Governing the Ungovernable: Cryptocurrencies in Insolvency Proceedings

Gregory Azeff, Stephanie De Caria and Matthew McGuire[*]

I. INTRODUCTION

One of the hottest technology stories of the past few years has been that of Bitcoin, other cryptocurrencies and digital assets, which have, among other things, minted millionaires at a pace not seen since the wildest years of the "dot com boom" of the late 1990s. One California Lamborghini dealer reported that its monthly sales quintupled when Bitcoin hit US$19,000.[1]

Yet despite the enthusiastic proclamations of tech geeks, anarchists and other cryptocurrency early adopters, cryptocurrencies are not a panacea. There is a dark side to the technology; the anonymity of certain blockchain structures, combined with their borderless nature and the stringent privacy policies adopted by some cryptocurrency providers, make them ideal for exploitation by unscrupulous individuals as a means of hiding assets and transactions.

* Gregory Azeff is a member of the Law Society of Ontario and a Partner in the Insolvency & Restructuring Group at Miller Thomson LLP in Toronto. Stephanie De Caria is a member of the Law Society of Ontario and an Associate in the Insolvency & Restructuring Group at Miller Thomson LLP in Toronto. Matthew McGuire, CPA, CA, CFF, CAMS, AMLP, DIFA MAcc is a forensic accountant with crypto tracing experience and internationally recognized expert in anti-money laundering and counter-terrorist financing.

1 Melia Robinson, "Bitcoin millionaires are buying Lamborghinis as a status symbol of crypto wealth, and the carmaker says sales are rocketing" (1 April 2018), online: *Business Insider* <www.businessinsider.com/bitcoin-millionaires-are-buying-lamborghinis-2018-3>.

Predictably, sophisticated criminals are now using cryptocurrencies at an increasing rate for two principal purposes: (1) to conduct illegal transactions; and (2) to launder ill-gotten gains.[2] There is a growing body of evidence that cryptocurrencies are being employed in drug and human trafficking,[3, 4] arms dealing[5] and terrorist financing,[6] both as means of payment as well as for washing the proceeds.[7]

In light of the above, a number of governments, including Canada, have taken steps toward incorporating cryptocurrencies in their domestic criminal, anti-money laundering and counter-terrorist financing legislation.[8] Yet such steps have been slow and tentative, and have not kept pace with the proliferation of cryptocurrencies. Courts dealing with criminal and black-market issues have tended to adopt pragmatic approaches that stretch the parameters of existing jurisprudence regarding "traditional" currencies to bring cryptocurrencies into the fold, so as to fulfill the policy purposes — if not the express content — of applicable

2 "Digital detergent — Crypto money-laundering: Will crypto help the money-launderers of the future?" (26 April 2018), online: *The Economist* <www.economist.com/finance-and-economics/2018/04/26/crypto-money-laundering> ["Digital Detergent"].

3 Timothy Revell, "AI uses bitcoin trail to find and help sex-trafficking victims" (24 August 2017), online: *NewScientist* <www.newscientist.com/article/2145355-ai-uses-bitcoin-trail-to-find-and-help-sex-trafficking-victims>.

4 See, for example, *R v Gray-Lewis*, 2018 ONCJ 560, and *R v Lopez*, 2018 ONSC 4749, where the accused used bitcoin to pay for online prostitution advertisements.

5 Giacomo Persi Paoli et al, "Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web" (19 July 2018), online: *RAND Corporation* <www.rand.org/pubs/research_reports/RR2091.html>.

6 Tom Keatinge, David Carlisle & Florence Keen, "Virtual currencies and terrorist financing: assessing the risks and evaluating responses" (May 2018), online: *Study for the TERR Committee of European Parliament* <www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf>.

7 Digital Detergent, *supra* note 2.

8 "Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2018" (2018) C Gaz I, 1830.

legislation.[9] But notwithstanding such efforts, neither existing legislation nor existing judicial tools are sufficient to deal with the unique nature of cryptocurrencies.

For good reason, even these modest efforts toward dealing with cryptocurrencies have thus far been almost entirely focused on the criminal sphere. Commercial law has been much slower to adapt to and accommodate the new reality of cryptocurrencies, particularly where — as is almost always the case with cryptocurrencies — the issues cross national borders. Domestically in Canada and other countries, legislative and judicial treatment of cryptocurrencies has been hesitant and inconsistent, and consequently there has been little cross-border effort toward a unified approach, despite the obvious need for same.

Insolvency practitioners faced with cryptocurrency-related issues for the first time have a steep learning curve to climb. Insolvency proceedings involving cryptocurrencies have often been frustrated by the complexities and characteristics of cryptocurrencies. As described below, in some cases bankruptcy trustees and other insolvency administrators have been unable to perform their basic duties to locate and secure assets where cryptocurrencies are involved, and even when these steps have been completed, the monetization and distribution processes that follow have been marked by stakeholder disagreement regarding fundamental procedural and substantive issues. The volatile nature of cryptocurrencies is such that decisions regarding such issues can result in massive swings in stakeholder recoveries.

Domestically, additional legislation and judicial action will be needed to assist insolvency administrators to locate, secure and monetize cryptocurrencies. In addition, national

9 See for example *United States v Faiella*, 39 F Supp (3d) 544 (SD NY 2014), in which the United States District Court, SDNY found that Bitcoin is "money" for the purpose of upholding an indictment for operating an unlicensed money transmitting business. See also *United States v Murgio*, 209 F Supp (3d) 698 (SD NY 2016).

governments will have to cooperate toward unified and consistent transnational treatment of cryptocurrencies. Regardless of the question of whether they have any real social utility, it seems clear that cryptocurrencies are not going away anytime soon. Absent the promulgation of carefully-crafted legislation, as well as an expansion of existing legal doctrines to account for the unique nature of cryptocurrencies and their remarkably volatile trading value, we will likely continue to see results at odds with the spirit and intent of existing bankruptcy and insolvency law.

Many of the insolvency cases considered in this article involve cryptocurrency exchanges, *ie*, entities in the business of facilitating the purchase, sale, trade and transfer of cryptocurrencies. However, the article will also consider cases involving cryptocurrency assets, focusing on the unique challenges associated with tracking and tracing them, and monetizing them.

The article commences with a primer on cryptocurrencies, describing their origin, technology basics, unique characteristics and resulting challenges. Next, the article reviews the domestic and international legislative and judicial treatment, with particular focus on insolvency proceedings and the difficulties faced by insolvency administrators and other professionals. The article concludes with a series of recommendations and proposals regarding, among other things, future legislative treatment, as well as diplomatic efforts toward a unified international approach.

II. BACKGROUND

It has been noted that the capital structures of companies in the 21st century starkly contrast with those of prior eras.[10] Once

10 Dean Baker, Arjun Jayadev & Joseph Stiglitz, "Innovation, Intellectual Property and Development: A Better Set of Approaches for the 21st Century" (July 2017), online: <www8.gsb.columbia.edu/faculty/jstiglitz/sites/jstiglitz/files/IP%20for%2021st%20Century%20-%20EN.pdf>.

driven by hard assets such as real property, natural resources and manufacturing capacity, many contemporary business enterprises are highly reliant — and valued upon — intangible assets such as copyright, licenses, trademarks, brand equity, etc.[11] Such intangibles are not new, but rather, have simply become more valuable.

Cryptocurrencies have disrupted the traditional order wherein national currencies are the only real trustworthy repository for value. What was once the purview of only central banks is now the responsibility of the coding for nearly 2,000 unique new cryptocurrencies created in less than a decade. Technology has once again birthed a new "thing" with its own value and characteristics, qualitatively and quantitatively different than anything we have seen before. As was the case during the dot com boom, we are again facing a new agent that is potentially incredibly disruptive to the existing marketplace.

1. The Origin of Cryptocurrencies

The creation of cryptocurrencies is shrouded in mystery, and is one of the more captivating stories in technology. "Satoshi Nakamoto" is the pseudonym used by the computer programmer(s) who created cryptocurrencies. In 2008, Nakamoto launched bitcoin with a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System", and in January 2009, Nakamoto released the first cryptocurrency software that launched the network and the first units of cryptocurrency, called bitcoins.[12] As part of the implementation, Nakamoto also devised the first blockchain database, and in the process, was the first to solve the so-called "double-spending problem", a potential flaw in any digital cash

11 Ocean Tomo, LLC, "Intangible Asset Market Value Study" (2017), online: *Ocean Tomo, LLC* <www.oceantomo.com/intangible-asset-market-value-study>. S&P market value attributable to intangible assets rose from 17 per cent in 1975 to 84 per cent in 2015.

