughly 30 per cent of Coinrail's vault containing primarily lesser-known cryptocurrencies.[209] Coinrail did not immediately disclose the value of the stolen coins, though some reports claimed the amount exceeded $40 million.[210] In the days following the Coinrail attack, the price of bitcoin dropped by 7 per cent and commentators claimed that nearly $30 billion in cryptocurrency wealth was lost.[211]

2. Credential Stuffing

Another threat to trading platforms and cryptocurrency exchanges is credential stuffing. Credential stuffing is a type of brute-force cyberattack whereby large sets of credentials are automatically inserted into login pages until a match with an existing account is found.[212] The stolen account credentials typically consist of lists of usernames and/or email addresses and the corresponding passwords. Rather than manually entering each individual credential set, criminals can automatically inject stolen username and password combinations into a login portal in order to fraudulently gain access to a user's account. The

---

[208] Sam Bourgi, *Binance Denies Being Hacked*, *as CEO Confirms "All Funds are Safe"* March 8, 2018, https://hacked.com/binance-denies-being-hacked-as-ceo-confirms-all-funds-are-safe/ (last accessed June 19, 2018).

[209] Daniel Shane, *Bitcoin Price Plunges Following Coinrail Exchange Hack*,, CNN MONEY, June 11, 2018, http://money.cnn.com/2018/06/11/investing/coinrail-hack-bitcoin-exchange/index.html (last accessed June 19, 2018).

[210] Jon Russell, *Korean Crypto Exchange Coinrail Loses over $40M in Tokens Following a Hack*, June 10, 2018, https://techcrunch.com/2018/06/10/korean-crypto-exchange-coinrail-loses-over-40m-in-tokens-following-a-hack/ (last accessed June 13, 2018).

[211] Shane, *supra* note 209.

[212] Dave Lewis, *How Hackers Become You with Credential Stuffing*, FORBES, Dec. 4, 2017, https://www.forbes.com/sites/davelewis/2017/12/04/how-hackers-become-you-with-credential-stuffing/#7699c28437d1 (last accessed June 13, 2018).

logic behind this common practice relates to the fact that individuals often use the same passwords for various websites, accounts or services.[213] Consequently, if fraudsters have legitimate credentials from one site, those same credentials are likely to have been used on other sites or accounts.[214]

To illustrate the widespread and extensive practice of credential stuffing, consider the following recent reports. A Fortune 100 company reported that cybercriminals had made over 5 million login attempts using hundreds of thousands of proxies in just one week's time. Similarly, a large retailer experienced over 10,000 login attempts during a single day.

Stolen credentials are not difficult to find online. Occasionally, hackers simply dump all the information on the Internet and it becomes available to the public at large. In addition, there are several credential stuffing tools in circulation such as SentryMBA, Vertex, and Account Hitman. These tools are typically sold on forums, social media or online marketplaces. In fact, numerous marketplaces on the dark web are devoted exclusively to the sale of credentials. The widespread availability of credential harvesting websites and credential stuffing tools lowers the barrier to entry for cybercriminals lacking more technical skills,[215] thereby making this attack methodology an easy and effective option for just about anyone with basic technical knowledge.[216]

3. Rogue Employees

In April 2018, it was reported that an employee of Coinsecure, one of India's largest cryptocurrency trading platforms, claimed to have

---

[213] Shane Chambers, *Credential Stuffing*, Nov. 10, 2017, https://www.techguard.ie/blog/credential-stuffing/ (last accessed June 13, 2018).

[214] Lewis, *supra* note 212.

[215] Sean Michael Kerner, *Sentry MBA Uses Credential Stuffing to Hack Sites*, EWEEK, Mar. 9, 2016, http://www.eweek.com/security/sentry-mba-uses-credential-stuffing-to-hack-sites (last accessed June 19, 2018).

[216] Kevin Townsend, *Credential Stuffing: A Successful and Growing Attack Methodology*, SECURITY WEEK, Jan. 17, 2017, https://www.securityweek.com/credential-stuffing-successful-and-growing-attack-methodology (last accessed June 13, 2018).

"lost" about 438 bitcoins while he was extracting the coins to distribute to customers. Coinsecure issued statements advising that the trading system had not been hacked or compromised, but that the funds had been "exposed and seemed to have been siphoned out to an address that is outside our control."[217]

C. Initial Coin Offerings

1. Manipulation of ICOs

Reports claim that ICO fundraising surpassed $5 billion in 2017.[218] As consumers rush to be the first to invest in a promising new cryptocurrency, their investments can instead go into the account of criminals. Consider the case of CoinDash, which is regarded as the first known breach of an ICO.[219] CoinDash is an Israeli startup which launched an ICO in July 2017 selling its own digital tokens in exchange for the cryptocurrency Ethereum.[220] The token sale began at 9:00 am on July 17, 2017. Within 13 minutes, a bad actor had hacked CoinDash's website and changed the address for sending Ethereum investments to a fake address controlled by the attacker.[221] By the time CoinDash discovered what happened and shut the site down, more than $7 million in investments had been diverted to the attacker over the course of about

[217] Anto Antony & Archana Chaudhary, *Bitcoins Worth $3M Stolen from India's Cryptocurrency Trading Platform Coinsecure*, INSURANCE JOURNAL, Apr. 13, 2018, https://www.insurancejournal.com/news/international/2018/04/13/486382.htm (last accessed June 13, 2018).

[218] Kate Rooney, *U.S. Regulator Warns of 'Pump-and-Dump' Cryptocurrency Frauds*, CNBC, Feb. 15, 2018, https://www.cnbc.com/2018/02/15/u-s-regulator-warns-of-pump-and-dump-cryptocurrency-frauds.html (last accessed June 13, 2018).

[219] Jen Wieczner, *Hackers Just Stole $7 Million in a Brazen Ethereum Cryptocurrency Heist*, FORTUNE, July 18, 2017, http://fortune.com/2017/07/18/ethereum-coindash-ico-hack/ (last accessed June 18, 2018).

[220] *Id.*

[221] *Id.*

a half an hour.[222] Even before the CoinDash hack, research estimated that up to $400 million has been stolen by targeting ICOs.[223]

Interestingly, on September 19, 2017, the attacker reportedly transferred 10,000 Ethereum tokens to CoinDash's Ethereum wallets, which at that time equated to roughly $3 million. Then, on February 23rd, 2018, the attacker returned an additional 20,000 Ethereum tokens to CoinDash's wallet, which then was valued at $17 million.[224]

2. Exit Scams

Although CoinDash was a legitimate ICO whose system was compromised by cybercriminals, there are numerous examples of criminals creating entirely fictitious cryptocurrencies and performing exit scams. Exit scams are confidence schemes whereby an established business ceases to provide its goods or services, but continues to accept payment for new orders for its product.

For example, Confido is a cryptocurrency startup that touted itself as developing "smart contracts" to act as an escrow between a buyer and seller in the course of a transaction. The smart contracts would supposedly be fulfilled when both sides had met particular conditions, thereby removing the need for a traditional third party escrow agent. Confido's ICO took place in November 2017 through TokenLot, a platform that facilitated the fundraising, and a total of $375,000 was raised. Investors were given "contract for differences" tokens, which at one point traded for as much as $1.20 per token. However, just a few weeks after the ICO, the company founders disappeared with the funds and the value of the coins then plunged to around 2 cents. TokenLot thereafter released a statement claiming the Confido founders had "pulled an exit scam." In the days that followed, all online assets related

[222] Alexandria Arnold, *CoinDash Says Hacker Stole $7 Million at Initial Coin Offering*, BLOOMBERG, July 17, 2017, https://www.bloomberg.com/news/articles/2017-07-17/coindash-says-hacker-stole-7-million-at-initial-coin-offering (last accessed June 13, 2018).

[223] Digital Shadows, *supra* note 4 at 16.

