Internet and E-Commerce Law in Canada

VOLUME 18, NUMBER 12 Cited as (2017-18), 18 I.E.C.L.C. APRIL 2018

• PREPARING FOR MANDATORY DATA BREACH REPORTING AND RECORD-KEEPING •

Jonathon Ward, Associate, DLA Piper
© DLA Piper, Calgary

Jonathon Ward

There was no shortage of high-profile data incidents in 2017, with massive increases in the number of data breaches over 2016 in both the United States and Canada. The increase in breaches, combined with significant recent developments in Canadian privacy legislation, have privacy issues as a top priority for many organizations this year.

It is difficult for companies to keep up with the ever-increasing regulatory burden under privacy legislation. As cyber security issues, data collection and data breaches increase, the legislation in turn becomes more robust. Even organizations that do not collect large amounts of personal information need to be aware of the legislative requirements, as employee information is subject to the same regulations.

CANADIAN PRIVACY LEGISLATION LANDSCAPE

In Canada, regulation of the protection of personal information for private-sector organizations is governed by either federal, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), or provincial legislation. Subject to some industry-specific exceptions, PIPEDA applies to all private-sector organizations, unless a province has enacted its own privacy laws that are substantially similar to PIPEDA (currently Alberta, British Columbia and Quebec), in which case the provincial legislation applies. In provinces with substantially similar legislation, PIPEDA will apply to personal information

• In This Issue •

INTERNET AND E-COMMERCE LAW IN CANADA

Internet and E-Commerce Law in Canada is published six times per year by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

ISBN 0-433-42472-9 (print) **ISSN 1494-4146**
ISBN 0-433-44674-9 (PDF)
ISBN 0-433-44385-5 (print & PDF)

Subscription rates: $275.00 per year (print or PDF)
$400.00 per year (print & PDF)

General Editor
Professor Michael A. Geist
Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

Please address all editorial inquiries to:

LexisNexis Canada Inc.
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: ieclc@lexisnexis.ca
Web site: www.lexisnexis.ca

Note: This newsletter solicits manuscripts for consideration by the Editors, who reserves the right to reject any manuscript or to publish it in revised form. The articles included in the *Internet and E-Commerce Law in Canada* reflect the views of the individual authors and do not necessarily reflect the views of the editorial board members. This newsletter is not intended to provide legal or other professional advice and readers should not act on the information contained in this newsletter without seeking specific independent advice on the particular matters with which they are concerned.

collected through interprovincial and international transactions, such as customer information collected through global internet sales.

In June of 2015, PIPEDA saw significant amendments under the *Digital Privacy Act*, including the introduction of mandatory breach reporting and record-keeping. The amendments introducing mandatory breach reporting and record-keeping are not yet in force, but many expect they will be introduced in the Spring of 2018. On September 2, 2017, the Canadian government published the *Breach of Security Safeguards Regulations*, which provides further details on mandatory breach reporting and record-keeping.

MANDATORY BREACH REPORTING

As organizations plan for upcoming quarters it is important to be cognizant of how the privacy regulatory landscape will change with the coming amendments to PIPEDA. Under the new mandatory breach reporting and record keeping provisions, PIPEDA will require that any “breach of security safeguards involving personal information” be disclosed where there is a “real risk of significant harm”. Once it is determined a data breach has occurred, an organization must disclose the breach “as soon as feasible”.

Alberta’s *Personal Information Protection Act* (“PIPA”) is the only piece of Canadian legislation currently requiring mandatory notification of data breaches. PIPA requires disclosure of a breach where there is a real risk of significant harm to an individual, which must occur without unreasonable delay. There are many similarities between the reporting provisions of PIPA and PIPEDA and we can look to PIPA in assessing how mandatory reporting will occur.

Learning of a potential data breach can be overwhelming, particularly for small and medium sized businesses without in-house privacy staff. The first step upon learning of a data breach is to determine whether the information disclosed creates a real risk of significant harm. The “real risk” criteria focuses on the context of the breach. Central to this determination is what caused the breach. Organizations must ask, was the breach due to inadvertence, for example an employee leaving their laptop containing employee personal information in an airport, or was the breach intentional, such as a hacker gaining access to the company's data? The context of the breach largely informs whether there is a real risk that the personal information disclosed is going to be misused.

