

Court File No. & Estate No. CV-19-627184-00CL (31-2560674)
CV-19-627185-00CL (31-2560984)
and CV-19-627186-00CL (31-2560986)

**ONTARIO
SUPERIOR COURT OF JUSTICE
(COMMERCIAL LIST)**

IN THE MATTER OF THE BANKRUPTCY OF QUADRIGA FINTECH
SOLUTIONS CORP., WHITESIDE CAPITAL CORPORATION AND 0984750
B.C. LTD. D/B/A QUADRIGA CX AND QUADRIGA COIN EXCHANGE

**BOOK OF AUTHORITIES
(Returnable January 26, 2021)**

January 19, 2021

STIKEMAN ELLIOTT LLP
Barristers & Solicitors
5300 Commerce Court West
199 Bay Street
Toronto, Canada M5L 1B9

Elizabeth Pillon LSO#: 35638M
Tel: (416) 869-5623
Email: lpillon@stikeman.com

Maria Konyukhova LSO#: 52880V
Tel: (416) 869-5230
Email: mkonyukhova@stikeman.com

Lee Nicholson LSO#: 66412I
Tel: (416) 869-5604
Email: leenicholson@stikeman.com

Nicholas Avis LSO#: 76781Q
Tel: (416) 869-5504
Email: navis@stikeman.com
Fax: (416) 947-0866

**Lawyers for the Trustee in Bankruptcy
of Quadriga Fintech Solutions Corp.,
Whiteside Capital Corporation and
0984750 B.C. Ltd.**

INDEX

Court File No. & Estate No. CV-19-627184-00CL (31-2560674)
CV-19-627185-00CL (31-2560984)
and CV-19-627186-00CL (31-2560986)

**ONTARIO
SUPERIOR COURT OF JUSTICE
(COMMERCIAL LIST)**

IN THE MATTER OF THE BANKRUPTCY OF QUADRIGA FINTECH
SOLUTIONS CORP., WHITESIDE CAPITAL CORPORATION AND 0984750
B.C. LTD. D/B/A QUADRIGA CX AND QUADRIGA COIN EXCHANGE

INDEX

TAB	DOCUMENT
1.	Financial Consumer Agency of Canada, Digital Currency (Ottawa: Financial Consumer Agency of Canada, 2018), available at https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html
2.	Canada Revenue Agency, Virtual Currency, (Ottawa: Canada Revenue Agency, 2019), available at https://www.canada.ca/en/revenue-agency/programs/about-canada-revenue-agency-cra/compliance/digital-currency.html
3.	Canada Energy Regulator, Market snapshot: Crypto-currency mining is booming in Canada. Here is why, (Ottawa: Canada Energy Regulator, 2018), available at: https://www.cer-rec.gc.ca/en/data-analysis/energy-markets/market-snapshots/2018/market-snapshot-crypto-currency-mining-is-booming-in-canada-here-is-why.html
4.	Bitwise, Bitcoin Trade Volume (undated) , available at https://www.bitcointradevolume.com/
5.	Janis Sarra and Louise Gullifer, “Crypto-claimants and bitcoin bankruptcy: Challenges for recognition and realization” (2019) 28 Int Insol Rev. 233 (Wiley)
6.	Canadian Securities Administrators and Investment Industry Regulatory Organization of Canada, Consultation Paper 21-402 – Proposed Framework for Crypto-Asset Trading Platforms (Canadian Securities Administrators and Investment Industry Regulatory Organization of Canada, 2019) (OSC Website)
7.	Canadian Securities Administrators, Staff Notice 46-308 – Securities Law Implications for Offerings of Tokens (Canadian Securities Administrators, 2018) (OSC Website)

TAB 1



Government
of Canada

Gouvernement
du Canada

[Canada.ca](#) > [Money and finances](#) > [Managing your money](#)

> [Payment options and money transfers](#)

Digital currency

From: [Financial Consumer Agency of Canada](#)

On this page

- [Using digital currencies](#)
- [Digital currencies are not a legal tender](#)
- [Automated exchangers \(Bitcoin ATMs\)](#)
- [How tax rules apply to digital currency](#)
- [Risks of using digital currency](#)
- [Tips for using digital currency](#)



Note:

This page is about cryptocurrencies, which are not issued or governed by a government or central bank.

Digital currency is electronic money. It's not available as bills or coins.

Cryptocurrencies are a type of digital currency created using computer algorithms. The most popular cryptocurrency is Bitcoin.

No single organization, such as a central bank, creates digital currencies. Digital currencies are based on a decentralized, peer-to-peer (P2P) network. The “peers” in this network are the people that take part in digital currency transactions, and their computers make up the network.

Using digital currencies

You can use digital currencies to buy goods and services on the Internet and in stores that accept digital currencies. You may also buy and sell digital currency on open exchanges, called digital currency or cryptocurrency exchanges. An open exchange is similar to a stock market.

To use digital currencies, you need to create a digital currency wallet to store and transfer digital currencies. You can store your wallet yourself or have a wallet provider manage your digital currency for you.

You need a “public key” and a “private key” to use your wallet. Keys are made up of a random sequence of numbers and letters.

Public keys are used to identify your wallet.

Private keys are used to unlock your wallet and access your money. Private keys should be kept secret.

All transactions are recorded to a public ledger or “blockchain” that everyone can see.

Digital currencies are not a legal tender

Digital currencies, such as Bitcoin or other cryptocurrencies, are not legal tender in Canada. Only the Canadian dollar is considered official currency in Canada.

The Currency Act defines legal tender.

Legal tender is defined as:

- bank notes issued by the Bank of Canada under the Bank of Canada Act
- coins issued under the Royal Canadian Mint Act

Digital currencies are not supported by any government or central authority, such as the Bank of Canada.

Financial institutions, such as banks or credit unions, don't manage or oversee digital currency.

Automated exchangers (Bitcoin ATM (Automated Teller Machine)s)

Automated exchangers are commonly referred to as Bitcoin ATM (Automated Teller Machine)s. They are vending machines that allow you to insert cash in exchange for bitcoins, and in some cases bitcoins for cash.

Unlike traditional ATMs, they are not connected to your bank, credit union or the Interac network. You may be charged a transaction fee for using a Bitcoin ATM. Shop around as exchange fees vary and you may be able to get lower rates elsewhere.

Generally, when you use a Bitcoin ATM, the machine:

- reads the bills you insert
- converts the amount into an amount of bitcoins
- sends the equivalent of bitcoins to the Bitcoin address you enter

How tax rules apply to digital currency

Tax rules apply to digital currency transactions, including those made with cryptocurrencies. Using digital currency does not exempt consumers from Canadian tax obligations.

This means digital currencies are subject to the Income Tax Act.

Buying goods or services using digital currency

Goods purchased using digital currency must be included in the seller's income for tax purposes. GST (Goods and Services Tax)/HST (Harmonized Sales Tax) also applies on the fair market value of any goods or services you buy using digital currency.

Buying and selling digital currency like a commodity

When you file your taxes you must report any gains or losses from selling or buying digital currencies.

Digital currencies are considered a commodity and are subject to the barter rules of the Income Tax Act. Not reporting income from such transactions is illegal.

[Learn more about the Canada Revenue Agency's reporting](#)

requirements for digital currencies.

Risks of using digital currency

Using digital currency has certain risks.

You may have fewer protections

You may not have access to a complaint-handling process like you would with other payment methods, such as debit and credit cards.

Even if you use a wallet provider to help you manage your digital currency, the provider does not have to help you get your funds back if something goes wrong with your transaction.

Your deposit is not insured

It's your responsibility to protect your digital currency wallet.

Federal or provincial deposit insurance plans don't cover digital currency.

For example, the Canada Deposit Insurance Corporation only covers eligible deposits in Canadian dollars at member financial institutions if the institution fails.

If the currency exchange or wallet provider that has your digital currency fails or goes bankrupt, your funds won't be protected.

Your investment may be high risk

Digital currencies can be risky investments because their value can change quickly. The value of a digital currency can increase or decrease over a very short period of time. Such changes in value can be difficult to predict.

When you exchange your digital currency for traditional currency, such as the Canadian dollar, it may be worth less than when you bought it.

You may have a hard time exchanging your digital currency

Digital currencies can be difficult to buy and use. You may not be able to exchange them easily for cash or to purchase goods and services.

Merchants don't have to accept digital currencies as payment. They don't have to exchange digital currencies for traditional currencies, such as the Canadian dollar.

You may be exposed to fraud

Digital currencies may be vulnerable to fraud, theft and hackers.

All transactions are recorded to a public ledger or “blockchain”. The blockchain may include information such as transaction amounts, wallet addresses and the public keys of the sender and recipient.

Digital currencies are also sometimes used to support illegal activities.

Transactions are not reversible

Purchases and transactions made with digital currencies are not reversible.

This means:

- you can't reverse the charges if you didn't receive the product
- you can't get your money back unless the seller agrees
- you might not be able to stop a payment

Tips for using digital currency

Here are a few tips to help you protect yourself when using digital currency.

Protect your wallet

Take steps to protect your wallet:

- keep your wallet, and any backups, in a safe place
- encrypt your wallet using encryption software
- encrypt any copies you make or online backups
- set a password to help prevent thieves from withdrawing your funds
- use a strong password that contains letters, numbers and symbols

Know the merchant's refund, return and dispute policies

Before you make a purchase, find out:

- what the exchange rate will be

- if refunds are available
- if refunds will be processed in digital currency, Canadian dollars or store credit
- how to contact someone if there's a problem

Wait for multiple confirmations before completing a transaction

It can take 10 minutes or more for a digital currency transaction to be confirmed. Confirmation happens when users on the network verify the transaction. During that time, a transaction could be reversed and you could lose your funds to a dishonest user.

Understand what the actual costs will be

Find out if there are any mark-ups or other fees. Find out what will happen if the rate changes before the exchange is completed.

Think about the future

Consider what will happen if you fall ill or die and can no longer access your wallet.

If no one knows the locations and passwords of your wallets when you are gone, the funds can't be recovered.

Consider having a backup plan for your peers and family.

Related links

- [Mobile wallets](#)
- [Paying with your mobile phone](#)

- Currency Act
- Bank of Canada Act
- Royal Canadian Mint Act

Date modified:

2018-01-19

TAB 2



Government
of Canada

Gouvernement
du Canada

[Canada.ca](#) > [Canada Revenue Agency](#) > [Compliance](#)

Virtual Currency

What is virtual currency?

Virtual currency is digital asset that can be used to buy and sell goods or services. Cryptocurrency is a blockchain-based, virtual currency. Bitcoins are an example of a cryptocurrency. However, there are thousands of other types. Cryptocurrencies are not controlled by central banks or any country, and they can be traded in a relatively anonymous way.

Many cryptocurrencies can be:

- bought with traditional currency (known as fiat currency / legal tender) and sold for fiat currency / legal tender
- transferred from one person to another
- exchanged for other cryptocurrencies or used to pay for goods or services directly

All of these types of transactions or exchanges may have tax implications.

For more information on virtual currency see our **[Guide for cryptocurrency users and tax professionals](#)**.

What tax rules apply when virtual currency is used to buy goods or services?

Income tax purposes



Note

This information is for individuals preparing income tax and benefit returns and corporations preparing income tax returns, who have sold a good or service and were paid in cryptocurrency. There are different rules for calculating GST/HST on a taxable transaction.

When cryptocurrency is used to pay for goods or services, the rules for barter transactions apply for income tax purposes.

A barter transaction occurs when any two persons agree to exchange goods or services and carry out that exchange without using legal tender. For example, paying for movies with virtual currency is a barter transaction. The Canadian-dollar value of the movies bought using cryptocurrency must be included in the seller's income for tax purposes.

For more information on the tax implications of barter transactions, see [Interpretation Bulletin IT-490, Barter Transactions](#).

Goods and services tax / harmonized sales tax (GST/HST) purposes



Note

This information is for GST/HST registrants reporting revenue and GST/HST on their GST34 return. There are different rules for calculating income reported on your income tax and benefit return or corporation income tax return.

Cryptocurrency may be accepted as payment for a taxable good or service by a GST/HST registrant. In such a case, the GST/HST rules require that the fair market value of the consideration that was received for the good or service be determined and GST/HST calculated based on that value.

For example, a GST/HST registrant who accepts cryptocurrency for a movie ticket at their theatre would have to determine what the fair market value of the cryptocurrency is at the time of the transaction. The value of the movie ticket bought using cryptocurrency must be included in the registrant's GST/HST return as revenue with the applicable amount of GST/HST. The amount of revenue and the related GST/HST would be reported in Canadian dollars.

For more information on the tax implications of when a consideration other than money is received for payment, see the Excise Tax Act, section 153(1)(b).

What tax rules apply when virtual currency is used like a commodity?

Virtual currency can also be bought or sold like a commodity. Any resulting gains or losses could be taxable income or capital for the taxpayer. To determine if a transaction is on account of income or capital, see paragraphs 9 to 32 of Interpretation Bulletin IT-479R, Transactions in Securities.

Also, there may be tax consequences if you choose to gift, trade, or use cryptocurrency to buy goods or services or convert cryptocurrency to a government-issued currency.

What tax rules apply when virtual currency is used to pay an employee?

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 according to subsection 5(1) of the *Income Tax Act*.

What tax rules apply when virtual currency is earned from mining or staking?

Mining involves using computers to solve mathematical problems that confirm cryptocurrency transactions. Miners will place cryptocurrency transactions in blocks and try to guess the number

that will create a valid block. A valid block is accepted by the corresponding cryptocurrency's network and becomes part of a public ledger, known as a blockchain. When a miner successfully creates a valid block, they will receive two amounts in one payment. One amount will represent the creation of a new cryptocurrency on the network and the other amount will represent the fees from transactions included in the newly validated block. Those who do the mining are paid in the cryptocurrency that they are validating.

Staking (proof of stake) is a different process to earn cryptocurrency payments but may still result in earnings that have tax implications. Proof of stake is an alternative distributed consensus mechanism where a person is selected out of a group of participants (forgers) to validate a block of transactions. Much like mining, when the selected person successfully creates a valid block, they will receive two amounts in one payment. One amount will represent the creation of a new cryptocurrency on the network and the other amount will represent the fees from transactions included in the newly validated block.

For more information on the tax implications of mining and staking, see our [cryptocurrency guide](#).

Should you be concerned about reporting requirements when using virtual currency?

Not reporting income from domestic or foreign sources is illegal. Canadians should know that the Canada Revenue Agency is very active in pursuing cases of non-compliance, in order to make sure that the tax system is fair for everyone.

If required, you can correct your tax affairs through our [Voluntary Disclosures Program](#).

Date modified:

2019-06-26

TAB 3



[Home](#) > [Data and analysis](#) > [Energy Markets](#) > [Market Snapshots](#)

> Market Snapshot: Crypto-currency mining is booming in Canada. Here is why.

Market Snapshot: Crypto-currency mining is booming in Canada. Here is why.

Release date: 2018-08-22

Key highlights

- Many crypto-currency miners have either started or have expressed interest in operating in Canada. Out of all provinces, Quebec has seen the highest number of requests for electricity to supply mining projects.
- The main reasons why crypto-currency miners are interested in operating in Canada are relatively cheap electricity, cold weather, and light regulation.

Connect/Contact Us

[Energy
Information RSS
Feed](#)

Please send
comments,
questions, or
suggestions for
Market Snapshot
topics to
[snapshots@cer-
rec.gc.ca](mailto:snapshots@cer-rec.gc.ca)

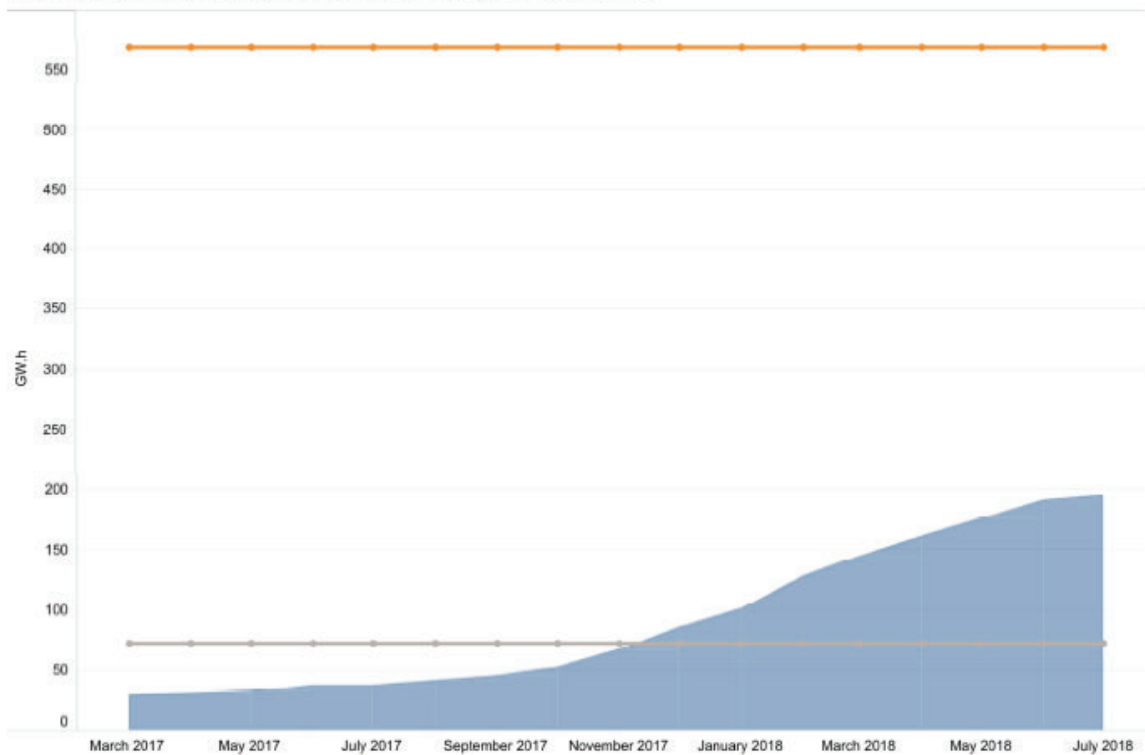
A crypto-currency is a form of virtual money where cryptography is used to secure transactions and to control how much money is available in the marketplace. [Blockchain](#) is a public database that lists transactions of a crypto-currency, where each transaction is a “block” and the list of transactions becomes the “chain”.¹

Essential to these transactions is [mining](#), which is equivalent to auditing or verification. Miners verify new transactions by solving complex computational problems, after which the new transactions are added to the blockchain.

Mining is very energy intensive because it requires a large amount of computer power. The mining of Bitcoin, the most widespread crypto-currency, consumes [an estimated 71.12 TW.h per year globally](#).² This is equivalent to 11% of the [electricity generated in Canada in 2016](#). On average, one bitcoin transaction uses [more electricity than a Canadian home for a month](#).

In the last few years, the crypto-currency market has experienced significant growth, both in terms of value and traded volume. This growth has mostly been supported by investors’ belief in the growth potential of this new asset class. This growth is now starting to pose a challenge to some electric utilities. As shown in the graph below, the estimated global Bitcoin electricity consumption largely surpasses Canada’s biggest power generation station’s capacity and amounts to a significant portion of Quebec’s electricity generation.

Estimated Global Daily Bitcoin Electricity Consumption



▼ Source and Description

Source: [Digiconomist](#), NEB Calculations

Description: The graph shows the estimated global energy consumption index of Bitcoin mining for every first day of the month between March 2017 and July 2018. On March 1st 2017, consumption was estimated at 28.04 GW.h. On July 1st 2018, consumption was estimated at 194.86 GW.h. The orange line represents the average daily power generation in Quebec (568 GW.h). The gray line represents the approximate average daily power generation of Robert-Bourassa hydroelectric power station over one year. It is Canada's biggest power station.

In the last year miners increasingly decided to move to Canada, mostly to Quebec. According to Hydro-Quebec, the province received requests for about 9 gigawatts (GW) of energy in 2018 from crypto-currency miners (about 24% of Hydro-Quebec's total generating capacity of 37 GW). There are three main reasons why Quebec is particularly attractive to crypto-currency miners:

- **Cold weather**

The computers of crypto-currency miners generate a significant amount of heat and require

cooling to prevent overheating. Locating in a relatively cool climate like Quebec helps to reduce the costs of cooling the computers.

- **Regulations**

The Bank of Canada regulates currency in Canada. However, it doesn't consider crypto-currencies a form of money. Therefore, crypto-currencies are still unregulated in Canada. Other countries have adopted or are considering adopting regulations to oversee the activity of crypto-currency miners.

- **Low electricity prices**

Power rates in Quebec are among the lowest in North America. For industrial consumers, rates are around 5 cents/kW.h. Energy consumption is the main cost of crypto-currency miners.

Although Quebec has seen the highest number of requests for electricity to supply mining projects, Manitoba is also, to a lesser extent, receiving significant amounts of requests.

In July 2018, following an increasing number of applications for electricity from miners, Hydro-Quebec tripled the price of electricity for new crypto-currency miners. This price increase is temporary, because Hydro-Quebec is currently proposing a new selection process to the Régie de l'énergie for future crypto-mining operations.

-
- 1 Although crypto-currencies all use a similar system, the most widely known is Bitcoin.
 - 2 There are currently no official and precise data on electricity consumption by crypto-miners. This article is one of the first peer-reviewed article estimating their energy consumption.
-

Date modified:

2020-09-29

TAB 4

95% of the reported bitcoin volume is fake. Below is the real volume. It's smaller, but more orderly and regulated than is widely understood.

[Read The Full Analysis →](#)

LATEST VOLUME DATA

\$5,103,400,765

Bitcoin Spot 24 hr Volume

Updated hourly. Data as of: 01/18/21 2pm ET.



Spot Exchange • Malta

\$2,817,955,718

24h Volume



Spot Exchange • United States

\$801,178,451

24h Volume



Spot Exchange · United States

\$541,969,193

24h Volume



Spot Exchange · Taiwan

\$462,417,884

24h Volume



Spot Exchange · United Kingdom

\$326,188,440

24h Volume



Spot Exchange · United States

\$74,417,401

24h Volume



Spot Exchange · United States

\$73,385,481

24h Volume



Spot Exchange · Japan

\$3,459,103

24h Volume



Spot Exchange · United States

\$1,250,909

24h Volume



Spot Exchange · United States

\$1,178,185

24h Volume

Source: CoinAPI

\$4,066,991,190

Bitcoin Futures 24 hr Volume

Updated hourly*. Data as of: 01/12/21 12:35 am ET.



Futures Exchange • United States

\$4,006,156,150

24h Volume



Futures Exchange • United States

\$60,835,040

24h Volume

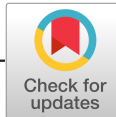
* Data is aggregated throughout the day using delayed quotes
Source: CME Group and Bakkt

Bitwise Asset Management, Inc. and its affiliates (collectively, the "Manager") has produced and distributes this Website ("Website") for informational purposes only. This is not an offer to sell or a solicitation of an offer to buy shares or interests in any Fund or offering. Any offer to sell or solicitation of an offer to buy Interests in any Fund will solely and exclusively be made through definitive offering documents, identified as such, in respect of each Fund and in compliance with the terms of all applicable securities and other laws. Such definitive offering documents, if any, will describe risks related to an investment in any Fund or offering (including loss of the entire investment) and will qualify in their entirety the information set forth in this Website.

Information May Change and Be Inaccurate, Incomplete, or Outdated: The information in this Website is for informational purposes only and no representations or warranties are given or implied. The information contained in this Website is subject to further completion, and amendment. All of the information presented herein is subject to change without notice.

Bitwise is not affiliated with any of the exchanges listed on this site.

TAB 5



RESEARCH ARTICLE



WILEY

Crypto-claimants and bitcoin bankruptcy: Challenges for recognition and realization

Janis Sarra¹ | Louise Gullifer QC (Hon)²¹Peter A. Allard School of Law, University of British Columbia, Vancouver, BC, Canada²Commercial Law, University of Oxford, Oxford, UK**Correspondence**

Janis Sarra, Professor, Peter A. Allard School of Law, University of British Columbia, Vancouver, BC, Canada.

Email: sarra@allard.ubc.ca

1 | INTRODUCTION

Bitcoin ATMs¹ dot the streets of cities from Prague to Hong Kong, and there are now more than 2,500 such machines in the United States.² One news source reports that there are approximately 15 million bitcoins in the global market and that USD 2 billion was pumped into cryptocurrency hedge funds in 2017 alone.³ In 2017, the price of bitcoin rose from about USD 1,000 in early January to an all-time high of USD 19,738 on December 17, with an average of about 360,000 transactions per day that month.⁴ The price has declined sharply in 2018, and by January 1, 2019, it stood at USD 3,817.⁵ Despite this “roller coaster” fluctuation in value, it still merits consideration in respect of its potential interaction with commercial law. Not unlike an onion, bitcoin has layers and layers in respect of its conceptualization, algorithmic underpinnings, and immutability of data. Peeling away some of the opaqueness reveals how it may be dealt with in insolvency. It might also identify issues that assist in understanding other digital assets.

What exactly bitcoin is and how to calculate its value are still unclear, which could be significant during insolvency, when creditors are looking to realize on their claims. This article is aimed at

¹An ATM machine is an “automated teller machine” or “at the moment” cash machine, depending on the jurisdiction, in this usage a machine that dispenses bitcoin or performs other transaction services when an account holder inserts a card (Oxford Dictionary 2018).

²See: <<https://coinatmradar.com/countries/>>; <<https://coinatmradar.com/country/226/bitcoin-atm-united-states/>>.

³Bloomberg Businessweek, “What Bitcoin Is Really Worth May No Longer Be Such a Mystery” (19 April 2018), available at: <<https://www.bloomberg.com/news/features/2018-04-19/what-bitcoin-is-really-worth-may-no-longer-be-such-a-mystery>>.

⁴Bank of Canada, *Bitcoin Awareness and Usage in Canada: An Update* (July 2018), available at: <<https://www.bankofcanada.ca/wp-content/uploads/2018/07/san2018-23.pdf>>.

⁵See: <<https://www.coindesk.com/price/bitcoin>>.

generating discussion on some of the challenges bitcoin poses for insolvency and bankruptcy.⁶ It looks at different definitions and uses of bitcoin, and although the article situates bitcoin within cryptocurrencies more generally, it focuses only on bitcoin as an example of a number of cryptocurrencies in the market and does not address the breadth of different products that could come under the broad definition of cryptocurrency.

Insolvency risk raises several important questions. What is the nature of bitcoin? Is it property, and if so, what type? Is it currency, commodity or another form of property? What does this characterization mean for insolvency and claims on the estate of the insolvent bitcoin holder? How is the cryptocurrency stored or otherwise protected or “possessed,” and what is the relationship of a bitcoin exchange or storage mechanism to the estate of the insolvent debtor? Are “rights” to the bitcoin personal rights or proprietary rights? What happens when a direct owner of bitcoin becomes insolvent in terms of the ability of creditors to realize on its value? The article raises the issue of what asset or value may be associated with bitcoin, such that an insolvency officer can access, realize on, and distribute that value among the debtor's creditors.

It is important to acknowledge at the outset that the answer to these questions may differ from one jurisdiction to the next, given the varying ways that insolvency is addressed. This article uses examples, mainly from the United Kingdom and Canada, to illustrate some of the challenges, although the approach of other jurisdictions is mentioned where there are relevant decided cases or other developments. While some issues discussed will resonate with other cryptocurrencies, each type has different variables that may alter the legal analysis, so for the purposes of this article, the discussion is confined to bitcoin. This article addresses only blockchains that are distributed technology ledgers used to host forms of bitcoin, as opposed to other types of blockchain.

Section 2 commences with how bitcoin is created and transferred. It continues with a discussion of distributed ledger technology/blockchain in bitcoin and cryptocurrency and some of the multiple potential uses of bitcoin, including as a method of payment, a store of value, or a form of investment. Section 3 contains an analysis of what bitcoin is, whether money or other form of property or asset, and continues with a discussion of whether security can be taken over bitcoin. Section 4 is aimed at the key question of what happens when a direct holder of bitcoin becomes insolvent, what remedies may exist for creditors, and what framework may help them realize on the value, and then examines whether the issues are the same or different where the insolvent debtor is holding bitcoin through one or more intermediaries. Section 5 posits some initial questions and challenges that may arise for creditors if a bitcoin exchange becomes insolvent. Although bitcoin exchange insolvency is not the focus of this article, the first bitcoin exchange insolvencies raise some important issues deserving of future research.