[224] Samuel Haig, *Hacker Returns 20,000 ETH to Coindash*, Feb. 25, 2018, https://news.bitcoin.com/hacker-returns-20000-eth-coindash/ (last accessed June 13, 2018).

to the founders and company had been deleted and the company's website, Twitter account and Facebook page were all erased.[225]

The popularity of exit scams in the ICO context can be seen not only on criminal forums and the dark web, but also on freelance job sites which have had posts where individuals are seeking assistance in cloning specific exchange sites or creating new cryptocurrencies.[226]

3. Pump and Dumps

The emergence of ICOs in recent years has also brought with it the threat of "pump and dump" schemes. In this scenario, investors in a new unknown cryptocurrency use social media platforms, messaging boards and fake news reports to advertise the coin and grow hype with the public in order to artificially inflate the price of the offering.[227] Once the coin reaches the desired price point, the group then sells all of its coins, leaving those who bought in with coins that are virtually worthless.

The prevalence of pump and dump scheme has garnered the attention of the CFTC and the Financial Industry Regulatory Authority ("FINRA"), with both entities warning investors to be skeptical about social media tips and claims of unrealistic returns in the context of ICOs.[228] Similarly, the SEC has cautioned investors considering ICOs that "experience shows that excessive touting in thinly traded and volatile markets can be an indicator of 'scalping,' 'pump and dump' and other manipulations and frauds."[229]

---

[225] Arjun Kharpal, *Cryptocurrency Start-Up Confido Disappears with $375,000 from an ICO, and Nobody Can Find the Founders*, CNBC, Nov. 21, 2017, https://www.cnbc.com/2017/11/21/confido-ico-exit-scam-founders-run-away-with-375k.html (last accessed June 13, 2018).

[226] Digital Shadows, *supra* note 4 at 17.

[227] Paterson, *supra* note 179.

[228] Rooney, *supra* note 218.

[229] SEC December Statement, *supra* note 45.

D. Cryptojacking / Mining Botnets

Successful cryptocurrency mining is a resource-intensive venture. The more computing resources a miner has, whether in terms of more computers or more computations per second, the greater the odds are that the miner will be the first to confirm a transaction and reap a reward.[230] Unscrupulous miners have attempted to illicitly use other persons' computers to perform mining operations. Illicit mining can either be carried out by authorized computer users employing them for unauthorized uses (such as the engineers at Russia's top nuclear research facility who were reportedly detained after they attempted to mine bitcoin on the facility's supercomputers),[231] or through cryptojacking. Cryptojacking occurs when an outside attacker secretly uses the victim's computer resources to mine cryptocurrencies. Since the middle of 2017, Internet browsers, browser extensions, and mobile apps have all been used to spread "Coinhive," a Javascript miner for Monero. Coinhive originated as a tool designed to allow developers to mine Monero using their Web browsers, but it was quickly adopted by malicious actors.

Cryptojacking was the biggest growth area in cybercrime in 2017, with antivirus detections increasing by 8,500 per cent. Between the months of September and December 2017, mining malware detection figures went from numbering in the tens of thousands skyrocketing to the millions. In fact, there were more than 8 million mining events blocked by Symantec in December 2017 alone. Mining activity is strongly linked to the increase in value of many cryptocurrencies; a sustained drop in their value may lead to this activity decreasing in prevalence just as quickly as it escalated.[232]

Cybercriminals who do not have ready access to a supercomputer develop "botnets" which are small programs that work in

---

[230] *See* discussion at § II.D.2. *supra*.

[231] Agence France-Presse, *Russians arrested for 'mining bitcoin' at nuclear facility*, GUARDIAN, March 4, 2018, https://www.theguardian.com/world/2018/feb/10/russians-arrested-for-mining-bitcoin-at-nuclear-facility (last accessed June 13, 2018).

[232] Symantec, INTERNET SECURITY THREAT REPORT NO. 23 at 15, March 2018, https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf (last accessed June 13, 2018).

the background, usually without the knowledge of the computer's owner. Mining botnets are designed to harness the computers' processing power to mine for a particular cryptocurrency. The more computers the malware infects, the more power the botnet has in the race to confirm cryptocurrency transactions and win coins. According to cyber security firm ProofPoint, one botnet known as Smominru Monero (designed to mine for the cryptocurrency Monero) made as much as $3.6 million for its operators at currency current value. The Monero botnet was estimated to have more than 526,000 nodes (i.e., computers) at its peak.[233]

IV.
CRYPTOCURRENCY AND CRIME INSURANCE

A. United States

Effective 2015, the Insurance Services Offices, Inc.'s commercial crime forms address cryptocurrency and related products. Specifically, the Insurance Services Office (ISO) Commercial Crime Policy (Discovery Form)[234] broadly excludes from coverage loss involving any form of virtual currency:

> **D. Exclusions**
>
> **1.** This Policy does not cover: . . . .
>
> **k. Virtual Currency**
>
> Loss involving virtual currency of any kind, by whatever name known, whether actual or fictitious including, but

[233] Nick Whigham, *Criminal cryptocurrency botnets make millions for their creators*, NEW YORK POST, February 2, 2018, https://nypost.com/2018/02/02/criminal-cryptocurrency-botnets-make-millions-for-their-creators (last accessed June 13, 2018).

[234] Ins. Servs. Office, Commercial Crime Policy (Discovery Form), Form CR 00 22 11 15.

> not limited to, digital currency, crypto currency or any other type of electronic currency.[235]

Insureds, however, may obtain virtual currency coverage under the Employee Theft and the Computer And Funds Transfer Fraud insuring agreements through the "Include Virtual Currency as Money" endorsement.[236] The endorsement schedule requires that certain information be identified, including the specific cryptocurrency covered and the exchange that will be referenced to determine valuation. Additionally, the schedule provides for a Virtual Currency Limit of Insurance for the Employee Theft and the Computer And Funds Transfer Fraud insuring agreements.[237]

The Include Virtual Currency as Money endorsement modifies the exclusion for virtual currency in the Commercial Crime Policy (Discovery Form) by creating an exception for the designated cryptocurrency:

> **k. Virtual Currency**
>
> 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. However, if a Virtual Currency Limit Of Insurance is shown in the Schedule, we will pay up to that amount for loss of virtual currency shown in the Schedule. That amount is part of, not in addition to, the Limit Of Insurance shown in the Declarations for the applicable Insuring Agreement.[238]

---

[235] Ins. Servs. Office, Commercial Crime Policy (Discovery Form), Form CR 00 22 11 15, § D(1)(k).

[236] Ins. Servs. Office, Include Virtual Currency As Money (Endorsement), Form CR 25 45 11 15.

[237] Ins. Servs. Office, Include Virtual Currency As Money (Endorsement), Form CR 25 45 11 15.