The "substantial harm" criteria relates to the nature of the information disclosed. Organizations must ask, was the personal information disclosed a list of customer names, or was it employee names, SIN numbers and health information? Some information is clearly more personal and potentially harmful than others, such as a SIN versus an email address. However, it is also important to consider the scope of the breach, as multiple pieces of less private information can add up to be more potentially damaging. For instance, an individual's first and last name, address and drivers licence number, which can facilitate identity theft, could be more potentially harmful than an individual's SIN number alone.

Privacy legislation requires timely disclosure, but it is important to take reasonable steps to assess the risk at the outset. Determining the exact nature of a potential data breach can avoid disclosing incorrect information and needlessly worrying customers and employees. Effective policies and procedures increase the efficiency of this analysis and significantly reduce a company's potential exposure to liability in the event of a data breach.

MANDATORY DATA BREACH RECORD-KEEPING

The amendments to PIPEDA will also require organizations to maintain records of every unauthorized disclosure of personal information for two years after it occurs. There is no threshold associated with this requirement, so even records relating to data breaches with no risk of significant harm must be kept. This record-keeping requirement is a significant regulatory burden on corporations, particularly smaller organizations without dedicated privacy departments. However, with potential fines of up to $100,000 under both PIPA and PIPEDA, organizations are well advised to ensure compliance with privacy requirements.

In addition to the OPC, who may request to inspect a corporations breach records at any time, the list of those interested in reviewing breach records includes:

- potential cyber insurers — who will almost certainly request to review an organizations breach records when negotiating premiums;
- service providers — who will likely be asked to disclose their breach records when negotiating service agreements with customers; and
- parties to corporation transactions — who are increasingly requesting disclosure from one another as part of transactional due diligence.

CANADIAN CHANGES REFLECTING GLOBAL TRENDS

The increasing importance of privacy legislation compliance in today's economy is compounded by global developments, namely the European Union's introduction of the General Data Protection Regulation ("GDPR"). The GDPR will impose a uniform, and stringent, privacy standard on all companies that process or hold the personal information of anyone residing in the EU, regardless of the company's location.

As the economy continues to become more digital, with data playing a central role, the regulatory requirements surrounding that data will grow more stringent. Mandatory breach reporting and record-keeping will soon be the global standard and organizations are well served by a pro-active approach and an early emphasis on privacy policies and procedures. Compliance with global privacy standards is a cost of doing business today and the up-front costs of a pro-active approach to privacy are far outweighed by the potential pitfalls of sub-par privacy procedures and policies.

• CRYPTOCURRENCY ASSETS UNDER INSOLVENCY AND PERSONAL PROPERTY SECURITY LAW •

Timothy Jones, Associate and Dillon Collett, Student-at-Law, Aird Berlis LLP

Timothy Jones

Dillon Collett

Encrypted digital currencies ("cryptocurrencies"),[1] particularly Bitcoin, have recently become the target of enormous international speculation and market scrutiny. Some expect cryptocurrency payments and other transactions tracked via distributed ledger technology ("DLT", of which "blockchain" technology is one example) to be the future of commercial interaction. The theory is that cryptocurrencies could become "the holy grail of commerce – a payment system that would eliminate or minimize the roles of third party intermediaries".[2]

Is Canadian commercial law ready for this brave new world? Specifically, how do the laws governing debtor-creditor relationships apply to cryptocurrencies?

This article discusses the legal characterization of cryptocurrency units ("tokens"), their utility as a commercial payment medium given current Canadian personal property security law, and, in light of several high-profile insolvencies of the platforms on which cryptocurrencies are traded ("exchanges"), the treatment of tokens in insolvency scenarios. It considers the following questions:

- Does Canadian law treat digital currencies as cash, commodities or something else?
- Can a lender take security over a borrower's cryptocurrency assets — and if so, can a third party accept a payment in tokens free and clear of the lender's security interest?
- If a token exchange or wallet provider enters insolvency proceedings, does a tokenholder have a creditor claim or a property claim in the estate?
- If such a claim is recoverable, will the tokenholder get tokens back or only their pre-filing cash value — which may be considerably lower or higher than the present-day value of the token in a volatile market?
- What challenges does an insolvency professional face in dealing with cryptocurrency assets?

As the term would suggest, cryptocurrencies are designed as payment systems, not simply targets for speculative investment (as Bitcoin is arguably becoming). The high valuations of many cryptocurrencies only make sense if they can one day be exchanged for a range of goods and services, circulating without friction and with finality and certainty.