⁶The terms “insolvency” and “bankruptcy” are used interchangeably in this article, although it is important to note that different jurisdictions have different meanings, for example, “insolvency” in both Canada and the United Kingdom is a defined term based on tests of generally being unable to meet debts as they become due or an asset/liability test. However, in Canada, “bankruptcy” refers to the process of liquidating the assets of the debtor for the benefit of creditors, and in the United Kingdom, “bankruptcy” refers to this process in relation to an insolvent individual, whereas in relation to companies, the term is “liquidation” or “winding up.”

2 | BITCOIN BASICS

2.1 | The context—Cryptocurrency generally

Although the idea of electronic payment denominated in fiat currency is not new,⁷ the generation and holding of value not so denominated, by the use of public ledgers operating blockchain technology, has developed rapidly over the last few years. Value is set by the “market” price, whereas the market includes all participants, not just those participants that are nodes.⁸ It also includes those individuals and entities that buy bitcoin for fiat currency and those who accept it for goods and services, even if they themselves are not nodes but do their transactions through intermediaries. Value is recognized by agreement within the community of users of the virtual currency.⁹

Cryptocurrencies can take many forms, and as a group, they share few common characteristics.¹⁰ A cryptocurrency is a digital asset designed to act as a store of value or medium of exchange in the digital economy. Cryptocurrencies are not controlled or regulated by any single authority and can, in some circumstances, be issued without any major approval process. There is no centralized issuer of such products or a trusted third party that manages them, and until very recently, they have been independent of central banks and other financial institutions.¹¹ In addition to being used for the “money-like” functions¹² of being a method of payment and a store of value, issues of digital “coins” are frequently used as a means of raising financing.¹³ One of the difficulties in defining cryptocurrencies such as bitcoin is that the holder of the cryptocurrency does not physically “hold” the coin. Unlike money,¹⁴ which is either in physical form or takes the form of a right against a trusted third party such as a deposit-taking bank, or securities, which are rights against the issuer and are either materialized or held by trusted intermediaries regulated by securities law, the coin holder¹⁵ has neither anything physical nor a right against an intermediary. Instead, at least in the case of bitcoin, the coin holder has the ability to transfer bitcoin that are recorded as being held by a particular “public key,” by use of a “private key.”

2.2 | The role of blockchain in bitcoin and other cryptocurrencies

Blockchain technology is critical to bitcoin and other cryptocurrencies. A blockchain is a distributed ledger containing a record of all transactions. The term “blockchain” was crafted as shorthand for a

⁷It has existed for many years through mechanisms such as bank debit cards and PayPal. See Dan Awrey and Kristin van Zwieten, “The Shadow Payment System” (2017) 43 *Journal of Corporation Law* 775.

⁸See Section 2.2 for a definition of “nodes.”

⁹Odiet observes that the utility of cryptocurrency often relies on recognition of the thing’s existence by other servers and users across a vast network: Christopher Odiet, “Bitproperty and Commercial Credit” (2017) 94 *Washington University Law Review* 649, 650–653.

¹⁰Financial Markets Law Committee, *Issues of Legal Uncertainty Arising in the Context of Virtual Currencies* (July 2016), 1, available at: <http://www.fmlc.org/uploads/2/6/5/8/26584807/virtual_currencies.pdf>. See also the Bank for International Settlements, which has drawn attention to the “potentially disruptive innovations associated with digital currency schemes that are issued automatically and that are not a liability of any party”: Committee on Payments and Market Infrastructures of the Bank for International Settlements, *Digital Currencies* (November 2015), 6.

¹¹Bank of Canada, *Decentralized E-Money (Bitcoin)* (2014), 1, available at: <<http://www.bankofcanada.ca/wp-content/uploads/2014/04/Decentralize-E-Money.pdf>>.

¹²See Charles Proctor (ed), *Mann on the Legal Aspect of Money* (7th edn) (OUP, 2012), paragraph 1.07.

¹³See below at Section 2.5.3, where these functions are examined in more detail.

¹⁴Usually referred to as “fiat money” because it is legal tender whose value is backed by the government that issued it.

¹⁵This refers to a direct coin holder, that is, not one who is holding through an intermediary. Most holders do not, in fact, hold in this way, because in order to do so, the holder needs to have very considerable computing power at his disposal.

“chain of blocks of transactions” that are part of the bitcoin system.¹⁶ Blockchain technology provides a way of holding information in a secure way. It can be used for many purposes, ranging from the holding of medical records to registers of interests in land. However, in this article, we are concerned with its use as the record of the creation and transfer of bitcoin.¹⁷ Bitcoin's blockchain is public in the sense that all transactions are visible, and it is “permissionless” in the sense that any computer may participate in validating transactions and adding them to the ledger.¹⁸

Blockchain technology has several components. One is that every piece of information added to it is heavily encrypted, so that it is very hard to change.¹⁹ Moreover, each piece that is subsequently added would have to be changed to change the previously recorded information. The practical result is that information stored on a blockchain is immutable.²⁰

Another component is that the record of transactions is held on a distributed ledger, that is, it is recorded on many computers (nodes), and the system includes a process whereby information is synchronized on all nodes simultaneously. Thus, the ledger contains every transaction ever processed.²¹ For any piece of information to be changed, the record on each computer would need to be changed, requiring all the computer users to agree.²² Thus, information can be held securely without the involvement of a trusted intermediary. It is also publicly available to anyone who can access the blockchain. The amount of information provided publicly does, of course, depend on the way the system is set up. Under the bitcoin system, for example, all transactions are public, but they are pseudo-anonymous in that the parties involved are only identified by their addresses, which are not linked to any real-world identification.

In addition to the security and immutability that blockchain technology provides, it also enables two other features that are important in relation to bitcoin. The first is that every transfer that is added to the blockchain is checked against all other transactions to ensure that there is no double spending, that is, that the same currency is not transferred twice. Under existing payment systems, this function has to be performed by a trusted intermediary.²³ The second is that the supply of bitcoin is artificially limited to those “created” when the system was originally set up.

¹⁶Hanna Halaburda, “Blockchain Revolution Without the Blockchain” (Bank of Canada Staff Analytical Note/Note analytique du personnel 2018-5), 1; <<https://www.marketsandmarkets.com/MarketReports/blockchain-technology-market-90100890.html>>.

¹⁷Stephen McJohn and Ian McJohn, “The Commercial Law of Bitcoin and Blockchain Transactions” (Suffolk University Law School Research Paper No. 16-13) (22 November 2016), 9, available at: <<https://ssrn.com/abstract=2874463>>.

¹⁸Halaburda, above note 16, 3.

¹⁹Some blockchain networks build immutability into the protocol, but for many, including bitcoin, the immutability comes from the practical improbability of change, see Michel Rauchs *et al.*, “Distributed Ledger Technology Systems: A Conceptual Framework” (Cambridge Centre for Alternative Finance, August 2018), 63–64 and 73, available at: <<https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/distributed-ledger-technology-systems/#.W4IM6vZuLug>>.

²⁰See: <<https://www.coindesk.com/information/how-do-bitcoin-transactions-work/>>.

²¹Each computer verifies each transaction, by checking that it complies with the prearranged protocol. See FAQs at: <<https://bitcoin.org/en/>>.

²²This immutability makes it impossible, in a technical sense, to void transactions, including fraudulent transfers and errors by debtors see Dirk Zetzsche, Ross Buckley, and Douglas Arner, “The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain” (2018) *University of Illinois Law Review* 1361. It does not, of course, mean that transactions cannot be void or voidable in a legal sense, giving the transferring party the right to obtain a court order requiring retransfer: David Fox, “Cryptocurrencies in the Common Law of Property” in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (OUP, 2019).

²³See the paper that first introduced bitcoin in 2008 by Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” available at: <<https://bitcoin.org/en/bitcoin-paper>>; BIS Annual Economic Report 2018, Part V, 95.

2.3 | How is bitcoin created and transferred?

Bitcoin is one of the most well-known and widely circulated cryptocurrencies, although many others are now very prominent in the market. The bitcoin network was created in 2008 by one or more software developers calling themselves “Satoshi Nakamoto.”²⁴ As with any distributed ledger technology system,²⁵ the rules of this system (the “protocol”) are fixed in advance²⁶ and can only be changed by whatever procedures are laid down in the protocol. The distributed network itself consists of “nodes,” that is, many computers around the world, each of which hold all the relevant data at any one time, which add to this store of data by a means laid down in the protocol.²⁷ The data held on this network are, in the case of bitcoin, a record of the creation and each transfer of bitcoin. The way in which the balance associated with each public key is recorded and displayed varies from network to network.

To give an example, the “balance” of bitcoin (known as the “unspent transaction output” or “UTXO”) is actually just an aggregate of transfers in and out.²⁸ It is not possible to transfer out part of one transfer in: the whole amount has to be transferred out and then any “change” has to be transferred back. Ethereum, on the other hand, works more like a bank account: The transfers in are mixed in what is called an “account” and transfers out come from the mixed balance in that account.²⁹ The difference in these methods masks a critically important underlying point: what is actually recorded on the blockchain are the transactions and not the coins. The “coins” are merely the result of the transaction, which is why it is so difficult to say what bitcoin is. Despite this challenge, most, if not all, of the discussion of bitcoin conceptualizes it as something, usually something analogous to something in the real world, such as a physical coin or a bank account, as these analogies are the only way to describe bitcoin sensibly. The following discussion will, to a large extent, follow this pattern.

All bitcoin were “created” when the system was set up and are released during the mining process, which is described below. Each unit is called a “bitcoin,” but bitcoin, which are now each worth several thousand pounds, can be divided into smaller units. One bitcoin is equivalent to 1,000 millibitcoins, 1,000,000 microbitcoins, or 100,000,000 satoshis.³⁰ Bitcoin are created in relation to, and can be transferred to, a unique address, which is derived from a public key: The address is a “hashed” public key³¹ and consists of 34 numbers and letters.³² A unique private key is associated with each public key, generated at the same time as the public key, and is mathematically related to it. The private key is a unique alphanumeric identifier, a cryptographic code that is essentially a long string of 64 numbers and letters,³³ which is used to verify any transactions related to the public key.

As mentioned above, these transactions are what is recorded on the blockchain, and both the public key and transaction information are publicly available to anyone with access to the blockchain. The public key contains no other information, so that it is not possible to identify the person who holds that public key without more information from outside the blockchain itself.³⁴ Any number of

²⁴Satoshi Nakamoto is not the inventor's real name: <<https://www.coindesk.com/information/who-is-satoshi-nakamoto/>>.

²⁵For a rigorous generic description of DLT systems, see Rauchs *et al.* (above note 19).

²⁶Bitcoin itself is run on open source software.

²⁷See Rauchs *et al.*, above note 19, 29.

²⁸Confusingly, transfers in are called “outputs” (i.e., the output from the transaction) and transfers out are called “inputs” (i.e., the input to the transaction). See: <<https://www.ccn.com/bitcoin-transaction-really-works/>>.

²⁹See: <<https://medium.com/@sunflora98/utxo-vs-account-balance-model-5e6470f4e0cf>>.

³⁰See: <<https://www.investopedia.com/terms/s/satoshi.asp>>.

³¹That is, it is made shorter by an encryption process.

³²Hashing operates in one direction, so that the public key cannot be deduced from knowledge of the address.

³³David Quest, “Taking Security over Bitcoins and other Virtual Currency” (2015) 7 *Journal of International Banking & Financial Law* 401, 402.

³⁴Such as details of real-world transactions associated with a transfer to or from that public key.

addresses can be created, and frequently, a new address is created for each transaction.³⁵ It is not possible to discover the link between the public and the private key from the information available on the blockchain,³⁶ and because the private key is necessary in order to transfer the bitcoin, the “holder” of the bitcoin needs to make sure that no one else has access to her private key.

There are various ways of storing the private key, such as recording it on a piece of paper, storing it in an offline cryptocurrency hardware wallet that can be held on a computer hard disk or server,³⁷ printing it on a metal disc or bracelet to make a physical bitcoin,³⁸ or storing it in an online or software wallet, such as an iOS wallet or an android wallet,³⁹ in the cloud and accessed through an app or held by third-party servers.⁴⁰ Secured storage is critically important because if the private key is lost, the bitcoin are lost as well.⁴¹

A transfer between addresses derived from public keys is effected by the transferor issuing an instruction, which is combined with the private key to generate a signature. This signature is then combined with the public key on the blockchain, which enables the blockchain network to verify the transaction. Although the network can only see the public key and the signature, the system is set up in such a way that only a signature created with the private key will work with that particular public key. The transaction is then checked by the network against all other transactions recorded against that public key, to check that there is no double counting,⁴² an important feature of the system. The next stage is that the transaction, together with many other transactions, becomes a block and is added to the blockchain.

The system is sometimes referred to as a “pseudo-anonymous system,” because although names are not used, every transfer identifies the address (public key) of the sender and the address of the recipient.⁴³ The private key is therefore used to verify the transaction and is both necessary and sufficient to effect a transfer of the associated bitcoin.⁴⁴ The person who holds (and uses) the private key thus controls (and, arguably, owns) the bitcoin associated with the public key. However, it is possible for an unauthorized person to obtain, and use, the owner's private key,⁴⁵ in which case the transaction would be unauthorized. This reasoning is important when considering what is meant by “owning”

³⁵Quest, above note 33, 401. This process is usually carried out for the user by the “wallet” and is largely to increase the anonymity of the transactions.

³⁶It may be possible, with difficulty, to match the public key to a name using other information available online. See McJohn and McJohn, above note 17, 7, where the authors observe that many bitcoin users avoid these complexities by using an intermediary to handle their transactions.

³⁷See for example: <<https://www.ebay.com/p/Ledger-Nano-S-Cryptocurrency-Bitcoin-Ethereum-Hardware-Wallet/1485659508>>. This method of holding bitcoin has the disadvantage that, if the computer is corrupted, lost or stolen, the bitcoin associated with the private key are lost.

³⁸Quest, above note 33, 402.

³⁹iOS wallet is a mobile wallet app on an Apple iOS operating platform. The wallet provider and software provided operates a number of services for investors, who do not have to understand details of the technology but who deal with an intuitive interface.

⁴⁰Such wallets are, of course, vulnerable to hacking.

⁴¹European Bank Authority, *Warning to Consumers on Virtual Currencies* (EBA/WRG/2013/01) (12 December 2013), available at: <<https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf>>. See, for example, the story of James Howells who threw away the computer on which his private keys were stored: <<https://www.telegraph.co.uk/technology/2017/12/03/unlucky-man-accidentally-threw-away-bitcoin-worth-100-million/>>.

⁴²The Bank of Canada notes that although Bitcoin is decentralized in that verification and settlement of transactions occurs in a decentralized way, issuance of bitcoins is very centralized and controlled by the algorithm: Halaburda, above note 16, 8.

⁴³McJohn and McJohn, above note 17, 7. See also Misha Tsukerman, “The Block Is Hot: A Survey of The State of Bitcoin Regulation and Suggestions for The Future” (2015) 30 *Berkeley Technology Law Journal* 1127.

⁴⁴McJohn and McJohn, above note 17, 7.

⁴⁵Through fraud, hacking or, if the private key is recorded in a tangible medium, theft.

bitcoin, and also what practical means are open to an insolvency practitioner to realize the value of bitcoin owned by an insolvent party.⁴⁶

The verification process and the adding of bitcoin transactions to the blockchain are done by a subset of the nodes known as “miners.”⁴⁷ The mining nodes use very considerable computing power⁴⁸ to group transactions into blocks and to add the blocks to the blockchain according to the strict rules of the protocol. The mining nodes compete to solve a complicated mathematical problem, the answer to which is used to add the block of transactions to the blockchain. The node that solves the problem first obtains, as a reward, a certain number of bitcoin, creating incentives in the system to add another layer to the blockchain.⁴⁹ These “new” bitcoin are actually already programmed into the system but have not yet become able to be held or transferred. Once they are “mined,” they become part of the system and can be held or transferred.

2.4 | Ways of holding bitcoin

There are different types of people and entities that hold bitcoin,⁵⁰ although only the first two types identified below actually hold them directly.⁵¹ First, there are the mining nodes who have the whole of the blockchain on their computers and who perform the mining process described above. Second, there are people who download nonmining nodes onto their computer,⁵² who are split into two groups: those individuals or entities that have downloaded the whole blockchain⁵³ and those who only have a limited copy.⁵⁴ These direct holders of bitcoin can give their own instructions as to transactions. Third, there are people who do not have any of the blockchain on their computer but who store their private keys⁵⁵ using “custodial wallets” that are often provided by bitcoin exchanges or other custodians.⁵⁶ In a custodial wallet, the wallet provider stores the private key for the owner and may also execute transactions for customers, including enabling them to exchange their bitcoin for fiat currency, such as USD, EUR, or GBP.⁵⁷

It is important to separate out the custody function and the trading function.⁵⁸ A bitcoin exchange is an entity that matches sellers of bitcoin to buyers, charging a fee for the service, like an exchange of any tradable asset. The price for the sale can be fiat currency or other cryptocurrency. This account focuses on the former. Since the exchange matches buyers and sellers, both need to be registered with

⁴⁶See below Section 4.

⁴⁷For an account of the mining process, see: <<https://www.coindesk.com/information/how-bitcoin-mining-works/>>, from which the information in this article is taken.

⁴⁸The bitcoin network, when held on a computer, takes up (at the moment) 145GB. This amount will increase over time as more transactions take place. At the time of writing (3 January 2019), bitcoin mining uses up as much power as the whole of Iraq. See: <<https://digiconomist.net/bitcoin-energy-consumption/>>.

⁴⁹Currently 12.5 bitcoin.

⁵⁰See Rausch *et al.*, above note 19, 58.

⁵¹See: <https://en.bitcoin.it/wiki/Storing_bitcoins>.

⁵²These “nodes” are used in conjunction with a “wallet,” which stores the owner’s private keys.

⁵³Every transaction that has ever taken place (since 2009).

⁵⁴See Rausch *et al.*, above note 19, 50.

⁵⁵Because possession and control of the private key gives access to the bitcoin associated with the public key, it is storage of the private key that is colloquially referred to as storage of bitcoin. See: <<https://www.coindesk.com/information/how-to-store-your-bitcoins/>>.

⁵⁶See below Section 5.

⁵⁷See: <<https://www.coindesk.com/information/how-to-store-your-bitcoins/>>.

⁵⁸See: <<https://www.howtogeek.com/347464/whats-the-difference-between-a-bitcoin-wallet-and-an-exchange/>>.

the exchange. A bitcoin exchange facilitates the purchase by effecting the transfer of money in one direction and bitcoin in the other direction.⁵⁹

The fiat currency price is usually paid by the client either uploading fiat currency to an “account” held with the exchange, which appears to be on a title transfer basis, with the exchange holding the fiat currency in a bank account in its name,⁶⁰ or by the client paying for a single transaction with a credit or debit card denominated in fiat currency. In the former case, the exchange will, on an authorized instruction, make the payment to the seller's account with it, or by a transfer of fiat currency into a nominated account.⁶¹ The transfer of bitcoin for the other leg of the purchase is also effected by the exchange, which is why clients on both sides also need to hold bitcoin in a wallet hosted by the exchange.⁶² This wallet is controlled by the exchange; in other words, the exchange controls the private key. Thus, the exchange can, on the instructions of the selling client, transfer the purchased bitcoin from the seller's wallet to the buyer's wallet.

The custodial services provided by an exchange, or an entity that only functions as a custodian, typically operate as follows. The client opens an “account” with the custodian and transfers bitcoin into its account from an external source or by purchasing it from another client (if the custodian is an exchange). The account will consist of a number of public keys, and the private keys for which are stored by the exchange. The possible legal consequences of this arrangement are discussed below.⁶³ The custodian, through the software running the wallet, will make transfers to and from the wallet as instructed by the client. Some custodians will only transfer to other wallets that it holds,⁶⁴ whereas others will transfer more widely.⁶⁵

Some entities function merely as a custodian,⁶⁶ without functioning primarily (or at all) as an exchange. They also maintain accounts for clients, consisting of one or more public keys and the associated private keys. They are likely to store the private keys offline in a process known as cold storage,⁶⁷ which is considered safer than online storage.⁶⁸ It is, of course, possible for one single entity to offer exchange services (trading and custody services together) and pure custody services as different possible service packages for clients.

2.5 | The functions of bitcoin

In this section, the various functions of bitcoin are briefly discussed in order to unpack what properties it may have.

⁵⁹Idem.

⁶⁰See, for example, Coinbase Terms and Conditions, 3.1, available at: <https://www.coinbase.com/legal/user_agreement?locale=en>. Coinbase calls fiat currency deposited in an account with them “E-Money” and it seems reasonably clear that the client's asset is a right against Coinbase, not a proprietary claim under a trust (see, e.g., Redemption Provisions 3.7).

⁶¹See Coinbase Terms and Conditions, 5.1, 5.3.

⁶²Although this need not be the only wallet a client has, and the client is at liberty to transfer any bitcoin to a wallet attached to a node held on his computer, many clients do not do this for reasons of convenience and therefore use the exchange wallet as their main custodial wallet.

⁶³See Section 5.

⁶⁴For example, Coinbase, whose Terms and Conditions, above note 60, 4.2, invite potential recipients to open a Coinbase account.

⁶⁵See Freewallet Terms and Conditions, 6.1, available at: <<https://freewallet.org/>>.

⁶⁶There are other providers of custodial wallet services which are not exchanges, for example, Freewallet and BTC.com.

⁶⁷See: <<https://www.investopedia.com/articles/investing/030515/what-cold-storage-bitcoin.asp>>.

⁶⁸Known as a “hot wallet.”

2.5.1 | Bitcoin as a method of payment

Bitcoin can serve as a method of payment for goods and services without the use of an intermediary, such as a bank or wire transfer office.⁶⁹ One initial goal, after the height of the 2008–2010 global financial crisis, was to create a payment system that completely removed any “trusted central authority” and replaced that trust with a “cryptographic proof.”⁷⁰ However, how much bitcoin are actually used for payment of goods and services is unknown, but it is probably infrequently.⁷¹ The Governor of the Bank of England has expressed doubt as to the extent to which bitcoin is actually used for payment and whether it will become a medium of exchange because of time delays in processing transactions and volatile fees.⁷²

However, the International Monetary Fund has reported that in the Philippines and Kenya, blockchain-based intermediaries offer money transfer services via bitcoin and subsequent conversion of bitcoins back into fiat currency for withdrawal by recipients through their mobile phones or a bank account.⁷³ In this usage, bitcoin as a method of payment is integrally linked to the fiat currency system, and its use is to facilitate electronic transfers in regions where physical accessibility to banks is an issue.

2.5.2 | Bitcoin as a store of value

Bitcoin can also be used as a store of value, in the same way as investors might buy volatile currencies or commodities. However, some doubts have been expressed by central bankers as to bitcoin's suitability as a store of value, because its value is so volatile.⁷⁴ These first two functions, method of payment and store of value, can exist simultaneously: Investors in bitcoin may use their holdings to buy goods or services directly if a market exists, or to maintain a right to obtain goods or services in the future.

2.5.3 | Bitcoin as a financing tool

A third, rather distinct, use of bitcoin and similar cryptocurrencies is as a means of raising financing for enterprises, foundations, and other projects. Coin or token offerings can be an investment in the entity raising the funds, similar to an equity or debt investment with a view to profit. In other instances, it is purchasing tokens to obtain good or services in the future.⁷⁵ There is a distinction

⁶⁹McJohn and McJohn (above note 17).

⁷⁰BIS Annual Economic Report 2018, Part V, available at: <<https://www.bis.org/publ/arpdf/ar2018e5.htm>>.

⁷¹The use of bitcoin has been banned in some countries, such as Bangladesh, Bolivia, Ecuador, and Morocco. See also Shobhit Seth, “Is Bitcoin Banned in China?” (Investopia, 12 February 2018), available at: <<https://www.investopedia.com/news/bitcoin-banned-china/>>.

⁷²Mark Carney, “The Future of Money” (2 March 2018), available at: <<https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/the-future-of-money-speech-by-mark-carney.pdf?la=en&hash=A51E1C8E90BDD3D071A8D6B4F8C1566E7AC91418>>.

⁷³Dong He *et al.*, “Virtual Currencies and Beyond: Initial Considerations” (IMF Staff Discussion Note, 2016), available at: <<https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>>.

⁷⁴See, for example, Agustin Carstens, “Money in the Digital Age: What Role for Central Banks?” available at: <<https://www.bis.org/speeches/sp180206.pdf>>.

⁷⁵For example, “access tokens,” such as Golem (<<https://golem.network/>>), which are tokens used to access a network, often not yet built. These tokens are analogous to a prepaid voucher, with the issuer promising that the tokens will provide access to a future blockchain-based product that usually does not exist at the time of the token sale. See Michael Bacina and Sina Kassra, “Unlocking Cryptocurrency Token Sales” (2017) 37 *Law Society of NSW Journal* 79.

between bitcoins and tokens.⁷⁶ Bitcoins, which are an example of “native” or “endogenous” tokens,⁷⁷ have their own blockchain platform that operates independently of any other platform,⁷⁸ whereas tokens (“non-native” or “exogenous” tokens) are a representation of a particular fungible and tradeable asset or utility.⁷⁹ This article only considers bitcoins and not exogenous tokens.

3 | IS BITCOIN MONEY, ANOTHER FORM OF PROPERTY, OR SOMETHING ELSE?

There is no global consensus on what exactly bitcoin is—whether it is a form of property or not, and, if so, what type of property: currency (or money), a commodity defined very expansively, or some other form of intangible asset. Although this article is unlikely to resolve this question entirely, it is important to examine both the normative question of whether bitcoin should be “property” and whether it will be treated as property under the law of the jurisdictions examined. As explained below, insolvency statutes specifically refer to property as comprising the estate of the insolvent party. It is therefore possible that bitcoin could fall within the definition of “property” within an insolvency statute but not within the definition of property under the general law. This position is not desirable, however.

It is a basic tenet of insolvency law that, on insolvency, the pre-insolvency entitlements are preserved as far as possible⁸⁰ and that pre-existing property rights are respected, to the extent that this protection aligns with insolvency law norms. A different view of bitcoin as property within and outside insolvency would cut across this principle. More generally, it is desirable, as far as possible, for the characterization of bitcoin to be consistent across all areas of law. The discussion in this section therefore focuses on whether bitcoin is property under the general law, and, if so, what type of property it is. This analysis will assist in thinking about how to realize its value in insolvency.

3.1 | Is bitcoin property?

It is possible to approach this question from two starting points. One is to ask whether bitcoin is “money,” in which case it would be a necessary corollary of that conclusion that it is a form of property. Another is to ask whether it is property and, if so, of what type? Whether it is money or not would come within this secondary discussion. The first approach is important when considering how it should be regulated,⁸¹ but in relation to private law, most issues that arise⁸² are rarely, if ever, relevant on insolvency.⁸³ The second approach will, therefore, be adopted here.

⁷⁶Although in the popular media, they are often referred to interchangeably.

⁷⁷See Rausch *et al.*, above note 19, 50–51.

⁷⁸Citowise, “The Basics: Coin vs Token. What is the Difference?” available at: <<https://blog.citowise.com/the-basics-coin-vs-token-what-is-the-difference-5cd270591538>>.

⁷⁹Aziz MastertheCrypto, available at: <<https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/>>.

⁸⁰Kristin van Zwieten, *Goode on Principles of Corporate Insolvency Law* (5th edn) (Sweet & Maxwell, 2018), 3-02.

⁸¹See, for example, Financial Markets Law Committee (above note 10); Mark Kalderon, Ferdisha Snagg and Claire Harrop, “Distributed Ledgers: A Future in Financial Services?” (2016) 31 *Journal of International Banking Law and Regulation* 243, 244.

⁸²For example, the particular exception to the *nemo dat* priority rule under *Miller v Race* (1758) 1 Burr. 452, the fact that a court that will not usually make an order of specific performance to enforce a money obligation and the jurisprudence surrounding the remedies available on an action in debt: Charles Proctor and Victoria Dixon (eds), *Goode on Payment Obligations* (Sweet & Maxwell, 2016), 9.4, referencing *South African Territories Ltd v Wallington* [1898] AC 309 (HL).

⁸³However, see below the discussion on bitcoin-denominated claims at Section 4.1 below.