12 L S, "Who is Satoshi Nakamoto?" (2 November 2015), online: *The Economist* <www.economist.com/the-economist-explains/2015/11/02/who-is-satoshi-nakamoto>.

protocol in which the same single unit of digital currency can be spent more than once.[13]

Yet Nakamoto did not step forward for applause for the accomplishment, or even recognition; to this day, no one even knows his, her or their identity. Adrian Chen observes that the "...search for Nakamoto has a tinge of irony: it's an old-school mystery born in an age of Internet-enabled access to all world knowledge, which threatens to make the entire concept of mystery obsolete".[14]

2. The Basics of Cryptocurrency Technology

A cryptocurrency is a digital asset based on blockchain technology. A blockchain is a digital transaction ledger, *ie*, a continuously growing list of records, called "blocks", which are linked and secured using cryptography. Once a certain amount of information has accumulated, a block is created and stored. Blocks are stored in chronological order, such that every new block is linked to the previous by storing information about the previous block on the newly created one.[15]

With each block connected to the previous, a chain of blocks is formed — in other words, a "blockchain". Each block in the chain contains a cryptographic hash of the previous block, a timestamp, and transaction data, such that new blocks cannot be added in between existing blocks and therefore, the chronological data contained in the blocks cannot be manipulated.[16]

A blockchain is "...an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable

13 Usman W Chohan, "The Double Spending Problem and Cryptocurrencies" (23 December 2017), online: *Social Science Research Network (SSRN)* <papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174>.

14 Adrian Chen, "We Need to Know Who Satoshi Nakamoto is" (9 May 2016), online: *The New Yorker* <www.newyorker.com/business/currency/we-need-to-know-who-satoshi-nakamoto-is>.

15 Zach Church, "Blockchain, Explained" (25 May 2017), online: *MIT Management Sloan School* <mitsloan.mit.edu/newsroom/articles/blockchain-explained/>.

16 *Ibid.*

and permanent way".[17] Blockchain technology has applications well beyond currency. In short, it offers a way for people who do not trust or even know each other to create a definitive record of ownership and transfer. "It is a way of making and preserving truths."[18] Other potential applications of blockchain technology include pharmaceutical manufacturing, produce tracking, financial institutions, real estate transactions, hospitals, corporate capital structures and governments.

Much of the strength and appeal of cryptocurrencies, and their users' faith in them, stems from this use of distributed transaction ledgers ("DTL"). DTL use a peer-to-peer network that collectively adheres to a protocol for inter-node communication and validating new blocks.[19] By design, a blockchain is resistant to modification of the data. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires network consensus.[20]

Cryptocurrencies are dependent on advanced cryptography. Cryptography is the practice and study of techniques for secure communication in the presence of third parties, referred to as "adversaries".[21] Modern cryptography is based heavily on

17 Marco Iansiti & Karim Lakhani, "The Truth About Blockchain" (January-February 2017), online: *Harvard Business Review* <hbr.org/2017/01/the-truth-about-blockchain>.

18 "The Great Chain of Being Sure About Things" (31 October 2015), online: *The Economist* <www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things>.

19 Andrea Pinna & Wiebe Ruttenberg, "Distributed Ledger Technologies in Securities Post-Trading" (2016) European Central Bank Occasional Paper Series No 172 at 8-9, online: <www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf>.

20 Indeed, a theoretical issue arising with cryptocurrencies is the control of a blockchain by renting sufficient processing power to achieve the consensus required of that chain and unilaterally impacting transaction outcomes. See, for instance: Joseph Bonneau, "On hostile blockchain takeovers or Goldfinger attacks revisited" (March 2017), online: <materials.dagstuhl.de/files/17/17132/17132.JosephBonneau.ExtendedAbstract.pdf>.

21 Ronald L Rivest, "Cryptography", in J Van Leeuwen, ed, *Handbook of Theoretical Computer Science* (New York**:** Elsevier, 1990).

mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms difficult to break in practice by any adversary.[22] The information contained in each block undergoes a process called cryptography, which essentially scrambles the data into a non-decipherable format.[23] With such a process, the data contained in the block chain is capable of being distributed but not copied, thereby protecting the information from being tampered with or edited.

Cryptocurrencies may be described as having six essential conditions:

1. The system tracks units and ownership.
2. No central authority is required.
3. The system determines the conditions for creation of new units.
4. Unit ownership can be transferred.
5. Exclusive unit ownership can be proved by a transferee.
6. The system prohibits "double spending" of a single unit.[24]

Cryptocurrencies have been described as being the only type of currencies with the following three features: (1) anonymity; (2) decentralized governance; and (3) protection from double spending.[25] The anonymity of cryptocurrencies has been increasingly challenged, particularly those where the chain of transactions is publicly available. Researchers have concluded that identity linkage was possible in over 60 per cent of Bitcoin transactions involving online purchases.[26]

---

22 *Ibid.*

23 *Ibid.*

24 Jan Lansky, "Possible State Approaches to Cryptocurrencies" (2018) 9:1 *Journal of Systems Integration* 19 at 19, online: <www.si-journal.org/index.php/JSI/article/view/335>.

25 *Ibid* at 20.

26 "Bitcoin Transactions Aren't as Anonymous as Everyone Hoped"

3. Acquisition of Cryptocurrencies

Cryptocurrency units may be acquired in four principal ways:

Initial Coin Offering. A person can "subscribe" for cryptocurrency units through an "initial coin offering" ("ICO") or subsequent issuance by a cryptocurrency provider. [27] The terms "coin" and "token" are often used interchangeably, however, the former refers to units issued and supported by its own blockchain, such as Bitcoin or Ethereum, whereas the latter refers to units issued and supported by another existing blockchain, such as Ethereum, or Stellar.[28] Since they have begun attracting the interest of securities regulators, some token issuers are referring to their ICOs as Security Token Offerings ("STO"), to indicate that the issuance is designed to comply with a recognized regulatory framework.[29]

Mining. Many cryptocurrencies depend on the DTL, in which at any given time, a particular blockchain exists on a peer-to-peer network of thousands of computers on the Internet. "Data miners" are persons who agree to certify transactions over the network, by solving an algorithm, and are remunerated by the issuance of a fixed number of cryptocurrency units per transaction. Each transaction adds a block to the chain, which is then corroborated across the network.[30] The constantly growing blockchain requires the

(23 August 2017), online: *MIT Technology Review* <www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/>.

27 Coin offerings may be offered without monetary consideration as a means of marketing the coin and increasing its adoption rate, known as an "Air Drop".

28 "Difference Between Coins and Tokens" (20 July 2018), online: *Token Desk* <www.tokendesk.io/difference-between-coins-and-tokens/>.

29 "Security Tokens Set to Take Centre Stage in 2019" (22 June 2018), online: *Nasdaq* <www.nasdaq.com/article/security-tokens-set-to-take-center-stage-in-2019-cm982207>.

30 See Michel Rauchs *et al*, "Distributed Ledger Technology Systems: A Conceptual Framework" (August 2018) at 26, online: *Cambridge Centre for Alternative Finance* <www.jbs.cam.ac.uk/fileadmin/

use of increasingly powerful computers. For example, as of June 2018, the Bitcoin blockchain reached approximately 173 gigabytes,[31] requiring a staggering amount of processing power to validate. This requirement has created an entire cottage industry, in which data miners establish enterprises in places like Siberia, where cheap electricity and cool a climate combine to create competitive advantages for businesses dependent on operating and cooling massive computer server farms.[32]

Secondary Markets. Parties can buy or sell cryptocurrency units through any number of online exchanges. Parties establish accounts with an exchange, and fund their accounts with traditional currencies and/or cryptocurrencies. The exchange matches buyers and sellers of cryptocurrencies, and accounts are credited accordingly, with the exchange receiving a commission per transaction.[33] Parties can also buy and sell cryptocurrencies directly, without the use of an exchange.

Commercial Transactions. Parties can use cryptocurrency units as payment in some commercial transactions. While the number of commercial vendors that accept cryptocurrency units as payment in day-to-day transactions continues to rapidly expand, such transactions still barely register as a percentage of overall gross domestic product ("GDP").[34]

---

user_upload/research/centres/alternative-finance/downloads/2018-08-20-conceptualising-dlt-systems.pdf>.

31 "Size of the Bitcoin blockchain from 2010 to 2018, by quarter (in megabytes)" (June 2018), online: *Statista* <www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/>.

32 Amelia Trapp, "Conditions of Eastern Siberia Appeal to Crypto Miners" (5 January 2018), online: *BitcoinNews* <bitcoinnews.com/conditions-of-eastern-siberia-appeal-to-crypto-miners>.

33 The top 3 exchanges by trailing 30-day volume on 17 September 2018 were Binance, OKEx and Huobi. "Top 100 Cryptocurrency Exchanges by Trade Volume" (17 September 2018), online: *CoinMarketCap* <coinmarketcap.com/rankings/exchanges/>.

34 See Kate Rooney, "Your guide to cryptocurrency regulations around the world and where they are headed" (27 March 2018),

Once acquired, cryptocurrency units are held in "digital wallets", which are accounts that utilize "public-key cryptography", or asymmetric cryptography.[35] This cryptographic system uses pairs of keys: "public keys" intended for widespread dissemination, and "private keys" known only by the owner. Such systems accomplish two functions: authentication and encryption. In a public-key encryption system, any person can encrypt a message using the receiver's public key, but the encrypted message can only be decrypted with the receiver's private key.[36]

As noted above, the public key can be openly distributed without compromising system security. Effective security only requires that the private key be kept private.[37] The private key is the "password" that allows a holder to spend or transfer cryptocurrency units.[38] Importantly, unlike symmetric key algorithms, public key algorithms do not require a secure channel for the initial exchange of secret keys between the parties.[39] This feature allows strangers to trust each other in a transaction notwithstanding their complete anonymity.