Unfortunately, North American personal property security law does not treat cryptocurrencies as negotiable instruments, and cryptocurrency assets (or claims against them) can be challenging to realize in insolvency scenarios. Both of these problems obstruct the mainstream adoption of cryptocurrencies as payment systems.

THE LEGAL CHARACTERIZATION OF TOKENS

As Aird & Berlis partner Donald B. Johnston has written, the legal characterization of cryptocurrency tokens is controversial, unsettled and variable by jurisdiction.[3]

Many cryptocurrencies, as the term suggests, are designed to function as digital currency or money. But is a token *money*? Is it even the holder's *personal property* at all?

The Canada Revenue Agency characterizes[4] cryptocurrencies as commodities rather than currency for tax purposes and applies the so-called "barter rules" to transactions in cryptocurrencies. Indeed, at the moment, a commodity like gold is a reasonable analogy to a cryptocurrency like Bitcoin; it is "mined", it is used as a target of speculation, and tokens, like gold certificates or gold itself, are somewhat fungible and occasionally used for commercial payments.

A Bank of Canada position paper[5] expressed a similar viewpoint in 2014, positing that no form of cryptocurrency had, at that time, the essential qualities that are ascribed to money: (i) a medium of exchange, (ii) a unit of account, and (iii) a stable store of value. Despite Bitcoin's price spike, this analysis still rings true.

Personal property security law in Canada (and its analogous legislation in the U.S.), as currently constituted, does not include tokens in the definition of "money", but rather treats them as "intangibles", a classification that severely restricts their utility as a mainstream payment medium and as an asset that can easily be made the subject of a security interest.

Other jurisdictions may differ significantly in their legal characterization of tokens. Indeed, a Japanese court has held that, under Japan's Civil Code, tokens are not capable of personal ownership at all — a holding that had significant implications for creditors in an insolvency proceeding, as this article discusses subsequently.

SECURED TRANSACTION ISSUES — THE "ACHILLES HEEL" OF CRYPTOCURRENCY ADOPTION?

Currently, there is no administrative guidance or case law that specifies how cryptocurrency tokens should be treated for the purposes of Canadian personal property legislation (in each common-law province, the "PPSA"). No PPSA has yet added definitions or collateral classifications that directly reference cryptocurrency assets.[6] Under the current definitions in the PPSA, a cryptocurrency token held directly by its owner would fall into the catch-all category of "intangible". The definitions under the U.S.' *Uniform Commercial Code* ("UCC") are similar and point to the same conclusion.[7]

As currently defined, cryptocurrency tokens would not qualify as "money". Money is a defined term under the PPSA, referring to a medium of exchange adopted by a government as part of a country's currency.[8] (Interestingly, this suggests that if a nation nominally adopted Bitcoin as an official form of legal tender, the treatment of cryptocurrency assets under personal property security law could shift dramatically.)

Similarly, unless a court were to find that the "distributed ledger" entry underlying the token constitutes "writing" for the purpose of the *Bills of Exchange Act* (Canada) or the PPSA, which seems unlikely, a token could not be "chattel paper" or an "instrument". It is possible to register shares of companies on the blockchain, as Mr. Johnston discusses in another recent article.[9] In such a circumstance, the PPSA's rules on uncertificated securities would likely apply.[10] However, as tokens do not meet the definition of "security" in the *Securities Transfer Act*, they are not "investment property".[11] By process of elimination then, tokens should likely be categorized as "intangibles".

This definitional question has commercial consequences. Intangibles are described as "the least negotiable of all UCC [and PPSA] forms of property".[12]

The PPSA allows money, cheques and other negotiable instruments to circulate free and clear of security interests.[13] The public policy behind this rule is obvious. Similarly, purchasers of goods, chattel paper, instruments and some other categories of collateral are able to take the purchased item free and clear of a security interest if the transaction is made in the ordinary course of business, with or without knowledge of the security interest.[14] (This was also the rule in s. 2 of the old Ontario *Factors Act*, which predates the PPSA.) Under the PPSA (and UCC), purchasers of intangibles have no such protections.

So, suppose a debtor has granted to a lender a security interest over all its present and after-acquired property (a common practice) — including, of course, intangibles. If the debtor then pays a third party with a token to which the lender's security has attached, the lender has a superior claim to the token as against the third party payee. DLT makes these payments almost infinitely traceable on a public register, accessible by anyone with the correct software and know-how.