The first thing that needs to be considered is what is the subject matter of the discussion. As described above, bitcoin is the subject matter of the record of a series of transactions recording the “creation” and “transfer” of something. This record is contained in code recorded on the blockchain. However, the subject matter of that record, the bitcoin, is not even a piece of code. What the “owner”⁸⁴ of bitcoin has is the ability to generate a transfer, in return for which the transferee is prepared to transfer valuable consideration, which is likely to be fiat or cryptocurrency, or a real-world asset. That ability to generate the transfer comes from the fact that the “owner” is the sole person who can use the private key. So what is the candidate for being considered property? The record of transfer, the private key,⁸⁵ or the “thing” that is the subject matter of the transfer, which does not even exist as a piece of code?

The answer appears to be that it is the last of these things. In a manner similar to money, it is, by consensus of the market, more valuable than its intrinsic value (arguably, the intrinsic value of bitcoin is zero). Unlike money (coins, notes, or bank money), however, bitcoin has neither a physical, tangible existence nor is it a right against another person. The main characteristic of the bitcoin system is that the record of transfers is made immutably,⁸⁶ and this fact gives value to the subject matter of the transfers by the common consensus of participants in the market. This section will concentrate, therefore, on whether the subject matter of the transfer is “property”: This subject matter will be referred to as “bitcoin.” In relation to insolvency, however, the possibility (and utility) of the private key (or at least the means by which it is recorded) being property, will be examined.

There is a lack of clarity in the market as to whether bitcoin and similar cryptocurrencies are property within the meaning of commercial law. *Black's Law Dictionary* defines property as denoting:

*everything that is the subject of ownership, corporeal or incorporeal, tangible or intangible, visible or invisible, real or personal; everything that has an exchangeable value or that goes to make up the wealth of an estate.*⁸⁷

Arguably, bitcoin falls within this very broad definition, and even if its value may fluctuate widely and transferability is sometimes uncertain, it is still a form of property the value of which could be realized on insolvency.

There is a vast common law literature discussing what property is, or, more accurately, what can be the subject of “property rights.”⁸⁸ The three most significant incidents of property have been analysed as transferability, excludability, and exigibility. On these criteria, bitcoin scores well. There is a well-developed and accepted method of transferring bitcoin from one public/private key holder to another. Showing excludability is also straightforward, because the need for the private key to be used to verify any transfer means that the holder of the private key can exclude the rest of the world from access to the bitcoin.⁸⁹ Here, this exclusion means preventing the ability to transfer the bitcoin and therefore realize its value. Of course, it is possible for more than one person to have access to the private key, but arguably, this situation is analogous to where several people have access to, and the ability to transfer possession of, tangible property.

⁸⁴This word is in inverted commas, because whether bitcoin is property that can be owned is the subject of the current discussion.

⁸⁵The possibility that the “property” held by the owner is in fact the private key is discussed by Quest (above note 33).

⁸⁶The immutability is technical and not legal: For example, it must be possible to reverse a transfer pursuant to court order.

⁸⁷*Black's Law Dictionary* (5th edn) (West Publishing Co, 1979), 1095.

⁸⁸See Michael Bridge *et al.*, *The Law of Personal Property* (2nd edn) (Sweet & Maxwell, 2017), 1-002 (footnote 1).

⁸⁹For the view that the ability to prohibit access is a “badge” of property, see Kevin Gray, “Property in Thin Air” [1991] *Current Law Journal* 252, 292 *et seq.*

Exigibility is more complicated. It means that the thing must exist as an asset that can be the subject of the property right (the right *in rem*), that is, a right that is enforceable against third parties, such as, in the present context, an insolvency officer. If the thing ceases to exist, the right ceases to exist.⁹⁰ Although this criterion is hard to conceptualize in relation to bitcoin, which does not exist in the physical world but only in terms of the autonomous system of the blockchain, once bitcoin is conceptualized as “something,” the criterion is met. If bitcoin is property, a person would cease to have a right *in rem* in relation to it if the system entirely collapses,⁹¹ so that that “bitcoin” no longer exists, but would continue to have a right *in rem* in relation to it while it continued to exist, as long as he, she, or it does not transfer it to someone else, even if, for example, the person lost the private key.

On a theoretical level, then, there is a reasonably strong argument that bitcoin is property. However, it is not at all clear whether a court would come to this conclusion. Such a finding would depend on both the normative arguments made above, and the application of doctrine. Most jurisdictions divide personal property⁹² into tangible and intangible property. Under English law, this division corresponds to “choses in possession” and “choses in action,” and it is difficult to bring bitcoin within either category.⁹³

Directly held bitcoin, although clearly intangible, are not *choses in action*. A *chose in action* is a right against another party, such as a receivable, or a right against a bank with whom the owner has an account. Holding bitcoin directly does not give the holder a right against anyone. If bitcoin is held by an intermediary, the counterparty of the intermediary would have a *chose in action* against the intermediary,⁹⁴ but this right does not make the bitcoin itself a *chose in action*.

3.1.1 | A challenge for U.K. law

Directly held bitcoin are clearly not tangible and therefore cannot be, on traditional English law analysis, a *chose in possession*. Recent English judgments have concluded that, in the absence of special statutory provisions,⁹⁵ possession cannot be taken of an intangible.⁹⁶ But it can be argued that because bitcoin are clearly not choses in action, they have more in common with choses in possession, and that the rules developed in the context of *choses in possession* should apply.⁹⁷ One possibility is to consider bitcoin as “other intangible property,” adapting existing property rules accordingly. The dichotomy in the analysis of personal property between *choses in possession* and *choses in action*, although possibly satisfactory in the past,⁹⁸ can, arguably, now no longer be seen as exclusive.⁹⁹

⁹⁰This point is famously illustrated by the phrase “you cannot own your cake and eat it,” for which see Peter Birks, *An Introduction to the Law of Restitution* (revised edn) (OUP, 1989), 49–50.

⁹¹Or is irretrievably changed by a 51% attack, for example. See: <<https://www.investopedia.com/terms/1/51-attack.asp>>.

⁹²That is, any property that is not land (immovable property).

⁹³*Colonial Bank v Whinney* (1886) 11 App Cas 426; *Your Response Ltd v Datateam Business Media Ltd* [2014] EWCA Civ 281, [13], [27].

⁹⁴See below, Section 2.5.1.

⁹⁵See, for example, Financial Collateral Arrangements (No.2) Regulations SI 2003/3226, regulation 3(2) (as amended by SI 2009/2462 and SI 2010/2993).

⁹⁶*OBG Ltd v Allan* [2007] UKHL 21; *Gray v GTP Group Ltd; In re F2G Realisations Ltd* [2010] EWHC 1772 (Ch); *Your Response Ltd v Datateam Business Media Ltd* [2014] EWCA Civ 281.

⁹⁷See, in relation to crypto-securities, Ferdisha Snagg and Sarah Green, “Distributed Ledger Technology and Intermediated Securities” in Louise Gullifer and Jennifer Payne (eds), *Intermediation and Beyond* (Hart, 2019).

⁹⁸For a historical argument that the binary analysis was never really English law, see Fox (above note 22).

⁹⁹Such a view would entail departing from the clear view of the Court of Appeal in *Your Response Ltd v Datateam Business Media Ltd* [2014] EWCA Civ 281.

A third category of “other intangible property” was suggested by Lord Bridge in the Privy Council in *Attorney General of Hong Kong v Nai-Keung*,¹⁰⁰ where the benefit of an export quota, which was freely bought and sold (though it did not give rise to an enforceable right to obtain a license to export textiles from Hong Kong), was said to be a form of other intangible property. The category was further extended (*obiter*) in *Armstrong DLW GmbH v Winnington Networks Ltd*¹⁰¹ to a carbon trading allowance known as a European Union Allowance.¹⁰² A reasonably strong argument can be made that the emergence of digital assets, of which bitcoin is only an example, necessitates the adoption of this third category and that what is really important is whether the contenders for inclusion in this category meet the criterion as to what can be “property” discussed above. If such a miscellaneous category were to be part of English law, bitcoin could fall within it, and rules could then be fashioned specifically to deal with this type of property.

If this recognition happens, a view will have to be taken as to how far the rules currently governing *choses in possession* can apply to bitcoin by analogy. For example, bitcoin can be transferred and stored in such a way that they may be lost, which the common law recognizes as a characteristic of *choses in possession* but not of *choses in action*.¹⁰³ Moreover, the factual manner in which the owner of bitcoin prevents others accessing the bitcoin could be seen as strongly analogous to the taking of possession of the bitcoin. Possession is a slippery concept but usually requires control of the possessed item and an intention to possess it.¹⁰⁴ Controlling the private key (e.g., by placing it in a “cold storage” device maintained by the bitcoin “owner”) can be seen as analogous to physical control of a tangible item, and the bitcoin “owner” also will have the intention to “possess.” If the private key is stored in a wallet provided by a third party, then this storage is analogous to giving custody of a physical item to a custodian.¹⁰⁵ Care would have to be taken, however, that the introduction of such a hybrid did not cause negative unintended consequences in other areas of English law, such as the law of conversion.¹⁰⁶

There are two other possible arguments as to whether cryptocurrencies are property in English law. The first is that what the owner actually has is the information on the private key, which is confidential information and could be valuable. The difficulty with this argument is that under English law, at present, information itself cannot properly be regarded as a form of property,¹⁰⁷ except where it has been given that status by legislation, as in the case of patents and trademarks.¹⁰⁸ Another argument is that if bitcoins are money (much discussed in other contexts),¹⁰⁹ they do not need to fulfil the criteria for any particular type of property. Such an argument is unlikely to succeed under English law, but it might in other, more functionally minded, jurisdictions. In fact, under English law, the

¹⁰⁰[1987] 1 WLR 1339, 1342. See also *In re Rae* [1995] BCC 102; *In re Celtic Extraction* [2001] Ch 487.

¹⁰¹[2012] EWHC 10 (Ch), [61].

¹⁰²See, further, Bridge *et al.*, above note 88, 1-018–1-019.

¹⁰³Joanna Perkins and Jennifer Enwezor, “The Legal Aspect of Virtual Currencies” (2016) *Journal of International Banking and Financial Law* 569, 569.

¹⁰⁴Ewan McKendrick, *Goode on Commercial Law* (5th edn) (Penguin, 2016), 2.40.

¹⁰⁵For more detailed discussion, see Section 5 below.

¹⁰⁶The House of Lords was clear in *OBG Ltd v Allan* [2007] UKHL 21 that intangible property could not be the subject of conversion, although this conclusion has been criticized, see, for example, Sarah Green and John Randall QC, *The Tort of Conversion* (Hart, 2009).

¹⁰⁷*OBG Ltd v Allan* [2007] UKHL 21.

¹⁰⁸English law protects confidential information by enforcing a duty of confidence or awarding damages for its breach: Quest, above note 33, 403.

¹⁰⁹See Carney (above note 72); Carstens (above note 74); Perkins and Enwezor (above note 103); John Holden, “Trifling and Gambling with Virtual Money” (2018) 25 *UCLA Entertainment Law Review* 41; Charles Proctor, “Cryptocurrencies in International and Public Law Conceptions of Money” in Fox and Green (eds) (above note 22).

issue is likely to arise the other way around. If bitcoin are property, are they money? Or, if not money, is bitcoin another form of property, such as a commodity?¹¹⁰ Although these are interesting questions, they are only peripherally relevant for the discussion in this article.¹¹¹

3.1.2 | Possibly a proprietary interest in Canada

In Canada, analogous judicial reasoning suggests that bitcoin claims may be considered proprietary in nature in future insolvency cases.

In the non-insolvency context, the Canadian Court in *Shair.Com Global Digital Services Ltd v Arnold* approved a preservation order in a case seeking damages for a former officer and employee of the company allegedly misappropriating bitcoin from the company.¹¹² The fourfold test for granting a preservation order in Canada includes finding that the plaintiff has a proprietary interest in the property in issue and that the threat of disposition of the property is reasonable. The court held that the plaintiff had established that it had a claim to a proprietary interest in the laptop computer and in the digital currencies purchased by the defendant flowing from the plaintiff's initial USD 18,500 investment in bitcoin.¹¹³ The court held that, given the nature of digital currencies and difficulty in tracking ownership of digital wallets, there was a reasonable apprehension that the currencies may be transferred out of the jurisdiction, and if the order were not granted, the plaintiff risked losing the wallet information and digital currencies forever, whereas there was no prejudice to the defendant in preserving the property and information.¹¹⁴

In another Canadian case, the British Columbia Supreme Court held that it did not need to determine the precise nature of cryptocurrency for purposes of ordering tracing and recovery. A Singapore company, Copytrack, had an initial coin offering (ICO) of its "CPY tokens."¹¹⁵ The defendant Wall subscribed for 530 CPY tokens and Copytrack mistakenly transferred 530 Ether tokens to Wall's cryptocurrency wallet ("Wall wallet"); the value of the CPY tokens intended to be transferred was about CAD 780, but the value transferred was CAD 495,000.¹¹⁶ Copytrack immediately notified Wall of the mistake and requested return of the Ether Tokens. Wall failed to do so, instead transferring them into a cryptocurrency trading account with a cryptocurrency exchange. Copytrack brought a summary judgment application for conversion and wrongful detention of the Ether tokens.

After exchanges between the parties, Wall transferred the Ether tokens back to the Wall wallet, but then they were transferred out into five different wallets, which Wall claimed was done by an

¹¹⁰Chelsea Deppert, "Bitcoin and Bankruptcy: Putting the Bits Together" (2015) 32 *Emory Bankruptcy Developments Journal* 123, 138; Devin Hahn, "Bitcoins in Bankruptcy: Taking a Byte Out of Chapter 11" (2016) 25(3) *Journal of Bankruptcy Law & Practice* 4.

¹¹¹One possible relevant issue is whether a security interests over bitcoin held "in an account" falls within the Financial Collateral (No 2) Regulations 2003 and the Financial Collateral Directive (see below Section 3.2).

¹¹²*Shair.Com Global Digital Services Ltd. v Arnold*, 2018 BCSC 1512 (BCSC).

¹¹³*Ibid.*, paragraphs 15–16.

¹¹⁴*Ibid.*, paragraphs 28–29. The court declined to grant a Mareva injunction, finding that the plaintiff was speculating about what that initial investment might be worth, and to tie up almost CAD 3 million of the defendant's assets in the face of such a speculative claim would be unreasonable. In December 2018, the court in this case ordered that the respondent could cross-examine the digital currency consultant who had sworn affidavits with results of an investigation she conducted at the request of the plaintiff, which found that plaintiff had more than CAD 5 million in digital currency assets unaccounted for; *Shair.com Global Digital Services Inc. v Arnold*, 2018 BCSC 2261. The case is ongoing as of March 2019.

¹¹⁵*Copytrack Pte Ltd v Wall*, 2018 BCSC 1709.

¹¹⁶*Ibid.*, paragraphs 3–5.

unknown third party.¹¹⁷ The court held that summary judgment was available because the essential facts underlying Copytrack's claim were undisputed. Although the court acknowledges that

the proper characterization of cryptocurrency, including the Ether tokens, is a central issue in this case, and one that informs the analysis of whether Copytrack's claims in conversion and detainee can succeed,

the evidentiary record was inadequate to permit a determination of that issue, as it is a complex and as of yet undecided question and not suitable for determination by way of a summary judgment.¹¹⁸ However, the court held that would be no practical utility in sending this matter to trial given Wall's death after the hearing and that, regardless of the characterization of the Ether tokens, it was undisputed that they were the property of Copytrack, they were sent to Wall in error, they were not returned when demand was made, and Wall had no proprietary claim to them.¹¹⁹ In the court's view,

*while the evidence of what has happened to the Ether tokens since is somewhat murky, this does not detract from the point that they should rightfully be returned to Copytrack and it would be both unreasonable and unjust to deny Copytrack a remedy.*¹²⁰

The court granted an order entitling Copytrack to trace and recover the Ether tokens, wherever they were currently held. Thus, the Canadian Court recognized a property interest, even in acknowledging that the precise nature of that interest was not clear.

There are a couple of analogies that can also be used to suggest that Canadian courts may find holding bitcoin to be a proprietary right. One recognized form of property at common law in Canada is a *profit à prendre*, enabling the holder to enter onto the land of another to extract some part of the natural produce, such as crops or game birds and “profit of piscary,” a type of *profit à prendre* right to fish in the privately owned waters of another.¹²¹ Canadian courts have found *profit à prendre* to be a proprietary right, even though it is contingent on the holder capturing or harvesting something of value in the future. By analogy, the holder of bitcoin, while not yet possessing anything, arguably has a right to the value if it is realized and thus could be framed as having a proprietary right.

The other analogous example is fishing licences, which in Canada are issued sparingly to preserve fish in Canadian oceans. The Supreme Court of Canada (SCC) in *Saulnier v Royal Bank of Canada* held that a fisher's licence¹²² constituted “property” within the scope of the Bankruptcy and Insolvency Act (BIA)¹²³ and provincial personal property securities legislation.¹²⁴ The SCC held that a licence confers to the holder a right to engage in fishing under the conditions imposed by the licence and a proprietary right in any fish harvested and earnings from their sale; and although these elements of the licence do not wholly correspond to the full range of rights necessary to characterize

¹¹⁷Ibid., paragraph 11.

¹¹⁸Ibid., paragraph 34.

¹¹⁹Ibid., paragraph 35.

¹²⁰Ibid., paragraphs 35, 36.

¹²¹*Saulnier v Royal Bank of Canada*, [2008] 3 SCR 166, 2008 SCC 58, paragraphs 28 and 33–34.

¹²²Issued pursuant to sections 7(1) and 9, Fisheries Act, RSC 1985, c F-14.

¹²³Section 2, Bankruptcy and Insolvency Act RSC 1985, c B-3, as amended (BIA), which states: “‘property’ means any type of property, whether situated in Canada or elsewhere, and includes money, goods, things in action, land and every description of property, whether real or personal, legal or equitable, as well as obligations, easements and every description of estate, interest and profit, present or future, vested or contingent, in, arising out of or incident to property.”

¹²⁴*Saulnier* (above note 121); section 2, Personal Property Security Act (Nova Scotia), SNS 1995–96, c 13 (PPSA).

something as “property” at common law, they were property within the meaning of the two statutes.¹²⁵ The court stated that

*because a fishing licence may not qualify as ‘property’ for the general purposes of the common law does not mean that it is also excluded from the reach of the statutes.*¹²⁶

The SCC held that the Parliament signalled an intention to sweep up a variety of assets of the bankrupt not normally considered “property” at common law, so that the value of those assets are made available to creditors, an intention that must be respected if the objectives of the legislation are to be achieved.¹²⁷ It is important to look at the substance of what is conferred, namely, a licence to participate coupled with a proprietary interest in the fish caught.¹²⁸ The SCC also held that the licence is also “personal property” within the meaning of the Personal Property Security Act (PPSA),¹²⁹ finding that the definition of “intangible” includes an interest created by statute and that the grant by the Minister of a licence, coupled with a proprietary interest in the fish caught, is thus sufficient to satisfy the PPSA definition.¹³⁰

The SCC held that both statutes should be interpreted in a way best suited to enable them to accomplish their respective commercial purposes.¹³¹ By analogy, the bitcoin does not strictly meet common law requirements of property, but it does arguably involve a right to claim any value that can be realized in the future if the bitcoin is exchanged for fiat currency or some other form of property. Whether or not that value is ever realized, the bitcoin holder may currently have a proprietary right in any future value realized by sale of the bitcoin or conversion to fiat currency.

In one of the first judgments granting exemption relief from securities law disclosure requirements in multiple jurisdictions for a plan of arrangement, the principal regulator, the Ontario Securities Commission, held that the direct holdings in bitcoin and other cryptocurrencies were assets within the meaning of securities law, without any real discussion on the nature of the assets.¹³²

3.2 | Can security be taken over bitcoin?

One practical consequence of whether bitcoin are property is that, if so, security could be taken over them. A holder of security over a debtor's bitcoin would then have priority on the insolvency of that debtor to the value of those bitcoin. The features of a secured claim are relatively similar across jurisdictions globally. Generally, in common law jurisdictions, absent a bankruptcy or insolvency law stay, a secured creditor can enforce its claim against the secured asset without the need for formal court proceedings. A secured creditor can enforce its claim in priority to other creditors and other

¹²⁵Saulnier, above note 121, paragraphs 16, 23, 43 and 46–47.

¹²⁶Ibid., paragraph 16, where the Court held that “The task is to interpret the statutory definitions in a purposeful way having regard to their entire context, in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act, and the intention of Parliament.”

¹²⁷Section 2, BIA.

¹²⁸The trustee was entitled to require the debtor to execute the appropriate documentation to obtain a transfer of the fishing licences to the third-party purchaser.

¹²⁹Section 2, PPSA.

¹³⁰Saulnier, above note 121, paragraphs 51–52. The registration is therefore valid to include the section 7(1) licence and, in the absence of any other PPSA defence, the bank is entitled to proceed with its PPSA remedies.

¹³¹Ibid., paragraphs 14 and 42.

¹³²Re Bradmer Pharmaceuticals Inc, 2018 CanLII 48607 (ON SEC).

claimants to the assets on the insolvency of the debtor or the holder of the asset¹³³ and can generally prevent or control dealings in the asset that might prejudice enforcement.¹³⁴

There are two issues here. The first, and most fundamental, is whether there is property over which to take security. The second is how, in practice, that security is enforced. This second issue could be overcome by a personal obligation to permit the secured creditor to have access to the key in certain situations. If the debtor refused, the creditor could sue on that obligation and get a court order for specific performance, on the grounds that damages would not be an adequate remedy, and then the creditor could use the key to realize the value of the bitcoin. If the debtor is outside the jurisdiction, however, enforcement of this obligation could be more difficult.¹³⁵

Even if a creditor obtains the private key on creation of a security interest, there is no practical means of preventing the debtor from spending the secured bitcoin or transferring them to another person before enforcement, if the debtor has retained or copied the private key,¹³⁶ although this behaviour would, of course, be a breach of the security agreement and would normally entitle the creditor to accelerate the loan and take other enforcement measures. The security interest, if created by a company, is likely to be registrable. For example, under English law, it would have to be registered in the company charges register,¹³⁷ but such registration would probably not result in a bona fide purchaser for value having constructive notice of the security interest, and therefore, such a transferee would be likely to take free.¹³⁸

If bitcoin are property, then, there would be no legal obstacle to a mortgage or charge being granted under English law. Such a security interest is very unlikely to fall within the Financial Collateral Arrangements (No 2) Regulations (FCAR),¹³⁹ which exempt financial collateral arrangements from registration and from certain insolvency provisions. Under these regulations, “financial collateral” is defined as “money in any currency, credited to an account.”¹⁴⁰ Directly held bitcoin are clearly not “credited to an account”; whether it is the case in relation to bitcoin held in an account on an exchange is more debatable. However, even if it is, there is very considerable doubt as to whether bitcoin would fall within the phrase “money in any currency,” at least at the moment.¹⁴¹

If bitcoin are not property, it is hard to see how a traditional security interest, particularly a charge, could be taken over them, at least under English or Canadian common law. It is certainly possible, however, to enter into a transaction that has the same effect as the giving of security.¹⁴² Because bitcoin are assets that can be transferred, they can be transferred into the name of the collateral taker. There should be no problem with this arrangement taking effect as an outright transfer: a title transfer collateral arrangement (to use the Financial Collateral Directive¹⁴³ terminology). This arrangement is like a Roman law *mutuum*: the taker owes a personal obligation to return equivalent assets on

¹³³Subject to any statutory priorities, see, for example, sections 60, 81.3, and 136, BIA; sections 175, 176A, 176ZA and Schedule B1, paragraphs 65(2) and 99, Insolvency Act 1986.

¹³⁴Quest, above note 33, 401. There are generally some exceptions in relation to dealings in the ordinary course of business, such as in relation to the English law floating charge.

¹³⁵*Ibid.*, 403.

¹³⁶*Idem.*

¹³⁷See discussion in the next paragraph.

¹³⁸For a discussion of the relevant priority rule, see Bridge *et al.* (above note 88).

¹³⁹SI 2003 No. 3226 (FCAR).

¹⁴⁰*Ibid.*, regulation 3(1).

¹⁴¹See Quest (above note 33); and Louise Gullifer (ed), *Goode and Gullifer on Legal Problems of Credit and Security* (6th edn) (Sweet & Maxwell, 2017), 6-05.

¹⁴²Quest (above note 33).

¹⁴³Directive 2002/47/EC on financial collateral arrangements (FCD).

payment of the secured obligation.¹⁴⁴ The collateral taker could then “enforce” by not returning the bitcoin if the obligation were not performed. Such an arrangement, like all title transfer collateral arrangements, exposes the debtor to the credit risk of the creditor, because the obligation to retransfer is merely personal, although this obligation only extends to the surplus value of the bitcoin over and above the value of the secured obligation.¹⁴⁵

More contentiously, the arrangement could take effect as a legal mortgage, that is, a legal transfer with an obligation to retransfer that equity will enforce, and so which is called the equity of redemption.¹⁴⁶ If the collateral taker enforces the security interest, for example, by realizing the value in fiat currency and paying itself out of the proceeds, it will, under English law, hold the surplus on trust for the security provider (unlike under a title transfer collateral arrangement). Even if English law did not recognize bitcoin as property, it would be possible to replicate the function of a mortgage by express agreement.

In Canada, given the recognition of fishing licences giving rise to proprietary rights, it is possible that courts will recognize and enforce security given on bitcoin, although there is no case law to date. In *Saulnier*,¹⁴⁷ discussed above, a general security agreement (GSA) that gave a bank a security interest in

all ... present and after acquired personal property including ... intangibles ... and in all proceeds and renewals thereof

was found to include fishing licenses as property over which the security could be taken.¹⁴⁸ The trustee had signed an agreement to sell four licences, but the bankrupt refused to sign the necessary documents, claiming the licences did not constitute property available to the secured creditor who had registered a GSA under the Nova Scotia PPSA.¹⁴⁹ The SCC held that the PPSA is designed to facilitate the creation of a security interest to enable holders of personal property to use it as collateral and to enable lenders to predict accurately the priority of their claims against the assets in question.¹⁵⁰ The question under the PPSA is whether the holder (*Saulnier*) had a qualifying interest in the licence either at the time he entered into a GSA with the bank or at the time the bank sought to realize on his after-acquired property.¹⁵¹

By analogy, if a lender registers its interest in bitcoin under personal property security legislation, will a court find that the definition of “intangible” includes an interest created by holding the bitcoin? Based on the *Saulnier* reasoning, there may need to be a statutory definition to peg to the bitcoin in addition to an interest at common law. However, even where a lender perfects its security interest in bitcoin through registration under the PPSA, the borrower will not be prevented from transferring them to a third party, unless some other protections are in place, as discussed above.

One other possibility is that the debtor's bitcoin are made subject to a smart contract, whereby they are automatically transferred to the creditor if the debt is not paid. Depending on how this agreement is done technically, it could result in a type of flawed asset (i.e., the conditional contract is part

¹⁴⁴*Ibid.*, Article 2(1).

¹⁴⁵See Gullifer, above note 141, 6–37.

¹⁴⁶*Ibid.*, 1–59.

¹⁴⁷*Saulnier* (above note 121).

¹⁴⁸*Ibid.*, at para 5.

¹⁴⁹Section 2, PPSA.

¹⁵⁰*Saulnier*, above note 121, paragraph 19.

¹⁵¹*Ibid.*, paragraph 40.

of the protocol governing the bitcoin, rather than externally imposed on it), which would have the same function as a security interest, but which would not require registration. Although such a smart contract may be technically possible in relation to bitcoin itself, it is much more likely to occur in relation to other types of cryptocurrencies such as Ethereum, which allow code to be embedded in relation to a token within the system.

4 | INSOLVENCY AND THE TREATMENT OF BITCOIN IN BANKRUPTCY

In Canada, the United States, and many EU member states, the insolvency regime is highly codified and considered a public policy regime, and thus, the statutory language will guide the treatment of bitcoin during insolvency. The concepts of property, eligible financial contracts, and other assets are highly defined and are given different treatment depending on what category they are in under insolvency legislation. In the United Kingdom, much of insolvency restructuring takes place outside statutory mechanisms, using private financing and workouts, in which case the approach would be to ask if the bitcoin is property subject to private law. Civil law countries frequently require precise statutory language before property comes within the definition of assets available for realization by creditors, enforceable under insolvency law.

However bitcoin is characterized, if it has value, it is an asset in a bankruptcy estate, which means that insolvency practitioners (IPs), such as trustees, should be able to realize the value of the bitcoin for purposes of distributing that value to creditors based on the priorities set out in domestic insolvency legislation. This section begins a discussion of the treatment of bitcoin during insolvency or bankruptcy. It looks at the insolvency of debtors that hold bitcoin directly and then where they hold bitcoin through intermediaries. Section 5 then briefly examines issues that can arise when an intermediary, such as a bitcoin exchange, becomes insolvent.