4. Problems with Cryptocurrencies

The disruptive pattern of the emergence of cryptocurrencies is very familiar in the digital age. First, a handful of computer

online: *CNBC*, <www.cnbc.com/2018/03/27/a-complete-guide-to-cyprocurrency-regulations-around-the-world.html>.

35 Toshendra Kumar Sharma, "How does blockchain use public key cryptography?" (27 January 2018), online: *Blockchain Council* <www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography>.

36 William Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed (Upper Saddle River, NJ: Prentice Hall, 2013) at 165.

37 *Ibid.*

38 For example, Bitcoin uses a 256-bit number, which in hexadecimal is 32 bytes, or 64 characters in the range 0-9 or A-F.

39 William Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed (Upper Saddle River, NJ: Prentice Hall, 2013) at 165.

wizards create and embrace a technology that threatens to undermine or even replace established markets and institutions. Second, market players such as regulators who should be paying the most attention to the emergence of such technologies instead choose to ignore the threat. Third, the technology proliferates, is embraced by the consumer, and starts to do exactly what it initially threatened to do: disrupt incumbent markets and institutions. At this point, regulators take action, often as a result of the pleading by the very same markets and institutions who initially advised the regulators against such action, on the basis that it is "just a fad". Given the speed of change in the digital world, the resulting delays can be catastrophic.

Efforts to regulate cryptocurrencies have been hampered by a lack of basic understanding among members of the public and government as to the nature and threat posed by cryptocurrencies, and a resulting lack of political impetus for legislators to address them. The Ontario Securities Commission recently published a report that analyses the results of a survey of over 2,500 Ontarians aged 18 or older regarding investment in cryptocurrencies.[40] According to the survey results, while approximately 500,000 individuals in Ontario own cryptocurrencies, only 5 per cent of respondents identified themselves as familiar enough with cryptocurrency details to explain them to others.[41] The survey found that 16 per cent of cryptocurrency owners participated in an ICO, but less than a third of them researched whether the ICO was regulated.[42]

In other words, despite the enthusiasm with which cryptocurrencies have been embraced by investors, to the

40 Ontario Securities Commission, Investor Office, "Taking Caution: Financial Consumers and the Cryptoasset Sector" (28 June 2018), online: *Ontario Securities Commission* <www.osc.gov.on.ca/documents/en/Investors/inv_research_20180628_taking-caution-report.pdf>.

41 *Ibid* at 1, 5.

42 *Ibid* at 3.

average consumer, cryptocurrency investments are akin to gambling without knowing the terms of the bet. Traditional disclosure requirements within public trading markets and other business market norms such as the "know your client" ("KYC") rules are generally non-existent. As such, cryptocurrencies are not suitable investments for all but the savviest investors. Yet the "gold rush" mentality and "fear of missing out" have given rise to a strong anti-regulation bias among those participants who most need regulatory oversight and protection.

5. Lack of Regulation

Domestic regulatory oversight of cryptocurrencies *qua* investment vehicles has not kept pace with their proliferation. Domestic regulatory authorities — often overburdened with coping with their existing mandates — have been reluctant to expand their attention to new areas, and/or have sought to shift the responsibility to other agencies, who are similarly reluctant to deal with them. Cryptocurrencies do not fit within traditional paradigms, and in many cases appear to have slipped between the cracks of existing regulatory scopes of authority.[43]

6. Utility in Black Market & Illegal Transactions

The United Nations Office on Drugs and Crime estimates that between US$800 billion and $2 trillion is laundered annually around the world, representing between 2 per cent and 5 per cent of global GDP.[44] The characteristics of cryptocurrencies — *ie*, their borderless nature, anonymity, irreversibility and speed — make them ideal for exploitation by

43 See, for example, Bank of Canada, "Decentralized E-Money (Bitcoin)" (April 2014), online: *Bank of Canada* <www.bankofcanada.ca/wp-content/uploads/2014/04/Decentralize-E-Money.pdf>.

44 See "Money-Laundering and Globalization", online: *United Nations Office on Drugs and Crime* <www.unodc.org/unodc/en/money-laundering/globalization.html>.

unscrupulous individuals as a means of hiding assets and transactions. The head of Europol, Europe's international police force, has estimated that 3-4 per cent of the continent's annual criminal revenues are now laundered through cryptocurrencies.[45]

Cryptocurrencies typically represent a single step in the money-laundering process. Notwithstanding their widespread and seemingly overnight proliferation, cryptocurrencies are not the same as cash, insofar as they lack the widespread and instant acceptance of same. Only the smallest fraction of ordinary-course consumer transactions can be carried out through cryptocurrencies. As such, large money launders are forced to combine sophisticated technology-based tactics such as "atomic swaps" — *ie*, pre-programmed, very high-speed series of transfers and exchange transactions — with traditional techniques such as "smurfing", which involves breaking up large deposits into very small amounts of cash, and the use of "money mules", *ie*, individuals who withdraw cash, which they then spread over numerous accounts in amounts small enough to avoid scrutiny.[46]

For example, in the Netherlands, a UK citizen was jailed in March 2018 for converting approximately US$13.2 million in dirty cryptocurrency by selling it and transferring amounts into his bank account, then withdrawing smaller amounts of cash and delivering it to criminals, minus a commission.[47] As another example, Europol recently determined the manner in which European criminal organizations used cryptocurrencies to pay a Colombian drug cartel for cocaine.[48] The European groups used cryptocurrency exchanges to convert euros into anonymous cryptocurrencies, which were then transferred to a digital wallet registered in Colombia and converted to pesos through an online exchange. Local currency was then

45 Digital Detergent, *supra* note 2.
46 *Ibid.*
47 *Ibid.*
48 *Ibid.*

withdrawn in cash in Colombia, then deposited by money mules into dozens of bank accounts.[49]

The need for money launderers to eventually bring digital currencies back into the "real world" is an important consideration, as it may represent an Achilles' heel to the washing process. In such cases, cryptocurrencies have created a break in the chain of traceable transactions. The conversion back to cash/traditional currencies is a critical point in uncovering the laundering scheme.

Techniques such as smurfing and the use of money mules may render individual laundering transactions effectively invisible to the average bank teller, but not to modern artificial intelligence-based ("AI-based") pattern recognition systems.[50] Financial market regulators have long used such technologies to identify anomalous transactions and patterns as a way of identifying, for example, insider trading and other capital market abuses.[51] Governments sincerely interested in curbing money laundering should adopt and apply these technologies on a fast track basis. Japan, for instance, is developing AI-based systems to predict money laundering and terrorist attacks.[52]

Unfortunately, the use of cryptocurrencies to conduct the illegal transactions themselves poses a much more difficult challenge. In addition to drug trafficking, cryptocurrencies are now used in terrorism financing, arms dealing, child

49 *Ibid.*

50 Patrick Craig and Mark Gregory, "How banks can trust AI to combat money laundering" (18 July 2018), online: *International Banker* <internationalbanker.com/finance/how-banks-can-trust-ai-to-combat-money-laundering/>.

51 Scott W Bauguess, "The Role of Machine Readability in an AI World" (3 May 2018), online: *US Securities and Exchange Commission* <www.sec.gov/news/speech/speech-bauguess-050318>.

52 "Japan developing 'pre-crime' artificial intelligence to predict money laundering and terror attacks" (31 August 2018), online: *South China Morning Post* <www.scmp.com/news/asia/east-asia/article/2162239/japan-developing-pre-crime-artificial-intelligence-predict-money>.

pornography, and human trafficking. With the stakes so high, it is incumbent on national governments to cooperate toward the creation of a united front and approach to the counterattack as quickly as possible. Such rules will not only aid in the identification and solution of illegal transactions, but will also help set some parameters around the economic space in which cryptocurrencies live and operate.

III. LEGISLATIVE TREATMENT OF CRYPTOCURRENCIES

1. Typical Pattern of Domestic Legislative Response

As noted above, current domestic treatment of cryptocurrencies varies around the globe. Legislative responses have ranged from outright bans by central banks, while in some cases allowing for the possibility of future national cryptocurrencies, to deeming all cryptocurrency transactions illegal, to attempts to normalize and regulate them.[53]

Predictable government self-interest has generally defined the typical pattern of progression of domestic legislative response. Many jurisdictions begin by addressing the tax implications of cryptocurrency use. Often, such opening steps involve little more than providing policy-based guidance as to transactional and asset characterization of cryptocurrencies in the context of existing tax regimes. Next, in the typical pattern the state takes steps to address cryptocurrencies in its existing anti-money laundering ("AML") statutes.[54]

---

53 Library of Congress, "Regulation of Cryptocurrency Around the World" (31 July 2018), online: *Library of Congress* <www.loc.gov/law/help/cryptocurrency/world-survey.php>. Algeria, Bolivia, Morocco, Nepal, Pakistan, and Vietnam ban any and all activities involving cryptocurrencies, for example.

54 Canada is a perfect example of this pattern. See Canada Revenue Agency, CRA Views 2013-0514701I7, "Bitcoins" (23 December 2013), in which the Canada Revenue Agency specified tax treatment of cryptocurrency tokens in 2013. This statement was followed shortly after by royal assent to Bill C-31, which amended Canada's

We are only now seeing the first tentative steps toward accommodation of cryptocurrencies in domestic commercial law in some jurisdictions.