This is obviously a problem for recipients of cryptocurrency payments — no third party would responsibly accept a payment that could be clawed back by the payor's secured creditor at any time.

For these reasons, some commentators have described the existing North American personal property security regime as an "Achilles heel" for the future of cryptocurrencies — at least for their utility as payment systems as opposed to commodities or targets of speculation.[15]

ARE TOKENHOLDERS PROTECTED IN INSOLVENCY?

Cryptocurrency deposits, unlike most Canadian bank deposits, are not insured. And, as noted above, the position of secured creditors in relation to tokens is uncertain. Blockchain technology adds further practical challenges, not to mention a steep learning curve for insolvency professionals and their consultants. As a result, it is difficult to predict outcomes in insolvency scenarios, a state of play that makes it difficult to imagine sophisticated commercial players doing business entirely in digital currencies, or investing in companies that do so.

Recent high-profile insolvencies of cryptocurrency exchanges show that these concerns are not simply theoretical. Fraud, theft and cybersecurity continue to be live issues in the space.

There have been some very public examples. In 2014, the largest bitcoin exchange at the time, Mt Gox, filed for bankruptcy[16] after hackers allegedly misappropriated US$467.5 million worth of bitcoin. The bankruptcy trustee of Mt Gox was able to obtain an order from the Ontario Superior Court of Justice recognizing the Mt Gox bankruptcy proceedings in Japan. Cryptsy, a U.S.-based exchange, was placed into a court-appointed receivership by certain Cryptsy users in May of 2016, amid allegations of fraud and misappropriation of tokens by the exchange's founder.[17] A South Korean exchange, YouBit, declared bankruptcy in December 2017 after another bitcoin heist, this time with North Korea allegedly implicated in the theft.[18]

An interesting question in any insolvency scenario involving an exchange is whether tokenholders can expect a proprietary remedy in tokens, or merely an unsecured creditor claim for the cash value of the tokens at the time of insolvency.

This question was at issue in the Mt Gox proceedings. A former exchange customer brought a lawsuit against the trustee seeking a return of the bitcoins that Mt Gox held on its behalf. The Tokyo District Court held that under the applicable provisions of Japan's Civil Code, the creditor did not (and could not) have proprietary ownership in the bitcoin on deposit (which would lead to recovery of the tokens themselves, *in specie*). The creditor instead only had a contractual right to the return of the value of the tokens (provable as an unsecured debt in bankruptcy).

Since no proprietary claims were possible, the creditor claims of Mt Gox tokenholders were valued at approximately US$438, the pre-filing value of bitcoin. Not only did the price of bitcoin subsequently skyrocket, but the trustee was able to recover approximately 202,185 of the supposedly-stolen bitcoins, at that time worth almost $2 billion. The subsequent bitcoin price spike resulted in the value of the estate's assets vastly exceeding total claims of its creditors, a surplus that could result in a multi-billion dollar windfall for the majority shareholder of Mt Gox, despite his alleged acts having caused the loss in the first place (although this is not to say that such windfall could not eventually be accessed by Mt Gox tokenholders by way of a personal claim).

As a result, some Mt Gox creditors have sought a conversion of the bankruptcy proceeding into "civil rehabilitation" (essentially, Japan's analogue to the *Companies' Creditors Arrangement Act* or Chapter 11) that could result in a plan of compromise by which creditors could recover a *pro-rata* share of their original holdings in the form of bitcoin rather than yen, allowing them to benefit from the massive appreciation in bitcoin value post-filing, as opposed to recovering an amount in yen that is capped at the pre-filing value of bitcoin.[19]

The Mt Gox situation should not imply that tokenholders can *never* assert a proprietary claim to tokens deposited in an exchange. As Japanese attorney Akihiro Shiba aptly points out in an article for trade publication Coindesk in which he discussed the implications of the case under Japanese law, the "ownability" of bitcoins could be decided differently under Japanese law if the tokenholder's "private key" were controlled and managed by the customer (in the Mt Gox scenario, Mt Gox managed tokenholders' private keys). Outcomes would vary according to the facts and to the jurisdiction in which the issue was heard.

Whether under the Japanese Civil Code or otherwise, there may be future cases in which tokenholders will be able to assert a trust or other proprietary remedy to recover, in full, their tokens held on a third-party exchange — it would depend on the structure of the relationship between the user and the platform and how the courts choose to characterize that relationship.