4.1 | The insolvency of debtors directly holding bitcoin

Where a debtor that directly holds bitcoin becomes insolvent, there are two main issues for creditors and IPs: transparency regarding the holding of the bitcoin and realizing the value, so that it can be distributed to creditors.

If a debtor (corporate or individual) enters insolvency proceedings, it is a basic duty of the IP to realize the debtor's estate, that is, to “get in” any property of the debtor, and to turn it into money so that it can be distributed to the creditors. Under English law, the estate of a bankrupt¹⁵² individual vests in the trustee in bankruptcy “without any conveyance, assignment or transfer.”¹⁵³ Where a company is wound up by the court, it is the duty of the liquidator to

*secure that the assets of the company are got in, realised and distributed*¹⁵⁴

and to take custody of

¹⁵²This comprises, with some exceptions such as goods necessary for the bankrupt's family and trade, “all property belonging to or vested in the bankrupt at the commencement of the bankruptcy”: section 283(1), Insolvency Act 1986 (1986 c 45).

¹⁵³*Ibid.*, section 306.

¹⁵⁴*Ibid.*, section 143(1).

*all the property and things in action to which the company is or appears to be entitled.*¹⁵⁵

An administrator has the power to

*take possession of, collect and get in the property of the company.*¹⁵⁶

It will be seen that all these powers and duties relate to the “property” of the company. There is not an exhaustive definition of property in the Insolvency Act 1986, but section 436 provides that the term includes

money, goods, things in action, land and every description of property wherever situated and also obligations and every description of interest, whether present or future or vested or contingent, arising out of, or incidental to, property.

The first question, therefore, is whether bitcoin falls within the definition of property for the purposes of the Insolvency Act 1986.

The earlier discussion as to whether bitcoin is property under the general law¹⁵⁷ is highly relevant to this issue. The English courts have taken a wide view of the definition of property in the Insolvency Act 1986,¹⁵⁸ and there is an argument that even if bitcoin is not “property” for all purposes, it should be included within the Insolvency Act 1986 definition.¹⁵⁹ The fact that the bitcoin can be realized for (considerable) value by anyone controlling the private key, although not determinative of whether bitcoin falls within the definition of property in section 436,¹⁶⁰ is a very strong normative argument for the conclusion that it does fall within the definition.

Moreover, even if bitcoin itself were not classified as property, arguably, the means by which the debtor held the private key could in some circumstances be “property” and fall within the debtor's assets, thus giving rise to an argument that it enables the IP to realize the value “locked up” in that private key.

The definition of property under the Canadian BIA is very broad:

property means any type of property, whether situated in Canada or elsewhere, and includes money, goods, things in action, land and every description of property, whether real or personal, legal or equitable, as well as obligations, easements and

¹⁵⁵Ibid., section 144(1).

¹⁵⁶Ibid., Schedule 1 paragraph 1.

¹⁵⁷Section 3.1 above.

¹⁵⁸*Bristol Airport v Powdrill* [1990] Ch 744, 759; *Akers v Samba Financial Group* [2017] UKSC 6, [43] (per Lord Mance). See also *Patel v Jones* [2001] PLR 217, [39]: “the statutory objective of the provisions of the 1986 Act [is] that, subject to certain specified exceptions, all a debtor's property capable of realisation should be vested in the trustee for him to realise and distribute the proceeds among the creditors.”

¹⁵⁹It would, of course, be unfortunate if there was a discrepancy between the treatment of bitcoin as “property” forming part of an insolvent's estate, and its treatment as “property” in the general law.

¹⁶⁰See *City of London Corporation v Brown* (1989) 22 HLR 32, 39; *Gwinnutt v George* [2018] EWHC 2169 (Ch), [81]–[84], holding that merely because a claim could be realized for value did not make it “property” if it were not legally enforceable. This was overturned on appeal at [2019] EWCA Civ 656 on the basis that the unique nature of the claim (barrister's fees) mean that “payment of such a fee was not to be regarded as voluntary” [29].

*every description of estate, interest and profit, present or future, vested or contingent, in, arising out of or incident to property.*¹⁶¹

This definition has been given a very purposive interpretation by the courts. Thus, bitcoin is likely to be treated as property for the purposes of insolvency law. To date, there are no insolvency decisions that consider this issue.

There have been relevant court decisions on the nature of bitcoin in relation to insolvency in various countries. For example, in Japan, the Tokyo District Court held that bitcoin units could not be an object of ownership, on the basis that ownership in Japan, the concept of “shoyûken,” is statutorily limited in its application to tangible objects; the operation of bitcoin was examined (including the fact that all that is recorded on the blockchain are records of transactions rather than bitcoin itself), and the court decided that bitcoin was not sufficiently corporeal to be the object of ownership nor could it be the subject of exclusive control because of the way in which it was transferred and “mined.”¹⁶² The bitcoin in question were held for the claimant by the insolvent exchange, and the result of the case was that the court refused to order segregation of the relevant bitcoin from the commingled bitcoin held by the exchange for its clients.

The Russian courts have also considered the issue in an insolvency context.¹⁶³ A debtor, Mr Tsarkov, went into bankruptcy proceedings and admitted that he owned a small quantity of bitcoin. However, he argued that bitcoin were not a form of property known to Russian law, and therefore, the insolvency officer could not realize the value of the bitcoin for the benefit of his creditors. The first instance court decided that, indeed, bitcoin could not be the subject of property rights under Russian law and therefore was not an asset for the purposes of insolvency law.¹⁶⁴ This decision was overturned on appeal,¹⁶⁵ on the grounds that, first, the provision in the Russian Civil Code listing the “objects of civil rights,”¹⁶⁶ included the term “other assets” in addition to the listed types of assets and that this phrase was wide enough to include cryptocurrencies and, second, that creditors should not be deprived of value that is the property of the debtor unless expressly excluded by law.¹⁶⁷ The appellate court also took into account the fact that the Russian Parliament was reviewing amendments

¹⁶¹Section 2, BIA.

¹⁶²Reference number 25541521 Case claiming the bitcoin transfer, etc., Tokyo District Court, Heisei 26 (Year of 2014), (Wa)33320, Judgement of Civil Division 28 of 5 August 2015 (Year of Heisei 27) (unofficial translation on file with authors, also available at: <https://www.law.ox.ac.uk/sites/files/oxlaw/mtgox_judgment_final.pdf>). See also introductory blog at: <<https://www.law.ox.ac.uk/research-subject-groups/commercial-law-centre/blog/2019/02/english-translation-mt-gox-judgment-legal>>.

¹⁶³Decision of the Moscow Arbitrazh Court (Case No. A40-124668/17-71-160F, 5 March 2018).

¹⁶⁴See Ilya Kokorin, “Where Bitcoin meets Insolvency” (Leiden Law Blog, 22 March 2018), available at: <<https://leidenlawblog.nl/category/private-law>>; Polina Lyadnova, Ekaterina Dorokhova and Hannah Whitney, “Cryptocurrencies in Insolvency: Evasive Reality” (2018) *Cleary Gottlieb Emerging Markets Restructuring Journal* 22.

¹⁶⁵Decision of the Ninth Arbitrazh Court of Appeals (No. 9AP-16416/18 in Case No. A40-124668/17, 15 May 2018).

¹⁶⁶Article 128, Civil Code of the Russian Federation, states: “Article 128. *The Kinds of the Objects of Civil Rights* To the objects of civil rights shall be referred the things, among them money and securities, and also the other kinds of the property, such as the rights of property; the works and services; information; the results of intellectual activities, including the exclusive right to these (the intellectual property); the non-material values.” See: <https://www.wto.org/english/thewto_e/acc_e/rus_e/WTACCRUS48A5_LEG_119.pdf>.

¹⁶⁷Ilya Kokorin and Anna Jeffrey, “When Bitcoin meets Insolvency: Is Bitcoin property? Dutch and Russian Responses” (LexisNexis Blog, 8 June 2018), available at: <<https://blogs.lexisnexis.co.uk/randi/when-bitcoin-meets-insolvency-is-bitcoin-property-dutch-and-russian-responses/>>; Lyadnova *et al.* (above note 164).

to the Civil Code that would provide expressly for cryptocurrencies to be recognized as “other assets.”¹⁶⁸

If the insolvent debtor is holding bitcoin directly,¹⁶⁹ he, she, or it¹⁷⁰ should disclose the existence of the bitcoin as an asset to the IP. This requirement to disclose, we argue, is irrespective of the precise legal classification of bitcoin as a type of property, because the bitcoin are valuable, and their value can be realized for the benefit of the creditors. The realization of the value will itself be in the form of property (e.g., fiat money such as cash in a bank account), so if the realization can take place, there will be property available for distribution to creditors.¹⁷¹ Insolvency law in most jurisdictions includes the obligation to cooperate with the IP and creditors,¹⁷² and thus, the trustee or other IP should be able to use the rights and remedies available to realize the value for the benefit of creditors. There may be initial challenges for the IP in accessing the private key, but any duty to cooperate should encompass the duty to disclose the private key. In theory, at least, if the debtor fails to cooperate, the IP can get a court order and, ultimately, a contempt order if there is a failure to cooperate by refusing to disclose the private key.¹⁷³ Once the IP has control of the private key, it can sell the bitcoin on an exchange for fiat currency, which can then be distributed to creditors.

In July 2018, a Canadian Court used a novel approach to allow a receiver to realize on bitcoin, without issuing reasoning on the nature of the bitcoin. Dominic Lacroix had previously been sentenced by the Québec Court to 2 months in jail and a CAD 10,000 fine in December 2017 for raising CAD 15 million in an ICO scam to fund a digital token startup called PlexCoin.¹⁷⁴ At the request of the *Autorité des marchés financiers* (AMF), on July 5, 2018, Justice Raymond Pronovost of the

¹⁶⁸Other states are also passing legislation providing for the proprietary status of digital assets; for example, the U.S. state of Wyoming has recently passed a Digital Assets Act (SEA No. 0039), which will be effective on 1 July 2019 and which provides that digital assets are intangible personal property for the purposes of UCC Article 9, as well as providing a legal structure for custodial holding of such assets. Discussion of these developments are beyond the scope of this article.

¹⁶⁹“Direct holding” means where the debtor had downloaded a node, either a full node or a lightweight node, and holds in a wallet connected to that node (and/or is itself a miner). See Section 2.3 above.

¹⁷⁰The debtor could be an individual or a company, partnership, etc.

¹⁷¹An analogous example might be *Gwinnutt v George* [2018] EWHC 2169 (Ch), where an insolvent barrister was owed fees by a solicitor but could not sue for them as the services had been provided on a “honorarium” basis. It was held that the claim to the fees did not fall within the definition of “property” in the Insolvency Act 1986 and therefore did not vest in the trustee in bankruptcy. However, it seems to have been envisaged that, if the trustee had been able to realize the fees, but putting moral pressure on the solicitor to pay them, he could have distributed the money received (although this point is not overtly discussed). Overturned on appeal, see footnote 160.

¹⁷²Under English law, see section 235, Insolvency Act 1986 (companies in liquidation or administration). A bankrupt individual must produce an inventory of assets for the official receiver and assist him as required (section 291, Insolvency Act 1986), and this duty is amplified by more detailed rules requiring co-operation with the official receiver and the trustee in bankruptcy who takes over the official receiver's role (see Rule 10.55 *et seq.*, Insolvency Rules 2016). In this discussion, the term “IP” includes any official receiver who is appointed.

¹⁷³Under English law, a bankrupt individual is in contempt of court for failing to give information to the official receiver (section 291(6), Insolvency Act 1986), whereas failure of a company's management to cooperate with the IP is punishable by an ongoing fine (section 235(5), Insolvency Act 1986).

¹⁷⁴Mark Cardwell, “Judge orders Cyber-scam Artist to pay Fine in Crypto-currency” (*Canadian Lawyer*, 31 July 2018), available at: <<https://www.canadianlawyer.com/author/mark-cardwell/judge-orders-cyber-scam-artist-to-pay-fine-in-crypto-currency-16043/>>. The AMF ordered Lacroix to stop the ICO before the launch, whereas the U.S. Securities and Exchange Commission filed claims against PlexCoin, Lacroix, and his partner for the “full-fledged cyber scam.” See *Autorité des marchés financiers*, “Virtual Currency - Orders issued against PlexCorps, PlexCoin, DL Innov inc, Gestio inc and Dominic Lacroix” (21 July 2017), available at: <<https://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-lacroix>>; *Autorité des marchés financiers c Lacroix*, 2017 QCCS 603 (C s Q), available at: <<http://citoyens.souqij.qc.ca/php/decision.php?ID=9E1FDFFF3CDC838C8A53B47E4FDD0045&page=1>>.

Superior Court of Québec appointed a receiver over certain property belonging to Lacroix and granted the receiver the powers necessary to take possession of the bitcoin held directly by Lacroix.¹⁷⁵

The court ordered Lacroix, upon service of the order, to transfer the bitcoin in his possession and to appear before the court the following day to confirm the transfer. The following day, Lacroix appeared and declared that he had not transferred the bitcoin, in part because his computer with his encrypted password into his bitcoin account had been seized by the administrator. The judge ordered the computer brought to the courtroom and ordered Lacroix to turn over the bitcoin to the receiver or face contempt and jail. Lacroix agreed and the transfer of 420.6 bitcoins, valued at CAD 3,700,000, took place in the courtroom.¹⁷⁶ Essentially, the court took a very functional approach to protecting any value associated with the bitcoin where there was concern that it would be placed out of reach of the receiver.

4.1.1 | Transparency risk

However, if a debtor directly holding bitcoin does not disclose the holdings, how would creditors or the IP ever know that the debtor holds bitcoin? Here, there is room for debtor misconduct in failing to disclose its existence. The debtor holds the private key, which may not be recorded on paper or in accessible computer files. Without an intermediary, it may be difficult to discern the existence of the bitcoin, let alone realize the value, because the blockchain will not contain any record of the name of a debtor controlling a public key.¹⁷⁷ The only way to discover that name is to link that public key with a transaction with the “real economy,” for example, where bitcoin are exchanged for fiat currency, which is then paid into a named bank account. If the debtor has used bitcoin in such a transaction, the IP is likely to come across its existence in its due diligence, even if the debtor has failed to disclose that he holds any bitcoin.

One of the main characteristics of bitcoin is confidentiality, and many methods of transfer currently include features to obscure the identity of the transacting parties, such as creating new public keys for each transaction¹⁷⁸ and “mixing” devices, which transfer clients' bitcoin to a common pool and then transfer them out again to break any connection between the transaction by which the client received them originally and the transaction by which the client receives it from the pool.¹⁷⁹ This mixing will increase the difficulty for an IP in discovering whether the debtor holds any bitcoin and in finding what bitcoin are held, even if there is no specific intent to conceal the assets in the event of insolvency.

Of course, deliberately concealing the existence of valuable assets from an IP is a serious matter that could lead to criminal charges, or in Canada, to sanctions for an offence under the BIA. Moreover, if a bankrupt individual or company intended to hide its bitcoin, it would do more than just hide the private key: it would be likely to have transferred the bitcoin to related parties, possibly in less creditor-friendly jurisdictions. In that case, tracking down the bitcoin will be a similar exercise for the IP as tracking down any other assets that have been disposed of at an undervalue, but with the added difficulty of the transfers being to pseudonymous public keys.

¹⁷⁵*Autorité des marchés financiers*, “Bitcoins transferred at request of AMF” (19 July 2018), available at: <<https://lautorite.qc.ca/en/general-public/media-centre/news/fiche-dactualites/transfert-de-bitcoins-obtenu-a-la-demande-de-lautorite-des-marches-financiers>>.

¹⁷⁶*Idem*.

¹⁷⁷See above Section 2.3.

¹⁷⁸*Idem*.

¹⁷⁹See: <<https://bestmixer.io/en>>.

In terms of whether a trustee or other IP can access the private key, if the private key is recorded on paper, in a hard-drive wallet, on a bracelet, or other physical representation of the private key or accessible computer or other files, the trustee should be able to access it under its broad investigatory authority in most jurisdictions.

A reality of bankruptcy in many countries is that the estate of the bankrupt may be viewed as too small to pursue actions to realize on assets. In such instances, where the trustee is not aware of the existence of the bitcoin, it may not expend the resources to ascertain what is held and its potential realization for creditors. Even where the trustee is aware, there may not be sufficient assets in the bankruptcy estate or a willingness by creditors to guarantee funding of the IP's fees by creditors to allow the trustee to pursue the value of the bitcoin.

Another issue in relation to realization of value is that different bitcoin exchanges have different timelines and fees for converting the bitcoin to fiat currency or other recognized media of exchange. There may be contractual limits on selling the bitcoin on limited platforms or state limits on transfer. Although timeliness and cost may impact the timing of bankruptcy discharge, it may not be any more disruptive or challenging than the trustee realizing on contingent claims, such as the value in a pending lawsuit.

Even where a court orders a freeze or turning over of bitcoin assets to a receiver, the process may be difficult. As the PlexCoin case discussed above reveals, parties can flagrantly ignore orders and transfer bitcoin assets.¹⁸⁰ The freeze orders against Lacroix and associates and companies did not stop the transfer of bitcoin or the further solicitation of bitcoin through various online offerings, generating numerous legal proceedings,¹⁸¹ nor did subsequent contempt orders.¹⁸² The investigation conducted by the AMF found that the respondents cashed in publicly invested funds in Québec amounting to over USD 3 million, BTC 1,677, LTC 4,042, and ETH 5,780.¹⁸³ The recitation of facts provides insight into the complexities of tracing bitcoin transactions, even where the investigators are aware of the existence of the bitcoin because of the number and ease of transfers, multiple bitcoin addresses, numerous intermediate portfolios, and public key user names.¹⁸⁴ For example, by 2018, the AMF had located 778.97 bitcoins, which were received through 8,397 PlexCoin addresses and 17 intermediate portfolios.¹⁸⁵ There were also orders received but not yet processed, as well as accounts that had received bitcoin and converted them into funds to purchase PlexCoin.¹⁸⁶

As of early 2019, the investigator was still trying to locate PlexCoin's other cryptocurrency.¹⁸⁷ The Québec *Tribunal administratif des marchés financiers* found a breach of freeze orders and diversion of funds from the receiver.¹⁸⁸ The tribunal imposed additional freeze orders as a conservatory measure.¹⁸⁹ The tribunal noted that cryptocurrency has changed the tribunal's approach to protecting

¹⁸⁰*Autorité des marchés financiers c Lacroix* 2018 QCTMF 53 (24 May 2018).

¹⁸¹*Ibid.*, paragraphs 3, 16, 19 and 29, including Lacroix pleading guilty before the Court of Quebec, Criminal and Penal Division, to six charges for unlawful investment, unlawful practice and transmission of false or misleading information concerning securities. *Autorité des marchés financiers v PlexCorps*, 2017 QCTMF 88.

¹⁸²Decision in file 200-05-020363-177, Exhibit D-4, *Autorité des marchés financiers v. Lacroix*, 2017 QCCS 6033 (leave to appeal); 2018 QCTMF 53 (CanLII).

¹⁸³*Autorité des marchés financiers c Lacroix*, above note 180, paragraph 76 (plus additional bitcoin and other assets later discovered).

¹⁸⁴*Idem.*

¹⁸⁵*Idem.*

¹⁸⁶*Ibid.*, paragraph 86.

¹⁸⁷*Ibid.*, paragraph 88.

¹⁸⁸*Ibid.*, paragraphs 103, 104 and 110.

¹⁸⁹*Ibid.*, paragraph 157.

monies in this form because there are no third parties, such as a financial institution, to ensure compliance with legal orders, and this ease of transfer without third-party intervention is one reason for the urgency of securing the bitcoins traced by the AMF.¹⁹⁰ The tribunal stated that

*accordingly, the tribunal considers that it has no alternative but to steer an uncharted course in applying s 249 of the Securities Act to ensure compliance with the orders it is compelled to issue to protect the investing public.*¹⁹¹

It concluded that it had no alternative but to order transfer of the coin to the AMF, given the repetitive offending attitude of the respondent.¹⁹² The tribunal held that section 94 of the AMF Act provides it with an opportunity to adapt an order to the virtual reality of bitcoins and to ensure the outcome of conservatory measures.¹⁹³ The tribunal held that new technologies and methods of holding assets today pose significant challenges for those who administer the Securities Act, and given that it is a statute in the public interest, it must be interpreted broadly in order to fulfil its role of protecting the investing public.¹⁹⁴ Interestingly, the tribunal held that it was premature to grant AMF's request to sell the bitcoin for fiat currency, worth CAD 4 million in May 2018, pending the outcome of the case, its concern being the huge volatility in the value of the bitcoin.¹⁹⁵

4.1.2 | Realization by secured creditors on insolvency

Provided that an effective security interest can be given over bitcoin,¹⁹⁶ many of the difficulties mentioned above will not arise, because the secured creditor knows of the existence of the bitcoin and, at least, knows the public key with which they are associated. If the security interest is a title transfer arrangement or mortgage,¹⁹⁷ the bitcoin will have been transferred to a public key controlled by the secured creditor, who will control the private key. In a title transfer arrangement, on default, the secured creditor will have the right to retain the bitcoin, with a personal obligation to account for any surplus value to the debtor or to the relevant IP.

In practice, this result is likely to be effected by a close out netting arrangement, whereby the creditor's obligation to return equivalent bitcoin will be converted, on default, into an obligation to pay fiat currency. Depending on how the close-out arrangement is drafted, the converted obligation will either be set off against the secured obligation in the debtor's insolvency or the two obligations will be netted off to create one net obligation.¹⁹⁸ Without an agreement for close-out netting, it is very unlikely that insolvency set-off under English law would apply to an obligation to return equivalent bitcoin, because it only applies to "money claims."¹⁹⁹ Claims denominated in foreign currency

¹⁹⁰Ibid., paragraph 165, citing also *SEC v Shavers et al.* (2014), U.S. District Court, Eastern District of Texas, No 13-00416, available at: <<https://www.law.du.edu/documents/corporate-governance/securities-matters/shavers/SEC-v-Shavers-No-4-13-CV-416-E-D-Tex-Sept-18-2014.pdf>>.

¹⁹¹Ibid., paragraph 174.

¹⁹²Ibid., paragraphs 175–176.

¹⁹³Ibid., paragraphs 179–180.

¹⁹⁴Ibid., paragraph 182.

¹⁹⁵Ibid., paragraphs 90–91.

¹⁹⁶This issue is discussed above at Section 3.2.

¹⁹⁷Idem.

¹⁹⁸The latter is the technique used under the ISDA Master agreement.

¹⁹⁹Rules 14.24 and 14.25, Insolvency Rules 2016.

are included,²⁰⁰ but for the reasons outlined above,²⁰¹ it is unlikely that bitcoin would count either as money or as a foreign currency.

If an English law mortgage is created by transfer to a public key controlled by the secured creditor, enforcement is less easy, because mere retention of the bitcoin is not an option in the absence of agreement of the debtor. In theory, the mortgagee would have the right to foreclose, that is, to retain the bitcoin, but because this foreclosure results in the mortgagor losing the surplus value, foreclosure requires an application to court, and in many cases, a 6-month waiting period before the absolute order is made.²⁰² Appropriation, which is similar to foreclosure, but with a duty to account for surplus value, is a remedy available under the FCAR, but as discussed above, bitcoin does not fall within the definition of “cash” within those regulations, and therefore, the remedy is not available here.²⁰³ Thus, the only method available to a mortgagee who already has control of the private key is to sell the bitcoin on an exchange, to pay itself out of the proceeds, and to account for any surplus to the IP. If the secured creditor does not control the private key (e.g., if it is an equitable mortgagee or charge), it will have to obtain control before selling the bitcoin. Therefore, any security agreement should include the right to obtain that control on default.

4.2 | The insolvency of debtors holding bitcoin through intermediaries

Ironically, though not surprisingly, there has been a large growth in the use of intermediaries in relation to the holding and trading of bitcoin. Ironical because the whole point of bitcoin and blockchain is supposed to be direct holding, that is, that there is nothing between the “owner” (the holder of the private key) and the value. However, it is not surprising, because most people cannot be bothered to work out how to manage the bitcoin themselves, and they may also want someone to sue if it all goes wrong: familiar territory in financial markets.²⁰⁴

Before considering the position of an insolvent debtor using an intermediary, it is necessary to analyse what the legal consequences are of the custodial wallet system described above.²⁰⁵ A custodial intermediary stores and controls the private keys paired with the public keys with which the bitcoin are associated. There are two possible analyses of this situation: both assume that bitcoin is property. One is that the custodian owns the bitcoin outright (the arrangement is based on title transfer) but owes a personal obligation to the client to carry out its instructions in relation to the bitcoin and to transfer bitcoin from the relevant public keys to another wallet, that is, one or more different public keys. The other is that the custodian does not own the bitcoin, which continues to be owned by the client: the custodian merely owes personal duties to the client in relation to safe custody of the private key.

There are various ways of conceptualizing this relationship. One, which would work in common law jurisdictions, is that the custodian holds the bitcoin on trust for the client, who is then the beneficial owner of the bitcoin, as is the case in some jurisdictions, including the United Kingdom, where securities are held through intermediaries.²⁰⁶ Another is that there is some sort of quasi-bailment, as

²⁰⁰Ibid., Rule 14.21.

²⁰¹See Section 3.2.

²⁰²Hugh Beale *et al.*, *The Law of Security and Title-based Financing* (3rd edn) OUP, 2018, 18.24.

²⁰³See Section 3.2.

²⁰⁴In relation to trading, of course, intermediaries are also important in matching sellers and buyers, which is what the exchanges do, for which see Section 2.4.

²⁰⁵Idem.

²⁰⁶See *Re Lehman Brothers International (Europe) (In Administration)* [2010] EWHC 2914 (Ch), [226].

is the case in some jurisdictions in relation to intermediated securities,²⁰⁷ which has the effect that the client is the absolute owner of the bitcoin. The agreements under which custodial wallets operate reviewed for the purposes of this article²⁰⁸ are not explicit as to which of these analyses apply. Many terms are consistent with the first analysis, in that there is no doubt that the custodian controls the private key, and, arguably, control of the private key is what it means to “own” bitcoin. The agreements are typically drafted using possessive pronouns in relation to the bitcoin, for example, “your bitcoin,” but this wording cannot be determinative, because these pronouns are also used in relation to money held in accounts by exchanges, and it is reasonably clear that these accounts are held on a title transfer basis.

In relation to the insolvency of the debtor, which of the two analyses is applied is not critical, as long as the intermediary is not insolvent itself. On the first analysis, the asset of the debtor is the right to instruct the intermediary to transfer the bitcoin to another address.²⁰⁹ On the second analysis, the asset of the debtor is the bitcoin itself, but this asset can only be realized by instructing the intermediary to transfer the bitcoin to another address. The analysis does matter when the intermediary is insolvent, which is discussed in the next section, together with a more normative discussion of the legal position.

4.2.1 | Realizing the value for the benefit of creditors

Thus, where an insolvent debtor holds bitcoin in a custodial wallet operated by an intermediary, in the same jurisdiction as the debtor, there is not likely to be a problem realizing the value of the bitcoin in bankruptcy, assuming that the debtor discloses the existence of the bitcoin or the IP investigates and finds the bitcoin, as discussed immediately above. The IP merely has to instruct the custodian to transfer the bitcoin to an address controlled by the IP or to sell the bitcoin and transmit the proceeds to the IP. If the debtor or the custodian fails to cooperate with the trustee, the trustee would use the same process as when the bankrupt debtor holds the bitcoin directly: It would exercise its authority pursuant to insolvency legislation, would seek a court order, and then, if the debtor or intermediary was still not compliant, would seek an order of the court for a remedy for contempt.

If an insolvent debtor's bitcoin is held by an intermediary in a jurisdiction different than the debtor's jurisdiction, there may be different kinds of challenges for realizing the value on bankruptcy. It may be possible for the IP to seek to be recognized in another jurisdiction, probably through vehicles such as the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Recognition and Enforcement of Insolvency-related Judgments.²¹⁰ Finalized and approved by UNCITRAL in July 2018 and thus not yet adopted by any country, adoption of the Model Law would allow the IP to take a judgment from its home jurisdiction, such as an order to realize the value of the bitcoin, to a foreign court to be enforced in the jurisdiction where the asset is held, that is, the jurisdiction of the intermediary, without there having to be a hearing on the merits in that foreign jurisdiction.

