DURAND
Avocats | Lawyers

Montreal, Canada, July 15, 2020

BY EMAIL : fsb@fsb.org

Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Subject : Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document[1] ("**Consultation**")

Dear Sirs and Madams :

We welcome the Financial Stability Board's ("**FSB**") invitation to respond to its Consulation on global stablecoin ("**GSC**") arrangements, and hope that the present submission will useful in your deliberations regarding the foregoing.

This submission forms part of a series of submissions filed before the Canadian Standing Committee of Finance (FINA)[2] in its statutory review of the *Proceeds of Crime and Terrorist Financing Act* (of which myself, David Durand, and Mr. Drew Dorweiler presented thereto) as well as IIROC/CSA[3] and IOSCO[4] consultation. A copy of our FINA submission is enclosed at Schedule 1[5] hereof; of which, our recommendations are found at Section 11 (at page 26) thereof, namely : concentrating regulatory efforts at the locus of cryptoasset transactions – the **convertibility mechanism**, as well as address **definitions of key terms**, such as commodity, currency, cryptoasset and securities.

INTRODUCTION

Little did we know the stir the Satoshi Nakatomo white paper[6] of October 2008 was going to create. Indeed the Nakatomo paper, cited over ten thousand times per Google®, has caused government, public and private sector, advocates, as well as the legal system to spend an incalculable amount of hours studying the attributes of cryptoassets and their impact on the financial system, monetary policy[7,8], data

[1] https://www.fsb.org/2020/04/addressing-the-regulatory-supervisory-and-oversight-challenges-raised-by-global-stablecoin-arrangements-consultative-document/.
[2] https://www.ourcommons.ca/Committees/en/FINA/StudyActivity?studyActivityId=9933703; Durand, D. and Dorweiler, D., "*Don't Block The Blockchain: How Canada Can Guard Against Money Laundering While Maintaining Global Competitiveness*" (July 2018), available at: https://www.ourcommons.ca/Content/Committee/421/FINA/Brief/BR10007367/br-external/IJWAndCoLtd-2018-09-17-Updated-Final-e.pdf.
[3] https://www.osc.gov.on.ca/documents/en/Securities-Category2-Comments/com_20190515_21-402_durandd_dorweilerd.pdf;
[4] https://www.iosco.org/library/pubdocs/627/pdf/Durand%20Morisseau%20LLP.pdf and Final Report FR02/2020, available: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf.
[5] https://www.durand-lex.com/blockchain-crypto-fintech.
[6] https://bitcoin.org/bitcoin.pdf.
[7] Perkins, David W., *Cryptocurrency: The economics of money and selected policy issues,* Report no. R-45427, Congressional Research Service (last updated April 9, 2020), available at: https://fas.org/sgp/crs/misc/R45427.pdf; Assenmacher, K., SUERF

DAVID DURAND, ATTORNEYS CORPORATION INC.
1255, Blvd. Robert-Bourassa, Suite 1500,
Montréal, Québec H3B 3X2
T. +1 (877) 490-1725 ext. 101 | F. +1 (877) 500-2520
info@durand-lex.com | www.durand-lex.com

and privacy law, amongst many other legal considerations. COVID-19 has only accelerated the push for an e-commerce and a cashless society[9,10].

Relevant highlights

- **there exists over 1500 types of cryptoassets**, with many more created monthly (*EY Cryptocurrencies and cryptoassets: Managing the new asset class,* published in early 2018)[11];

- **there exists over 500 crypto-exchanges** (*Report on International Bitcoin Flows 2013–2019*, published in the month of September 2019)[12];

- **new forms of cryptoassets** are being constantly being contemplated, such as : (i) central bank digital currencys' ("CBDC") ("to counter GSCs[13]"), (ii) amongst other forms of cryptoassets, as well as through (iii) various initiatives (e.g., "Digital Dollar Project"[14] for "needed dollar innovation"); and

- **Numerous studies on cryptoassets have been conducted by various stakeholders**, including, for example : the BIS[15], CPMI[16], FATF, securities regulators (U.S. SEC[17], Ontario Securities

---

Policy Note, Issue no. 165 (May 2020), available at: https://www.suerf.org/docx/f_ec9b954aefd15bc4fffe92f5683d1dd2_13537_suerf.pdf.