CHALLENGES FOR INSOLVENCY PROFESSIONALS

Most insolvency professionals are familiar with the vagaries of tracing and recovering traditional currencies. However, digital currencies create even more complex issues for insolvency professionals.

At the outset of a mandate, bringing assets under control presents a significant challenge. Even if a debtor's anonymous "public key" could be determined (which would allow for the debtor's transactions on the distributed ledger to be followed), the debtor's cooperation would be required in order for a receiver or trustee to obtain and use the debtor's "private key" and thus control the assets. Many tokenholders wisely opt to store their digital credentials offline and in secure areas. In some extreme cases, tokenholders with significant holdings are apparently storing their "private key" on an offline computer locked underground in a decommissioned Swiss military bunker due to security concerns.[20] Further, although DLT is intended to ensure the integrity and traceability of assets, the preponderance of fraud and hacking in this area, as seen in the "loss" of over 2 million tokens in the Mt Gox scenario, suggests that the integrity of the system may not be guaranteed.

The Cryptsy receivership illustrates the practical difficulties of recovering assets — a process described by the receiver as "lengthy and tedious" in its fourth report to court, and detailed in the report as follows:

(i) Cryptsy had an entire array of servers running the wallets and syncing block chains, as well as a team of employees that maintained smooth operation of the wallets; (ii) there are numerous wallets containing different alternative coins that are under my control; (iii) each alternative coin wallet requires its own unique software to run its own block chain; (iv) the receivership estate has billions of individual alternate coins under its control, each coin has its own block chain, and the entire block chain history needs to be linked with the recovered wallets in order to verify the current balance of coins in that wallet; and (v) due to the fact that Cryptsy was an exchange, each wallet contains hundreds of thousands of entries for transactions, and in many cases, the wallets have become corrupted, clogged and unresponsive, requiring more time and effort to recover remaining coins in that wallet.[21]

In addition to these hair-raising technological challenges, Cryptsy's founder attempted to obfuscate or dissipate the assets (destroying servers, starting up a new exchange in China, buying diamond rings and houses with $USD derived from Cryptsy tokens, and other such roguery). To recover assets, the cooperation of dozens of international non-parties (coin exchanges, banks, etc.) was required.

Even if tokens can be recovered, can they be liquidated? Not all tokens are created equal in terms of discoverability and fungibility. At present, there is a strong market for bitcoin, but there are a great many alternative cryptocurrencies that have low to medium liquidity, and very little demand.[22]

Unwinding fraudulent conveyances and other reviewable transactions is another challenge. The anonymity of the blockchain makes it hard to link a particular transaction to a particular recipient, and unwinding one transaction would be a technical challenge that would affect all subsequent transactions on the same "block", if any.[23]

Cryptocurrencies, by design, are intended to be borderless solutions to payment problems, attracting worldwide users, many of whom are tech-savvy and comfortable organizing themselves online.[24] Resulting insolvencies will likely be international, and the location of the foreign main proceeding (being the jurisdiction where the key court decisions are made, and therefore the jurisdiction where the status of cryptocurrency assets under local law will influence results the most) may have major implications for creditor recovery. Forum shopping can be expected.

CONCLUSION

DLT is poised to disrupt any number of commercial frameworks, and debtor-creditor law is no exception. As more and more cases of fraudulent behaviour and/or insolvency on cryptocurrency platforms make their way through the world's insolvency systems, it will be of great interest to see how courts and legislators respond. In the interim, the varying legal treatments of property ownership and security interests could be barriers to the adoption of digital currencies as mainstream payment systems.

Canada can take the lead by reforming personal property security law to recognize the negotiability and fungibility of blockchain assets, while also ensuring that insolvency law protects the reasonable expectations of tokenholders and provides a sensible solution to the real possibility of a cryptocurrency crash. One option is a separate collateral classification for tokens; the "control" regime already in place for securities accounts could be an excellent starting point for a regulatory system that allows secured cryptocurrency assets to retain their liquidity and negotiability. Conversely, expanding the definition of "investment property" under the PPSA to potentially include certain cryptocurrencies (perhaps only tokens issued pursuant to a regulated ICO), either through legislative amendment or judicial interpretation, could lead to a similar result.

In any event, there is no doubt that the world is watching closely to see whether cryptocurrencies can become more than a target of speculation and function as the borderless, low-friction payment systems that many of them were intended to become. The treatment of cryptocurrency units under commercial law, in Canada and elsewhere, will be crucial to the ultimate outcome.