²⁰⁷For example, the German, Austrian, and Japanese systems, although this is on the basis that intermediaries have a type of possession of the global security that is actually possessed by a party further up the chain, see Pierre-Henri Conac, Ulrich Segna and Luc Thévenoz (eds), *Intermediated Securities: The impact of the Geneva Securities Convention and the Future European Legislation* (Cambridge University Press, 2013), 33 and 252–253.

²⁰⁸Contracts available on the websites of the following: Binance, Bitfinex, Bitstamp, Bittrex, BTC, Coinbase, Coinsquare, Exmo, Freewallet, Gemini, Kraken, Kucoin, Poloinex, and QuadrigaCX.

²⁰⁹This right is analogous to the asset that is bank money.

²¹⁰UNCITRAL Working Group V, A/CN.9/WG.V/WP.156, endorsed by UNCITRAL in July 2018, available at: <<https://documents-dds-ny.un.org/doc/UNDOC/LTD/V18/009/50/PDF/V1800950.pdf?OpenElement>>.

5 | WHEN THE BITCOIN INTERMEDIARY BECOMES INSOLVENT

5.1 | Bankruptcy of an intermediary

Different issues arise if the insolvent debtor company is a bitcoin intermediary. The insolvency of bitcoin exchanges (or custodians) is the next inevitable development in the cryptocurrency market. Although the focus of this article is on insolvent debtors holding bitcoin directly or indirectly, the first bitcoin exchanges have now commenced insolvency proceedings, and this part flags some early questions in respect of how exchanges and other custodians will be treated on insolvency.²¹¹ How can the insolvency regime respond to these insolvencies in terms of protection of creditors, efficient restructuring or liquidation of the exchange, and the integrity of the system?

In terms of legal analysis, what we are considering is the custodian function of the intermediary. As mentioned above,²¹² an exchange will have a trading function and a custody function. The claims of the customers considered here relate solely to the custody function, that is, the provision and operation of custodial wallets in which the private keys (and therefore, the bitcoin²¹³) are held. In relation to the trading function, there still may be a claim against the exchange for failing to execute a transaction instruction because of the intervening insolvency. Here, the claim is likely to be just for the value that is being eroded by the inability to transact with the bitcoin held in the custodial wallet during the bankruptcy, until it is transferred to another platform or the value returned. In such instances, any claim is likely to be excluded contractually, because the exchange contracts have broad waivers from liability.

The following sections consider the custody function of an exchange in the context of its insolvency, and also the custody function performed by entities that do not act as an exchange but that do provide custodian services.²¹⁴ Therefore, the insolvent intermediary will be called “custodian.”²¹⁵ The discussion focuses on whether the customers whose bitcoin are “held” in the custodial wallet have a proprietary claim against the insolvent intermediary, in which case, they will, in relation to their bitcoin, have a claim that ranks in priority to all the other creditors of the insolvency intermediary or whether they have a personal claim, in which case, they will share in any liquidation distribution on a *pro rata* basis, which is likely to be at a substantial loss.

5.2 | What is the nature of a claim against an insolvent bitcoin intermediary?

Given that bitcoin intermediaries are not financial institutions within the meaning of banks excluded under most domestic insolvency law, the insolvency of an intermediary, whether an exchange or a “pure” custodian, is likely to fall under the insolvency or bankruptcy legislation of the jurisdiction in

²¹¹For example, South Korean bitcoin exchange Youbit declared bankruptcy in December 2017, following disclosure of a debilitating hack and theft that resulted in the loss of 17% of its total assets: Stan Higgins, “Bitcoin Exchange Youbit to Declare Bankruptcy After Hack” (CoinDesk, 19 December 2017), available at: <<https://www.coindesk.com/south-korean-bitcoin-exchange-declare-bankruptcy-hack/>>. The cyber-attack is the second for Youbit, previously known as Yapizon.

²¹²See Section 2.4.

²¹³Here, the term “bitcoin” is being used for the thing which is transferred. See Section 3.1.

²¹⁴See Section 2.4.

²¹⁵The normative analysis in Section 5.2 below will consider the argument that there should be different treatment for exchanges and for pure custodians.

which the intermediary company is registered. This jurisdiction may not be known at the time that the users commence using the intermediary.²¹⁶

As discussed above, the nature of the claim of a bitcoin investor against a bankrupt custodian will depend on the legal analysis of the services offered, namely, whether the claim of the investors in respect of their bitcoin are personal or proprietary.²¹⁷ If the claims are personal, the investors will have to share in the assets *pari passu* with all the other creditors of the company. If they are proprietary, the client will be able to claim those assets *in specie* and therefore should seek a transfer of the bitcoin from the account in which it was held by the intermediary to another, separate, public key controlled by the client.

As mentioned above,²¹⁸ a proprietary claim could either come from the intermediary holding the bitcoin on trust for the customer or from an analysis whereby the intermediary was acting like a bailee. In a trust analysis, the legal owner of the bitcoin would be the intermediary. The intermediary would owe the customer the duties of a trustee,²¹⁹ qualified by the terms of the agreement between them,²²⁰ and the customer would be the beneficial owner of the bitcoin. This analysis is perfectly possible, in a common law jurisdiction, once it was determined that bitcoin were property.

A bailment analysis, however, would have to apply by analogy to that which applies to tangible property. The owner of tangible property, for example, gold, can deliver it to a custodian under a bailment agreement. The custodian, the bailee, owes duties to the owner to take care of the gold, not to use it itself and so on. The custodian has actual possession of the gold and attorns to the customer, who has constructive possession. The customer remains the legal owner of the gold at all times. Bailment up until now has only applied to tangible assets. However, the building blocks of the concept can also apply to bitcoin. The intermediary providing the custodial account owes duties to the customer to take care of the bitcoin (and the private key) and other bailee-like duties. The intermediary has control of the private key, which, although not possession, has many similarities to it.²²¹ The advantage of the quasi-bailment analysis is that, first, it fits better with the duties of the intermediary in the actual custody agreements and, second, would be easier to apply in civil law jurisdictions.

The legal analysis may vary according to the applicable law, which is unfortunate because bitcoin is an international asset, and many transactions are cross-border. Ideally, the same substantive analysis would apply in all jurisdictions, but in the absence of an effective harmonization initiative, it is unlikely to be the case.²²² The first part of the following analysis will identify the relevant factors that will determine the substantive law analysis of any one jurisdiction and the second part will consider factors that normatively should be taken into account in crafting the most appropriate legal response.

²¹⁶The details of the company should be available on the website, but it is not always obvious which company is actually carrying out the custodian services.

²¹⁷See Nick Lister and Matthew Kimber, "Bitcoin: Exposure or Exposed? Risks relating to Cryptocurrency Exchange Insolvency" (2018) 9 *Journal of International Banking and Financial Law* 538.

²¹⁸See Section 4.2.

²¹⁹One important duty is to keep trust property separate from that of the trustee's own property, that is, segregation of client assets. If this is not present, a trust, while not impossible, is unlikely to be found in the absence of very explicit intention to create one. See Lister and Kimber (above note 217); *Henry v Hammond* [1913] 2 KB 515, 521.

²²⁰It is possible for there to be a trust even if the agreement between the parties excludes many duties that would otherwise arise. See *Citibank NA v MBIA Assurance SA* [2007] EWCA Civ 11; cf *Armitage v Nurse* [1998] Ch 241, 253.

²²¹See Section 3.1.

²²²The position in relation to the holding of securities with an intermediary is analogous: The one substantive harmonization initiative (the Geneva Securities Convention 2009) has only been ratified by one state and is not yet in force.

5.2.1 | Determining the current law

One possibility is that a jurisdiction might apply a statutory regime by analogy, resulting in a pre-determined outcome in the insolvency of the intermediary. For example, in a jurisdiction with a statutory code governing the holding of securities through an intermediated system,²²³ although it is unlikely that bitcoin would fall within the definition of “securities,” since it is not an exogenous asset,²²⁴ a similar statutory code could apply to endogenous assets by analogy.

Canadian financial services tribunals have now recognized coin offerings as distributions in contravention of both registration and distribution requirements under securities law in at least three cases.²²⁵ Even where the offering sites do not have a juridical personality, the tribunal has found the group of individuals making the offering to be a patrimony.²²⁶ To come within the meaning of investment contract offered as a security, the bitcoin must be a contract whereby a person enters an undertaking, in the expectation of profit, to participate in the risk of a venture through contribution of capital, without obtaining the right to participate directly in carrying on the business; and the tribunal will look to the economic reality behind the offer made to the public.²²⁷

In PlexCorp, for example, the public was offered an opportunity to invest in “cryptocurrency” in exchange for a return on investment amounting to as much as 1,354%.²²⁸ In the PlexCoin series of judgments, the tribunal found a distribution was made in contravention of the Québec Securities Act²²⁹ and that it was in the public interest to maintain a prohibition order.²³⁰ The tribunal has held that the ultimate registration of a token on a cryptocurrency platform would not in itself change the nature of the product that would be exchanged on such a platform, which would remain a security.²³¹

In bankruptcy, Canada's BIA has a clear statutory framework for dealing with securities firm insolvency, “securities firm” being broadly defined under the BIA.²³² Thus, if a bitcoin exchange becomes insolvent (and found to be a securities firm), “customer name securities,” which are securities that on the date of bankruptcy are held by or on behalf of the securities firm for the account of a customer and recorded as such, the trustee must deliver the securities to the customer.²³³ Since bitcoin is usually held in a “segregated identifiable account,” the trustee can distribute the bitcoin if they come within the meaning of customer name securities: a return of the bitcoin *in specie*. Distribution could be relatively straightforward because each wallet can be associated with public keys that have only received transfers to them arising from transactions authorized and generated by that one customer. These transfers, which are outputs from particular transactions, are, in a real sense, separate from any other transfers recorded on the blockchain.

²²³For example, Article 8, UCC.

²²⁴For the distinction between “endogenous” and “exogenous” assets, see Section 2.2.

²²⁵*Autorité des marchés financiers c PlexCorps*, 2018 QCTMF 91 (20 September 2018), paragraph 286. See also *Autorité des marchés financiers c Usi-Tech Limited*, 2018 QCTMF 24; *Autorité des marchés financiers v. CreUnite*, 2018 QCTMF 8 (CanLII), in which CreUnite was allegedly offering the public an opportunity to invest in the purchase of CUT tokens, a cryptocurrency offering a return on investment.

²²⁶*Autorité des marchés financiers c PlexCorps*, above note 225, paragraph 61.

²²⁷*Ibid.*, paragraphs 247 and 263.

²²⁸*Ibid.*, paragraphs 232 and 267.

²²⁹Québec Securities Act, CQLR c V-1.1.

²³⁰*Autorité des marchés financiers c PlexCorps*, above note 225, paragraph 309.

²³¹*Autorité des marchés financiers v. CreUnite*, above note 225, paragraph 138.

²³²Part VII, BIA. Section 253 provides a definition: “‘Securities firm’ means a person who carries on the business of buying and selling securities from, to or for a customer, whether or not as a member of an exchange, as principal, or agent or mandatary, and includes any person required to be registered to enter into securities transactions with the public.”

²³³*Ibid.*, section 253. Unless a customer is indebted to the intermediary, in which case there are measures for netting out the claims.

However, in practice, bitcoin may be transferred from the client's public keys into commingled accounts controlled by the custodian.²³⁴ If the bankrupt intermediary has converted the bitcoin in some way that results in there being no identifiable "customer" (holder), pursuant to Canadian bankruptcy law, the security vests in the trustee, and the trustee is to establish a "customer pool fund."²³⁵ Securities in the customer pool fund must be allocated by the priority specified in the BIA, and to the extent that securities of a particular type are available in the customer pool fund, the trustee is to distribute them to customers with claims to the securities, in proportion to their claims.²³⁶ The trustee can determine, however, that, in the circumstances, it would be more appropriate to sell the securities and distribute the proceeds to the customers with claims to the securities.²³⁷ Thus, if bitcoin is held by an insolvency intermediary in a commingled account, Canadian bankruptcy law directs how it is to be realized and distributed.

Another possibility is that there is no applicable statute, and the general law has to determine the relationship between the custodian and the client. Under the common law, the lack of legislation is no problem: The courts will, and have to, determine the legal position by applying the general law. The starting point is the terms of the contract between the parties, and the question will be asked: What kind of interest is created by this contract? The terms, however, are unlikely to be completely determinative, first, because typical terms and conditions of custodian wallets do not contain a legal analysis of the proprietary rights in the bitcoin and, second, because even were the terms to include a particular analysis, a court would consider whether this analysis was appropriate in the light of what the parties actually did and any relevant applicable property law.

In fact, most agreements for custodial wallet services (whether or not as part of a wider exchange agreement) only contain broad statements regarding the nature of the relationship between the customer and the exchange.²³⁸ Moreover, they are standard form contracts in which the terms are imposed on the client with no negotiation, even though they are bilateral in form and require acceptance from the client. The following section considers a number of contracts for custodial wallets governed by a variety of legal regimes.

One example of an exchange that also provides custodial wallet services is Coinbase, which is based in San Francisco, but whose contracts are made with a U.K. company (Coinbase UK Ltd) and whose terms and conditions are governed by UK law.²³⁹ Another example is Bitfinex,²⁴⁰ where the contract is made with one of two U.S. companies, depending on whether the client is a U.S. person or not,²⁴¹ whereas the governing law is the law of the British Virgin Islands. An example of a provider of custodial wallets that is not an exchange is Freewallet: The contract appears to be made with Wallet Services Ltd (the wording is not clear) and is it governed by Hong Kong law.²⁴² None of these contracts contain express characterization of the relationship between the intermediary and the customer in relation to the bitcoin held in the custodial wallets.

The Bitfinex contract gives the least information about the legal analysis of bitcoin held in a custodial wallet, because the entire purpose of the company is trading bitcoin and other

²³⁴For example, the bitcoin held by MtGox for clients were held in "commingled accounts." See Tokyo District Court judgment in MtGox (translation) (above note 162).

²³⁵Section 263, BIA, stipulates that the rest of the estate goes into a general fund.

²³⁶*Ibid.*, section 262(2).

²³⁷*Idem.*

²³⁸This analysis comes from examination of a number of contracts. See above note 208.

²³⁹See: <<https://www.coinbase.com/>>; <https://www.coinbase.com/legal/user_agreement> (for the terms and conditions).

²⁴⁰See: <<https://www.bitfinex.com/about>>.

²⁴¹BFXNA Inc for a U.S. person and BFXWW Inc for a non-U.S. person.

²⁴²See: <<https://freewallet.org/>>.

cryptocurrencies. Moreover, its main speciality is margin trading,²⁴³ and most of the contract relates to the financing aspects. The only custodial services provided by Bitfinex are in order to facilitate trading: Fiat money or cryptocurrency must be deposited in an “exchange wallet.”²⁴⁴ Transfers to and from the wallet are made using the website and appear to be mere instructions to Bitfinex to make the transfer, thus indicating that Bitfinex controls the private keys associated with the public keys of which the wallet consists.

The terms of the contract (such as they are) and the information on the website do not distinguish between deposits into and withdrawals from the wallet in fiat currency and in cryptocurrency.²⁴⁵ Because the former deposits are very likely to be on a title transfer basis, one conclusion is that this analysis also applies to the cryptocurrencies deposited into the wallet. On the other hand, the contract (and the website) refer to “your funds”²⁴⁶ and “your balance.”²⁴⁷ Moreover, where the purchase of bitcoin is financed, the agreement states that a financier will have a “lien” over the bitcoin for the outstanding finance, which, like any security interest, can be redeemed by payment of the outstanding obligation.²⁴⁸ This provision also appears to be consistent with the customer having a proprietary right in the bitcoin. There are very extensive limitations of Bitfinex's liability in the agreement,²⁴⁹ which could be seen as inconsistent with the existence of duties of a trustee or a (quasi)bailee. However, the basic duty to safeguard the bitcoin seems to remain intact.

The Coinbase contract is rather more informative but still does not expressly address the question discussed here. Again, it is clear that the “Digital Currency Wallet” is provided largely for the purposes of trading on the site.²⁵⁰ Transfers to and from the wallet, usually in the course of trading, are made by Coinbase on the instructions of the client,²⁵¹ and Coinbase stores (and therefore controls) the private keys, which enable these transactions to take place.²⁵² In this contract, there are separate terms dealing with fiat currency deposits. These terms seem to be on a title transfer basis.²⁵³ Deposits of fiat currency are “converted” into “E-Money,” which is credited to the client's E-Money wallet and debited and credited as a result of trading activity.²⁵⁴ The actual funds are held by Coinbase Payments.

*in a designated safekeeping account with a regulated financial institution.*²⁵⁵

²⁴³That is, lending funds which are used to buy investments. The gearing this provides gives investors a higher return on their investment.

²⁴⁴See: <<https://support.bitfinex.com/hc/en-us/articles/115004405873-A-Beginner-s-Guide-to-Bitfinex>>.

²⁴⁵Idem, where the word “funds” is used for USD, EUR and crypto-currencies.

²⁴⁶See, for example, Clause 5, Bitfinex Terms and Conditions.

²⁴⁷Of course, this could be irrelevant: The same terminology tends to be used for funds in a bank account, which, of course, is analysed in law as a personal right against the bank (*Foley v Hill* (1848) 2 H L Cas 28).

²⁴⁸Clause 2, Bitfinex Terms and Conditions.

²⁴⁹Ibid., Clause 17.

²⁵⁰Coinbase has recently launched a Digital Asset Custody service for institutions, for which see: <<https://custody.coinbase.com/>>; <<https://www.anythingcrypto.com/guides/coinbase-custody-launch-2018>>. The main feature of this product for the purposes of this paper appears to be that the private keys are held in offline “cold storage” and that there is segregation of accounts.

²⁵¹Coinbase Terms and Conditions, Clause 4.2.

²⁵²Ibid., Clause 4.4.

²⁵³See the analysis in Section 2.2 above.

²⁵⁴Coinbase Terms and Conditions, Clause 3.1.

²⁵⁵Idem.

Although this terminology might be considered to indicate that the bank holds the funds on trust for Coinbase, the legal position is still not clear. First, a trust analysis is unlikely to be the analysis without very special arrangements. Second, for the E-Money to be held on trust for the client would result in a chain of trusts and subtrusts analysis similar to that in relation to intermediated securities. Third, money is virtually never held on this basis: even a custodian of intermediated securities who holds the securities on trust for its client holds any money on a title transfer basis.²⁵⁶ Again, in the Coinbase contract, the E-Money wallets, and the Digital Currency wallets are treated in a similar way, giving rise to the argument made above that the same analysis applies to both. However, the agreement does refer to “your balance”²⁵⁷ and “your digital currency,”²⁵⁸ and the basic safeguarding duty survives intact despite the wide exclusions of liability.²⁵⁹

Freewallet is not an exchange and merely provides custodial services. It largely stores the bitcoin (i.e., the private keys) offline in a process known as cold storage,²⁶⁰ but the Freewallet software enables clients to give transfer instructions at any time, as well as providing information about the balance of bitcoin available to transfer.²⁶¹ The Freewallet agreement permits Wallet Services Ltd to decide whether storage is in a “hot wallet” (i.e., online) or cold storage.²⁶² Again, the agreement is ambiguous as to the relationship between the parties. It refers to the “transfer”²⁶³ and “remittance”²⁶⁴ of the bitcoin to the wallet, and these words are also used in relation to the transfer of bitcoin from the client to a public key controlled by a third party.

This latter transfer would be a transfer of ownership, so arguably, the “transfer” or “remittance” to the Freewallet account has the same effect. Moreover, it is clear that the private key is ultimately controlled by Freewallet, although it is used on the instructions of the client to make transfers. While the exclusion clauses are drafted in the widest possible terms,²⁶⁵ they are qualified by “except as otherwise required by law,” which would enable a trust or quasi-bailment analysis to override the exclusions as far as inconsistent with it.

This analysis of a small number of contracts is inconclusive. It is certainly possible to conclude that a custodial wallet contract creates a title transfer arrangement, so that the client's claim in the insolvency of the custodian is personal rather than proprietary. Apart from the legal difficulties relating to bailment of intangible property, a quasi-bailment analysis is also possible. A trust analysis is more difficult, because there is little evidence of an intention to create a trust, although this analysis could be the only proprietary analysis available under the common law.²⁶⁶

²⁵⁶See *In re LBIE* [2009] EWHC 2545.

²⁵⁷Coinbase Terms and Conditions, Clause 1.3.

²⁵⁸*Ibid.*, Clause 5.7.

²⁵⁹*Ibid.*, Clause 8.3.

²⁶⁰See: <<https://www.investopedia.com/articles/investing/030515/what-cold-storage-bitcoin.asp>>.

²⁶¹See: <<https://support.freewallet.org/support/solutions/articles/9000138889-cold-storage>>.

²⁶²Freewallet Terms and Conditions, Clause 3.1.

²⁶³*Ibid.*, Clause 1.1(d).

²⁶⁴*Ibid.*, Clause 6.1(a)(b).

²⁶⁵*Ibid.*, Clause 8.

²⁶⁶In the very recent case of *B2C2 Ltd v Quoine Pty Ltd* [2019] SGHC(I) 03 (Singapore International Commercial Court), a client of an exchange made a claim, *inter alia*, for breach of trust when the exchange reversed a bitcoin trade (on the grounds that the rate of exchange was the result of a mistake) and debited the client's bitcoin account without authorization. The bitcoin of all clients were held by the exchange in an offline wallet [139]. Both parties conceded that bitcoin were property which could be the subject of a trust, a concession which the judge said they were right to make [142]. There was no express declaration of trust, and the contract contained no express characterization of the relationship between the parties, although the appended “risk disclosure statement” did say, under a heading of “bankruptcy risk,” that “client fund safety measures such as depositing [customer assets] in an account with a trust bank, etc.” were not taken so that, if the exchange became bankrupt, it will not be able to return customer assets and customers may suffer losses. Despite this, the fact that the exchange kept client

5.2.2 | Normative analysis: What should the law be?

From an insolvency perspective, every time a creditor has a proprietary claim, it means that other creditors lose out. Secured creditors lose out to the extent that the proprietary claim has priority over them, and unsecured creditors lose out generally. It is therefore important to think normatively about the most desirable analysis for all parties concerned. This section attempts to set out the relevant considerations for this debate. It does not attempt to reach any conclusions. Here, the phrase “proprietary claim” encompasses both a claim as a beneficiary under a trust and a claim as owner under a quasi-bailment: No attempt is made to distinguish between the two in this discussion.

The arguments in favour of customers having a proprietary claim are as follows. First, they have been led to believe that they have a proprietary interest, that is, that they “own” the bitcoin. A representation giving rise to an estoppel cannot found a proprietary interest as it cannot bind third parties.²⁶⁷ However, thinking normatively, such a representation may be a reason for the customers to have this protection on insolvency.

Second, the customers are investing in the bitcoin as a store of value. There are therefore systemic consequences if they only have a personal claim against custodial intermediaries who are not regulated by capital requirements. Moreover, there should be good reasons why investors who use an intermediary to look after their store of value should lose their proprietary rights to that store of value. Those reasons do not apply here in relation to pure custodians and may well not apply to exchanges.

Third, the bitcoin are capable of segregation and identification, both conceptually and in reality, given the record of transactions on the blockchain. This criterion is necessary for a proprietary claim to exist, and, arguably, where it is present, there need to be good reasons for that claim not to be honoured.

Fourth, a customer with merely a personal claim to fiat currency is protected in the insolvency of the custodian insofar as that customer owes money to the custodian (in any currency) by the operation of insolvency set-off.²⁶⁸ However, it is not at all clear that insolvency set-off does (or should) apply to a claim in fiat currency and a cross-claim in bitcoin. Therefore, if the customer only has a personal claim in relation to the bitcoin held for it, the protection of insolvency set-off is not available.

The arguments in favour of customers having only a personal claim are as follows. First, if there are good reasons for the intermediary to have freedom to use the bitcoin for value-producing purposes. A bank, for example, lends out the money deposited with it, thereby providing finance for businesses and consumers, and earning money, which both enables it to operate and which can be passed on to the depositor. At least at present, such activities are not carried on by bitcoin intermediaries, although a few exchanges now permit lending of bitcoin (in exchange for interest payments) by clients, either to other clients²⁶⁹ or, more recently, to the exchange.²⁷⁰

assets separately from its own was sufficiently clear evidence to show that the exchange intended to hold these assets on trust for clients [145]. The judge did, however, comment that what the effect of this arrangement would be were the exchange to go into insolvency was not a matter for him to decide.

²⁶⁷ *Simm v Anglo-American Telegraph Co* (1879) 5 QBD 188, 206–207.

²⁶⁸ The scope and operation of insolvency set-off varies from jurisdiction to jurisdiction: The scope is very wide in the United Kingdom and permits set-off between claims in different (fiat) currencies.

²⁶⁹ For example, the peer-to-peer financing function on Bitfinex, for which see: <<https://www.bitfinex.com/howitworks>>.

²⁷⁰ This is the case with Japanese exchanges Bitbank and GMO, for which see: <<https://www.ccn.com/this-japanese-exchange-will-burrow-your-bitcoin-for-a-yearly-fee/>>.

Second, because such activities are already developing and are likely to be developed further in the future (in the way that securities financing developed in the intermediated securities markets), it might be best to start with a personal claim analysis (maybe with insolvency law protection, see below) rather than a proprietary claim analysis that becomes increasingly convoluted.²⁷¹

Third, giving customers a proprietary claim in relation to “their” bitcoin would have a detrimental effect on other creditors of the intermediary, such as trade creditors and employees. This argument is weak where those creditors know (as they should) that they are dealing with a company that provides custodial services.

Fourth, if a customer has a proprietary claim in relation to “its” bitcoin, this claim only exists while the bitcoin are “held” in that wallet. If the bitcoin have been transferred out of the wallet in an unauthorized transfer, the client will only have a personal claim against the intermediary in any event: The asset needs to be identifiable and in the “ownership” of the insolvent party for a proprietary claim to succeed.²⁷² If an intermediary is hacked, for example, those clients whose accounts are emptied become unsecured creditors; however, those clients whose accounts are not emptied will recover in full, thus reducing the available assets even further for those in the former class.

This last point leads to another possible analysis. Specifically, on insolvency, the bitcoin held in custodial wallets is “ring fenced” for customers who have custodial contracts. Thus, the bitcoin that remains is not available to satisfy unsecured creditors, but all custodial customers claim *pari passu* in relation to it. They would each have their claims reduced proportionately for any shortfall in bitcoin held in the wallets, but they would not share *pari passu* with other creditors.

5.3 | Intermediary insolvency: Observations from two cases

In most cases, intermediary insolvency is likely to result in bankruptcy liquidation; however, there has been at least one case in which rehabilitation proceedings have been used to try to get around definitional challenges in respect of claims to the value of the intermediary's assets on insolvency. The Tokyo-based bitcoin exchange MtGox Co Ltd (MtGox), then one of the world's largest,²⁷³ filed for commencement of a civil rehabilitation proceedings in 2014.²⁷⁴ Subsequently, bankruptcy proceedings were commenced, and Nobuaki Kobayashi was appointed as bankruptcy trustee.²⁷⁵ Precipitating the filing was the theft or disappearance of almost 750,000 of its customers' bitcoins and around 100,000 of its own bitcoins, totalling around 7% of all bitcoins globally, worth around USD 473 million at the time.²⁷⁶ Also, in 2014, MtGox filed for Chapter 15 U.S. Bankruptcy Code protection in the United States, in order to benefit from a bankruptcy stay that would prevent enforcement by aggrieved customers against assets situated in the United States.²⁷⁷ Litigation continues in four

²⁷¹See the reasoning in *In re LBIE* [2009] EWHC 2545, [63]–[64] required to reach the conclusion that the right of an intermediary to use securities held in a client account did not prevent the securities being held on trust for the client.

²⁷²Of course, the IP could try and trace the asset into the hands of a third party and then return it to the client. This paper will not consider the possibility of tracing bitcoin, for a discussion, see Fox (above note 22).

²⁷³Tokyo District Court (above note 162).

²⁷⁴In the Tokyo District Court on 28 February 2014.

²⁷⁵*Idem*.

²⁷⁶*In re MtGox Co, Ltd*, Emergency Application for an Order Granting Provisional Relief pursuant to sections 105(a) and 1519 of the U.S. Bankruptcy Code (10 March 2014), paragraph 11, available at: <<http://docs.dpaq.de/6692-mtgox1.pdf>>.