[8] Benigno, Pierpaolo, Monetary Policy in a World of Cryptocurrencies (February 2019). CEPR Discussion Paper No. DP13517, Available at SSRN: https://ssrn.com/abstract=3332321.

[9] https://www.europarl.europa.eu/thinktank/de/document.html?reference=EPRS_BRI%282020%29649341.

[10] According to a Payments Canada report "75 per cent of Canadians spending less than pre-pandemic; 62 per cent using less cash; 42 per cent avoid shopping at places that don't accept contactless payments", available at: https://www.payments.ca/about-us/news/covid-19-pandemic-dramatically-shifts-canadians'-spending-habits (published on May 13, 2020), as cited in a CTV News article, available at: https://www.ctvnews.ca/health/coronavirus/are-canadians-ready-to-go-cashless-after-coronavirus-1.4970838 (published on June 5, 2020). In Canada, it has created the resurgence of discussions on open banking (*cf.* https://financialpost.com/opinion/open-banking-would-help-the-recovery, published on June 5, 2020, and https://financialpost.com/technology/canadas-refusal-to-embrace-open-banking-puts-us-behind-yet-another-curve, published July 10, 2020).

[11] https://www.ey.com/Publication/vwLUAssets/ey-cryptocurrencies-and-cryptoassets-managing-the-new-asset-class/$File/ey-cryptocurrencies-and-cryptoassets-managing-the-new-asset-class.pdf.

[12] https://crystalblockchain.com/assets/reports/International%20Bitcoin%20Flows%20Report%20for%202013-2019%20-%20by%20Crystal%20Blockchain,%20Bitfury.pdf.

[13] According to the Bank of Canada's Staff Analytical Note 2020-5, "[i]ssuing a central bank digital currency (CBDC) could potentially counter the use of Libra. A CDBC could offer a new digital payment rail and an asset for real-time final settlement between individuals—a similar niche that physical cash has today. As noted by He (2018), modern monetary policy, based on the collective action of monetary policy committees and supported by central bank independence, is likely to offer the best hope for maintaining a stable unit of account. However, central banks also need to continue to make central bank money attractive as a payment instrument", available at: cf. https://www.bankofcanada.ca/2020/02/staff-analytical-note-2020-5/.

[14] The Digital Dollar Project proposes "*to study potential avenues to utilize U.S. digital dollar tokenization and its implications on the U.S. and global economic and financial systems*", available at : https://www.digitaldollarproject.org.

[15] *Designing a prudential treatment for crypto-assets*, available at https://www.bis.org/bcbs/publ/d490.htm.

[16] On July 13, 2020, the CPMI released its report entitled "*Enhancing cross-border payments: building blocks of a global roadmap – Stage 2 report to the G20 - Technical background report*" (July 2020, CPMI Papers, no. 193), at section 2.5 and *ff.,* para. 67, and Schedule 18.

[17] https://www.sec.gov/ICO.

DAVID DURAND, ATTORNEYS CORPORATION INC.
1255, Blvd. Robert-Bourassa, Suite 1500,
Montréal, Québec H3B 3X2
T. +1 (877) 490-1725 ext. 101 | F. +1 (877) 500-2520
info@durand-lex.com | www.durand-lex.com

Commission, IIROC/CSA, IOSCO, etc.), U.S. CFTC[18], the FCA (U.K.)[19], IMF[20], central banks, amongst many others; thereby leading to a lack of harmonization of cryptoasset taxonomy.

As a result of the increasing number of stakeholder opinions, including those of VASPs (e.g., exchanges, custodians, *etc.*) and unsettled issues of cryptoasset taxonomy, a "**tug of war**" as to who should regulate said cryptoassets (or under which regulators' purview (or competence) should the cryptoasset fall under), has arisen and caused, for instance (a) a lack of harmonization of cryptoasset taxonomy, as well as (b) litigation[21]. Indeed, a cryptoasset can exhibit one or more functions or features (or hybrid nature thereof), e.g., (i) a commodity, (ii) currency, (iii) a security, or (iv) an alternative form (e.g., form of payment).