[238] *Id.*

The Include Virtual Currency as Money endorsement modifies the valuation condition, replacing paragraph (1) of the Valuation—Settlement Condition with the following:

> **(1) Money**
>
> **(a) Other Than Virtual Currency**
>
> Loss of "money", other than virtual currency, but only up to and including its face value. We will, at your option, pay for loss of "money" issued by any country other than the United States of America:
>
> **(i)** At face value in the "money" issued by that country; or
>
> **(ii)** In the United States of America dollar equivalent, determined by the rate of exchange published in The Wall Street Journal on the day the loss was "discovered".
>
> **(b) Virtual Currency**
>
> Loss of "money" in the form of virtual currency but only up to and including its value at the close of business on the day the loss was "discovered" as determined by the rate of exchange published by the Exchange shown in the Schedule. We may, at our option, pay the value of the virtual currency in the United States of America dollar equivalent or replace it in kind.[239]

In June 2014, Great American Insurance Group's Fidelity/Crime Division launched commercial coverage for Bitcoin. Great American created the coverage by adding an endorsement to its existing crime

[239] *Id.*

policies for mercantile and governmental customers.[240] The endorsement adds Bitcoin to the definition of "securities" as follows:

> **C. DEFINITIONS, 16. Securities,** is amended to include: . . . .
>
> **c.** bitcoins, which are a form of virtual or on-line peer to peer mediums of exchange, used to pay for goods or services, or held for investment, which can be purchased and which can be exchanged into cash.[241]

Under the Great American endorsement, the loss is valued based on the Coinbase Exchange rate at the close of business on the day the loss was discovered.[242]

B. Canada

Canadian insurers have thus far taken a relatively conservative approach to offering insurance for cryptocurrency. Most of the major Canadian crime insurers are affiliates of their American counterparts, with the notable exception of the Guarantee Company of North America (the Guarantee), which was established in Canada in 1872 and is today the second-largest Canadian fidelity insurer. Canadian crime policies tend to derive their wordings from their American affiliates, and from other American sources such as the Surety & Fidelity Association of America (SFAA) and ISO. When a new innovation is introduced in the United States, Canadian crime insurers tend to adopt it shortly thereafter. For example, after the first discrete social engineering fraud (SEF) coverages were introduced in the United States in 2013, numerous Canadian insurers offered similar coverages within a year.

---

[240] *Great American Launches Bitcoin Coverage for Commercial Entities*, INS. J., June 3, 2014), http://www.insurancejournal.com/news/national/2014/06/03/330879.htm (last accessed June 13, 2018).

[241] Great Am. Ins. Group, Bitcoin Coverage, Form SA 71 49 (ed. 06/14).

[242] *Id.*

To date, no Canadian insurer has introduced a specific affirmative grant of coverage for cryptocurrency,[243] although some insurers are either in the process of doing so, or at least exploring the possibility. In its recently-released crime wording, the Guarantee is the first Canadian insurer to add a specific exclusion for cryptocurrency to its base crime wording, which reinforces the current wording's intention to cover Money, Securities and Other Property as those terms have been traditionally interpreted and applied. It may be that the Guarantee and other Canadian insurers will come to offer cryptocurrency-specific coverage by endorsement in the future.

C. Crime Insurance and Cryptocurrency Loss Claims

1. Whether There Is a Loss of Covered Property

Under "traditional" crime policy language, there would appear to be no intent to insure for loss of cryptocurrency. The threshold difficulty is that cryptocurrency is not "Money, Securities or Other Property" as defined in most crime policies. As cryptocurrency is neither tangible nor legal tender, its classification as covered property is not yet established. The first possibility, "other property," is easily dismissed. As crime policies define "other property" to mean tangible property only, cryptocurrency does not meet that criterion. Thus, cryptocurrency does not fall within the meaning of "other property."

Might cryptocurrencies be considered to be "money", even though it is not a fiat currency? Although there is no case law directly on point, it is not inconceivable that a court could find a cryptocurrency like bitcoin to fall within the definition of "money" in policies that define the

[243] In Canada, National Bank Insurance has taken the position in advertising material that its homeowners policy responds to loss of virtual currency as loss of "Goods." However, the policy sublimits any such loss at CAD $200 (about USD $150): https://www.nbc-insurance.ca/content/bna/en/accueil/avantages-et-conseils/monnaies-virtuelles-assurances.html (last accessed June 13, 2018).

term to include currency. For example, the ISO Commercial Crime Policy defines "money" as follows:[244]

> "Money" means:
>
> a. Currency, coins and bank notes in current use and having a face value;
>
> b. Traveler's checks and money orders held for sale to the public . . . .

Inasmuch as cryptocurrency exists as a medium of exchange—albeit one not in wide acceptance—a court could theoretically be persuaded that cryptocurrency is a form of "currency" and thus is "money,"[245] but that appears to strain the plain intent of the definition, in part because it would be difficult to credibly argue that cryptocurrency is "in current use" in the same sense as coins and banknotes.

An argument could be made that cryptocurrency is "money" by looking to statements by FinCEN, as discussed above, or by authority such as *Shavers,*[246] where the defendant sought to defeat charges that he violated federal securities laws arising from Bitcoin-related investment opportunities on the basis that bitcoins are not money. Noting that bitcoins can be used to purchase goods and services, and can be exchanged for conventional currencies such as the dollar, the Court held that Bitcoin is a "currency" or form of "money," for the purpose of the securities laws in issue.[247] Again, however, the purpose underlying that legislation makes *Shavers*' applicability in the commercial crime insurance context questionable at best.

---

[244] Commercial Crime Policy (Discovery Form), Form CR 00 22 05 06, § F. (ISO 2005) (on file with ISO).

[245] *See*, *e.g.*, McKee v. State Farm Fire & Cas. Co., 193 Cal. Rptr. 745 (Ct. App. 1983) (collectable coins, though not in circulation, were "money" under homeowner's policy); De Biase v. Comm'l Union Ins. Co. of N.Y., 278 N.Y.S.2d 145 (Civ. Ct. 1967) ("'money' is any matter . . . which has currency as a medium in commerce").

[246] 2013 WL 4028182.

[247] *Id.* at 2.

Cryptocurrency is unlikely to fall within the meaning of "money" under the SFAA Crime Protection Policy, which defines the term as:

> a. Cash;
>
> b. Demand and savings deposits at financial institutions; and
>
> c. Travelers check, register checks and money orders held for sale to the public.[248]

The SFAA Crime Protection Policy defines "cash" to mean "United States or Canadian bills and coins in current use and having a face value that are accepted by the United States or by the government of Canada as legal tender for the payment of debts."[249] Cryptocurrency is not legal tender. Thus, it is neither "cash" nor "money" under the SFAA form.

The term "securities" is typically defined to mean "*negotiable and nonnegotiable instruments or contracts*" representing either money or other property.[250] As such, it would not appear to extend to cryptocurrency. Further, cryptocurrency is not a negotiable instrument under the UCC because it is not an unconditional promise or order to pay a fixed amount of money.[251] Additionally, whatever value the cryptocurrency has is in the cryptocurrency itself; a "promise to pay" is superfluous. The same reasoning would follow under the SFAA Crime Protection Policy.

While it is difficult to predict the outcome of a case that has not arisen, it seems that a court is unlikely to find that cryptocurrency falls within the definition of "securities" or "other property," and only marginally more likely to find that it is "money."

---

[248] Crime Protection Policy, SP 00 01 04 12, § C.9 (SFAA 2012).

[249] *Id.*, s. C.2.

[250] Commercial Crime Policy (Discovery Form), Form CR 00 22 05 06, § F (ISO Props., Inc. 2005).

[251] U.C.C. § 3-104.

Great American and ISO have addressed the issue by crafting specific endorsements for cryptocurrency, but using different approaches. Under the Great American endorsement, cryptocurrency is included within the definition of "security," whereas ISO includes cryptocurrency within the definition of "money." These endorsements reflect the fact that existing crime policies were not drafted to address cryptocurrency. As for policies that do not specifically address cryptocurrency, no court has yet ruled upon the classification of cryptocurrency for the purpose of first-party insurance.