2. Canadian Legislative Response

Canada has followed the most common pattern of cryptocurrency regulation. The Government of Canada has confirmed that cryptocurrencies are a digital type of currency and are a form of electronic money, not available as bills or coins.[55] While the Government of Canada has recognized that the public can use digital currencies to buy goods and services on the Internet or in stores that accept digital currencies, and that digital currencies are capable of being bought and sold on an open exchange (*ie*, a stock market), cryptocurrencies are not considered "legal tender" in Canada.[56]

Under the Canada *Currency Act,*[57] a tender of payment is a legal payment if it is made in coins issued under the *Royal Canadian Mint Act*,[58] or bank notes issued under the *Bank of Canada Act*.[59] Digital currencies do not fall within this definition of legal tender. Cryptocurrencies are not supported by any government or central authority, such as the Bank of Canada, and are not managed or overseen in the same manner

---

Proceeds of Crime (Money Laundering) and Terrorist Financing Act, SC 2000, c 17, so as to treat virtual currencies as "money service businesses" for purposes of anti-money laundering laws. See Bill C-31, *An Act to implement certain provisions of the budget tabled in Parliament on February 11, 2014 and other measures*, 2nd Sess, 41st Parl, 2014, cl 23 (assented to 19 June 2014), SC 2014, c 20.

55 Government of Canada, "Economic Action Plan 2014" (14 February 2014), online: *Government of Canada* <www.budget.gc.ca/2014/docs/plan/pdf/budget2014-eng.pdf>.

56 Financial Consumer Agency of Canada, "Digital Currency" (19 January 2018), online: *Government of Canada*<www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html> ["Digital Currency"].

57 *Currency Act*, RSC 1985, c C-52, s 8(1).

58 *Royal Canadian Mint Act*, RSC 1985, c R-9.

59 *Bank of Canada Act,* RSC 1985, c B-2.

as are financial institutions like banks or credit unions. Only the Canadian dollar is considered official currency in Canada.[60]

Nonetheless, Canadian tax rules apply to digital currency transactions and cryptocurrencies are subject to the *Income Tax Act*[61] as if it was official Canadian currency. Specifically:

- Where digital currency is used to pay for goods or services, the rules for barter transactions apply.[62] A barter transaction occurs when two people, dealing with each other at arm's length, agree to a reciprocal exchange of goods or services and carry out that exchange without using legal currency. In such transaction, the value must be brought into the "givers" income and is taxable income. The amount is the price which the tax payer would have normally charged for such services in Canadian dollars.[63]
- When digital currency is bought or sold like a commodity (*ie*, like a security), the resulting gains or losses are to be declared as taxable income or capital for the taxpayer[64] in accordance with the tax rules for disposition of securities.[65]

60 Digital Currency, *supra* note 56.

61 *Income Tax Act*, RSC 1985, c 1 (5th Supp).

62 Canada Revenue Agency, "What You Should Know About Digital Currencies" (17 March 2015), online: *Canada Revenue Agency Fact Sheets 2015* <www.canada.ca/en/revenue-agency/news/newsroom/fact-sheets/fact-sheets-2015/what-you-should-know-about-digital-currency.html> ["What You Should Know"].

63 Canada Revenue Agency, Interpretation Bulletin IT-490, "Barter Transactions" (5 July 1982), online: *Canada Revenue Agency Forms and Publications* <www.canada.ca/en/revenue-agency/services/forms-publications/publications/it490/archived-barter-transactions.html>.

64 What You Should Know, *supra* note 62.

65 Canada Revenue Agency, Interpretation Bulletin IT-479R, "Transactions in Securities" (29 February 1984), online: *Canada Revenue Agency Forms and Publications* <www.canada.ca/en/revenue-agency/services/forms-publications/publications/it479r/archived-transactions-securities.html>.

- Where an employee receives digital currency as payment for salary or wages, the amount, computed in Canadian dollars, will be included in the employee's income pursuant to subsection 5(1) of the *Income Tax Act*.[66]

The variations in treatment described above reflect the different roles that cryptocurrencies can play in a transaction.

3. Canadian Commercial and Insolvency Law

Canadian insolvency legislation does not directly address cryptocurrencies. For constitutional reasons, the treatment of property in insolvency administration is typically defined under the laws of the provinces, generally by personal property legislation such as the *Personal Property Security Act (PPSA)*[67] of Ontario and other common law provinces. Under Ontario personal property legislation, "money" is defined as a medium of exchange authorized and adopted by the Parliament of Canada as part of the currency of Canada or by a foreign government as part of its currency.[68]

As noted earlier in this article, cryptocurrency is not authorized or adopted by the Parliament of Canada and is not considered legal tender. While it resembles money in that it is used for the purposes of purchase or trade and is taxable, it is not considered money for the purposes of Canadian personal property legislation.

Of the many categories of personal property, cryptocurrencies would most appropriately fit within the definition of an "intangible". Under Ontario's personal property legislation an intangible is defined as all personal property, including choses in action, that is not goods, chattel paper, documents of title, instruments, money or investment

66 What You Should Know, *supra* note 62.

67 *Personal Property Security Act*, RSO 1990, c P.10 [*PPSA*], s 29. Note that due to the substantial similarity among the various provincial personal property security regimes, the term "*PPSA*" applies to them interchangeably unless otherwise noted.

68 *Ibid*, s 1(1).

property.[69] Other provincial personal property legislation adopts either the same, or a very similar definition of money.[70]

There is no Canadian jurisdiction that has enacted amendments to directly address cryptocurrency assets or to address the consequences of accepting payment in cryptocurrency in a commercial transaction. *PPSA* legislation typically allows money, cheques and other negotiable instruments to be transferred free and clear of security interests.[71] But these provisions do not apply to cryptocurrencies. As such, a party accepting cryptocurrency as payment takes it subject to any existing security interests. Further, personal property law has not yet enacted amendments to address how to realize on cryptocurrency collateral, making enforcement of cryptocurrency security difficult.

4. Other Issues with Cryptocurrencies Qua Collateral

As described above, parties accepting cryptocurrency units as payment must be cognizant of the risk that the units do so subject to any security interests. Cryptocurrencies pose different risks to lenders seeking to secure loans against them.

In addition to the weakness of cryptocurrencies for value storage due to their extreme volatility,[72] lenders accepting

69 *Ibid.*

70 *Personal Property Security Act*, RSBC 1996, c 359, s 1(1); *Personal Property Security Act*, RSA 2000, c P-7, s 1(1)(cc); *The Personal Property Security Act*, SS 1993, c P-6.2, s 2(1)(bb); *The Personal Property Security Act*, SM 1993, c 14, CCSM c P35, s 1; *Personal Property Security Act*, SNB 1993, c P-7.1, s 1(1); *Personal Property Security Act*, SNS 1995-96, c 13, s 2(1)(aa); *Personal Property Security Act*, RSPEI 1988, c P-3.1, s 1(aa); *Personal Property Security Act*, SNL 1998, c P-7.1, s 2(1)(aa); *Personal Property Security Act*, RSY 2002, c 169, s 1(1); *Personal Property Security Act*, SNWT 1994, c 8, s 1(1); *Personal Property Security Act*, SNWT (Nu) 1994, c 8, s 1(1).

71 Ontario *PPSA, supra* note 67.

72 See David Yermack, "Is Bitcoin a Real Currency? An Economic Appraisal" (2013), National Bureau of Economic Research Work-

cryptocurrency units as collateral face three principal types of risk: (1) that the borrower will deal with the collateral despite the lender's security interest; (2) unauthorized access by third parties; and (3) that the lender will be unable to access the borrower's private key or wallet.

Even where a lender perfects its security interest in cryptocurrency units through registration under the *PPSA*, the borrower will not be prevented from transferring them to a third party. Treating cryptocurrency units as intangibles rather than currency creates complications, uncertainty and inefficiencies, particularly in commercial transactions. For example, it would be unreasonable to expect that vendors in ordinary course transactions would conduct *PPSA* searches for every sale in which cryptocurrency units are used as payment, yet the existing regime would seem to make this a requirement of the due diligence process.[73]

As discussed above, digital wallets are encrypted to protect them from unauthorized access.[74] The cryptography associated with cryptocurrencies makes it effectively impossible to determine a private key. However, digital wallets can be the targets of hacking, phishing, and other scams that plague traditional bank accounts, giving rise to the risk of digital theft.[75]

---

ing Paper No 19747, online: <www.nber.org/papers/w19747.pdf> at 2 ["Yermack"].

73 Timothy Jones & Dillon Collett, "Cryptocurrency Assets Under Insolvency and Personal Property Security Law" (2018) 30:4 *Commercial Insolvency Reporter* 27 ["Jones"].

74 At page 7.

75 See Alhuseen O Alsayed, "E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities" (January 2017) *International Journal of Emerging Technology and Advanced Engineering*, 7:1 at 110-112. Phishing attacks have become one of the most common financial crimes. Phishing is the fraudulent attempt to obtain sensitive information, such as usernames and passwords, by posing as a trustworthy entity in an electronic communication.

Should this footnote be revised to refer to specific section of article instead? Part, title number?

A party seeking to enforce a security interest in cryptocurrency may face a number of different issues that could frustrate its efforts to locate, secure and monetize such collateral. Even assuming that the borrower has not transferred the units to a third party, the lender (or insolvency administrator, as discussed in section IV below) will not be able to assert control over the collateral without access to the digital wallet and private key.