HIGH-LEVEL RECOMMENDATIONS

As the FSB explores GSC arrangements, we respectfully submit that it should: (i) address and/or (ii) provide guidance with respect to the following important issues, namely:

1. **Cryptoasset taxonomy**, and establishing the parameters that allows the ecosystem to distinguish GSCs from other types of crypto-assets, in particular securities; such to determine : (a) the appropriate regulatory treatment of said cryptoasset, and (b) level of oversight required for said cryptoasset, in a proportionate manner;

2. **Cross-border data transfers** and determine how data, including personal information (if any), is collected, stored, used and processed by the ecosystem (e.g., issuers, custodians, wallet holders, exchanges, *etc.*) so as to ensure compliance with national **data privacy laws**[22];

3. **Cybersecurity** and identify which information security (IS) protocols are to be used for purposes of dealing in cryptoassets; such from "source to exit" point(s) (e.g., from issuance to use of the

[18] https://www.cftc.gov/PressRoom/PressReleases/8139-20.
[19] https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime.
[20] Cuervo, C. et als., *Regulation of Crypto Assets*, available at: https://www.imf.org/en/Publications/fintech-notes/Issues/2020/01/09/Regulation-of-Crypto-Assets-48810.
[21] *3iQ Corp (Re)*, 2019 ONSEC 37 (CanLII), http://canlii.ca/t/j34bz, wherein it is written at para. [85], *in orbiter*: "Like any valuable commodity, I accept that bitcoin can be stolen or lost. The Applicants also concede that point. But Staff did not establish that Cidel or Gemini, specifically, do not follow sufficient practices for safeguarding bitcoin. Rather, Staff relies on evidence of examples of losses incurred by crypto□asset trading platforms, all but one of which were unregulated and most of which involved hacks of hot wallets. I am not persuaded that there was sufficient evidence that professional, regulated crypto□asset custodians, like Gemini, have suffered losses of customer assets." In the United States, many claims have filed against crypto firms, *cf.* https://www.coindesk.com/top-crypto-firms-including-binance-civic-tron-targeted-in-flood-of-lawsuits (published April 6, 2020, with respect to Binance, Civic, Tron, *etc.*), https://www.reuters.com/article/legal-us-otc-telegram/sec-wins-injunction-against-telegram-blockchain-launch-in-key-ico-case-idUSKBN21C3N0 (Published May 12, 2020, with respect to Telegram Open Network ("TON")), https://www.sec.gov/news/press-release/2020-153 (published July 13, 2020, with respect to an App Developer for Unregistered Security-Based Swap Transactions), amongst many other examples), as well as https://www-coindesk-com.cdn.ampproject.org/c/s/www.coindesk.com/cftc-charges-florida-resident-with-defrauding-crypto-investors-out-of-1-6m?amp=1 (Published April 16, 2020), in which the CFTC charged a Florida resident with defrauding crypto investors our of $1.6M USD.
[22] Data protection laws of the World – Full handbook (March 2019, available at: https://iapp.org/media/pdf/resource_center/Data-Protection-Full.pdf.

DAVID DURAND, ATTORNEYS CORPORATION INC.
1255, Blvd. Robert-Bourassa, Suite 1500,
Montréal, Québec H3B 3X2
T. +1 (877) 490-1725 ext. 101 | F. +1 (877) 500-2520
info@durand-lex.com | www.durand-lex.com

GSC), especially considering the increase of hacking events[23,24,25], including phishing[26] and ransomware[27] attacks. In this regard, various protections should be explored, such as : SOC and PCI-DSS (payment security) compliance and the role of encryption in data protection "in transit" and "at rest"[28];

4. **Digital identification**, and providing guidance[29] to the ecosystem with respect to acceptable digital identification practices for purposes of dealing in cryptoassets, such within the proposed GSC framework;

5. **International coordination.** For stablecoins that have cross-application or global reach, having a globally consistent regulatory approach on stablecoins regulatory oversight is crucial to foster the development of a globally consistent regulatory treatment of cryptoassets, including GSCs.