²⁷⁷*Ibid.*, paragraphs 11–12; *Gregory Greene and Joseph Black v. MtGox et al.*, First Amended Class Action Complaint (14 March 2014), available at: <<https://cdn.arstechnica.net/wp-content/uploads/2014/03/Greene-MtGox-1st-Amend-Complaint.pdf>>.

bankruptcy proceedings in the United States, Japan, and New Zealand, with competing claims from creditors, legal uncertainty, and costly lawsuits.²⁷⁸

A plaintiff brought an action in the Tokyo District Court seeking return of its bitcoin from MtGox's trustee, seeking to exercise its right of segregation and payment pursuant to Article 62 of Japan's Bankruptcy Act.²⁷⁹ As noted above, the Tokyo District Court in 2015 rejected the petition, finding that the bitcoin lacked the necessary corporeality and exclusivity of control to meet the definition of "thing" owned within the meaning of the Civil Code, and thus failed to meet the criteria for segregation pursuant to the Bankruptcy Act. The court distinguished between right and ownership at law.²⁸⁰ As a result, the bitcoin at issue could not be viewed as property and therefore benefit from the right of segregation from the bankruptcy pursuant to Japan's Bankruptcy Act.²⁸¹

This uncertainty regarding bankruptcy realization led some creditors of MtGox to petition for commencement of civil rehabilitation proceedings in respect of MtGox, and on June 22, 2018, the Tokyo District Court issued an order commencing civil rehabilitation proceedings, staying the ongoing bankruptcy proceedings and appointing the bankruptcy trustee as Civil Rehabilitation Trustee.²⁸² Despite the analysis of the Tokyo District Court mentioned above, the trustee issued a statement about the assessment of the value of the customers' claims.²⁸³ The trustee said that, in Japanese bankruptcy proceedings, nonmonetary claims are converted into monetary claims based on the valuation as at the time of the commencement of the bankruptcy proceedings; however, in civil rehabilitation proceedings, nonmonetary claims are not converted into monetary claims at the time of commencement of the civil rehabilitation proceedings, but the valuation of the bitcoin in customer accounts as at the time of commencement of the civil rehabilitation proceedings determines their voting rights in relation to resolutions on the rehabilitation plan.²⁸⁴

What is clear from the trustee's statement²⁸⁵ is that the method and timing of payment to claimants will be determined in the plan established in the civil rehabilitation proceedings; the implication being that customer creditors could either be reimbursed with bitcoin or in fiat currency based on a valuation at the time of reimbursement. What is less clear is whether the customer claimants are to be treated as unsecured creditors and will have to bear losses *pari passu* or whether their claims are likely to be met in full, which would suggest that they are being treated as proprietary claims.

It may be that civil rehabilitation proceedings are flexible enough to permit this type of payment out by a trustee even if the claimant did not, under property law, have a proprietary right. It appears

²⁷⁸Alexandra Harney and Steve Stecklow, "Twice burned - How Mt. Gox's bitcoin customers could lose again" (Reuters, 16 November 2017), available at: <<https://www.reuters.com/investigates/special-report/bitcoin-gox/>>.

²⁷⁹Article 62, Japan Bankruptcy Act, which states "62 The commencement of bankruptcy proceedings shall not affect a right to segregate, from the bankruptcy estate, property that does not belong to the bankrupt (referred to as a "right of segregation" in Article 64 and Article 78(2)(xiii))." After commencement of the bankruptcy proceedings, the remaining balance in the plaintiff's account included BTC 458.8812618.

²⁸⁰Article 206, Civil Code. See also Article 85, Civil Code, which states: "The term "Things" as used in this Code shall mean tangible thing." See official Government translation at: <<http://www.japaneselawtranslation.go.jp/law/detail/?re=02&ky=ruling&ia=03&page=116&la=01>>. The Court held that the Civil Code basically limits the object of ownership to a tangible thing, with the exception specified by the Code or admitted in relation to special laws such as Copyright Law.

²⁸¹*Idem*. The Court also rejected a related claim in tort that the trustee had failed to segregate the bitcoin.

²⁸²*Re Civil Rehabilitation Debtor: MtGox Co., Ltd. Civil Rehabilitation Trustee: Nobuaki Kobayashi, Attorney-at-law* (22 June 2018) (Petition November 2017), available at: <https://www.mtgox.com/img/pdf/20180622_announcement_en.pdf>.

²⁸³*Idem*.

²⁸⁴*Ibid.*, Question and Answer 1(2).

²⁸⁵*Ibid.*, Question and Answer 17.

that, in such proceedings, the debtor, overseen by the trustee, prepares a rehabilitation plan setting out modifications to the rights of claimants and a payment plan. If the creditors and the court approve the proposed plan, payments will then be made by the debtor (again overseen by the trustee) in accordance with the plan. If the creditors and the court do not approve the plan, the matter reverts to the bankruptcy procedure.²⁸⁶ Even under the bankruptcy procedure, the trustee does appear to have treated the bitcoin remaining in the control of MtGox as, at least, an asset separate from the rest of the exchange's assets. The trustee has realized the value of some of this bitcoin and says he has established a trust with some of this money to "secure" the interests of the creditors who had already submitted monetary claims in the bankruptcy.²⁸⁷ The exact legal status of this trust is unclear.

Effective April 2017, largely in response to the MtGox insolvency, cryptocurrency exchange businesses operating in Japan have been regulated by the Payment Services Act, which provides a definition of virtual currency that recognizes bitcoin as having a recorded property value and requires cryptocurrency exchanges to manage customers' money or cryptocurrency apart from their own.²⁸⁸ It may be that the new statutory provisions, not unlike other "special law," now address the Civil Code restriction of recognizing an intangible such as bitcoin, although, as of the time of writing, that issue is still not clear.

The second case to watch in the coming months is the Canadian insolvency proceedings in Quadriga Fintech, which operated an online cryptocurrency exchange platform (QCX Platform) to facilitate the buying, selling, or exchange of various cryptocurrencies.²⁸⁹ The QCX Platform operated from a series of third-party servers located in various jurisdictions.²⁹⁰ The founder, CEO and sole director of Quadriga Fintech, Gerald Cotten, died suddenly in December 2018.²⁹¹ Employees of Quadriga Fintech were unable to access cryptocurrency held in Cotten's cold wallets, and the missing coins are valued at about CAD 190 million.²⁹²

Experiencing a liquidity crisis and unable to satisfy withdrawal requests from users, in February 2019, Quadriga Fintech and related companies ("the debtors") commenced proceedings pursuant to the Companies' Creditors Arrangement Act (CCAA),²⁹³ and a monitor was appointed.²⁹⁴ At the time of filing, an estimated 115,000 users of the platform were owed approximately CAD 260 million.²⁹⁵ The Supreme Court of Nova Scotia observed that the proceeding was unique in the sense that there was no operating business of any significant size in terms of physical assets, employees, suppliers, or

²⁸⁶Ibid., Question and Answer 1(4).

²⁸⁷Ibid., Question and Answer 14.

²⁸⁸Article 63(11), Payment Services Act (Act No. 59 of 2009, amended by Act No. 62 of 2016, the amendments taking effect on 1 April 2017) (translation available at: <<http://www.japaneselawtranslation.go.jp/law/detail/?id=3078&vm=02&re=02>>). In Japanese, the phrase 想 ("virtual currency") is used.

²⁸⁹Pre-Filing Report of the Proposed Monitor (31 January 2019), paragraph 3 ("Pre-filing Report").

²⁹⁰First Monitor's Report (12 February 2019), paragraph 23.

²⁹¹*Re Quadriga Fintech Solutions Corp*, 2019 NSSC 65 (19 February 2019), paragraph 3.

²⁹²Pre-filing Report, paragraph 32.

²⁹³Quadriga Fintech Solutions Corp, Whiteside Capital Corporation and 0984750 BC Ltd, d/b/a Quadriga CX and Quadriga Coin Exchange (collectively "Quadriga Fintech" or "debtors"). Quadriga Fintech is wholly owned by Whiteside capital Corporation, which is in turn wholly owned by Quadriga Fintech Solutions Corp, which is widely held and is a reporting issuer in British Columbia: Pre-filing Report, paragraph 2. See: <www.ey.com/ca/quadriga>.

²⁹⁴The monitor gave broad notice and in cooperation with the debtors, prepared a list of creditors in accordance with section 23(1)(a), CCAA.

²⁹⁵*Re Quadriga Fintech Solutions Corp*, above note 291, paragraph 2. At the date of commencing proceedings, the current price of bitcoin was approximately CAD 4,552 (Pre-filing Report, paragraph 19).

secured creditors; however, there is a very large group of diverse users who have no access to many millions of dollars' worth of crypto assets and cash that they had given to the debtors.²⁹⁶

The QCX Platform allowed users to deposit cash or cryptocurrency with Quadriga Fintech, and after deposit, the user's QCX Platform account would be credited with the appropriate currency and the user could place buy or sell orders on the QCX Platform. If a counterparty was found via the QCX Platform, a trade would occur, and Quadriga Fintech would owe the seller cash or the appropriate cryptocurrency and owe the buyer cryptocurrency for the amount of coins purchased.²⁹⁷ Quadriga Fintech used a number of third-party payment processors to receive and disburse currency associated with the trades, as opposed to hosting these services itself.²⁹⁸ The debtors did not have bank accounts in their own names for these transactions nor did the debtors keep accounting records.²⁹⁹ Quadriga Fintech had both hot and cold wallets. At the time of filing, the QCX Platform had about 363,000 users.³⁰⁰

In granting the initial order and stay under the CCAA, the court authorized the debtors to continue control of business.³⁰¹ A monitor was appointed to monitor the business and affairs of the debtors, assist in preparation of cash flow statements, assist with development and negotiation of a restructuring plan, and to establish a postfiling cash management account, given the lack of pre-filing accounting records.³⁰² The court also authorized the monitor to transfer the debtors' remaining cryptocurrency into a cold wallet.³⁰³ The court ordered any person in possession of the debtors' property, including third-party payment providers, to grant to the monitor and debtors:

*immediate and continued access to the property and information and documentation related to it.*³⁰⁴

The monitor also identified that certain receiving wallet addresses from transactions in the cold wallets are wallet addresses associated with identifiable cryptocurrency exchanges and are in the process of contacting those exchanges to identify possible accounts controlled by Quadriga or Cotten.³⁰⁵ The debtor also disclosed to the monitor 14 user accounts that may have been created outside the normal process by Quadriga, under various aliases, without a corresponding customer, and then used to trade on the QCX Platform with deposits that may have been artificially created. A chief restructuring officer was appointed in early March 2019, in part to address identified governance issues.³⁰⁶

²⁹⁶Another unusual feature is that the only creditors of any significance are the users; the one secured creditor agreed to advance CAD 300,000 in order to get the CCAA process underway, the plan being to repay the money as soon as assets become available, the Court observing that: "The lack of any secured creditors means that the users' money is effectively funding all of the professional fees being incurred. It is extremely important to manage those, in order to maximize recovery for the users." See *Re Quadriga Fintech Solutions Corp.*, above note 291, paragraphs 43, 44.

²⁹⁷Pre-filing Report, paragraph 21. See description of how bitcoin are held by exchanges in Section 2.4 above.

²⁹⁸*Ibid.*, paragraph 22.

²⁹⁹*Ibid.*, paragraph 38. Cotten's payment instructions were issued via email, and payment inflows and outflows were not systematically tracked.

³⁰⁰*Ibid.*, paragraph 25.

³⁰¹Initial CCAA Order, Nova Scotia Supreme Court (Justice Michael J Wood, 5 February 2019) ("Initial Order"), paragraph 4.

³⁰²*Ibid.*, paragraphs 18, 20, and 22–23. See also Pre-filing Report, paragraph 40.

³⁰³*Ibid.*, paragraph 25. See also Second Monitor's Report (20 February 2019).

³⁰⁴*Ibid.*, paragraph 28.

³⁰⁵*Idem.*

³⁰⁶*Re Quadriga Fintech Solutions Corp.*, 2019 NSSC 65 (5 March 2019).

The creditors primarily affected are users of the QCX Platform, who are owed cash and cryptocurrency of CAD 260 million, the claims ranging from very small to millions of dollars.³⁰⁷ The CCAA supervising judge issued an order appointing representative counsel to represent about 100,000 affected users.³⁰⁸ As this article goes to press in April 2019, no claims process has yet been established and potential claimants have not yet identified whether their claims are personal or proprietary.³⁰⁹ Given the myriad types of transactions, there may in fact be different types of claims. When the issue comes before the CCAA judge, many of the issues discussed above are likely to be part of the court's consideration of the nature of the claims.

6 | CONCLUSION

In order to consider the treatment of bitcoin in insolvency and, in particular, the realization of its value for the benefit of creditors, this article has discussed the factual and legal nature of bitcoin. It is necessary to understand how it works and what it is, in order to make any sort of analysis as to its legal nature. As discussed above, in one sense, bitcoin does not exist at all. What exists is a record of transactions that is held immutably on a distributed ledger (a blockchain). The subject matter of those transactions has no physical existence, not even as a line of code. Instead, it is a construct that, by common consensus, has value in that people will exchange fiat currency, goods, or services (things that are considered to have value in the “real world”) for it. Because of that, *inter alia*, it has to be taken seriously as an asset if a person who has it (to use a neutral term) becomes insolvent.

Although there are doctrinal difficulties in analysing whether bitcoin is property and what sort of property it is, there is both a strong normative argument that it should be property and an analytical argument that fulfils the criteria normally applied to decide if an asset is property. However, because bitcoin has no independent existence from the transaction involving its creation and transfer, all discussion of it as property has to involve a certain amount of analogy. The discussion in the latter part of the article is conducted on the basis that there is something, called bitcoin, which is the subject matter of the transfers. Given that this something has value, this value should be realizable by an IP when a person who has the exclusive power to transfer the thing (i.e., controls the private key) and who can be thought of as the “owner” of the bitcoin becomes insolvent.³¹⁰ Bitcoin should therefore fall within the definition of “property” in insolvency statutes.

That said, the factual nature of bitcoin presents some difficulties for the IP of a debtor holding bitcoin. These differences are identified and discussed in the article, and some of the issues that need to be determined are identified and analysed. Even more difficulties arise when bitcoin are held in custodial wallets provided by a custodian who has become insolvent. The main question here is whether the clients who have deposited their bitcoin in these wallets have a proprietary or personal claim against the custodian, as it will determine the nature of their claim in the insolvency. The possible legal analyses are discussed here, and the normative arguments are set out.

³⁰⁷ Third Monitor's Report (1 March 2019), paragraph 25.

³⁰⁸ *Re Quadriga Fintech Solutions Corp* (above note 291), factors that a Canadian court will consider are the vulnerability and resources of the group seeking representation, facilitation of administration of the proceedings and efficiency, and the avoidance of a multiplicity of legal retainers.

³⁰⁹ An official committee of “affected users” is just being set up by representative counsel, and it may be weeks or months before the nature of claims is disclosed by the claimants or is determined by the court.

³¹⁰ This statement needs to be qualified by the fact that sometimes the person who controls the private key is not entitled to do so (e.g., a thief of a paper wallet). Control of the private key can only give a presumption of ownership, whatever that concept means in relation to bitcoin.

Finally, the example of the insolvency of the custodian MtGox is discussed briefly. Although the Japanese court held that a customer did not have a proprietary claim, the treatment of customers in the civil rehabilitation proceedings appears to be moving in a direction that gives them an analogous claim. Again, the main question here is whether customers should have priority over other creditors, and on what basis. Whatever the answer to this difficult normative question, it is clear that, given the international nature of bitcoin and the transactions involving it, it is desirable for insolvency regimes to reach similar, rather than different, conclusions in this regard.

How to cite this article: Sarra J, Gullifer QC (Hon) L. Crypto-claimants and bitcoin bankruptcy: Challenges for recognition and realization. *Int Insolv Rev.* 2019;28:233–272.

<https://doi.org/10.1002/iir.1346>

TAB 6



**Canadian Securities
Administrators**

**Autorités canadiennes
en valeurs mobilières**

**Joint Canadian Securities Administrators/Investment Industry
Regulatory Organization of Canada**

Consultation Paper 21-402

Proposed Framework for Crypto-Asset Trading Platforms

March 14, 2019

PART 1 – Introduction and purpose

The emergence of “digital assets” or “crypto assets” continues to be a growing area of interest for regulators globally. Innovations like distributed ledger technology (**DLT**) and crypto assets are relatively new and are transforming the landscape of the financial industry. Interest in crypto assets among investors, governments and regulators globally has increased significantly since the creation of bitcoin in 2008 and continues to grow. Early in 2018, at its peak, the total value of crypto assets was estimated, by one source, at more than US\$800 billion.¹ While the value has since fallen, trading volumes remain significant. Today, there are over 2000 crypto assets² that may be traded for government-issued currencies or other types of crypto assets on over 200 platforms³ that facilitate the buying and selling or transferring of crypto assets (**Platforms**). Many of these Platforms operate globally and without any regulatory oversight.

Although DLT may provide benefits, global incidents point to crypto assets having heightened risks related to loss and theft as compared to other assets. Regulators around the world are currently considering important issues surrounding the regulation of crypto assets including the appropriate regulation of Platforms. The Canadian Securities Administrators (the **CSA**) and the Investment Industry Regulatory Organization of Canada (**IIROC**, and together with the CSA, **we**), have been engaged with regulators globally, through IOSCO and other innovation initiatives, to seek input on a variety of regulatory approaches that exist in this area.

Platforms, depending on how they operate and the crypto assets they make available for trading may be subject to securities regulation. The CSA, through its Regulatory Sandbox⁴, is in discussions with several Platforms that are seeking guidance on the requirements that apply to them. We have heard directly from Platform operators and their advisers that a regulatory framework is welcome, as they seek to build consumer confidence and expand their businesses across Canada and globally.

Currently there are no Platforms recognized as an exchange or otherwise authorized to operate as a marketplace or dealer in Canada. As such, the CSA has urged Canadians to be cautious when buying crypto assets.⁵

Platforms facilitate the buying and selling of crypto assets and perform functions similar to one or more of exchanges, alternative trading systems (**ATSs**), clearing agencies, custodians and dealers. Depending on their structure, they may also introduce novel features which create risks to investors and our capital markets that may not be fully addressed by the existing regulatory framework. Where securities legislation applies to Platforms we are considering a set of tailored regulatory requirements for them to address the novel features and risks (the **Proposed Platform Framework**).

¹ <https://coinmarketcap.com/charts/>.

² Coinmarketcap.com listed 2098 different crypto assets as of March 1, 2019. See: <https://coinmarketcap.com/all/views/all/>.

³ Coinmarketcap.com listed 241 Platforms as of March 1, 2019. See: <https://coinmarketcap.com/rankings/exchanges/3>.

⁴ The CSA Regulatory Sandbox is an initiative of the CSA to support businesses seeking to offer innovative products, services and applications in Canada.

⁵ The CSA has previously issued investor alerts reminding investors of the [inherent risks associated with crypto asset futures contracts](#) and [the need for caution when investing with crypto asset trading platforms](#).

We endeavor to facilitate innovation that benefits investors and our capital markets, while ensuring that we have the appropriate tools and understanding to keep pace with evolving markets. The purpose of this joint CSA/IIROC Consultation Paper (the **Consultation Paper**) is to seek feedback from the financial technology (**fintech**) community, market participants, investors and other stakeholders on how requirements may be tailored for Platforms operating in Canada whose operations engage securities law. We intend to use this feedback to establish a framework that provides regulatory clarity to Platforms, addresses risks to investors and creates greater market integrity.

Throughout the Consultation Paper, investors participating on Platforms may be referred to as either **investors** or **participants**.

PART 2 – Nature of crypto assets and application of securities legislation⁶

Crypto assets differ in their functions, structures, governance and rights. Some crypto assets, commonly referred to as “utility tokens”, are created to allow holders to access or purchase goods or services on a DLT network being developed by the creators of the token. As set out in [CSA Staff Notice 46-307 Cryptocurrency Offerings](#) and [CSA Staff Notice 46-308 Securities Law Implications for Offerings of Tokens](#), staff of the CSA have found that most of the offerings of utility tokens have involved a distribution of securities, usually as investment contracts. Other crypto assets are tokenized forms of traditional securities or derivatives and may represent an interest in assets or have their value may be based on an underlying interest. If crypto assets that are securities and/or derivatives are traded on a Platform, the Platform would be subject to securities and/or derivatives regulatory requirements.

We note that it is widely accepted that at least some of the well established crypto assets that function as a form of payment or means of exchange on a decentralized network, such as bitcoin, are not currently in and of themselves, securities or derivatives. Instead, they have certain features that are analogous to existing commodities such as currencies and precious metals.

However, securities legislation may still apply to Platforms that offer trading of crypto assets that are commodities, because the investor’s contractual right to the crypto asset may constitute a security or derivative. We are evaluating the specific facts and circumstances of how trading occurs on Platforms to assess whether or not a security or derivative may be involved. Some of the factors we are currently considering in this evaluation include:

- whether the Platform is structured so that there is intended to be and is delivery of crypto assets to investors,
- if there is delivery, when that occurs, and whether it is to an investor’s wallet over which the Platform does not have control or custody,
- whether investors’ crypto assets are pooled together with those of other investors and with the assets of the Platform,
- whether the Platform or a related party holds or controls the investors’ assets,

⁶ As defined in National Instrument 14-101 *Definitions*.

- if the Platform holds or stores assets for its participants, how the Platform makes use of those assets,
- whether the investor can trade, or rollover positions held by the Platform, and
- having regard to the legal arrangements between the Platform and its participants, the actual functions of the Platform and the manner in which transactions occur on it
 - who has control or custody of crypto assets,
 - who the legal owner of such crypto assets is, and
 - what rights investors will have in the event of the Platform's insolvency.

Consultation question

1. Are there factors in addition to those noted above that we should consider?

The CSA wishes to remind market participants that any person or company advertising, offering, selling or otherwise trading or matching trades in crypto assets that are securities or derivatives, or derivatives that are based on crypto assets to persons or companies in Canada, or conducting such activities from a place of business in Canada is subject to securities legislation in Canada. Further, as noted above, although some crypto assets may be commodities, securities legislation may still apply to Platforms that offer trading of such crypto assets because the investor's contractual right to the crypto asset/commodity may constitute a security or derivative. Further, in most jurisdictions in Canada, the provisions of securities legislation relating to fraud, market manipulation and misleading statements apply not just to the trading of securities and derivatives but also to trading of the underlying interest of a derivative (e.g. the commodity).

The Proposed Platform Framework referred to in this Consultation Paper considers how existing regulatory requirements may be tailored for Platforms and should not be construed as acceptance by the CSA that securities and/or derivatives legislation may not apply to any particular offering involving crypto assets.

PART 3 – Risks related to Platforms

The operational models and the risks related to Platforms may vary from one platform to another; however, the risks are not entirely different than those applicable to other types of regulated entities such as marketplaces and dealers. The introduction of crypto assets and the operational models of Platforms, however, raise different and in some cases heightened, areas of risk. Key areas of risk include:

- **Investors' crypto assets may not be adequately safeguarded** – Many Platforms have control of their participants' crypto assets (e.g. they keep participants' crypto assets in a single account on the distributed ledger under the Platform's private key or the Platform holds its participants' private keys on their behalf). Platforms may not have necessary processes and controls in place to segregate participants' assets from their own and to safeguard those assets, including maintaining and safeguarding any private keys associated with wallets held by the Platform. There are also current challenges associated with auditing the internal controls surrounding custody of participants' assets.

- **Processes, policies and procedures may be inadequate** – Platforms may not have sufficient processes, policies and procedures in place to establish an internal system of controls and supervision sufficient to prudently manage the risks associated with their business, including business continuity risks, key personnel risks and regulatory compliance risks.
- **Investors' assets may be at risk in the event of a Platform's bankruptcy or insolvency** – Platforms may not segregate participants' assets from their own or may use participants' assets to fund operating costs and other expenses. As a result, Platforms may not hold sufficient assets to cover investor claims and return investors' assets in the event of bankruptcy or insolvency. In addition, Platforms may operate in jurisdictions that have limited asset protection and insolvency regimes.
- **Investors may not have important information about the crypto assets that are available for trading on the Platform** – Each crypto asset has its own functions, associated rights and risks. Platforms may not provide sufficient or clear information about the crypto assets for participants to make informed investment decisions. Examples of information may include the standards that the crypto asset had to meet before being admitted for trading on the Platform and any potential difficulties in liquidating the crypto asset.
- **Investors may not have important information about the Platform's operations** – Platforms may not provide sufficient information about the functions they perform and their fees. For example, some Platforms do not deliver crypto assets to a wallet controlled by the participant unless requested, but participants may not be aware of this or the risks associated with the Platform retaining custody of their crypto assets, including that they may not be able to access their crypto assets.
- **Investors may purchase products that are not suitable for them** – Exchanges and other regulated marketplaces do not interact directly with retail investors; instead they interact through regulated intermediaries (i.e. registered dealers). In contrast, Platforms may offer investors (including retail investors) direct access to the Platform without the use of a regulated intermediary that performs know-your-client and suitability assessments. As a result, participants may purchase crypto assets, many of which can be complex, high risk and volatile products, that are not suitable investments for them.
- **Conflicts of interest may not be appropriately managed** – There may be conflicts of interest between the Platform's operator and participants who access the Platform, including the inherent conflicts of interest where Platforms act as market makers and trade as principal.
- **Manipulative and deceptive trading may occur** – Platforms may be susceptible to manipulative and deceptive trading given the market volatility, lack of reliable pricing information for crypto assets, the fact that they trade 24 hours daily and the fact that trading on many Platforms is not currently monitored.
- **There may not be transparency of order and trade information** – Information relating to the price and volume of orders and trades may not be publicly available or sufficient to support efficient price discovery.
- **System resiliency, integrity and security controls may be inadequate** – Platforms have significant cybersecurity risks. DLT is a nascent technology and Platform operators may not have sufficient experience or possess the necessary skills to ensure that systems function properly and there is adequate protection against cyber theft of participants' crypto asset investments.

Consultation question

2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

PART 4 – Regulatory approaches in other jurisdictions

In developing the Proposed Platform Framework, we considered the approaches taken by securities and financial regulators in other jurisdictions. We found that in many jurisdictions the existing regulatory requirements will apply to regulate Platforms within those jurisdictions. Some jurisdictions may tailor requirements or provide exemptions. This means that the regulatory requirements applicable to exchanges, ATSs (in the U.S. or Canada), multilateral trading venues (in Europe) and other regulated markets may apply to a Platform.

In the U.S., the Securities and Exchange Commission (SEC) issued a statement indicating that, if a platform offers trading of digital securities and operates a marketplace, it must be registered with the SEC as a national securities exchange, registered with the Financial Industry Regulatory Authority as a broker-dealer operating an ATS, or be exempt from registration.⁷ The Commodity Futures Trading Commission (CFTC) has indicated that bitcoin and certain other crypto assets are encompassed in the definition of “commodity”. In the context of retail commodity transactions in crypto assets, for example on Platforms, the CFTC has consulted with market participants on its approach to the proposed interpretation of the term “actual delivery”.⁸

In European jurisdictions, the regulatory framework under the Markets in Financial Instruments Directive (MiFID) applies when crypto assets qualify as financial instruments. The European Securities and Markets Authority (ESMA) recently published a report with their advice on initial coin offerings and crypto assets where they identify the risks in the crypto asset sector.⁹ In the report, ESMA indicates that where crypto assets qualify as transferable securities or other types of MiFID financial instruments, the existing regulatory framework will apply. ESMA also noted that the existing requirements may not address all the risks, and in some areas, the requirements may not be relevant in a DLT framework.

In Singapore, Platforms that trade crypto assets that are securities may be approved exchanges or be recognised market operators and, in both cases, are subject to regulation by the Monetary Authority of Singapore.¹⁰

⁷ SEC 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>.

⁸ CFTC, Retail Commodity Transactions Involving Virtual Currency, Proposed Interpretation, 82 Fed. Reg. 60335 (December 20, 2017): <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrfederalregister/documents/file/2017-27421a.pdf>.

⁹ ESMA Advice – Initial Coin Offerings and Crypto-Assets (January 9, 2019):

https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.