* The authors thank Donald B. Johnston, Sanjeev Mitra, Steven L. Graff, Ian Aversa and Jeremy Nemers, each of Aird & Berlis LLP, for their contributions to and commentary on this article.

[***Timothy Jones*** *is a member of the Aird & Berlis Financial Services Group. His practice focuses on debt financing transactions, including secured lending and debt restructuring, as well as insolvency-related business transactions.*

Dillon Collett *is an articling student at Aird & Berlis. He holds a BA from Concordia University and recently graduated from University of Toronto Faculty of Law.*]

[1] Terms such as "cryptocurrency," "bitcoin", "blockchain" and "token" are industry jargon, so some notes on terminology follow. Johnston has written a helpful article

explaining the "blockchain" as a type of "distributed ledger technology" that provides "a bullet-proof record of proven transactions that everybody (with the appropriate software) can check": see Johnston, Donald B., "What is the Law of the Blockchain?" (March 10, 2016), online: Aird & Berlis LLP http://www.airdberlis.com/insights/blogs/thespotlight/post/ts-item/what-is-the-law-of-the-blockchain. Bitcoin and other cryptocurrency providers offer digital payment methods that operate via DLT, as another article of Johnston's describes: see Johnston, Donald B., "Digital Currencies" (May 6, 2016), online: Aird & Berlis LLP http://www.airdberlis.com/insights/blogs/startupsource/post/ss-item/digital-currencies. An individual unit of Bitcoin currency is called a bitcoin. An individual unit of digital currency on the Ripple platform (Ripple is currently second to Bitcoin in market penetration) is "XRP". This article refers to individual cryptocurrency units as "bitcoins" if specific reference is being made to the Bitcoin platform or, if reference is made to units of cryptocurrency in general, as "tokens".

[2] Schroeder, Jeanne L., "Bitcoin and the Uniform Commercial Code" (August 22, 2015). Cardozo Legal Studies Research Paper No. 458, at p. 3. Available at SSRN: https://ssrn.com/abstract=2649441 or http://dx.doi.org/10.2139/ssrn.2649441.

[3] Johnston, Donald B., "Digital Currencies", (May 6, 2016), online: Aird & Berlis LLP http://www.airdberlis.com/insights/blogs/startupsource/post/ss-item/digital-currencies.

[4] Canada Revenue Agency Fact Sheets, "What You Should Know About Digital Currency" (December 3, 2014), online: Government of Canada https://www.canada.ca/en/revenue-agency/news/newsroom/fact-sheets/fact-sheets-2013/what-you-should-know-about-digital-currency.html.

[5] Bank of Canada, "Decentralized E-Money (Bitcoin)" (April 2014), online: Bank of Canada http://www.bankofcanada.ca/wp-content/uploads/2014/04/Decentralize-E-Money.pdf.

[6] On this issue, the PPSAs in each province are fundamentally similar. Article 9 of the *Uniform Commercial Code* is similarly structured, so the conclusion in this article — that cryptocurrencies are intangibles for the purpose of personal property security legislation — would likely also apply in the U.S. For a detailed analysis in the U.S. context, see Schroeder, *supra*. note 4.

[7] Schroeder, *supra.* note 4 at p. 5.

[8] *Personal Property Security Act*, R.S.O. 1990, c. P.10, s. 1(1).

[9] Johnston, Donald B., "How Blockchains Will Change Stockholder Democracy" (December 14, 2017), online: Aird & Berlis LLP http://www.airdberlis.com/insights/blogs/TheSpotlight/post/ts-item/how-blockchains-will-change-stockholder-democracy.

[10] From a policy perspective, the rules applicable to uncertificated securities (see s. 30.1 of the PPSA — the party with control of the tokens would have priority over a security interest of a secured party that does not have control of the tokens) may be the best way to accurately capture and support how blockchain assets currently circulate, particularly since control can exist by way of a third-party intermediary (in the investment property regime, a "securities intermediary" *i.e.*, a broker; with Bitcoin, the wallet provider or exchange). This makes them freely tradeable, as the party controlling the tokens, even through a wallet provider, is assured of priority in most cases.

[11] It is arguable, however, that tokens issued pursuant to an "initial coin offering", or "ICO" and held by a third-party exchange could qualify as "investment property" under the PPSA definition if the ICO was lawfully regulated by a securities regulator. In this case, again, the tokens would be subject to the control regime described in the immediately preceding footnote.