IV. CRYPTOCURRENCY ISSUES IN INSOLVENCY CASES

While currencies may have many different forms, they are intended to play three roles: (1) a medium of exchange; (2) a unit of account; and (3) a store of value. While the increasing acceptance of cryptocurrencies by merchants arguably satisfies the first of these, cryptocurrencies perform the second and third poorly.

As described above, cryptocurrencies are incredibly volatile. This volatility severely undermines the utility of cryptocurrencies utility as a unit of account or value store.[76]

The poor performance of cryptocurrencies as a unit of account or store of value pose particular problems for insolvency professionals, who are called on to solve "money problems". But how do you solve a problem that is not ascertainable? How do you locate and define a problem when the problem is in a constant state of flux? The volatility associated with cryptocurrencies is such that quantifying the scale of the problem may be a continuing exercise that requires ever-evolving approaches and solutions.

Given the relative novelty of cryptocurrencies, it can be safely assumed that most insolvency professionals have little more knowledge of cryptocurrencies than the average consumer, and no experience in dealing with them in the context of an administration. As such, for the purposes of discussion, it may

76 Yermack, *supra* note 72.

be useful to describe several cryptocurrency-related challenges that may be faced by a bankruptcy trustee or other estate administrator in insolvency proceedings.

1. Cryptocurrency Issues in Insolvency Proceedings

Consider the following scenario: A company ("debtor") invests in cryptocurrencies, lusting after the promise of massive returns. Third parties invest in the debtor, also hoping for outsized gains. But unfortunately, threats such as massive volatility, insider fraud or outsider hacking materialize, rendering the debtor insolvent, and an insolvency proceeding is commenced.

An estate administrator is appointed by a court to manage the estate. The administrator takes over the debtor and investigates its books and records, and begins its efforts to identify, locate and secure the debtor's assets for the benefit of the creditors and other stakeholders. It is here that things fall apart.

In the normal course, traditional assets can be readily identified, itemized, ascribed a monetary value and tallied up to a grand total. But in the case of cryptocurrency assets, an administrator may discover that the value has apparently disappeared into thin air. In some cases, this may be the result of "hacking" — *ie*, a third party has exploited vulnerabilities in the debtor's information systems and stolen the cryptocurrencies by effecting unauthorized transfers of same. In other cases, unscrupulous company insiders may have removed the digital assets from the reach of the administrator. Or, almost equally disastrous, the economic value of the digital asset may have evaporated overnight. In any of these circumstances, the administrator's efforts to secure and monetize the assets are effectively stonewalled.

2. Challenges for Insolvency Administrators

The scenario posited above raises a myriad of challenges to an insolvency administrator armed with only traditional tools.

The first step for insolvency administrators is typically to identify and secure assets. But when it comes to cryptocurrencies, existing enforcement mechanisms such as mandatory or prohibitive injunctions, stays of proceedings, contempt proceedings, etc, may be rendered meaningless. Court orders cannot crack cryptography, domestic legislation loses its effect at national borders, and injunctions are ineffective when a perpetrator is outside of the court's geographic jurisdiction. Even the speediest cross-border cooperation between courts in different jurisdictions cannot possibly keep pace with a practically instantaneous sequence of electronic cross-border transfers.

Furthermore, even where cryptocurrency units can be secured, the administrator next faces the question of what to do with them. Cryptocurrency volatility can undermine even the most tightly-scripted asset recovery and monetization processes. A court cannot compel the value of the assets, or even the value of the liabilities, to remain stagnant, and ultimately administrators find themselves trying to solve money problems with no true sense of what they are working with.

The timing of decisions regarding liquidation of cryptocurrency assets is critical, due to market volatility. In addition, some cryptocurrencies are more widely traded than others, mandating different marketing and sale process structures.[77] Finally, the sale of large amounts of even the most widely-traded cryptocurrency units at once can adversely impact market pricing, giving rise to a need for significant subject-matter expertise.[78]

These issues were highlighted in the *Cryptsy* case, a Florida class action in which a receiver was appointed to administer and manage the business affairs of an online business intended to

77 See *Fourth Report of Receiver James D Sallah* (30 January 2017), online: *Cryptsy Receivership* <cryptsyreceivership.com/v1/wp-content/uploads/2016/06/Fourth-Report.pdf> at 7-9 [*Cryptsy 4th Report*].

78 *Ibid* at 9.

facilitate the trade of cryptocurrencies for the general public.[79] Established in 2013, Cryptsy was registered with the US Financial Crimes Enforcement Network as a Money Services Business,[80] and as such was obligated to maintain certain financial records and allow unfettered access to consumer accounts.[81] The class action complainants alleged that Cryptsy solicited members of the public to register new accounts, deposit cryptocurrencies, and engage in the trade of same.[82]

The class action complainants alleged that starting in November 2015, certain Cryptsy users had trouble accessing their accounts.[83] Following several months of excuses from the company, the class action was commenced in January 2016, and in April 2016 the receiver was appointed by the court.[84] The receiver's immediate duties upon appointment included determining the nature, location and value of all property interests of Cryptsy, including, but not limited to, cryptocurrencies.[85]

The receiver in the *Cryptsy* was eventually tasked with monetizing many different types of cryptocurrencies of varying degrees of liquidity and value in dozens of dozens of cryptocurrency wallets.[86] The receiver divided the cryptocurrencies into two categories: "high liquidity" and "low to medium liquidity".[87] It was the receiver's view that the highly liquid cryptocurrencies included those that, if sold

79 *Brandon Leidel et al v Project Investors, Inc d/b/a Cryptsy et al*, Case No 9:16-cv-80060-MARRA (SD Fla) [*Cryptsy*].

80 *Brandon Leidel v Coinbase, Inc*, No 17-12728 (11th Cir 2018) at 2.

81 See "Registration of money services businesses", 31 CFR § 1022.380.

82 *Cryptsy, supra* note 79, Amended Class Action Complaint (22 February 2016) at para 20-22.

83 *Ibid* at para 24.

84 *Crypsty, supra* note 79, Order Granting Plaintiffs' Renewed Motion for Appointment of James D Sallah, Esq, as Receiver/Corporate Monitor over Defendant, Project Investors, Inc d/b/a Cryptsy (4 April 2016).

85 *Ibid* at para 8.

86 See *Cryptsy 4th Report*, *supra* note 77.

87 *Ibid* at 8.

through a cryptocurrency exchange, would in all probability net a monetary value close to market value.[88] The receiver advised that such "easily monetized" cryptocurrencies included, among others, Bitcoin, Ethereum, Ethereum Classic, Dash, Dodge and Litecoin.[89] The receiver advised the court that the liquidation of the majority of the high liquidity coins had been completed, with minimal market impact at values close to market as of the liquidation dates.[90] The liquidation of the high liquidity coins involved more than 2,000 individual trades over a two to three-week period.[91]

In contrast to the highly liquid cryptocurrency units, the receiver had also secured 78 other types of coins that, if sold through a cryptocurrency exchange, would have netted proceeds that were significantly less than the posted market value.[92] The receiver advised the court that any attempt to liquidate a significant amount of these low to medium liquidity coins would adversely affect the market price. As such, the receiver recommended to the court that in order to maximize recovery, these types of coins should be sold to private buyers and/or through auctions, rather than through an exchange.[93]

More recently, issues related to the liquidation of cryptocurrencies was considered in Ontario in the NextBlock Global Limited ("NextBlock") case.[94] Although NextBlock is not an insolvency case, it includes a court-supervised liquidation process in respect of multiple types of cryptocurrencies and the court's approach to asset disposition is thus informative.

NextBlock raised capital to invest in the purchase of exchange-traded cryptocurrencies and early-stage blockchain

88 *Ibid.*
89 *Ibid.*
90 *Ibid.*
91 *Ibid.*
92 *Ibid* at 9.
93 *Ibid.*
94 *In the Matter of the Winding-Up of NextBlock Global Limited*, Ontario Superior Court of Justice (Commercial List) Court File No CV-17-587226-00CL (Unreported) [*NextBlock*].

projects, platforms and companies.[95] NextBlock made an application to the Ontario Superior Court of Justice under section 207 of the Ontario *Business Corporations Act*[96] to be wound up pursuant to a proposed plan.[97] NextBlock held a mix of relatively liquid and illiquid cryptocurrency assets. Although the NextBlock Appointment Order prescribed a sale process with specific milestone dates,[98] as a result of deteriorating market conditions the Court subsequently ordered that the time to commence the sale of the cryptocurrency units would be left in the discretion of NextBlock — *ie*, they would be sold when NextBlock deemed it commercially reasonable so as to maximize value.[99] The order also included an alternative sale process for the comparatively illiquid cryptocurrencies. Similar to the *Cryptsy* case, the proposed process of selling relatively illiquid cryptocurrencies incorporates the targeting of sophisticated parties to buy the units privately.[100]

The *Cryptsy* and *NextBlock* cases are illustrative of many of the challenges that insolvency professionals dealing with cryptocurrencies will face. In particular, the cases suggest that Canadian courts will have to eschew the usual rigid, tightly prescribed court-supervised sale processes in favour of a more fluid, flexible approach that gives more discretion to the insolvency administrator tasked with maximizing the return on assets.