2. Traditional Loss Scenarios

Assuming that an insured could get over the threshold issue of demonstrating that cryptocurrency was covered property under its policy, some of the "traditional" commercial crime insuring agreements could theoretically have scope to apply in respect of losses involving cryptocurrency. Other insuring agreements do not readily "fit" with cryptocurrency loss scenarios. Examples of the former may include employee dishonesty, SEF and, with some qualifications, computer fraud and funds transfer fraud. Examples of the latter may include loss inside the premises, loss outside the premises and counterfeit currency.

a. "Traditional" Employee Dishonesty

There is nothing about cryptocurrency which prevents it from being the subject-matter of employee defalcation. Consider the hypothetical situation of an insured online retailer that, in addition to transacting through traditional channels, also makes and accepts payments in bitcoin. The bitcoin side of the operation would be susceptible to loss where a rogue employee invests his employer's unused capacity to day trade in the bitcoins, reaping the profits from volatility. For example, the dishonest employee might purchase a certain cryptocurrency in the morning for $100,000. If the price increased 10 per cent, he could sell for $110,000 and divert the $10,000 gain to a personal account, leaving the original $100,000 in the employer's account as though it had been untouched. In another hypothetical, the dishonest

employee could skim fees in exchanges and cause them to appear simply as exchange fees.[252]

The pairing of employee dishonesty with cryptocurrency loss is not just hypothetical. In April 2018, India-based cryptocurrency trading platform Coinsecure alleged that, in the process of extracting Bitcoin to distribute to customers, a rogue employee directed 438 bitcoins held by Coinsecure to an unauthorized public key.[253] In principle, there seems to be no reason why such a loss would not fall within prima facie coverage, depending on the specific wording of the insuring agreement in issue.

Consideration would then shift to applicable exclusions, such as exclusions for acts of directors, partners or major shareholders,[254] as well as the related alter ego defense.[255] There have been instances of proprietors of currency exchanges or similar services stealing customers' cryptocurrency holdings.[256] In such circumstances, it would be necessary to carefully review the facts to ascertain which exclusions or defenses, if any, might apply. It is reasonably well-established in both the United States[257] and Canada[258] that there is no direct right of action by a third party on a crime policy.

---

[252] C. Kevin Eller & Karen Y. Green, "Tales From The Crypt: A Cryptocurrency Fraud" THOMSON REUTERS/TAX & ACCOUNTING (March/April 2018), 2018 WL 1666404.

[253] Antony & Chaudhary, *supra* note 217.

[254] See, *e.g.*, *Tactical Stop-Loss, LLC v. Travelers Casualty and Surety Co. of America*, 657 F.3d 757 (8th Cir. 2011).

[255] See, *e.g.*, *In Re Taylor, Bean & Whitaker Mortgage Corporation*, 2015 WL 728493 (M.D.Fla.).

[256] Reuters, "Feds sue three cryptocurrency operators for fraud." NEW YORK POST (January 19, 2018) https://nypost.com/2018/01/19/feds-sue-three-cryptocurrency-operators-for-fraud/ (last accessed June 13, 2018).

[257] See, *e.g.*, *Western Alliance Bank v. National Union Fire Insurance Company of Pittsburgh, Pa.*, 2016 WL 641648 (N.D. Cal.).

[258] *Swinkels v. American Home Assurance Co.*, 2013 ONSC 4163 at para. 14.

b. Evidentiary Issues Surrounding Employee Dishonesty and Cryptocurrency

As with any loss alleged to have been caused by an employee, there will be evidentiary issues surrounding the proof offered by the insured that an employee did, in fact, cause the loss, rather than an outside third party. One challenge particular to the investigation of cryptocurrency losses is that the transfer mechanism is, by design, nearly anonymous. In order to effect a cryptocurrency transfer, the transferor simply needs a copy of the private key, which is a string of alphanumeric characters. As described above, the "thing" that is stolen is not tangible, nor is it even a discrete computer file; all that need be stolen is the private key, which is then melded with the public key of the payment destination in order to add another link to the Blockchain.

In order to prove an employee dishonesty loss in such circumstances, it would be necessary to demonstrate that the employee in question had access to the private key, and to negate the possibility that a copy of the data comprising the private key simply fell into the hands of a third-party fraudster. As infinite copies of a private key can exist, this can pose a practical challenge in demonstrating employee culpability. Corroborating circumstantial evidence, perhaps in the form of forensic evidence regarding an employee's access to an insured's wallet (either digitally or in "cold storage" on a hard drive), may become critical in such circumstances.

Further, until such time as cryptocurrency is converted into funds or used to purchase a good or service, its ownership remains (nearly) anonymous within the cryptocurrency ecosystem. This presents practical challenges for demonstrating employee benefit. In contrast, a traditional theft of cash or tangible property may be traced to a particular employee based on records of physical access, eyewitness accounts or bank or financial records of the employee. In such a phony vendor fraud, funds can be traced from the insured to the phony vendor, the ownership of which can then be demonstrated by appropriate evidence.

c. Workplace Cryptomining as Employee Dishonesty?

An interesting issue arises as to employee-caused loss of assets that are neither traditional Money, Securities or Other Property, nor cryptocurrency. In addition to the computer processing capacity itself, the cryptocurrency mining process utilizes electrical power to such a tremendous extent that there are online comparisons showing which jurisdictions have the cheapest electricity, so as to guide would-be miners on where to set up their server farms.[259]

Cybersecurity experts have reported a sharp increase in workplace cryptomining, with one expert reporting in April 2018 that, during the preceding six months, her company saw more than 1,000 instances of employees stealing computing power from their employers in order to mine bitcoin. By way of example, she told of one situation where a junior banker at an Italian bank stole 12 servers that he had signed for and set them up hidden beneath the floorboards of the bank to create his own cryptomining range.[260] As noted above, it was reported in February 2018 that engineers at Russia's top nuclear research facility in Sarov had been improperly using the facility's supercomputer to mine bitcoin.[261] This would carry a significant associated cost in electricity paid for by the facility. Thus, it is arguable that the engineers were stealing an asset belonging to their employer.

Would a crime policy respond in such circumstances? The first issue would be to determine whether computing power and/or electricity fell within the definition of "Other Property." If that threshold requirement could be satisfied, one could contend that coverage might

[259] Sean Williams, "Bitcoin Mining Costs: The Most and Least Expensive Countries" *The Motley Fool*, January 28, 2018, https://www.fool.com/investing/2018/01/28/bitcoin-mining-costs-the-most-and-least-expensive.aspx (last accessed June 13, 2018).

[260] Oscar Williams-Grut, *A Junior Banker in Italy Hijacked Servers from his Company to Mine Bitcoin—and Thousands of Others Are Doing Similar Things*, BUSINESS INSIDER, Apr. 14, 2018, http://www.businessinsider.com/darktrace-ceo-staff-stealing-company-computer-power-mine-bitcoin-2018-4 (last accessed June 13, 2018).

[261] Agence France-Presse, *supra* note 231.

potentially be available. In *Diversified Group, Inc. v. Van Tassel*,[262] employees of the insured, DGI, secretly used their own company to submit a competing (and ultimately successful) bid for a government contract on which the insured was also bidding. The insured sought indemnity with respect to the profits it allegedly lost in not being awarded the contract. The Fifth Circuit applied the "potential income" exclusion to the lost profits claim, but noted that coverage potentially existed for diverted corporate resources under the broad insuring agreement there in issue:

> In addition to the loss of profits, DGI seeks recovery for other losses allegedly sustained, including funds used by Burgstiner and Van Tassel for travel, in furtherance of their scheme, the salaries they received for personally diverted time, telephone services, corporate facilities and overhead, secretarial assistance, and supplies attributable to their efforts on behalf of their competing enterprise. It may be that DGI will be unable to carry the burden of proof on some or all of these and perhaps other similar items of loss, but we are not prepared to say as a matter of law that such items are not covered by the St. Paul policy.
>
> By its express terms the St. Paul policy covers the loss of "money . . . and other property" caused "directly from one or more fraudulent or dishonest acts" of employees. Although minor when considered against the claim for lost profits, we are neither persuaded that these claimed losses are so inconsequential as to be unrecoverable nor that, as a matter of law, they do not result directly from the alleged acts of misconduct. We observe that overhead expenses, lost due to a compensable event, have been held recoverable.[263]

[262] 806 F.2d 1275 (5th Cir. 1987). *See* discussion in David T. DiBiase & David J. Billings, *"Loss? What Loss?": Unique Claims on Crime Policies/Fidelity Bonds*, XIV FID. L.J. 271, 290 (2008).

[263] *Id.* at 1278.