¹⁰ Monetary Authority of Singapore, A Guide to Digital Token Offerings (last updated November 30, 2018):

<http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20last%20updated%20on%2030%20Nov%202018.pdf>

In Hong Kong, Platforms that are trading products that are not within the remit of the Hong Kong Securities and Futures Commission (**HKSFC**) can apply to use HKSFC's Regulatory Sandbox, particularly if they will, in the future, seek to offer trading of products that are within the remit of the HKSFC. This will allow the HKSFC to engage in an exploratory stage where it observes the Platform's operations and considers the effectiveness of proposed regulatory requirements for Platforms and whether Platforms are appropriate to be regulated by the HKSFC. If the decision is made to license the Platform, additional restrictions may apply.¹¹

In Malaysia, the *Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019* came into force on January 15, 2019 and specifies that all digital currencies, tokens and crypto assets are classified as securities, placing them under the authority of the Securities Commission Malaysia.¹²

Many financial regulators are proactively conducting inquiries into the activities of Platforms to determine if they are carrying on activities that require them to comply with their requirements.

Consultation question

3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

PART 5 – The Proposed Platform Framework

5.1 Overview of the Proposed Platform Framework

The Proposed Platform Framework will apply to Platforms that are subject to securities legislation and that may not fit within the existing regulatory framework. It will apply both to Platforms that operate in Canada and to those that have Canadian participants.¹³

In developing the Proposed Platform Framework, the CSA considered that some of the Platforms are hybrid in nature and may perform functions typically performed by one or more of the following types of market participants: ATSS¹⁴, exchanges¹⁵ (exchanges and ATSS are both types of marketplaces¹⁶), dealers, custodians and clearing agencies. Specifically:

¹¹ HKSFC Conceptual framework for the potential regulation of virtual asset trading platform operators (November 1, 2018): https://www.sfc.hk/web/EN/files/ER/PDF/App%20-%20Conceptual%20framework%20for%20VA%20trading%20platform_eng.pdf

¹² Securities Commission Malaysia media release (January 14, 2019): <https://www.sc.com.my/news/media-releases-and-announcements/sc-to-regulate-offering-and-trading-of-digital-assets>

¹³ The CSA may consider exemptive relief from the applicable requirements if the Platform is located outside of Canada and is regulated by a foreign regulator in a manner that is similar to domestic oversight.

¹⁴ ATS is defined in every jurisdiction other than Ontario in s. 1.1 of National Instrument 21-101 *Marketplace Operation* (NI 21-101), and in Ontario in ss. 1(1) of the *Securities Act* (Ontario).

¹⁵ An exchange is a marketplace that may, among other things, lists the securities of issuers; provides a guarantee of a two-sided market for a security on a continuous or reasonably continuous basis; sets requirements governing the conduct of marketplace participants; or disciplines marketplace participants. Securities legislation enables securities regulatory authorities to recognize exchanges or exempt an exchange from recognition.

¹⁶ Marketplace is defined in every jurisdiction other than Ontario in s. 1.1 on NI 21-101, and in Ontario in ss. 1(1) of the *Securities Act* (Ontario).

- like an exchange or ATS, they may be a market or facility where orders of multiple buyers and sellers are brought together and matched;
- like an exchange, they may facilitate the creation or “listing” of a crypto asset;
- like an ATS or exchange, they may decide which crypto assets will be eligible for trading;
- like an exchange, they may offer a guarantee of a two-sided market and conduct regulatory activities;
- like a dealer, they may perform know-your-client and suitability reviews to grant access to investors (retail and institutional) and they may trade as principal;
- like a dealer or a custodian, they may self-custody investor’s assets or otherwise have control over investors’ assets; and
- like a clearing agency, they may enable the clearing and settlement of trades.

Application of marketplace requirements

The Proposed Platform Framework is based on the existing regulatory framework applicable to marketplaces and incorporates relevant requirements for dealers facilitating trading or dealing in securities. It is tailored to take into account the functions that may be performed by each Platform. Specifically, a Platform that brings together orders of buyers and sellers of securities and uses non-discretionary methods for these orders to interact is a marketplace.

As a marketplace, a Platform will be subject to requirements that will address many of the risks outlined in Part 3 of the Consultation Paper, such as those set out in NI 21-101, National Instrument 23-101 *Trading Rules* (**NI 23-101** and, together with NI 21-101, the **Marketplace Rules**) and National Instrument 23-103 *Electronic Trading and Direct Access to Marketplaces* (**NI 23-103**).

Application of dealer requirements

In addition to marketplace functions, the Platform may also perform dealer functions, for example, providing custody of crypto assets and permitting direct access to trading by retail investors. As a result, the Proposed Platform Framework will include requirements that address the risks relating to these additional functions. Many of these requirements already exist in regulatory frameworks applicable to dealers.

Some entities will not fall within the definition of a marketplace. For example, an entity that is trading crypto assets that are securities but always trades against its participants and does not facilitate trading between buyers and sellers may be regulated as a dealer only and therefore not be subject to the Marketplace Rules and the Proposed Platform Framework. For example, firms that are currently registered in the category of exempt market dealer and that are currently permitted under securities legislation to facilitate the sale of securities, including crypto assets, in reliance on available prospectus exemptions in National Instrument 45-106 *Prospectus Exemptions* can continue to offer this service as long as they do not fall within the definition of “marketplace”.

Registered firms introducing crypto asset products and/or services are required to report changes in their business activities to their principal regulator and the proposed activities may be subject to review to assess whether there is adequate investor protection.

Investment dealer registration and IIROC membership

Like the Marketplace Rules, the Proposed Platform Framework contemplates Platforms both becoming registered as investment dealers and becoming IIROC dealer and marketplace members (**IIROC Members**)¹⁷. IIROC currently oversees all investment dealers as well as trading activity on debt and equity marketplaces in Canada and, accordingly,

- has a comprehensive body of rules governing the business, financial and trading conduct of IIROC Members which are tailored to the different types of products and services offered by IIROC Members;
- has established programs to assess compliance with both IIROC's rules applicable to dealers (**IIROC Dealer Member Rules**) and the Universal Market Integrity Rules (**UMIR**) that govern trading on a marketplace;
- has experience with dealers and marketplaces that trade a variety of securities and has developed tailored compliance programs and applied tailored rules for marketplaces; and
- operates in a regulatory capacity in every province in Canada.

Recognition as an exchange

A Platform that intends to carry on business as an exchange should contact the relevant securities regulatory authority to discuss whether recognition as an exchange is appropriate or, if such Platforms offer direct retail access or trade as principal, the Proposed Platform Framework is more appropriate to address risks arising from these activities.

Derivatives requirements

The CSA plans to consult on the appropriate regulatory framework to apply to marketplaces that trade over-the-counter derivatives, including platforms that offer derivatives with exposure to a crypto asset (e.g. a derivatives trading facility or swap execution facility that facilitate transactions in bitcoin-based derivatives). In the interim, if a Platform is trading or dealing in crypto assets that may be classified as derivatives, to the extent that the Platform has similar functions or operations to those contemplated in this Consultation Paper, it may be appropriate to apply requirements to those Platforms that are similar to the requirements contemplated by the Proposed Platform Framework. We anticipate, however, that such requirements may need to be specifically tailored to reflect the requirements that currently apply to derivatives or are otherwise appropriate to apply to those products and marketplaces.¹⁸

¹⁷ We note that IIROC membership may not be appropriate in all cases, depending on the facts and circumstances.

¹⁸ We would also like to remind market participants of the requirements relating to commodity futures exchange contracts in securities and commodity futures legislation.

5.2 Proposed Platform Framework - Key areas for consultation

While the Proposed Platform Framework builds on an existing regulatory regime that was designed for a wide variety of market participants, we recognize that the existing regulatory requirements, and particularly the Marketplace Rules, were designed for marketplaces trading traditional securities (such as equities and debt). The CSA supports innovation in our capital markets while protecting investors and promoting fair and efficient capital markets. We are therefore considering a set of requirements tailored to Platforms' operations that appropriately addresses the new risks introduced.

Below, we seek feedback on a number of areas that will assist in determining appropriate requirements for Platforms.

5.2.1 Custody and verification of assets

It has been reported that crypto assets with a value of almost US\$1 billion were stolen in 2018 from Platforms that operate globally.¹⁹ The ownership of crypto assets is evidenced by private keys which are required to execute crypto asset transactions. As the loss or theft of a private key may result in the loss of assets, the safeguarding of private keys is especially critical.

The operational model of many Platforms involves the Platform having custody of its participants' assets including private keys or the Platform holding the crypto assets in its own wallet with the Platform's private key. As a result, appropriate custody controls are a necessary part of managing risks to investors. To the extent that the Platform holds or has control over investors' assets, a significant risk is that investors' assets are not sufficiently accounted for or protected by the Platform. As a result, the Platform might not have sufficient crypto assets or cash to satisfy demand or could be vulnerable to theft. This risk increases substantially if there is insufficient insurance to cover the full amount of the theft.

When looking at the operations of a Platform, we will assess whether a Platform's risk management policies and procedures are appropriate to manage and mitigate the custodial risks. Expectations will be guided by the operational model of the Platform. For example, if the trades on a Platform do not occur on the distributed ledger, and instead the Platform keeps track of changes in ownership on its own internal ledger, we will evaluate whether the Platform has a robust system of internal controls, including records, that ensures that a participant's crypto assets are accurately accounted for by the Platform and appropriately segregated from assets belonging to the Platform.

Traditional custodians that hold assets for clients typically engage an independent auditor to perform an audit of the custodian's internal controls and prepare an assurance report. There are different types of assurance reports; however, it is common for custodians to engage external auditors to issue system and organization controls reports such as SOC 1 Reports²⁰ and SOC 2 Reports²¹ regarding the suitability of internal controls in financial reporting and controls

¹⁹ <https://www.reuters.com/article/us-crypto-currency-crime/cryptocurrency-theft-hits-nearly-1-billion-in-first-nine-months-report-idUSKCN1MK1J2>.

²⁰ Report on controls at a service organization relevant to participant entities' internal control over financial reporting.

²¹ Report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy.

surrounding the custody of investors' assets. The auditor will issue a report pertaining to the design of the controls (**Type I Report**), and a report assessing whether such controls are operating as intended over a defined period (**Type II Report**). We anticipate that these reports will play an important role in the authorization and oversight of the Platform, reporting of transactions, internal risk management and verification of the existence of investors' assets. We contemplate requiring that Platforms obtain SOC 2, Type I and II Reports for their custody system and, if they use third-party custodians, to ensure that they have SOC 2, Type I and II Reports.

We understand, however, that there have been challenges with crypto asset custodians and Platforms obtaining SOC 2, Type II Reports, in part due to the novel nature of crypto asset custody solutions and the limited period of time that Platforms have been in operation to allow for the testing of internal controls. Nevertheless, we contemplate that Platforms seeking registration as an investment dealer registration and IIROC membership that plan to provide custody of crypto assets will not only need to satisfy existing custody requirements but will also be expected to meet other yet-to-be determined standards specific to the custody of crypto assets.

Consultation questions

4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.
5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?
6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

5.2.2 Price determination

Fair and efficient capital markets are dependent on price discovery. The wide availability of information on orders and/or trades is important to foster efficient price discovery and investor confidence. As with traditional marketplaces, Platforms will be required to foster price discovery for the crypto assets they offer for trading. It is important for regulators and for the participants on the Platform to understand how prices on a Platform are determined. In addition, where the Platform or an affiliate acts as a market maker and provides quotes, the mechanisms for determining those quotes are expected to be available to participants. When trading as a market maker against its participants, a Platform will also be required to provide participants with a fair price.

Consultation questions

7. What factors should be considered in determining a fair price for crypto assets?

8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

5.2.3 Surveillance of trading activities

The existing types of marketplaces have different regulatory responsibilities. Exchanges are responsible for conducting market surveillance of trading activities on the exchange and enforcing market integrity rules. All of the existing equity exchanges have retained IIROC to monitor trading activity and enforce market integrity rules. ATs, by contrast, are not permitted to conduct market surveillance or enforcement activities and are required to engage a regulation services provider (**RSP**). IIROC currently acts as an RSP to all equity and fixed income marketplaces.

If IIROC were retained as an RSP by a Platform, IIROC would conduct market surveillance for that Platform. We understand that some of the types of manipulative and deceptive trading activities that may occur on Platforms that trade crypto assets are similar to those on marketplaces trading traditional securities. A unique challenge associated with market surveillance on Platforms is the fact that crypto assets trade on a global basis, on and off Platforms, outside regular trading hours, and may be illiquid and highly volatile. This, and the fact that there is currently no central source for pricing, may affect the price of a crypto asset trading on a Platform. This may also make it difficult to obtain reliable reference data that is needed to conduct effective surveillance.

To reduce the risks of potentially manipulative or deceptive activities, in the near term, we propose that Platforms not permit dark trading or short selling activities, or extend margin to their participants. We may revisit this once we have a better understanding of the risks introduced to the market by the trading of crypto assets.

Some Platforms have indicated that they intend to set rules and monitor the trading activities of their marketplace participants rather than retaining an RSP. This may raise conflicts of interest issues that will need to be addressed.

Consultation questions

9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?
10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.
11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?
12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?

5.2.4 Systems and business continuity planning

System resiliency, reliability and security controls are important for investor protection. System failures may result in investors being unable to access their crypto assets and may have an impact on market efficiency and investor protection. Marketplaces are required to have adequate internal and information technology controls over their trading, surveillance and clearing systems and information security controls that relate to security threats and cyber-attacks.²² Marketplaces are also required to maintain business continuity and disaster recovery plans to provide uninterrupted provision of key services.²³ To ensure that marketplaces have adequate internal and technology controls in place over their trading, surveillance and clearing systems and that their systems function as designed, marketplaces are required to engage an entity with relevant experience both in information technology and in the evaluation of related internal controls to conduct an independent systems review (ISR).²⁴

Technology and cyber security are key risks for Platforms. For these reasons they will also be required to comply with the systems and business continuity planning requirements applicable to existing marketplaces in NI 21-101. One key difference between Platforms and traditional marketplaces is that there is a greater risk for participants when a Platform provides custody of investors' crypto assets and does not have the appropriate internal controls.

In the normal course, all marketplaces are required to have an ISR conducted for other critical systems including order entry, execution or data. These requirements are in place to manage risks associated with the use of technology and to ensure that minimum standards are maintained. In some cases, we have granted temporary exemptions from the ISR requirements, provided the marketplace did not pose a significant risk to the capital markets and certain reports and information are provided to regulators.

Consultation question

13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.

5.2.5 Conflicts of interest

Platforms may have certain conflicts of interests, similar to other marketplaces. They may also raise a number of unique conflicts. For example, they may provide advice to their participants, which raises a conflict because the Platform may be providing advice on the same crypto assets that they have made eligible for trading on the Platform.

Another conflict relates to proprietary trading. Like dealers, it is possible that some Platforms trade for their own account against their participants, including retail investors. This raises conflicts of

²² Part 12 of NI 21-101.

²³ *Ibid.*

²⁴ *Ibid.*

interest and a number of risks, including that the Platform's participants may not know that the Platform operator also trades on the marketplace against the investor and the risk that investors may not receive a fair price when trading against the Platform operator.

To address these risks, we contemplate that Platforms will be required to identify and manage potential conflicts of interest and will be required to disclose whether they trade against their participants, including acting as a market maker, and the associated conflicts of interest. Disclosure will assist investors in assessing whether they want to participate on the Platform. To the extent Platforms are required to become IIROC Members, they will also be subject to requirements in the UMIR aimed at mitigating the risks associated with trading against their participants.²⁵

Consultation questions

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?
15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

5.2.6 Insurance

Some Platforms have custody of investors' assets. This makes them attractive targets for cyber-attacks and theft by insiders. Accordingly, insurance will also be an important safeguard. Dealers are required to maintain bonding or insurance against specific risks and in specified amounts.²⁶ This requirement may not address the specific operational risks of Platforms.

Many Platforms currently operate without any insurance covering investors' assets. We note that there may be significant difficulty and costs for a Platform to obtain insurance, in part due to the limited number of crypto asset insurance providers, and the high risk of cyber-attacks. Therefore, some Platforms have indicated that they are considering limited coverage that only extends to certain crypto assets, crypto assets in "hot wallets" or "cold wallets", loss as result of hacking, or loss from insider theft.

Consultation questions

16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.
17. Are there specific difficulties with obtaining insurance coverage? Please explain.
18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

²⁵ These include UMIR 5.3 *Client Priority*, UMIR 8.1 *Client Principal Trading* and UMIR 4.1 *Frontrunning*.

²⁶ s. 12.3 of NI 31-103.

5.2.7 Clearing and settlement

All trades executed on a marketplace are required to be reported and settled through a clearing agency.²⁷ A regulated clearing agency improves the efficiency of marketplaces and brings stability to the financial system.

Without exemptive relief, this requirement would also apply to Platforms that are marketplaces. However, currently there are no regulated clearing agencies for crypto assets that are securities or derivatives. As indicated above, we understand that on some Platforms, transaction settlement occurs on the Platform's internal ledger and is not recorded on the distributed ledger. We are considering whether an exemption from the requirement to report and settle trades through a clearing agency is appropriate. In these circumstances, Platforms will still be subject to certain requirements applicable to clearing agencies and will therefore be required to have policies, procedures and controls to address certain risks including operational, custody, liquidity, investment and credit risk.²⁸ We plan to revisit such exemptions in the future, as the space continues to develop and evolve.

Some Platforms may operate a non-custodial (decentralized) model where the transfer of crypto assets that are securities or derivatives occurs between the two parties of a trade on a decentralized blockchain protocol (e.g. smart contract). These types of Platforms will be required to have controls in place to address the specific technology and operational risks of the Platform.

Consultation questions

19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?
20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.
21. What other risks are associated with clearing and settlement models that are not identified here?

5.2.8 Applicable regulatory requirements

Platforms that are marketplaces are subject to existing marketplace regulatory requirements, including those summarized at **Appendix B**. Some of these requirements may not be relevant for Platforms and others may need to be tailored to address specific risks.

Platforms may perform additional functions typically performed by dealers and clearing agencies. We are also considering how the requirements summarized at **Appendices C and D** may apply. Leveraging the existing regulatory frameworks will ensure that Platforms are treated similarly to

²⁷ Part 13 of NI 21-101.

²⁸ If not already addressed by rules applicable to IIROC Members, to the extent they apply.

other marketplaces, but with appropriately tailored requirements that are relevant for the functions they perform.

Please note that Appendices B, C and D provide only an overview of certain requirements and therefore they should not be relied upon as exhaustive lists of the requirements applicable to marketplaces, dealers and clearing agencies.

Consultation question

22. What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

PART 6 – Providing Feedback

The CSA Regulatory Sandbox is an initiative of the CSA to support business seeking to offer innovative products, services and applications in Canada. The CSA Regulatory Sandbox is a part of the CSA's 2016-2019 Business Plan's objectives to gain a better understanding of how fintech innovations are impacting capital markets and assess the scope and nature of regulatory implications.²⁹

We invite interested parties to make written submissions on the consultation questions identified throughout this Consultation Paper. A complete list of the consultation questions referred to throughout this paper is provided in **Appendix A**. We also welcome you to provide any other comments on the appropriate regulation of Platforms. The information provided will assist us in refining the Proposed Platform Framework and our understanding of this area of innovation.

Please submit your comments in writing by **May 15, 2019**. Please send your comments by email in Microsoft Word format. Address your submission to IIROC and all members of the CSA as follows:

British Columbia Securities Commission
Alberta Securities Commission
Financial and Consumer Affairs Authority of Saskatchewan
Manitoba Securities Commission
Ontario Securities Commission
Autorité des marchés financiers
Financial and Consumer Services Commission (New Brunswick)
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island
Nova Scotia Securities Commission
Securities Commission of Newfoundland and Labrador
Superintendent of Securities, Northwest Territories
Superintendent of Securities, Yukon
Superintendent of Securities, Nunavut

²⁹ CSA Business Plan, 2016-2019: https://www.securities-administrators.ca/uploadedFiles/General/pdfs/CSA_Business_Plan_2016-2019.pdf

Please deliver your comments **only** to the addresses below. Your comments will be distributed to IIROC and the other CSA members.

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8
Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca

IIROC
Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada
Suite 2000, 121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

Certain CSA regulators require publication of the written comments received during the comment period. We will publish all responses received on the websites of the Autorité des marchés financiers (www.lautorite.qc.ca), the Ontario Securities Commission (www.osc.gov.on.ca), and the Alberta Securities Commission (www.albertasecurities.com). Therefore, you should not include personal information directly in comments to be published. It is important that you state on whose behalf you are making the submission.

PART 7 – Questions

Please refer your questions to any of the following CSA and IIROC staff:

Amanda Ramkissoon Fintech Regulatory Adviser, OSC LaunchPad Ontario Securities Commission aramkissoon@osc.gov.on.ca	Ruxandra Smith Senior Accountant, Market Regulation Ontario Securities Commission ruxsmith@osc.gov.on.ca
Timothy Baikie Senior Legal Counsel Market Regulation Ontario Securities Commission tbaikie@osc.gov.on.ca	Serge Boisvert Senior Policy Advisor Exchanges and SRO Oversight Autorité des marchés financiers serge.boisvert@lautorite.qc.ca
Marc-Olivier St-Jacques Senior Policy Advisor Supervision of Intermediaries Autorité des marchés financiers marco.st-jacques@lautorite.qc.ca	Denise Weeres Director, New Economy Alberta Securities Commission denise.weeres@asc.ca
Katrina Prokopy Senior Legal Counsel, Market Regulation Alberta Securities Commission katrina.prokopy@asc.ca	Sasha Cekerevac Senior Analyst, Market Structure Alberta Securities Commission sasha.cekerevac@asc.ca
Dean Murrison Director, Securities Division Financial and Consumer Affairs Authority of Saskatchewan dean.murrison@gov.sk.ca	Zach Masum Manager, Legal Services, Capital Markets Regulation British Columbia Securities Commission zmasum@bcsc.bc.ca
Ami Iaria Senior Legal Counsel, Capital Markets Regulation British Columbia Securities Commission aiaria@bcsc.bc.ca	Peter Lamey Legal Analyst, Corporate Finance Nova Scotia Securities Commission peter.lamey@novascotia.ca
Chris Besko Director, General Counsel The Manitoba Securities Commission chris.besko@gov.mb.ca	Wendy Morgan Deputy Director, Policy Financial and Consumer Services Commission (New Brunswick) wendy.morgan@fcnb.com
Victoria Pinnington Senior Vice President, Market Regulation IIROC vpinnington@iiroc.ca	Sonali GuptaBhaya Director, Market Regulation Policy IIROC sguptabhaya@iiroc.ca

APPENDIX A

Consultation Questions

1. Are there factors in addition to those noted in Part 2 that we should consider?
2. What best practices exist for Platforms to mitigate the risks outlined in Part 3? Are there any other significant risks which we have not identified?
3. Are there any global approaches to regulating Platforms that are appropriate to be considered in Canada?
4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.
5. Other than issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?
6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of the Platforms holding or storing crypto assets on their behalf?
7. What factors should be considered in determining a fair price for crypto assets?
8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?
9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?
10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.
11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?
12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?
13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be appropriate? What services should be included/excluded from the scope of the ISR? Please explain.

14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?
15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?
16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.
17. Are there specific difficulties with obtaining insurance coverage? Please explain.
18. Are there alternative measures that address investor protection that could be considered that are equivalent to insurance coverage?
19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?
20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks could be mitigated.
21. What other risks could be associated with clearing and settlement models that are not identified here?
22. What regulatory requirements (summarized at Appendices B, C, and D), both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

APPENDIX B

Summary of Regulatory Requirements Applicable to Marketplaces

Marketplaces are subject to the Marketplace Rules and NI 23-103. These include high-level principles relating to access to the marketplaces and trading on the marketplaces. A summary of the regulatory requirements is included below. Please note that this summary should not be relied upon as being an exhaustive list of the requirements applicable to marketplaces.

1. Market integrity

The Marketplace Rules and NI 23-103 have a number of requirements covering market integrity. For example, NI 21-101 requires a marketplace to take reasonable steps to ensure it operates in a way that does not interfere with fair and orderly markets.³⁰ NI 23-101 and securities legislation in some jurisdictions also prohibit any person or company from engaging in transactions that they know, or should know, result in market manipulation or are fraudulent. NI 23-103 also has requirements for marketplaces aimed at maintaining market integrity. For example, marketplaces are required to assess, on a regular basis, whether they require risk management and supervisory controls, policies and procedures, in addition to those of their participants. Marketplaces are also required to assess on a regular basis the continuing adequacy and effectiveness of these controls, policies and procedures.³¹

While the Marketplace Rules and NI 23-103 establish the high-level principles for marketplaces that trade in Canada, the specific requirements applicable to participants on a marketplace are included in the UMIR, which are administered by IIROC.

2. Transparency of operations

Marketplaces are required to make transparent, on their websites, a description of how their orders are entered, interact and are executed, the hours of operation, their fees (including fees for facilitation, routing and mark-ups, if applicable), their affiliates' fees, access requirements, conflicts of interest policies and procedures, and referral arrangements between the marketplace and service providers.³² The purpose of these requirements is to ensure that market participants understand how the marketplace works, as well as the associated risks, its features and its fees.

3. Transparency of orders and trades

Except in certain circumstances, marketplaces must make transparent their order and trade information for securities traded on a marketplace by providing it to an information processor.³³ The information processor collects, consolidates and disseminates their data, and also sets the requirements for the order and trade information that must be provided to it by marketplaces.

4. Transparency to regulators

Marketplaces are required to provide certain information to the securities regulators, so that they

³⁰ s. 5.7 of NI 21-101.

³¹ Part 4 of NI 23-103.

³² s. 10.1 of NI 21-101.

³³ Part 7 of NI 21-101 and Part 8 of NI 21-101 for equity and fixed income securities, respectively.

understand the business of the marketplace and the risks it introduces to the market. Such information is described in the exhibits included in Forms 21-101F1 *Information Statement Exchange or Quotation and Trade Reporting System* and 21-101F2 *Information Statement Alternative Trading System*, for exchanges and ATSS respectively, and relates to: governance, marketplace operations, outsourcing arrangements, systems, custody, the types of securities traded, how access to services is provided, and fees. These forms must be filed prior to the commencement of the operations and must be kept up to date. Changes to the information included in these forms must also be reported to the securities regulators, either in advance, if the change is significant, or subsequent to its implementation if it is not.

In addition, marketplaces report their trading activities on a quarterly basis.³⁴ The quarterly reports are provided to the securities regulators in electronic form. The information reported is included in Form 21-101F3 *Quarterly Report of Marketplace Activities* and includes trading activity information (value, volume and number of trades) by category of security, information about orders and order types, and information about the most traded securities.

5. Listing securities

Exchanges may list securities of an issuer.³⁵ They are required to comply with the fair access requirements in NI 21-101 (and in their recognition orders), which include the requirement to establish written standards for granting access to each of their services,³⁶ including listings. Since exchanges have listings requirements in the form of rules, they must ensure that these rules require compliance with securities legislation³⁷ and that they provide appropriate sanctions for violations of the rules.³⁸

6. Fair access

Marketplaces must not unreasonably prohibit or limit access by a person or company to services offered by the marketplace. A marketplace must establish written standards for granting access to each of its services and must keep records of each access grant or denial of access.³⁹ It must neither permit unreasonable discrimination among participants, issuers and marketplace participants nor impose any burden on competition that is not reasonably necessary and appropriate.⁴⁰ Lastly, a marketplace must not prohibit, condition or otherwise limit a marketplace participant from trading on any marketplace.⁴¹

7. Conflict of interest

A marketplace must establish, maintain and ensure compliance with policies and procedures that identify and manage any conflicts of interest arising from the operation of a marketplace or the

³⁴ Part 3 of NI 21-101.

³⁵ An issuer is listed when there is a formal arrangement between the exchange and the issuer to have the issuer's securities listed, and the exchange has and enforces listing requirements.

³⁶ para. 5.1(2)(a) of NI 21-101.

³⁷ para. 5.3(b) of NI 21-101.

³⁸ para. 5.4(b) of NI 21-101.

³⁹ s. 5.1 of NI 21-101.

⁴⁰ ss. 5.1(3) of NI 21-101.

⁴¹ s. 5.1 of NI 21-101.

services it provides, and any conflicts that owners of the marketplace may have.⁴² These policies must be disclosed on the marketplace's website.