V. OTHER CHALLENGES

The nature of cryptocurrencies is such that they have posed significant challenges for courts. These challenges appear to

95 See *Nextblock, ibid*, First Report of the Monitor (13 March 2018).
96 *Business Corporations Act,* RSO 1990, c B.16.
97 *NextBlock*, *supra* note 94, Order of Justice Conway (4 December 2017) [*NextBlock Appointment Order*].
98 *Ibid.*
99 See *NextBlock*, *supra* note 94, Order of Justice Pattillo (16 May 2018) at Schedule "A".
100 *Ibid.*

have arisen principally from the law's unfamiliarity with the unique nature of cryptocurrencies.

1. Procedural and Substantive Challenges

The Japanese insolvency proceeding involving Mt Gox Co, Ltd ("Mt Gox") is an example of the manner in which uncertainties regarding cryptocurrencies and their incredible volatility can wreak havoc on procedural considerations in insolvency proceedings.[101]

should citation for Act be included in footnote?

Japan is the only jurisdiction in the world to recognize cryptocurrency as a form of money. In June 2016, Japan's *Payment Services Act* was amended to include cryptocurrency and rules surrounding its regulation.[102] These amendments and regulations were largely made in response to the Mt Gox insolvency proceeding, described below.

According to the *Payment Services Act*, "cryptocurrency" is defined as either: (i) property value that can be used as payment for the purchase or rental of goods or provision of services by unspecified persons, that can be purchased from or sold to unspecified persons, and that is transferable *via* an electronic data processing system; or (ii) property value that can be mutually exchangeable for the above property value with unspecified persons and is transferable *via* an electronic data processing system.[103] Cryptocurrency is limited to property values stored electronically on electronic devices, and currency and currency-denominated assets are excluded.[104] This

101 Marius-Christian Frunza, "Cryptocurrencies: A New Monetary Vehicle", in *Solving Modern Crime in Financial Markets: Analytics and Case Studies*, 1st ed (Academic Press, 2016) at 65, online: <books.google.ca/books?id=EokpCgAAQBAJ&pg=PA65&dq=mt.+gox+70&hl=en&sa=X&redir_esc=y#v=onepage&q=mt.%20gox%2070&f=false> ["Frunza"]

102 Library of Congress, "Regulation of Cryptocurrency: Japan" (18 June 2018), online: *Library of Congress* <www.loc.gov/law/help/cryptocurrency/japan.php>.

103 *Ibid.*

104 *Ibid.*

definition means that ordinary forms of currency, *ie* coins, are not captured by the definition.

The *Payment Services Act* imposes certain requirements in order to operate a cryptocurrency exchange business in Japan, which must first be approved by the Finance Bureau upon application.[105] Such business must: (i) be registered with the local Finance Bureau;[106] (ii) be a stock company or a "foreign cryptocurrency exchange business" that is a company that has a representative who is resident in Japan, and an office in Japan;[107] (iii) if a "foreign cryptocurrency exchange business", be registered with a foreign government in the foreign country under a law that provides an equivalent registration system to the Finance Bureau system under the Japanese *Payment Services Act*;[108] and (iv) provide supporting documents to demonstrate that it can properly conduct a cryptocurrency exchange business.[109]

Once the exchange has been approved and is operating, the *Payment Services Act* imposes certain regulations on the operation of the business, including but not limited to, the requirement to: (i) establish security systems to protect business information, to provide fee information, and contract terms to its customers; (ii) ensure measures are taken if external contractors operate; (iii) separately manage customers' cryptocurrency apart from their own; (iv) have certified public accounting firms audit its management; (v) have a contract with a dispute resolution centre, and if one does not exist, to establish its own dispute resolution center in order to resolve customer complaints; (vi) keep accounting records of cryptocurrency transactions; and (vii) submit annual reports on business to the Financial Services Agency, which is a government agency that supervises the businesses.[110]

105 *Ibid.*
106 *Ibid.*
107 *Ibid.*
108 *Ibid.*
109 *Ibid.*
110 *Ibid.*

Mt Gox was founded as a bitcoin exchange in 2010 by Jed McCaleb, an entrepreneur.[111] However, the domain name was repurposed from a previous project, Magic: The Gathering Online Exchange, which McCabe had developed in 2007 for trading the playing cards used in the game.[112] At the time, there were few options for trading cryptocurrencies, and the exchange grew quickly. It was subsequently acquired by Mark Karpelès, a French entrepreneur living in Japan.[113]

By 2013, Mt Gox was the world's largest bitcoin exchange, and by some estimates, it accounted for more than 70 per cent of global cryptocurrency exchange activity.[114] By February 2014, Mt Gox had shut down its website, frozen customer accounts, and ceased trading.[115] It appeared that hackers had gained access to Mt Gox's online wallets and stolen an estimated 744,000 bitcoins, each then worth approximately US$470 (*ie*, lost value of approximately US$350 million, as of when Mt Gox froze its operations in early 2014).[116] Later that month, Mt Gox commenced insolvency proceedings in Japan, and thereafter filed a corresponding proceedings in Canada and the US.[117]

The Mt Gox case raised a number of questions in relation to the position where an exchange enters administration or liquidation. The question arose as to whether or not those creditors had a proprietary claim in respect of the digital currency, or alternatively, a claim for the cash value of the cryptocurrency units as at the date of insolvency.[118] The latter approach would have resulted in a billion-dollar windfall for

111 Paul Vigna, "5 things about Mt Gox's crisis" (25 February 2014), online: *The Wall Street Journal* <blogs.wsj.com/briefly/2014/02/25/5-things-about-mt-goxs-crisis/> ["5 Things"].
112 *Ibid.*
113 *Ibid.*
114 *Ibid.*
115 Frunza, *supra* note 101 at 65.
116 *Ibid.*
117 *Ibid.*
118 Jones, *supra* note 73 at 28.

the majority shareholder of Mt Gox, Mark Karpelès, whose alleged conduct had in fact caused the loss.[119]

The Tokyo District Court ruled that the cryptocurrency at issue was not capable of ownership under Japanese law and dismissed the lawsuit.[120] Under Japan's *Civil Code*, the Japanese District Court found that the creditors could not have proprietary ownership in the cryptocurrency and as such, they were only entitled to the cash equivalent as at the date of insolvency.[121] Specifically, the Japanese court ruled that Article 85 of the *Civil Code* of Japan provides that an object of ownership must be a tangible "thing", in contrast to intangible rights (like contract or tort claims) or natural forces (like sunlight or electricity).[122] Bitcoin, the Japanese court ruled, does not meet the definition of a "thing" under the statute and, therefore, does not qualify for private ownership.[123]

should this have citation included in footnote?

In bankruptcy proceedings under Japanese law, non-monetary claims are converted into monetary claims based on the valuation as at the time of the commencement of the proceedings.[124] The ruling effectively left Mt Gox's customers with claims for damages in the insolvency proceeding rather than proprietary claims for the return of the cryptocurrency units.

However, on 22 June 2018, the Tokyo District Court issued an order for the commencement of civil rehabilitation proceedings for Mt Gox under the *Civil Rehabilitation Act*, and the bankruptcy proceedings were stayed.[125] In contrast to

citation included in footnote?

119 *Ibid.*
120 *Ibid.*
121 *Ibid.*
122 Mai Ishikawa, "Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case" (2017) 3:1 *Journal of Financial Regulation* 125, online: <doi.org/10.1093/jfr/fjw015>.
123 *Ibid.*
124 Jones, *supra* note 73 at 28-29.
125 See "Announcement of Commencement of Civil Rehabilitation Proceedings" (22 June 2018), online: <www.mtgox.com/img/pdf/20180622_announcement_en.pdf>.

bankruptcy proceedings, in civil rehabilitation proceedings, non-monetary claims are not converted into monetary claims; creditors in civil rehabilitation proceedings can instead seek a "refund" of their cryptocurrency units.

While the Mt Gox proceeding is ongoing, the case highlights the difficulties that creditors may face in a scenario where an exchange enters insolvency. While in Japan the *Payment Services Act* was amended to respond to such cases, we have not seen the same trend in Canada.

Uncertainties regarding treatment of cryptocurrencies in insolvency proceedings have given rise to a host of other substantive issues, some of which were raised in the Tsarkov bankruptcy case, recently considered by the Commercial Court of Moscow (Russia) in March 2018.[126] Ilya Tsarkov was declared bankrupt in October 2017, after the Commercial Court found that his assets and salary were not enough to pay off his indebtedness in the amount of 19 million rubles (*ie*, approximately US$333,000) to Rikas Investment Group.[127] In the Tsarkov case, the insolvency administrator filed a motion with the court for an order that the contents of the cryptocurrency wallet allegedly owned by Mr Tsarkov be included in the estate.[128] In addition, the administrator demanded delivery of the private key to the cryptocurrency wallet. Mr Tsarkov objected, claiming that as the current laws of Russia did not address cryptocurrencies, they could not be characterized as "property" for the purposes of the proceeding.[129]

126 See *Re Tsarkov*, Commercial Court of Moscow (Russia), Case No A40-124668/17-71-160.

127 Kevin Helms, "Russian Bankruptcy Court Orders Debtor to Disclose Cryptocurrency Assets" (6 February 2018), online: *Bitcoin.com* <news.bitcoin.com/Russian-bankruptcy-court-orders-debtor-disclose-cryptocurrency-holdings>.