Unlike telephone, paper and ink expenses in the 1980s, cryptomining costs in the 2010s are in no sense "minor." Although modern employee dishonesty and theft insuring agreements are generally more restrictive than the one in issue in *Diversified Group* (in part because of more restrictive causation requirements that losses be "direct," in the sense of flowing immediately in space and time from the loss-causing act), a creative insured could still argue the applicability of *Diversified Group* where an employee misuses the insured's electricity to mine cryptocurrency. One solution for insurers may be a cryptomining/cryptojacking exclusion, which would apply both to employees and to outside third parties.

d. SEF Losses

Assuming that a policy recognizes cryptocurrency as covered property, there would seem to be no reason, in principle, why coverage could not be extended to SEF losses. At their most basic level, SEF losses involve the insured's voluntary transfer of property on the basis of a fraudulently-induced misapprehension as to the ownership of that property. Phony client scams, phony vendor scams and executive impersonation scams all seek to induce the insured to voluntarily part with funds, either immediately or through the provision of fraudulent "new bank account" information.

These elements find ready analogues with cryptocurrency. An employee can be duped into making a cryptocurrency payment. An employee can be duped into believing that a public key represents the legitimate destination for a cryptocurrency payment, when in fact the public key is connected to a fraudster.

SEF coverages are typically sublimited, whereas employee dishonesty coverages are typically not. This creates an incentive on the part of the insured to identify evidence of employee collusion in the loss-causing act. One challenge that may arise with respect to SEF losses is that, given the pseudonymity and limitations on traceability of cryptocurrency discussed above, it may not be possible to easily distinguish between an employee's actions in a SEF loss and an employee's actions in a fraudulent transfer of cryptocurrency to an outside confederate.

Thus, where the insured alleges circumstances which could fit either a SEF loss scenario or an employee dishonesty scenario, it will be necessary for the carrier to carefully scrutinize the corroborating circumstantial evidence (including computer forensic evidence) to ascertain evidence of employee involvement and, where appropriate, employee intent.

e. Computer Fraud

With some exceptions, it is now reasonably well-established in the case law that the intent of computer fraud coverage is to indemnify the insured with respect to hacking incidents, i.e., where a computer is used to cause another computer to make an unauthorized, direct transfer of property or money, without any involvement on the part of an employee of the insured.[264] It is possible that a form of specialized computer fraud coverage could be created for hacking incidents involving cryptocurrency. To date, some carriers that have ventured into the cryptocurrency world have made it clear that their policies are not intended to provide indemnity for hacking incidents.[265] For example, Great American's Bitcoin coverage endorsement applies only in respect of its Employee Theft insuring agreement,[266] and does not extend to hacking.[267]

Hacking is an extremely significant problem in the cryptocurrency word, with everything from individual wallets to entire exchanges being targeted by hackers seeking to obtain private keys. Cryptocurrency must be stored in wallets or equivalent storage, but wallets can be hacked and compromised. As noted above, the BBC

[264] American Tooling Center, Inc. v. Travelers Cas. & Sur. Co. of Am., No. 16-12108, 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017). *See also* Pestmaster Services, Inc. v. Travelers Cas. and Sur. Co. of Am., No. 14-56294, 2016 WL 4056068 (9th Cir. July 29, 2016).

[265] Suzanne Barlyn, *Insurers Gingerly Test Bitcoin Business with Heist Policies*, REUTERS, Feb. 1 2018, https://www.reuters.com/article/markets-bitcoin-insurance/rpt-insight-insurers-gingerly-test-bitcoin-business-with-heist-policies-idUSL2N1PR03F (last accessed June 13, 2018).

[266] Great American Bitcoin coverage endorsement, Form CR 79 85 (Ed. 11/16).

[267] Barlyn, *supra* note 265.

reported in March 2018 that a 15-year old "white hat" hacker had successfully written code to create a "back door" into the supposedly tamper-proof Ledger Nano S hardware wallet.[268] This back door would permit a malicious hacker to drain the wallet of funds.

Cryptocurrency exchanges present the same problem, just on a larger scale. As noted above, one of the first major exchanges, Mt. Gox, collapsed and filed for bankruptcy following the discovery of an ongoing series of hacking incidents. In January 2018, another Japanese cryptocurrency exchange, Coincheck, announced that it had lost some USD $534 million worth of the NEM cryptocurrency through a hacking incident.[269] Apparently, Coincheck maintained the NEM in a hot wallet, rather than a cold wallet, and also failed to utilize a multi-signature system to protect the wallet.[270]

There have been numerous other instances of exchange hacks with losses in the hundreds of thousands or millions of dollars,[271] and one pundit suspects that as much as 14 per cent of all bitcoin and ether in existence (worth billions of dollars) has been stolen by hackers.[272] Some exchanges have taken to publicly announcing that they only maintain a very small proportion of their holdings in hot storage. For example,

---

[268] BBC, *supra* note 192. The teenager shared the code with the manufacturer.

[269] Aatif Sulleyman, *Coincheck Hack: Bitcoin Exchange Security Under Scrutiny After $534M Cryptocurrency Theft*, THE INDEPENDENT, Jan. 29 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/coincheck-hack-nem-latest-updates-japan-bitcoin-theft-cryptocurrency-inspect-exchanges-south-korea-a8183281.html (last accessed June 13, 2018).

[270] *Id.*

[271] Ed Zwirn, *Cryptocurrency leaves investors vulnerable to hacking*, NEW YORK POST, Mar. 18, 2018, https://nypost.com/2018/03/18/cryptocurrency-leaves-investors-vulnerable-to-hacking/ (last accessed June 13, 2018).

[272] Olga Kharif, *Hackers Have Walked off with About 14% of Big Digital Currencies*, BLOOMBERG, Jan. 18, 2018, https://www.bloomberg.com/news/articles/2018-01-18/hackers-have-walked-off-with-about-14-of-big-digital-currencies (last accessed June 13, 2018).

cryptocurrency exchange Coinbase states on its website that it maintains 98 per cent of customer holdings in cold storage.[273]

It may be that some carriers will simply not entertain the prospect of indemnity for hacking with respect to cryptocurrency, at least given the current state of wallet security. However, there are already some market entrants. Mitsui Sumitomo Insurance began offering cryptocurrency insurance in November 2016 to cryptocurrency exchanges.[274] According to online descriptions, the Mitsui Sumitomo policy covers loss from both internal and external causes, *e.g.*, theft by employees or third parties, cyberattacks, unauthorized access and mistakes.[275] Coinbase's website states that it maintains commercial crime insurance in an aggregate amount exceeding the value of the cryptocurrency it maintains in hot storage. The coverage is underwritten through a combination of carriers and Coinbase itself as co-insurer under the policy, which insures against theft of digital currency that results from a security breach or hack, employee theft, or fraudulent transfer.[276]

In June 2018, it was reported that the VanEck SolidX Bitcoin Trust ETF (exchange-traded fund) was seeking to become the first SEC-approved cryptocurrency ETF.[277] The proposed ETF would carry bitcoin theft insurance to protect shareholders from exchange hacks and other fraudulent activity. The initial policy will cover losses up to $10 million, but will increase as the value of assets in the trust rises. According to the fund's SEC filing:

> the trust will maintain a crime insurance that will cover the loss of bitcoin due to 'theft, destruction, bitcoin in

[273] https://www.coinbase.com/legal/insurance (last accessed June 13, 2018).

[274] John S. Rossiter, P*repare for the Future With Cryptocurrency Insurance*, *Perkins Coie News & Insight* (October 2017) https://www.perkinscoie.com/en/news-insights/prepare-for-the-future-with-cryptocurrency-insurance.html (last accessed June 13, 2018).

[275] *Id.*

[276] https://www.coinbase.com/legal/insurance (last accessed June 13, 2018).