[12] Schroeder, *supra*. note 3 at p. 12.

[13] *Personal Property Security Act*, R.S.O. 1990, c. P.10, s. 29.

[14] *Ibid.*, s. 28.

[15] Lawless, Bob, "Is UCC Article 9 the Achilles Heel of Bitcoin?" (March 10, 2014), online: Credit Slips http://www.creditslips.org/creditslips/2014/03/is-ucc-article-9-the-achilles-heel-of-bitcoin.html.Again, the control regime applicable to certificated and uncertificated securities could be a solution.

[16] Mt Gox Bankruptcy Trustee Press Release (May 25, 2016), online: Mt Gox https://www.mtgox.com/.

[17] Case website of James D. Sallah, Court-Appointed Receiver for Project Investors, Inc. d/b/a Cryptsy, online: Cryptsy Receivership http://cryptsyreceivership.com/. See also Cryptsy Cryptocurrency Class Action Settlement Notice, online: Cryptsy Settlement http://www.cryptsysettlement.com/.

[18] Gallagher, Sean, "North Korea suspected in latest bitcoin heist, bankrupting Youbit exchange" (December 20, 2017), online: Ars Technica https://arstechnica.com/tech-policy/2017/12/north-korea-suspected-in-latest-bitcoin-heist-bankrupting-youbit-exchange/.

[19] Meyer, David, "After Bitcoin Spike, MtGox Creditors Want to Yank the Failed Exchange Out of Bankruptcy" (December 13, 2017), online: Fortune http://fortune.com/2017/12/13/bitcoin-mtgox-bankruptcy-creditors/.

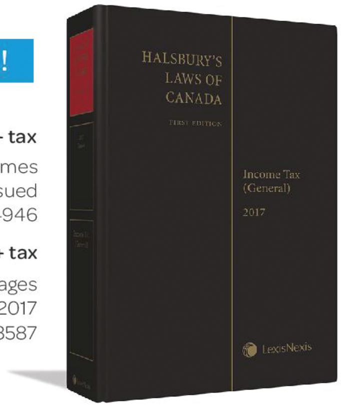
[20] Wong, Joon Ian "Switzerland's bitcoin bunker" (November 29, 2017), online: Quartz Media LLC https://qz.com/email/quartz-obsession/1130471/.

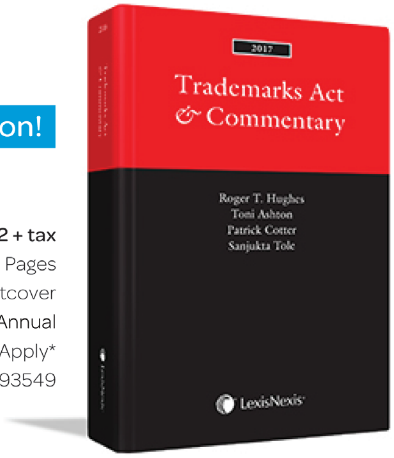
[21] Fourth Report of James D. Sallah, Court-Appointed Receiver for Project Investors, Inc. d/b/a Cryptsy, online: Cryptsy Receivership http://cryptsyreceivership.com/v1/wp-content/uploads/2016/06/Fourth-Report.pdf.

[22] *Ibid.*, at p. 9.

[23] For details on the technical aspects of this process from the standpoint of the insolvency professional, see Møller, Charlotte & Claude Brown, "Insolvency of Virtual Currencies – a New Reality?" (June 2017), online: ReedSmith https://www.reedsmith.com/en/perspectives/2017/06/insolvency-of-virtual-currencies-a-new-reality.

[24] Cryptocurrency aficionados often frequent online forums such as Reddit. This can lead to highly organized, and highly disruptive, creditor committees. See, for example, the Subreddit for the Mt Gox proceedings, where tokenholders from all over the globe worked together to "crowdfund" litigation efforts, hire a Japanese representative counsel, and discuss legal issues — it is a fascinating, real-time insight into the workings of an organically-formed "creditors committee". See https://www.reddit.com/r/mtgoxinsolvency/.


HALSBURY'S
LAWS OF
CANADA
FIRST EDITION
Income Tax
(General)
2017
LexisNexis


2017
Trademarks Act & Commentary
Roger T. Hughes
Toni Ashton
Patrick Cotter
Sanjukta Tole
LexisNexis