128 See "When Bitcoin meets insolvency: Is Bitcoin property? Dutch and Russian responses" (8 June 2018), online: *LexisNexis* <blogs.lexisnexis.co.uk/randi/when-bitcoin-meets-insolvency-is-bitcoin-property-dutch-and-russian-responses> ["Is Bitcoin Property?"].

129 *Ibid.*

The Russian court of first instance refused to recognize the cryptocurrency as an asset for the purposes of insolvency law, on the following bases: First, the Russian court found that the legal nature of cryptocurrency was so unclear that it was not analogous to traditional asset classes.[130] Second, the court pointed out that ownership of cryptocurrency units could be impossible to ascertain, due to the anonymity of cryptocurrency wallets.[131]

The bases relied on by the Russian court of first instance are unpersuasive, and were criticized by the 9th Appellate Court, which noted that the objects of property rights are not exhaustively listed in Russian law.[132] Article 128 of the Russian *Civil Code* specifically includes the catch-all "other assets".[133] The appellate court stated that "...taking into account current economic realities and the level of development of information technologies, the broadest interpretation [of 'other assets'] was justified".[134]

The appellate court also took into account the fact that the Russian Ministry of Finance had recently proposed draft legislation defining "cryptocurrency" as a digital financial asset existing in the distributed ledger of digital transactions, and remarked that any property of the debtor having economic value, including cryptocurrency, should not be arbitrarily excluded from the estate.[135] Finally, the appellate court noted that Mr Tsarkov did not dispute ownership of the cryptocurrency wallet.[136] The appellate court ultimately reversed the judgment of the Commercial Court and obliged

130 *Ibid.*
131 *Ibid.*
132 See *Re Tsarkov*, 9th Commercial Court of Appeals (Moscow) Case No A40-124668/2017 (7 May 2018).
133 Russian Federation, *The Civil Code of the Russian Federation* (Parts One to Four), art 128, online: <www.wto.org/english/thewto_e/acc_e/rus_e/WTACCRUS48A5_LEG_119.pdf>.
134 Is Bitcoin Property?, *supra* note 128.
135 *Ibid.*
136 *Ibid.*

Mr Tsarkov to surrender the private key to the cryptocurrency wallet.[137]

2. Disregard for Court Orders

Ultimately, a court order is only as effective as the court's ability to enforce it. Parties subject to court orders may ignore them if they determine that there will not be any adverse consequences. The transnational structure, and in many cases, the deliberately selected location of certain components, transaction speed, and anonymity of many cryptocurrencies effectively renders them immune to court orders and regulatory procedures.[138] Traditional asset tracking and freezing approaches are ineffective; courts cannot act quickly enough to keep up with instantaneous cross-border cryptocurrency transfers.

A party may also elect to disregard a court order where, despite the court's ability to enforce it against the party, on a cost/benefit analysis, the likely consequences of disregarding the order are such that an unscrupulous person may consider it worth it to flout the order. Cryptocurrency values and volatility are such that such a person can take hundreds of millions of dollars out of the law's reach simply by refusing to disclose a private key.

Courts have been frustrated by the transnational structures of cryptocurrencies.[139] Absent specific legislation, in common-law jurisdictions cross-border cooperation is often premised upon comity.[140] But, as the *Cryptsy* case has demonstrated, comity has its limits.

---

137 *Ibid.*

138 Nicky Woolf, "Why the US Government Wants to Bring Cryptocurrency Out of the Shadows" (27 November 2016), online: *The Guardian, International Edition* <www.theguardian.com/technology/2016/nov/27/coinbase-bitcoin-irs-government-summons-data-cryptocurrency>.

139 *Cryptsy 4th Report, supra* note 77 at 13.

140 See United Nations, *UNCITRAL Model Law on Cross-Border Insolvency with Guide to Enactment and Interpretation* (New York:

In the *Cryptsy* case,[141] the receiver was successful in identifying and securing a significant body of traditional assets and proceeds of preferences, fraudulent transfers and outright embezzlement and misappropriation by Cryptsy's principal.[142] However, after more than a year of efforts, the receiver found itself stymied by overseas exchanges which failed to respond to inquiries or demands, and advised the court that the exchanges failed to respond because "...they are overseas and apparently do not feel compelled to respond to the Appointment Order".[143]

With traditional types of assets and financial instruments, it is rare that an insolvency administrator will not have an alternative means of tracing assets in the event a "guiding mind" refuses to disclose the relevant information. Assets with low liquidity generally leave visible trails, easily followed by an experienced insolvency administrator.[144] Cryptocurrencies are different; for all intents and purposes, a person can make them disappear without a trace with the push of a button.

In situations wherein a party refuses to surrender assets to an insolvency administrator, Canadian judges have an extensive toolbox. Such judicial tools include Mareva injunctions,[145] which prevent the dissipation of assets, and Norwich orders,[146] pursuant to which third parties such as financial institutions can be compelled to preserve and provide records, which have

---

2014) at 21, online: < https://www.uncitral.org/pdf/english/texts/insolven/1997-Model-Law-Insol-2013-Guide-Enactment-e.pdf>.

141 *Cryptsy, supra* note 79.

142 *Cryptsy 4th Report, supra* note 77 at 5.

143 See *Fifth Report of the Receiver James D Sallah* (1 May 2017), online: <cryptsyreceivership.com/v1/wp-content/uploads/2016/06/Fifth-Report.pdf> at 13.

144 Tan Yock Lin, "Fraud on Creditors" (2012) *Singapore Journal of Legal Studies* 134 at 144, online: <law.nus.edu.sg/sjls/articles/SJLS-Jul-12-134.pdf>.

145 *Mareva Compania Naviera SA v. International Bulkcarriers SA*, [1975] 2 Lloyd's Rep 509, [1980] 1 All ER 213 (Eng CA).

146 *Norwich Pharmacal Company & Ors v Customs And Excise*, [1973] UKHL 6, [1974] AC 133.

proved extremely effective in identifying, locating and securing the assets of insolvent persons. When combined with the principle of judicial comity, bilateral and multinational treaties and cross-border insolvency protocols, these types of orders have made it very difficult to hide traditional assets from the reach of sophisticated insolvency practitioners.[147]

A court's primary tool for enforcing compliance with its orders is its power to find a party in contempt. There are two types of contempt of court: criminal and civil. While criminal contempt is essentially a public offence that interferes with and undermines public confidence in the due course of justice and are thus deserving of penal sanctions,[148] a court's jurisdiction in respect of civil contempt is primarily remedial, the basic object of same being the coercion of the offender toward obeying the court judgment or order. [149] Sanctions targeted at coercing compliance with civil court orders have been relatively lenient in comparison to criminal sanctions.[150] Sentences imposed in recent years by Canadian courts for civil contempt of court have been found to be based on the "application of the principle of proportionality".[151] Imprisonment for civil contempt in Canada is rare and sentences are ordinarily not lengthy, ranging from several days to more than a year.[152]

147 See Felicity Toube, *International Asset Tracing in Insolvency,* 1st ed (Oxford University Press, 2010) at 59-64; Canada: Asset Recovery Guide (Lexis PSL).

148 See *Poje v Attorney General for British Columbia*, [1953] 1 SCR 516 at para 522; see also *R v Glasner* (1994), 93 CCC (3d) 226 (Ont CA) at 242-43.

149 See *Kopaniak v MacLellan*, 2002 CanLII 44919 (Ont CA) at para 28, citing Lowe & Sufrin in *Borrie and Lowe on the Law of Contempt*, 3rd ed (London: Butterworths, 1996) at 655-56.

150 See *Gee Nam John et al v Byung Kyu Lee et al*, 2009 BCSC 1157 at para 14, in which Justice Burnyeat surveyed a number of decisions regarding incarceration for civil contempt. The most severe sanction referenced by Justice Burnyeat was a sentence of 45 days of imprisonment.

151 *Mercedes Benz Financial v Kovacevic* (2009), 308 DLR (4th) 562, 2009 CarswellOnt 1142 (SCJ) at para 10.

152 *Ibid* at 12.

The distinction between treatment of and sanction for civil and criminal contempt is not unique to Canada. For example, in *US v Perry*, Justice Selya of the United States Court of Appeals made a clear distinction between the option of purging in a civil contempt proceeding, as opposed to the irrelevancy of purging actions in a criminal contempt proceeding: "[T]he paradigmatic civil contempt sanction is coercive, designed to exact compliance with a prior court order."[153]

A Québec court recently employed a somewhat novel — and apparently effective — approach to a case involving cryptocurrencies, wherein a party failed to surrender them to the administrator.[154] Dominic Lacroix and his wife and business partner have been under investigation by Canadian and US authorities over their PlexCoin ICO, which allegedly received the equivalent of approximately $19 million from Canadian and US investors in 2017.[155] On 5 July 2018, at the request of the *Autorité des marchés financiers*, Judge Pronovost of the Superior Court of Québec appointed a receiver over certain property belonging to Lacroix, including cryptocurrency units.[156] At the hearing, Judge Pronovost ordered Lacroix (who was in court) to give control of his cryptocurrency units to the court administrator, and to reappear the next day to confirm the transfer had been completed.[157]

153 *In United States v George Perry, A/K/A King Animal*, 116 F 3d 952 at 956 (1997).