[277] Dave Dierking, *XBTC: Are We Finally Getting Close To The Elusive Bitcoin ETF?,* June 18, 2018, https://seekingalpha.com/article/4182226-xbtc-finally-getting-close-elusive-bitcoin-etf (last accessed June 18, 2018).

> transit, computer fraud and other loss of the private keys that are necessary to access the bitcoin held by the Trust'.[278]

There are several considerations that could inform the design of a specialized insurance product that provides computer fraud coverage for cryptocurrency:

(a) given the risks inherent in hot storage, would such a product be restricted to cold storage, or sublimited for cryptocurrency maintained in hot storage?

(b) as with some iterations of SEF coverage, would there be conditions precedent to coverage for hacking losses such as, for example, a requirement that any wallet include a multi-signature security system?

(c) given the loss experience to date, what sort of limits are feasible, either for individual holders or (especially) exchanges?

(d) in the absence of significant historical industry loss experience data, how do carriers (and reinsurers) appropriately set premium?

f. Funds Transfer Fraud

The ISO Include Virtual Currency As Money Endorsement permits an insured to obtain coverage under the Computer and Funds Transfer Fraud insuring agreement. It is therefore useful to consider what a Funds Transfer Fraud loss of cryptocurrency might look like, and what underwriting and coverage issues could arise. The ISO Commercial Crime Policy insuring agreement with respect to Computer and Funds Transfer Fraud is a hybrid, with the Funds Transfer Fraud portion of the provision indemnifying for:

[278] *Id.*

6. Computer And Funds Transfer Fraud

a. We will pay for: . . .

(2) Loss resulting directly from a "fraudulent instruction" directing a "financial institution" to debit your "transfer account" and to transfer, pay or deliver "money" or "securities" from that account.[279]

A "financial institution" is in turn defined as:

9. "Financial institution" means: . . .

b. With regard to Insuring Agreement **A.6.**:

(1) A bank, savings bank, savings and loan association, trust company, credit union or similar depository institution; . . . .[280]

A "transfer account" is defined as:

an account maintained by you at a "financial institution" from which you can initiate the transfer, payment or delivery of "money" or "securities":

a. By means of computer, telefacsimile, telephone or other electronic instructions; or

b. By means of written instructions (other than those covered under Insuring Agreement **A.2**.) establishing the conditions under which such transfers

[279] Ins. Servs. Office, Commercial Crime Policy (Discovery Form), Form CR 00 22 11 15. §A.6.a.(2).

[280] Ins. Servs. Office, Commercial Crime Policy (Discovery Form), Form CR 00 22 11 15. §F.9.b.

> are to be initiated by such "financial institution" through an electronic funds transfer system.[281]

It is difficult to see how the Funds Transfer Fraud insuring agreement would be triggered, as several elements of the insuring agreement do not "fit" with the current cryptocurrency ecosystem. While there have been some working partnerships between banks and cryptocurrency exchanges,[282] banks and other traditional depository institutions such as credit unions and trust companies do not, at present, maintain accounts denominated in cryptocurrency. As such, the issue becomes whether a cryptocurrency exchange could be considered to be a "similar depository institution." It is not immediately clear that the answer is yes; the real locus of a deposit is a wallet, in the sense of storage of private keys, whereas the primary purpose of an exchange is trading cryptocurrencies, either into or out of fiat currency and for other cryptocurrency. In that sense, an exchange is more analogous to a stock or commodities market. Some exchanges also serve a wallet function, in the sense of storing client cryptocurrency, but many of these exchanges expressly do not wish to maintain large amounts of client cryptocurrency on hand, or for extended periods of time, due to liability concerns.

If we were to assume that exchanges are "financial institutions" (at least to the extent that they carry on a storage or depository function, as opposed to serving as a trading platform), it then follows that coverage could conceivably be available to the owner of cryptocurrency to the extent that a third party successfully brings about an improper transfer of that cryptocurrency out of an exchange on the basis of fraudulent instructions.

What about insurance for the exchange itself? It appears that some early adapters (notably Coinbase and Mitsui Sumitomo) have worked out individually-tailored solutions, although the Mitsui Sumitomo policy is not in the public domain. At a minimum, an

---

[281] Ins. Servs. Office, Commercial Crime Policy (Discovery Form), Form CR 00 22 11 15. §F.24.

[282] Arjun Kharpal, *Barclays Strikes Banking Deal with Major Cryptocurrency exchange Coinbase*, CNBC TECH, Mar. 14, 2018, https://www.cnbc.com/2018/03/14/coinbase-cryptocurrency-exchange-opens-bank-account-with-barclays-in-uk.html (last accessed 14 June 2018).

exchange would have to maintain appropriate crime insurance, and either satisfy itself that the policy's ownership condition encompasses client cryptocurrency or, alternatively, ensure that client coverage is specifically underwritten by endorsement. At some point in the future, once the regulatory environment has sufficiently matured, an exchange may seek a form of coverage that looks similar to a financial institution bond.

g. Loss Inside the Premises / Loss Outside the Premises

The ISO Crime Policy includes the following insuring agreements:

> **3. Inside The Premises – Theft Of Money And Securities**
>
> We will pay for:
>
> **a.** Loss of "money" and "securities" inside the "premises" or "financial institution premises":
>
> **(1)** Resulting directly from "theft" committed by a person present inside such "premises" or "financial institution premises"; or
>
> **(2)** Resulting directly from disappearance or destruction. . . .
>
> **5. Outside The Premises**
>
> We will pay for:
>
> **a.** Loss of "money" and "securities" outside the "premises" in the care and custody of a "messenger" or an armored motor vehicle company resulting directly from "theft", disappearance or destruction.
>
> **b.** Loss of or damage to "other property" outside the "premises" in the care and custody of a "messenger"

> or an armored motor vehicle company resulting directly from an actual or attempted "robbery".[283]

Assuming that cryptocurrency were to be defined as "money" (as in the ISO form) or "securities" (as in the Great American coverage), do these insuring agreements have any scope to operate with respect to cryptocurrency? The "traditional" coverages would not appear to readily apply in the case of cryptocurrency, because they are tied to the existence of physical premises. The ISO endorsement only extends to employee dishonesty and computer and funds transfer frauds, not on-premises losses. This makes sense; the ISO Crime Policy defines "premises" as "the interior of that portion of any building you occupy in conducting your business." Similarly, "financial institution premises" is defined as the "interior of that portion of any building occupied by a 'financial institution' . . . ." With one important qualification, cryptocurrency does not occupy any physical space. Cryptocurrency "exists" solely in private keys and in the record of transactions and user balances that comprise a Blockchain.

What happens if the private key is given physical manifestation? This could take the form of a hardware wallet on a USB drive or, more simply, a piece of paper with the alphanumeric combination comprising the private key written on it. At first blush, it would seem that coverage for loss inside or outside the premises could now arise, as there is now something that can be physically transported off of those premises. However, the issue is not that clear. A piece of paper containing the written private key is simply a piece of paper with data on it; it is not the cryptocurrency itself. Such a piece of paper has no more intrinsic value than a monthly bank statement which has a dollar-denominated bank balance written on it.

The easiest illustration of this distinction is that one could write the same private key for a bitcoin on multiple pieces of paper. No particular piece of paper actually represents the value of the bitcoin; the private key only has value at the moment that a bitcoin payment is made. One can reason by analogy to the decision of the Ninth Circuit Court of

---

[283] Ins. Servs. Office, Commercial Crime Policy (Discovery Form), Form CR 00 22 11 15. §§ A.3 & A.5.

Appeals in *Avery Dennison Corp. v. Allendale Mutual Insurance Co*.,[284] in which the insured's employee had been bribed to provide a trade competitor with the insured's confidential formulas for adhesives for labels. The insured asserted a loss of $150 million with respect to the theft of its trade secrets. The Court rejected the insured's claim for indemnity, observing that, while the paper on which the formula was written was covered property and had (minimal) tangible value, the trade secrets themselves could not be considered to be "tangible property" within the meaning of the policy. As in *Avery Dennison*, the piece of paper that contains a private key has utility value, but no intrinsic value.