8. Outsourcing

A marketplace that outsources key services or systems to a service provider must have policies and procedures relating to the selection of the service provider, must maintain access to the books and records of the service provider, must ensure that the securities regulatory authorities have access to data that is maintained at the service provider and must review, on a regular basis, the performance of the service provider.⁴³ The outsourcing requirements seek to ensure that the marketplace retains responsibility and control over the outsourced services or systems.⁴⁴

9. Confidential treatment of trading information

A marketplace must not release the order or trade information of any of its participants. This requirement protects each marketplace participant's trading history and strategy. There is an exception to this requirement in limited situations, where data is used for capital markets research and provided certain conditions are met.⁴⁵

10. Recordkeeping requirements

Marketplaces are required to keep books, records and other documents that are reasonably necessary for the proper recording of its business in electronic form.⁴⁶

11. Systems and business continuity planning

Marketplaces are required to have adequate internal and information technology controls over their trading, surveillance and clearing systems and information security controls that relate to security threats and cyber attacks. A marketplace is also required to maintain business continuity and disaster recovery plans. A marketplace is required to develop, maintain and test a business continuity plan to ensure uninterrupted provision of key services. A marketplace is required to engage a qualified third party to conduct an independent system review to assess whether it has adequate internal and information technology controls and if they function as designed.⁴⁷

12. Clearing and settlement

All trades executed on a marketplace must be reported and settled through a clearing agency.⁴⁸ Marketplace participants have a choice as to the clearing agency that they would like to use for the clearing and settlement of their trades, provided that the clearing agency is appropriately regulated in Canada.

⁴² s. 5.11 of NI 21-101.

⁴³ s. 5.12 of NI 21-101.

⁴⁴ *Ibid.*

⁴⁵ s. 5.10 of NI 21-101.

⁴⁶ Part 11 of NI 21-101.

⁴⁷ Part 12 of NI 21-101.

⁴⁸ Part 13 of NI 21-101.

APPENDIX C

Summary of Regulatory Requirements Applicable to Dealers

Registration is required if a person or company is in the business of or is holding itself out as being in the business of, trading securities. We have generally found Platforms that intermediate trades of securities between buyers and sellers to be “in the business” of trading securities and subject to the registration requirements set out in National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations*, and, where applicable, IIROC Dealer Member Rules and UMIR.

Although the details of the specific requirements applicable to different categories of dealers vary, the summary below captures the basic requirements applicable to a dealer. Please note that this summary should not be relied upon as an exhaustive list of the requirements applicable to dealers.

1. Proficiency

Dealers are in the business of buying and selling securities and derivatives on behalf of the clients and are implicitly or explicitly holding themselves out as having a certain level of knowledge or expertise. Accordingly, individuals registered as dealing representatives are expected to have the education, training and experience that a reasonable person would consider necessary to perform their activities competently, including understanding the structure, features and risks of each security the individual recommends.⁴⁹

Similarly, firms are required to employ individuals as ultimate designated persons (**UDP**) and chief compliance officers (**CCO**) who meet certain additional educational and experience requirements and who will have responsibilities respecting promoting compliance with securities legislation and establishing and monitoring policies and procedures designed to assess compliance by the firm and its dealing representatives with securities legislation.⁵⁰

2. Books and records

Dealers may hold the assets of and conduct transactions on behalf of a multitude of clients. Accordingly, it is important that they maintain books and records that accurately reflect their business activities, financial affairs and client transactions. These books and records requirements help dealers ensure that they are able to prepare and file financial information, determine their capital adequacy, and generally demonstrate compliance with the capital and insurance requirements, among other securities law requirements.⁵¹ Maintaining proper books and records allows dealers to document information about their relationships with their clients and with other entities, as well as, to report to their clients the trades they have transacted on behalf of their clients.⁵²

⁴⁹ The proficiency requirements for registered individuals at investment dealers are set out in IIROC Dealer Member Rule 2900 *Proficiency and Education*. The requirements for registered individuals at dealers other than investment dealers are included in Part 3 of NI 31-103.

⁵⁰ s. 11.2 and 11.3 of NI 31-103, respectively.

⁵¹ s. 11.5 of NI 31-103.

⁵² s. 14.12 and 14.14 of NI 31-103.

3. Compliance system

Given the significant role registered dealers play vis-à-vis their clients and to the capital markets, dealers are required to establish, maintain and apply policies and procedures that establish a system of controls and supervision sufficient to provide reasonable assurance that the firm and each individual acting on its behalf complies with securities legislation and to manage the risks associated with its business in accordance with prudent business practices.⁵³ An effective compliance system includes internal controls and day-to-day monitoring and supervision elements that are appropriately documented. These elements are intended to ensure the integrity of the practices of the dealer, as well as the appropriate segregation of key duties and functions, and includes employee proficiency and training.

As part of a compliance system, a registered firm must appoint both a CCO and an UDP. The CCO is responsible for monitoring, updating and reviewing policies and procedures a registered firm must have as part of its compliance system. The UDP promotes compliance with securities legislation and sets the tone for firm-wide compliance. Investment dealers are also required to appoint a Chief Financial Officer.

4. Financial condition and required capital

Dealers may have access to the assets of a multitude of clients and the insolvency of a dealer could have serious implications for clients and confidence in the capital markets. Accordingly, firms are subject to ongoing financial requirements.⁵⁴

Registered firms are required to calculate regulatory capital to ensure that it is not less than zero. The minimum capital for an exempt market dealer and a restricted dealer is \$50,000 (unless an alternative minimum is imposed). Investment dealers are required to maintain risk adjusted capital, calculated in accordance with IIROC requirements, that is greater than zero.⁵⁵

5. Insurance

Similarly, because of the significance of the financial condition of registered dealers to their clients and the capital markets, registered dealers must also maintain bonding or insurance that contains certain specific clauses and coverage. The amount of insurance coverage depends on the category of dealer involved.⁵⁶

6. Financial reporting

Securities regulators monitor the financial condition of registered firms by requiring them to prepare and deliver to regulators annual and interim financial information, and to abide by requirements in IIROC Dealer Member Rule 16 *Dealer Members' Auditors and Financial Reporting*.

⁵³ s. 11.1 of NI 31-103.

⁵⁴ The financial requirements for investment dealers are found in IIROC Dealer Member Rule 17 *Dealer Member Minimum Capital, Conduct of Business and Insurance* and Form 1. The financial requirements for dealers other than investment dealers are in s. 12.1 of NI 31-103.

⁵⁵ Part 12, Division 1 of NI 31-103.

⁵⁶ The insurance requirements for dealers other than investment dealers are included in s. 12.3 of NI 31-103. The insurance requirements for investment dealers are in IIROC Rule 400 *Insurance*.

7. KYC and suitability

Know-your-client and suitability obligations require dealers to collect information to establish the identity of their clients, to understand their investment needs and objectives, overall financial circumstances, and risk tolerance and to then take reasonable steps to use that information to ensure a proposed transaction is suitable to the client. In order to make that suitability assessment, the dealer also needs to understand the features and risks of the security or derivative to be transacted (the know-your-product requirement).⁵⁷ In addition, dealers also have separate, specific obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and the associated regulations, including the requirement to verify the identity of clients for certain activities and transactions.

8. Conflicts of interest

Dealers are faced with many potential conflicts of interest between their and their clients' interests. Accordingly, securities legislation requires that a dealer take reasonable steps to identify conflicts of interests that exist and may exist between itself and its clients. Among other requirements, a dealer must identify conflicts of interest that should be avoided and respond appropriately to other conflicts of interest given the level of risk each conflict raises (e.g. through control and/or disclosure of the conflict of interest).⁵⁸

9. Custody

As dealers may have access to clients' assets, there are a number of requirements and prohibitions regarding custody of client cash and securities. Investment dealers, as IIROC members, must comply with the custodial requirements of IIROC.⁵⁹ Depending on the location where such assets are held, investment dealers may have to provide additional capital to reflect increased risk.⁶⁰ Exempt market dealers must comply with the requirements regarding holding client cash and securities set out in NI 31-103 which prohibits them from holding client assets and acting as custodians themselves.⁶¹ Instead, client assets of exempt market dealers are normally held by a custodian that is a separate legal entity.

10. Best execution and fair pricing

Investment dealers are required to establish, maintain and follow written policies and procedures that are reasonably designed to achieve best execution when acting for a client.⁶² What constitutes "best execution" varies depending on the particular circumstances and, for transactions that are executed over the counter, such as transactions in fixed income securities, the expectation is that dealers have policies and procedures to ensure that prices to their clients for these securities are fair and reasonable, both for the pricing of principal transactions and for commissions that may be charged by the dealer.

⁵⁷ The suitability requirements for dealers other than investment dealers are included in Part 13 of NI 31-103. The requirements for investment dealers are in IIROC Rule 1300 *Supervision of Accounts*.

⁵⁸ s. 13.4 of NI 31-103.

⁵⁹ IIROC Dealer Member Rule 2000 *Segregation Requirements*, Dealer Member Rule 17 *Dealer Member Minimum Capital, Conduct of Business and Insurance* and Dealer Member Rule 2600 *Internal Control Policy Statements*.

⁶⁰ IIROC Form 1 General Notes and Definitions, (d) "acceptable securities locations".

⁶¹ s. 14.5.2 of NI 31-103.

⁶² IIROC Dealer Member Rule 3300 *Best Execution of Client Orders*.

11. Handling Complaints

Dealers are required to document complaints and to effectively and fairly respond to them. These procedures should include monitoring of complaints, to allow the detection of frequent and repetitive complaints made with respect to the same matter, which may, on a cumulative basis, indicate a serious problem. Registered firms are required to be a member of the Ombudsman for Banking Services and Investments,⁶³ except in Québec where the dispute resolution service is administered by the Autorité des marchés financiers.

⁶³ Part 13, Division 5 of NI 31-103.

APPENDIX D

Requirements Applicable to Clearing Agencies

A clearing agency is defined in securities legislation as a person or company that, among other activities, provides centralized facilities for clearing and settlement of transactions in securities or, in some jurisdictions, derivatives.

National Instrument 24-102 *Clearing Agency Requirements* (**NI 24-102**) sets out certain requirements in connection with the application process for recognition as a clearing agency or exemption from the recognition requirement. Please note that this summary should not be relied upon as being an exhaustive list of the requirements applicable to clearing agencies.

NI 24-102 also sets out the ongoing requirements applicable to recognized clearing agencies. This includes the requirement to meet or exceed applicable principles as set up in the April 2012 report *Principles for financial market infrastructures* published by the Committee on Payments and Market Infrastructure and the International Organization of Securities Commissions (**PFMI**). The PFMI cover all areas associated with activities carried out by a clearing agency: systemic risk, legal risk, credit risk, liquidity risk, general business risk, custody and investment risk and operational risk. Clearing agencies are required to:

- have appropriate rules and procedures on how transactions are cleared and settled, including when settlement is final;
- minimize and control their credit and liquidity risks;
- have rules that clearly state their obligations with respect to the delivery of securities traded; and
- identify, monitor and manage the risks and costs associated with the delivery of crypto assets, including the risk of loss of these crypto assets.

TAB 7

CSA Staff Notice 46-308

Securities Law Implications for Offerings of Tokens

June 11, 2018

Purpose and background

CSA staff (**we** or **staff**) are issuing this notice to respond to inquiries on the applicability of securities laws to offerings of coins or tokens, including ones that are commonly referred to as “utility tokens”.

In CSA Staff Notice 46-307 *Cryptocurrency Offerings (SN 46-307)*, we stated that many cryptocurrency offerings, such as initial coin offerings (**ICO**) and initial token offerings (**ITO**), involve sales of securities. This is because the offering and/or the coins or tokens issued under the offering constitute investment contracts or are otherwise securities, when the totality of the offering or arrangement is considered. We also stated that, depending on the facts and circumstances, these products may also be considered to be derivatives and subject to legislation and regulatory requirements that apply to derivatives.

Since SN 46-307 was published, staff have engaged with numerous businesses wishing to complete offerings of tokens and have found that most of these offerings have involved securities.

As part of this engagement with businesses, we have received various inquiries relating to offerings of tokens referred to as “utility tokens”. “Utility token” is an industry term often used to refer to a token that has one or more specific functions, such as allowing its holder to access or purchase services or assets based on blockchain technology.

We have seen many businesses offering tokens to raise capital for the development of their software, online platform or application. In many of these cases, the offering will involve securities despite the fact that the tokens have one or more utility functions.

This notice provides guidance on the following issues relating to offerings of tokens:

- when an offering of tokens may or may not involve an offering of securities; and
- offerings of tokens that are structured in multiple steps.

The views outlined in this notice are based on the features we have seen in offerings to date and may change over time, as the market and business models continue to evolve.

When an offering of tokens may or may not involve an offering of securities

As we indicated in SN 46-307, every offering is unique and must be assessed on its own characteristics. An offering of tokens may involve the distribution of securities, including because:

- the offering involves the distribution of an investment contract; and/or

- the offering and/or the tokens issued are securities under one or more of the other enumerated branches of the definition of security or may be a security that is not covered by the non-exclusive list of enumerated categories of securities.

In determining whether or not an investment contract exists, the case law endorses a purposive interpretation that includes considering the objective of investor protection. This is especially important for businesses to consider in the context of offerings of tokens where the risk of loss to investors can be high. Businesses and their professional advisors should consider and apply the case law interpreting the term “investment contract”¹, including considering whether the offering involves:

1. An investment of money
2. In a common enterprise
3. With the expectation of profit
4. To come significantly from the efforts of others

In analyzing whether an offering of tokens involves an investment contract, businesses and their professional advisors should assess not only the technical characteristics of the token itself, but the economic realities of the offering as a whole, with a focus on substance over form.

We have received submissions from businesses and their professional advisors that a proposed offering of tokens does not involve securities because the tokens will be used in software, on an online platform or application, or to purchase goods and services. However, we have found that most of the offerings of tokens purporting to be utility tokens that we have reviewed to date have involved the distribution of a security, namely an investment contract. The fact that a token has a utility is not, on its own, determinative as to whether an offering involves the distribution of a security.

Examples of situations and their possible implication on one or more of the elements of an investment contract

We have identified in the table below situations that have an implication on the presence of one or more of the elements of an investment contract.

The examples that we have provided are intended to be illustrative and are based on situations that staff have seen to date. This list is not exhaustive and we expect that it will change over time, as the market and business models continue to evolve. Also, we emphasize that none of these examples should be interpreted as determinative on its own of whether or not a security exists. It is possible that an offering of tokens may be viewed as involving, or not involving, a security even with the existence, or absence, of one or more of the characteristics listed below. As such, businesses and their professional advisors should complete a meaningful analysis based on the unique characteristics of their offering of tokens and should not use the following table to complete a mechanical “tick the box” exercise.

¹ See, for example: the Supreme Court of Canada’s decision in *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*, [1978] 2 SCR 112, the Ontario Securities Commission’s decision in [Universal Settlements International Inc.](#) (2006), 29 OSCB 7880, and the Alberta Securities Commission’s decisions in [The Land Development Company Inc. et al](#) (2002), ABSECCOM REA #1248840 v1 and [Kustom Design Financial Services Inc. \(Re\)](#), 2010 ABASC 179.

	Examples of situations	Possible implications
1.	The proposed function of the token is to use software or an online platform or application, or to purchase goods and services, but the software, online platform or application or goods and services do not exist, are not yet available or are still in development.	This could indicate that the purchaser is not purchasing the tokens for their immediate utility, but because of an expectation of profit, which will depend on the issuer's ability to complete the development of the software, online platform or application or to offer the goods and services. Although some purchasers may be purchasing the token for the utility function, many purchasers may be purchasing the token in order to sell it on a cryptoasset trading platform or otherwise in the secondary market. This could also indicate the existence of a common enterprise because management's efforts are still needed to develop or deliver the software, online platform or application or goods and services. Regardless of the motivation of the purchaser, the purchaser bears the risk of loss if management's efforts are not successful. Whether or not a functional software or online platform or application has been developed is a question of fact. For example, we may consider that a platform is not fully developed in cases where the significant intended functions are not yet available or where end users are unable to participate, even where there may be developer functionality.
2.	The tokens are not immediately delivered to purchasers.	This could indicate that the software, online platform or application or goods and services are not yet available and purchasers are not purchasing the tokens for their immediate utility but because of an expectation of profit. It could also indicate a common enterprise exists because of the purchaser's reliance on management to deliver the tokens.
3.	The stated purpose of the offering is to raise capital, which will be used to perform key actions that will support the value of the token, the value of the issuer's business or the platform's usability. These key actions may include	This could indicate the existence of a common enterprise between management and purchasers. This could also indicate that the purchaser is not purchasing the tokens for their immediate utility, but to invest in a business under development

	Examples of situations	Possible implications
	expanding the team of developers, developing relevant applications and products, expanding the network of participants on the platform, installing necessary infrastructure and marketing efforts.	with an expectation of profit, which will be dependent on the issuer's ability to perform key actions.
4.	The issuer has set up a "bounty" or similar program that offers free tokens or other benefits to persons who promote the offering through various channels, including on social media, in blogs or elsewhere on the Internet.	Persons participating in this kind of program may have an incentive to make statements promoting the offering as an investment; for example, by suggesting the tokens have the potential to increase in value. Such statements create an expectation of profit.
5.	The issuer's management retains for themselves a significant number of unsold tokens from the offering or "pre-mines" a significant number of tokens before they are publicly available as a form of compensation for their efforts.	This could indicate the existence of a common enterprise, as any future increase in the value of the tokens will financially benefit both management and the investor.
6.	The issuer suggests that the tokens will be used as a currency or have a utility beyond the issuer's platform, but at the time of these suggestions, the issuer is not able to demonstrate that the tokens are widely used or accepted.	This could indicate a common enterprise because of the reliance on management to take key actions to establish uses for the token beyond the platform.
7.	The issuer's management has represented that it has specific skills or expertise that will likely increase the value of the token.	This could indicate a common enterprise because of the reliance on management and could also indicate an expectation of profit.
8.	Tokens have a fixed value on the platform that does not automatically increase over time, or change based on non-commercial factors.	This may reduce the purchaser's expectation of profit if tokens are continually available from the platform at a fixed value.
9.	The number of tokens issuable is finite or there is a reasonable expectation that access to new tokens will be limited in the future.	As there is a limited or reduced supply of tokens, initial purchasers may have an expectation of profit as increased demand with limited or reduced supply should lead to an increase in price. In contrast, a continuous or unlimited supply of tokens may reduce the probability that purchasers buy with an expectation of profit.
10.	The issuer permits or requires purchasers to purchase tokens for an amount that does	This could indicate that some purchasers are not purchasing the tokens for personal

	Examples of situations	Possible implications
	not align with the purported utility of tokens. For example, the issuer permits a purchaser to acquire a disproportionately large purchase amount (e.g. \$100,000) of tokens that can be used only for downloading music for personal use.	use, but rather with an expectation to sell them at a profit.
11.	Marketing of the offering targets persons or companies who would not reasonably be expected to use the issuer's product, service or application. For example, an offering of a token that permits holders to use an existing application is marketed in Canada, but Canadian residents cannot use the product, service or application.	This could indicate that purchasers are primarily motivated by the potential for profit, not the ability to use the product, service or application. Performing know your client on purchasers may help issuers to establish the general profile of their purchasers, potentially enabling the issuer to demonstrate a purchaser's intended use of the token.
12.	Management makes statements suggesting that the tokens will appreciate in value, or compares them to other cryptocurrencies that have increased in value. Management encourages others to make, or acquiesces in others making, such statements.	This could indicate that the offering is being marketed and sold as an investment, thus creating an expectation of profit. In contrast, to the extent that management clearly and uniformly promotes the token in a manner that, taken as a whole, promotes only its utility and not its investment value, the implication that purchasers have an expectation of profit may be reduced.
13.	Tokens are distributed to users for free.	The distribution of tokens for free will likely not involve an investment of money. However, the distribution of free tokens as part of an overall sale of an ancillary or secondary product or service, may involve an investment of money if it is appropriate to "look through" the token distribution to the investment of money in the overall offering.
14.	Tokens are not fungible or interchangeable and each token has unique characteristics that result in the purchaser exercising their personal preferences to value it as a mode of entertainment or as a collectible item; any objective future market value of the token is primarily based on market forces and not on continued development of a business by	The value of the token may be based on its unique characteristics, and not on the efforts of others. There may not be a common enterprise.

	Examples of situations	Possible implications
	the issuer.	

Tokens reasonably expected or marketed to trade on cryptoasset trading platforms.

Another situation that may have an implication on the presence of one or more of the elements of an investment contract is the fact that tokens are reasonably expected or marketed to trade on one or more cryptoasset trading platforms (including decentralized or “peer-to-peer” trading platforms) or to otherwise be freely tradeable in the secondary market.

This fact indicates that purchasers may purchase the tokens with an expectation to resell them at a profit. This is particularly true where the existence of secondary trading is critical to the success of the offering of tokens or is featured prominently in the marketing of the offering.

To determine whether tokens are reasonably expected to trade in the secondary market, we consider representations made by the issuer either formally in a whitepaper or informally through social media channels (e.g., messaging platforms, community meetups, online videos). We also consider representations made by third parties that have been explicitly or implicitly endorsed by the issuer or management.

We have heard from some token issuers, for example those using the Ethereum ERC20 token standard, that they may have no control over the transferability of their token, or the creation of a market by other parties, including cryptoasset trading platforms. This possible absence of control over secondary trading is generally not, on its own, relevant in assessing whether purchasers expect a profit.

In general, with the offerings of tokens we have seen that have involved securities, the public transferability of the tokens has not been restricted, potentially placing persons trading the tokens offside resale restrictions in securities laws.

Offerings of tokens that are structured in multiple steps

We are aware of offerings of tokens that are structured in multiple steps.

As a general statement, nothing in this notice should be interpreted as staff supporting or endorsing the use of multiple step transactions to offer tokens.

For example, staff have seen offerings with two steps. In the first step, the purchaser agrees to contribute money in exchange for a right to receive tokens at a future date. This may be completed pursuant to an agreement referred to as a “simple agreement for future tokens” or “SAFT”. At the time of purchase, no token is delivered. In the first step, there is generally a distribution of a security, specifically the right to a future token, which is often made under a prospectus exemption, such as the accredited investor exemption.

In the second step, the token is delivered. At that time, the issuer has generally represented that the software, online platform or application is built or the goods or services are available and the token is functional. In several instances, issuers have taken the position that the token itself is not a security.

Staff would like to note the following:

- We may consider that a token delivered at a second or later step is a security, despite the fact that the token may have some utility. This may be because the token that is unlocked or delivered involves an investment contract because it continues to have a number of the factors identified above or because the token has other security-like attributes, such as a profit-sharing interest.
- The distribution of the security is subject to the prospectus requirement. Issuers may contemplate relying on prospectus exemptions, such as the accredited investor exemption or the offering memorandum exemption provided in National Instrument 45-106 *Prospectus Exemptions*. An issuer that uses a prospectus exemption must ensure that it meets all conditions of the exemption. Securities that are distributed using capital-raising prospectus exemptions are typically subject to the resale restrictions in National Instrument 45-102 *Resale of Securities*, including, in the case of a non-reporting issuer, that they cannot be resold for an indefinite period except under another prospectus exemption.
- A person or company that is in the business of trading in securities is subject to the dealer registration requirement under securities laws². The term “trade” is broad and includes acts, advertisements, solicitations, conduct or negotiation directly or indirectly in furtherance of a trade.
- If the distribution of the security at the first step is made without complying with securities law requirements, the issuer will remain in default of securities law requirements, even though subsequent steps may have occurred.
- We will have concerns where a multiple step transaction is used in an attempt to avoid securities legislation. As stated earlier in this notice, businesses and their professional advisors should assess the economic realities of the offering as a whole, with a focus on substance over form.

Enforcement Activity

Staff are conducting active surveillance of coin and token offerings activity to identify past, ongoing and potential future violations of securities laws or conduct in the capital markets that is contrary to the public interest. CSA members have taken and intend to continue taking regulatory and/or enforcement action against businesses that do not comply with securities laws.

Complying with Securities Legislation

In order to avoid costly regulatory surprises, we encourage businesses with proposed offerings of tokens to consult qualified securities legal counsel in their local jurisdiction about the potential application of, and possible approaches required to comply with, securities legislation.

As trends in the cryptocurrency industry are evolving quickly, we encourage businesses seeking flexible approaches to compliance with securities laws to contact their local securities regulatory

² Please refer to section 1.3 of Companion Policy 31-103CP *Registration Requirements, Exemptions and Ongoing Registrant Obligations* for a description of the factors that we consider relevant in determining whether a person or company is trading securities for a business purpose.

authority to discuss their project at the contact information below. When contacting their local securities regulatory authority, businesses should be ready to provide a draft whitepaper, a business plan or a detailed description of their proposed offering. We may also ask for copies of promotional materials in connection with the offering, and a description of the promotional activities and marketing efforts in respect of the offering, as well as information on the corporate structure and principals involved.

We remind businesses to consider securities law requirements that may apply to their activities, regardless of where investors are located. A Canadian securities regulatory authority may have jurisdiction over trades to investors outside of that jurisdiction where there is a real and substantial connection between the transaction and that jurisdiction.³

CSA Regulatory Sandbox

We welcome digital innovation and we recognize that new fintech businesses may not fit neatly into the existing securities law framework. The CSA Regulatory Sandbox is an initiative of the CSA to support fintech businesses seeking to offer innovative products, services and applications in Canada. It allows firms to register and/or obtain exemptive relief from securities law requirements, under a faster and more flexible process than through a standard application, in order to test their products, services and applications throughout the Canadian market, generally on a time-limited basis.

The CSA have granted, through the CSA Regulatory Sandbox, exemptive relief from certain securities law requirements to firms in the context of offerings of tokens that involve the distribution of securities, subject to conditions to ensure adequate investor protection. A list of the firms that have been authorized in the CSA Regulatory Sandbox is available on the CSA website at <https://www.securities-administrators.ca/>.

Applications to the CSA Regulatory Sandbox are analyzed on a case-by-case basis.

Businesses contemplating offerings of tokens are invited to contact the securities regulatory authority in the jurisdiction where their head office is located:

Province	Contact Information
British Columbia	The BCSC Tech Team at TechTeam@bcsc.bc.ca
Alberta	Mark Franko at Mark.Franko@asc.ca, Denise Weeres at Denise.Weeres@asc.ca, Danielle Grover at Danielle.Grover@asc.ca or Christopher Peng at Christopher.Peng@asc.ca
Saskatchewan	Dean Murrison at dean.murrison@gov.sk.ca or Liz Kutarna at liz.kutarna@gov.sk.ca
Manitoba	Chris Besko at chris.besko@gov.mb.ca
Ontario	The OSC LaunchPad Team at osclaunchpad@osc.gov.on.ca
Québec	The Fintech Working Group at fintech@lautorite.qc.ca.
New Brunswick	Susan Powell at registration-inscription@fcnb.ca
Nova Scotia	Jane Anderson at Jane.Anderson@novascotia.ca

³ The Supreme Court of Canada's decision in *Gregory & Co. v. Quebec (Securities Commission)*, [1961] S.C.R. 584; as well as the various decisions that have been issued subsequent to that case. See also *Reference Re Securities Act (Canada)* 2011 SCC 66, 3 SCR 837 at para. 45.

IN THE MATTER OF THE BANKRUPTCY OF QUADRIGA FINTECH SOLUTIONS CORP.,
WHITESIDE CAPITAL CORPORATION AND 0984750 B.C. LTD. D/B/A QUADRIGA CX AND
QUADRIGA COIN EXCHANGE

Court File No. & Estate No.:
CV-19-627184-00CL (31-2560674)
CV-19-627185-00CL (31-2560984)
and CV-19-627186-00CL (31-2560986)

**ONTARIO
SUPERIOR COURT OF JUSTICE
(COMMERCIAL LIST)**

Proceeding commenced at Toronto

**BOOK OF AUTHORITIES
(RETURNABLE JANUARY 26, 2021)**

STIKEMAN ELLIOTT LLP

Barristers & Solicitors
5300 Commerce Court West
199 Bay Street
Toronto, Canada M5L 1B9

Elizabeth Pillon LSO#: 35638M

Tel: (416) 869-5623
E-mail: lpillon@stikeman.com

Maria Konyukhova LSO#: 52880V

Tel: (416) 869-5230
Email: mkonyukhova@stikeman.com

Lee Nicholson LSO#: 66412I

Tel: (416) 869-5604
Email: leenicholson@stikeman.com

Nicholas Avis LSO#: 76781Q

Tel: (416) 869-5504
Fax: (416) 947-0866

**Lawyers for the Trustee in Bankruptcy of
Quadriga Fintech Solutions Corp., Whiteside
Capital Corporation and 0984750 B.C. Ltd.**