154 Autorité des marchés financiers, "Bitcoins transferred at request of AMF" (19 July 2018), online: *Autorité des marchés financiers Media Centre* <lautorite.qc.ca/en/general-public/media-centre/news/fiche-dactualites/transfert-de-bitcoins-obtenu-a-la-demande-de-lautorite-des-marches-financiers> ["Bitcoins Transferred"].

155 Autorité des marchés financiers, "Virtual Currency — Orders issued against PlexCorps, PlexCoin, DL Innov inc, Gestio inc and Dominic Lacroix" (21 July 2017), online: *Autorité des marchés financiers Media Centre* <lautorite.qc.ca/en/general-public/media-centre/news/fiche-dactualites/virtual-currency-orders-issued-against-plexcorps-plexcoin-dl-innov-inc-gestio-inc-and-dominic>.

156 Bitcoins Transferred, *supra* note 154.

157 *Ibid.*

On 6 July 2018, Lacroix attended court and advised Judge Pronovost that he had not completed the transfer as the task had been complicated, in part by the seizure of his computers.[158] In response to the administrator's concerns and Lacroix's failure to comply, at the judge's direction the confiscated computer equipment was brought into the courtroom, and Lacroix was ordered to immediately transfer the cryptocurrency units worth approximately $3.7 million in court.[159] Judge Pronovost warned Lacroix that if he did not complete the transfer he would be held in contempt and jailed.[160]

Lacroix opted to make the transfer in the courtroom.[161] As of the date of this article, the case is continuing.

Yet notwithstanding the *PlexCorps* case and Mr Lacroix's hasty in-court compliance with Judge Pronovost's direction, it is not hard to imagine a different party that, when considering the amount at issue versus the range of possible court sanctions, would have opted to disregard the judge's orders. It is not difficult to imagine that to some, even a lengthy incarceration for criminal contempt[162] would be seen as nothing more than a minor inconvenience in the course of protecting access to tens or even hundreds of millions of dollars of cryptocurrency units.

The Canadian *Bankruptcy and Insolvency Act*[163] includes provisions with marginally more "teeth" for enforcing compliance with court orders and the statutory duties of a bankrupt. For example, the maximum penalties faced by a bankrupt who intentionally conceals property or documents

158 *Ibid.*
159 *Ibid.*
160 Mark Caldwell, "Judge Orders Cyber-Scam Artist to Pay Fine in Crypto-Currency" (31 July 2018), online: *Canadian Lawyer Magazine* <www.canadianlawyermag.com/author/mark-cardwell/judge-orders-cyber-scam-artist-to-pay-fine-in-crypto-currency-16043/>.
161 Bitcoins Transferred, *supra* note 154.
162 *Criminal Code*, RSC 1985, c C-46, s 9.
163 *Bankruptcy and Insolvency Act*, RSC 1985, c B-3, as amended, s 198(1)(d), (f).

related thereto includes, among other things, imprisonment for a term of up to three years, on conviction on indictment.

VI. CONCLUSION

Many of the challenges posed by cryptocurrencies arise from the same characteristics that make them appealing in the first place: they exist and operate outside the scope of traditional governance structures. As described above, such characteristics make them inherently useful to criminals. But their disruptive nature and relatively ungovernable nature also enhances their appeal to the technology community, which tends to embrace such anarchistic developments more readily — and enthusiastically — than the general public.[164]

The extent of social or marketplace utility to cryptocurrencies is unknown. In fact, during the preparation of this article, a schism developed among the authors as to whether the appropriate response would be to simply ban them outright, on the basis that they make no *bona fide* contribution to the commercial marketplace. Regardless, the authors agreed that at least some of the more than 2,000 known existing cryptocurrencies[165] are here to stay.

Cryptocurrencies represent an unprecedented threat to any party whose task it is to identify transactions and parties, and to identify, locate and secure assets, including bankruptcy trustees and other insolvency administrators. As such, it will become increasingly important to answer the questions of how to transact business with cryptocurrencies and how to regulate them so as to bring their treatment into line with the policy objectives of insolvency law. Such answers must ensure that

164 Jamie Bartlett, "Forget far-right populism — crypto-anarchists are the new masters" (4 June 2017), online: *The Guardian* <www.theguardian.com/technology/2017/jun/04/forget-far-right-populism-crypto-anarchists-are-the-new-masters-internet-politics>.

165 The top three exchanges by trailing 30-day volume on 17 September 2018 were Binance, OKEx and Huobi. "Top 100 Cryptocurrency Exchanges by Trade Volume" (17 September 2018), online: *CoinMarketCap* <coinmarketcap.com/rankings/exchanges/>.

cryptocurrencies can be identified, located and secured by insolvency administrators, and liquidated or otherwise monetized so as to maximize recovery and distribute value to creditors and other stakeholders in a manner that is fair, equitable and consistent with market expectations.

To ensure cryptocurrencies are dealt with in a manner consistent with insolvency law policy objectives, both lenders and legislators must respond in ways that accomplish the following:

- Protect the rights of parties with an interest in the cryptocurrency units.
- Simplify and expedite the process of identifying, locating and securing cryptocurrencies.
- Clarify the manner in which cryptocurrencies should be liquidated or otherwise monetized.
- Specify the manner in which assets and/or proceeds should be distributed to stakeholders.

1. Recommendations for Lenders

As set out above, a lender accepting cryptocurrency units as collateral faces a number of risks, including transfer by the borrower despite the security interest, third party theft and lack of access to the borrower's private key or wallet.

The most effective way in which a lender can protect its security interest is to require that the borrower transfer the units to the lender, or to a neutral third-party intermediary (*ie*, an escrow agent). This step is not a substitution for registration of the security interest — the *PPSA* does not contemplate perfection of a security interest in an intangible through possession or control[166] — but rather, it may serve to mitigate certain of the practical risks associated with cryptocurrencies.

166 *PPSA, supra* note 67, s 22(1).

To address the risk of unauthorized third-party access to the digital wallet, lenders should store the cryptocurrency units in wallets on a computer that is not connected to the Internet.[167] But regardless of where the digital wallet is maintained, it is critical that the borrower relinquish the private key and thus effective control over the units.[168]

Lenders should also ensure that security agreements used in respect of cryptocurrencies accommodate their distinctive features. While cryptocurrencies may share some characteristics with currencies, intellectual property, securities and other traditional asset classes, they do not fit squarely within any of them. Security agreements must be carefully drafted to deal with the unique attributes of cryptocurrencies and ensure that, among other things, the lender — or insolvency administrator — has all of the information and access required to deal with the collateral in an enforcement scenario.

Unfortunately, while the above recommendations may deal with some of the concerns regarding a lender's ultimate ability to secure and realize on the security, they cannot fully address the problem of cryptocurrency volatility. As previously noted, cryptocurrencies have thus far proved themselves to be poor at storing value. Where a lender is relying on the market value of cryptocurrency units as security for a borrower's indebtedness the lender must monitor the market in real time, and be prepared to take immediate action if the value suddenly plummets.

In enforcement situations, lenders applying for the court appointment of a receiver or other insolvency administrator should ensure that the appointment order provides for a high degree of flexibility and discretion to deal with such market

167 See Lance P Martin, "Can I Secure a Loan With Bitcoin? Part II" (23 September 2018), online: *The National Law Review*, online: <https://www.natlawreview.com/article/can-i-secure-loan-bitcoin-part-ii>.

168 *Ibid.*

volatility and other factors such as the wide variations in relative liquidity among different types of cryptocurrencies.

2. Recommendations Regarding Legislative Response

Canada and the provinces should focus on promulgating laws carefully targeted and coordinated toward achieving insolvency and general commercial law policy objectives in order to reduce the current commercial uncertainties. At the same time, governments must also be cautious against "over-regulating" the burgeoning industry to the point of stifling opportunity.

One possible relatively straightforward way in which to accommodate cryptocurrencies in commercial transactions would be to amend the *PPSA* to define "digital currency" as a new asset class, to be treated in different ways depending on the context. For example, cryptocurrency units could be treated under the *PPSA* as "money" in the context of ordinary course sale transactions such that a vendor could be assured that the units that it accepts as payment are unencumbered, but as "investment property" when used as collateral, so as to allow for perfection by control by the lender.[169]

Domestically, accomplishing policy objectives and normalizing cryptocurrencies may ultimately require such grand legislative action as instituting a comprehensive licensing system for cryptocurrency exchanges that, among other things, requires compliance with KYC and AML standards, and enforcing use of such licensed exchanges by banning all other cryptocurrency trading. But there is nothing to indicate such ambitious steps are on the horizon and in any event, they alone will not be enough to address the darker side of cryptocurrencies.

Even a broad international consensus and cooperation on treatment and regulation of cryptocurrencies will not be effective at eliminating their misuse so long as individual non-state actors

169 See *PPSA, supra* note 67 at s 22.1.

continue to have faith in their ability to transfer and maintain value outside of the regulatory regime. Cryptocurrencies do not depend on central authority, so government intervention will likely have little impact on criminal utility so long as criminal organizations continue to have faith in them as storehouses of value and units of transfer. Their key vulnerability is the point at which they are converted back to traditional fiat currency. Of course, in the event cryptocurrencies continue to proliferate at the current pace, and their mainstream acceptance continues to grow, even this vulnerability will be rendered meaningless.