Similarly, the copying of a private key is analogous to gift card fraud, whereby the fraudster copies the gift card data for accounts with balances. In one iteration of the scheme, a botnet[285] uses infected computers ("bots") to test a rolling list of potential gift card account numbers and request the balance. If the retailer's site returned a balance in response to the query, then the botnet has obtained a gift card account number and balance. That number is then recorded and used to make a phony gift card with the duplicate information.[286] Unless and until the duplicated card data is used to make a purchase, neither the retailer nor the legitimate gift card holder has sustained a loss. Assuming that the legitimate holder uses the gift card before the fraudsters, they may both proceed with the gift card transaction normally, regardless of the fact that a third party also has the card information. In fact, if the legitimate customer uses the card before the schemer, then the schemer's data for that card loses value. Therefore, the schemers' acquisition of card data is not the loss that must be analyzed, because no money has transferred at

[284] Avery Dennison Corp. v. Allendale Mutual Insurance Co., 310 F.3d 1114 (9th. Cir. 2002). *See* discussion in DiBiase and Billings, *supra* note 262 at 278-280.

[285] A botnet a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, to perform computational function in the background, e.g., to send spam messages.

[286] Distil Networks. "GiftGhostBot Attacks Ecommerce Gift Card Systems Across Major Online Retailers" https://resources.distilnetworks.com/all-blog-posts/giftghostbot-attacks-ecommerce-gift-card-systems (last accessed June 13, 2018).

the time of the acquisitions.[287] It is no different for cryptocurrency—even if a fraudster wrongfully acquires the legitimate owner's private key, the legitimate owner can still use that cryptocurrency as long as the fraudster has not acted upon the wrongfully obtained private data.

Similarly, a wallet is just software (a hardware wallet is just a USB device that contains certain software). A wallet can be cloned or copied. While cryptocurrencies such as Bitcoin have reasonably robust protocols to guard against double-spending, such protocols cannot prevent the wrongful *single*-spending of a bitcoin from a copied wallet. So far as the Blockchain is concerned, the private key has been used as part of a payment; the Blockchain is indifferent as to whether the spender is the legitimate owner.

Given that there can be multiple copies of the same wallet (software or hardware), it is not conceptually satisfactory to state that a physical wallet or USB drive can be the "property" that can be removed from the insured's premises or banking premises for the purposes of these coverages. An example illustrates the point: the insured maintains a legitimate hardware wallet at its premises. A third party thief gains access to the insured's premises, surreptitiously copies the wallet onto another USB stick, and exits the premises, leaving the original wallet in place. If the insured spends its cryptocurrency first, there can be no loss, as the Blockchain will prevent the thief from also spending the same cryptocurrency. If the thief spends the cryptocurrency first, then the insured has incurred a loss. The loss is entirely contingent on events other than the thief physically removing the USB stick from the premises.

Obviously, it is possible for a thief to surreptitiously remove the *sole* copy of an insured's hardware wallet from the insured's premises. This moves us closer to an analogy to Money or Securities under the inside or outside the premises insuring agreements.

---

[287] *See, e.g.*, FDIC v. United Pac. Ins. Co., 20 F.3d 1070, 1080 (10th Cir. 1994) (holding that insured bank suffers a loss when funds are disbursed due to the employee's wrongful conduct); Transwest Credit Union v. Cumis Ins. Soc'y, Inc., No. 2:09-CV-297-TS, 2010 U.S. Dist. LEXIS 99245, at 15 (D. Utah Sep. 21, 2010) ("loss must be determined from the time the funds were wrongfully distributed.").

h. Counterfeit Currency

This coverage grant seems to have no conceptual fit with cryptocurrency, assuming that the Blockchain environment utilized by any particular cryptocurrency (there have been over 1,400 to date)[288] contains reasonably robust protections against double-spending such as are found with Bitcoin.

3. Cryptocurrency—Specific Loss Scenarios

We have already addressed wallet thefts, wallet hacks and exchange hacks insofar as they might or might not be covered under existing commercial crime insuring agreements. It is important to consider some of the unique types of losses that occur in the cryptocurrency ecosystem. To what extent are these reconcilable with "traditional" loss scenarios? In what circumstances might crime coverage respond?

a. Phishing / Credential Harvesting / Credential Stuffing

It is estimated that over $225 million worth of cryptocurrency was lost to phishing scams in 2017. In one notable fraud discussed above, phishing emails were sent to users of an online Ethereum wallet site www.myetherwallet.com. The email claimed that the wallet site had published a new update and directed customers to a spoof of the wallet site, which used the similar-domain name www.myetherwalleţ.com, replacing the second "t" with a "ţ" symbol. Users typed their passwords into the webpage, which permitted the fraudsters to access the users' wallets and access the ether cryptocurrency.

On the one hand, this is somewhat similar to an SEF scam, in that the insured (in this scenario, the ether wallet client, not the wallet host) has been fraudulently induced to part with information which is then used by the fraudster to access and remove the insured's cryptocurrency. However, this scenario also has some similarities to a Funds Transfer Fraud loss, in that the wallet host receives fraudulent instructions from a third party directing it to transfer cryptocurrency out

[288] Digital Shadows, *supra* note 4 at 2.

of the insured's online wallet. Given that there are often significant differences in limits between SEF coverages and other forms of coverage (at least outside of the cryptocurrency context, to date), carriers in the cryptocurrency sphere would be well-advised to consider how these novel types of losses could potentially fit into multiple insuring agreements.

It is important to consider whether and how cyber policies may respond to such losses, both with first-party coverage for cryptocurrency owners, as well as third-party liability coverage for wallet hosts or exchanges. Its is especially true that losses can result from username/password combinations that were already compromised prior to the loss at issue. In the event of a covered cryptocurrency loss under a crime policy, there may potentially also be coverage available under a cyber policy, and a crime carrier would be well-advised to ascertain what other coverages were in place at the time of the loss.

b. ICOs—Exit Scams and other Manipulation

In some ways, ICOs represent the "Wild West" of cryptocurrency. There have been numerous fraudulent ICOs and, as described above, there are problems and risks involved even with legitimate, or quasi-legitimate, ICOs. This entire arena is rife with opportunities for unscrupulous individuals to separate investors from their money and/or cryptocurrency.

However, it is not clear that crime coverage has any role to play in responding to ICO losses. Crime policies do not indemnify when an insured voluntarily invests in a "traditional" securities offering that turns out to have been fraudulent, and there is no obvious candidate among the crime policy's insuring agreements that would respond to an analogous ICO loss, although it is useful to consider whether some broader forms of SEF coverages might be engaged where an ICO is a completely fictitious exit scam which forms one element in a larger fraud against an insured. Moreover, most forms of crime coverage carry either a "voluntary partying" and/or an "exchange or purchase" exclusion, which would seem to encompass the act of exchanging funds for what turn out to be fraudulent coins or tokens.

*c. **Regulatory Seizure and other Government Action***

The regulatory environment for cryptocurrency is in its infancy, but it is already fairly clear that one of the primary concerns of governments and regulatory authorities is money laundering, and most of the jurisdictions that have introduced regulation have focused on AML objectives. Further, some nations have banned cryptocurrency altogether. These developments raise the possibility of government seizure as a cause of "loss" of cryptocurrency.

Some crime policies carry exclusions for government action. For example, the ISO Commercial Crime Policy includes the following exclusion:

> **D. Exclusions**
>
> **1.** This Policy does not cover: . . .
>
> **f. Governmental Action**
>
> Loss resulting from seizure or destruction of property by order of governmental authority.[289]

To the extent that carriers seek to insure for loss of cryptocurrency at all, carriers would be well-advised to consider how their policies are to respond in the event of government seizure of such cryptocurrency.

4. Ownership / Proof of Ownership

Every commercial crime policy has some form of ownership requirement. For example, the ISO Commercial Crime Policy (Loss Sustained Form) provides:

[289] Ins. Servs. Office, Commercial Crime Policy (Discovery Form), Form CR 00 22 11 15, § D.1.f.

r. Ownership of Property; Interests Covered

The property covered under this Policy is limited to property:

(1) That you own or lease;

(2) That is held by you in any capacity; or

(3) For which you are legally liable, provided you were liable for the property prior to the time the loss was sustained. . . . .[290]

In a traditional crime claim, the loss typically involves the loss of fiat currency—in other words, dollars. This fact benefits the adjustment of the loss and analysis of coverage. Fiat currencies are transferred and transacted through trusted third-party intermediaries and financial networks such as banks and credit card companies. Considering that bank and credit balances may be reliably verified, this enables the insurer to determine whether the money that was lost is the same money the insured owned, held, or was legally liable for.

Cryptocurrency, which is decentralized and pseudonymous, makes verification that the claimant owned or held the lost asset far more difficult. Analysis of the claim will require a determination of how the cryptocurrency was held and how it was lost. For example, if the currency was held in an online wallet or in an exchange, it may be possible to obtain the transaction records from the wallet provider, which expedites the claim investigation and avoids the possibility that an unscrupulous claimant provided falsified wallet data in support of a claim.

If the loss involves a digital wallet, then it may be possible to establish a history of cryptocurrency movement. Digital wallet applications vary. Some are desktop applications and others are wholly online. Some wallet providers require that the user provide proof of

[290] Ins. Servs. Office, Commercial Crime Policy (Loss Sustained Form) (Form CR 00 23 08 13). Reprinted in ANNOTATED COMMERCIAL CRIME POLICY, 3d ed. (ABA Press 2015).

identity, such as a copy of the driver's license. Others allow their users to be nearly anonymous.[291] Depending on the wallet provider, it may be possible to obtain the user's transaction data.

If the victim keeps the funds in "cold storage," that is, completely offline in a physical drive or memory unit, the insured may not be able to prove it has satisfied the ownership requirements. Such losses would be analogous to theft of cash from a safe. Though the loss may be within the scope of coverage, the insured may never be able to reasonably prove what was in the safe and what was taken. The safe analogy breaks down when one considers that it is not possible to make a backup copy of cash. Cryptocurrency, however, is digital and any number of copies can be made.

Ideally, the user works through a cryptocurrency exchange, such as Coinbase. In these situations, the exchange is usually able to provide the account and transactional data necessary to establish both ownership of currency in question and the transaction in question.

5. Determining the Amount of the Loss—Valuation of the Loss

One of the most noteworthy characteristics of cryptocurrency has been price volatility. The most well-known cryptocurrency, Bitcoin, rose in price 1,289 per cent from USD $998 to $13,860 during 2017, reaching a peak valuation of $19,343 on December 16, 2017.[292] As of June 13, 2018, the price had slid back down to $6,278—a 68 per cent decline off the December 16 peak. In the face of such volatility, what is the appropriate measure of valuation under a crime policy?

Most forms of property coverage provide for valuation as of the date that the loss occurred. However, as most crime polices are discovery-based, valuation provisions are typically geared toward the date of discovery, as with the Commercial Crime Policy and the Crime Protection Policy. Consistent with this approach, the ISO Include Virtual

[291] Al Modof, *Accountability: Bitcoin & Blockchain Insights: Making Digital Wallets Safer*, Warren Gorham & Lamont—Internal Auditing, 2018 WL 1666409.

[292] Digital Shadows, *supra* note 4 at 3.

Currency As Money Endorsement incorporates the following valuation provision:

> Valuation—Settlement
>
> (b) Virtual Currency
>
> Loss of "money" in the form of virtual currency but only up to and including its value at the close of business on the day the loss was "discovered" as determined by the rate of exchange published by the Exchange shown in the Schedule. We may, at our option, pay the value of the virtual currency in the United States of America dollar equivalent or replace it in kind.[293]

In the case of cryptocurrency, pricing volatility has the potential to produce perceived windfalls for either the insured or the carrier depending on the date used. Different valuation provisions apply depending on the type of covered property involved. Valuation of lost "money" is addressed in the Commercial Crime Policy as follows:

> Loss of "money" but only up to and including its face value. We will, at your option, pay for loss of "money" issued by any country other than the United States of America:
>
> (a) At face value in the "money" issued by that country; or
>
> (b) In the United States of America dollar equivalent, determined by the rate of exchange published in The Wall Street Journal on the day the loss was "discovered".

Valuation of lost "securities" is addressed in the Commercial Crime Policy as follows:

---

[293] Ins. Servs. Office, Include Virtual Currency As Money (Endorsement), Form CR 25 45 11 15.

> Loss of "securities" but only up to and including their value at the close of business on the day the loss was "discovered". We may, at our option:
>
> (a) Pay the market value of such "securities" or replace them in kind, in which event you must assign us all your rights, title and interest in and to those securities; or
>
> (b) Pay the cost of any Lost Securities Bond in connection with issuing duplicates of the "securities". . . . [emphasis added]

Whether cryptocurrency is defined as "money" (as in the ISO form) or as "securities" (as in the Great American coverage), it is submitted that the valuation provisions applicable to those categories of covered property should not automatically extend to the valuation of cryptocurrency. Cryptocurrency has unique characteristics which may justify a hybrid approach to valuation to reflect pricing volatility over time. Underwriting judgments will need to be made as to whether any time-based election would be at the option of the carrier or of the insured.

Given the extreme pricing volatility of many cryptocurrencies, it might even make sense to provide that the value of the indemnity—whether it takes the form of dollars or an in-kind cryptocurrency payment—be the average value of the dollar/cryptocurrency between the date of discovery and the date of indemnity. This can be illustrated with the following claim adjustment scenario:

> Date of discovery: December 16, 2017
> Loss: 10 bitcoins
> Equivalent USD: $193,430
>
> Date of indemnity payment: June 13, 2018
> Loss: 10 bitcoins
> Equivalent USD: $62,780

If the amount of indemnity is dollars or in-kind payment as of the date of settlement, the carrier will opt to pay 10 bitcoins, which the

insured may consider a windfall for the carrier. If the payment is at the option of the insured, it will opt for the dollar value as of the date of discovery ($193,430), which the carrier may likewise consider to be a windfall for its insured. A provision that averages the value of the two, resulting in an indemnity payment on June 13 of either $128,105 or 20.4 bitcoins,[294] may appropriately hedge the risk for both parties.[295]

It should be noted that the concept of a "Lost Securities Bond" would seem to have no cryptocurrency analogue, as there is no way to issue "replacement" cryptocurrency (nor any central authority capable of doing the issuing).

V.
CONCLUSION

Once one looks behind the "hype" surrounding cryptocurrency, it becomes apparent that cryptocurrency is establishing itself as part of the legitimate commercial ecosystem—a part that displays significant growth potential in years to come as fraud, security, regulatory and price volatility concerns are addressed. The question for crime and other insurers is not whether there should be coverage for cryptocurrency. That question is moot, given the market entrants already in the field in 2018. Rather, the question is what forms such coverage will take. Consequently, it is incumbent on insurers to carefully consider how they will address coverage for cryptocurrency, balancing the reasonable expectations of insureds with prudent underwriting and claim handling practices.

[294] Averaged U.S. dollar loss figure of $128,105, divided by $6,278 price of Bitcoin as of date of indemnity payment.

[295] It is appreciated that this might lead to concerns surrounding the carrier's control over the timing of payment. One way to address that might be to use the date not of actual payment, but rather the date that insurance proceeds legally become payable under the relevant state or provincial insurance legislation.