RESPONSES TO QUESTIONS

1. **Do you agree with the analysis of the characteristics of stablecoins that distinguish them from other cryptoassets?**

In as long as there is an unresolved "**tug-of-war**" between securities and ML/TF regulators' with respect to cryptoasset taxonomy (also referred to as "definitional issues" of said cryptoasset), including GSCs, and what falls within their respective regulatory baskets, resolution, at the risk of stifling innovation, will be difficult. By way of example:

(i) the FATF has indicated that "it is clear that the revised FATF Standards apply to so-called stablecoins" (at para. 48 of the *FATF Report to G20 on So-Called Stablecoins*); said GSCs defined as being : (i) centralized (at paras. 53 and *ff.* thereof), or (ii) decentralized (at paras. 64 and *ff.* thereof);

(ii) IOSCO takes the position that GSC initiatives may also fall under securities regulators' purview[30], as they "…depending on their structure, present features that are typical of

[23] https://www.wired.com/story/cryptocurrency-hardware-wallets-can-get-hacked-too/ (Published on May 12, 2020) ("Cryptocurrency Hardware Wallets Can Get Hacked Too -
New research shows vulnerabilities in popular cold-storage options that would have revealed their PINs").
[24] https://cointelegraph.com/news/sim-swap-hackers-target-crypto-investors-cell-services-not-available (published June 16, 2020) ("SIM Swap Hackers Target Crypto Investors — Cell Services Not Available").
[25] https://cointelegraph.com/news/crypto-under-attack-the-five-worst-hacks-that-shook-the-crypto-world (published November 4, 2019 ("Crypto Under Attack: The Five Worst Hacks That Shook the Crypto World").
[26] https://cointelegraph.com/news/someone-has-been-on-a-200m-crypto-exchange-hacking-spree (published June 24, 2020) ("Someone Has Been on a $200M Crypto Exchange Hacking Spree").
[27] https://cointelegraph.com/news/crypto-ransomware-attacks-are-spreading-like-a-hacking-wildfire (Published June 17, 2020) ("Crypto-Ransomware Attacks Are Spreading Like a Hacking Wildfire").
[28] https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest.
[29] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html
[30] https://www.coindesk.com/global-stablecoins-may-be-subject-to-securities-regulation-says-iosco, and more particularly in IOSCO's Report OR01/2020 (released in the month of March 2020), available at : https://www.iosco.org/library/pubdocs/pdf/IOSCOPD650.pdf.

regulated securities or other regulated financial instruments or services." We **agree** with IOSCO's recommendation that a globally coordinated cross-sector response to the international regulatory challenges posed by GSCs should be explored.

In this regard, it is submitted that further guidance is required to clarify cryptoasset taxonomy so as to know in which circumstances cryptoassets, including GSCs, fall under the purview of a (1) ML/TF framework, or (2) a securities framework, as well as providing the criterion used to arrive to said classification[31,32] (or definitional issues)[33]. Criterion could include, without limitation :

(i) whether the GSC is to be used for domestic use, or for purposes of cross-border arrangements (or payments) involving multiple jurisdictions and counterparties;

(ii) the nature of the thing being sought in exchange for the GSC; for example whether : (a) it is accepted in exchange for goods and services (outside Platform) (e.g., a form of payment[34]),

[31] By way of example, Jens Lausen proposes a system of taxonomy based on dimensions and characteristics, such in Regulating Initial Coin Offerings? A Taxonomy Of Crypto-Assets, available at: https://www.researchgate.net/publication/333339654_REGULATING_INITIAL_COIN_OFFERINGS_A_TAXONOMY_OF_CRYPTO-ASSETS.

[32] This particular issue to taxonomy was also addressed within the European Commission Consultation on an EU framework for markets in crypto-assets (cf. https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-crypto-assets-consultation-document_en.pdf), as well as the numerous responses there, including the Financial Markets Law Commission, at section 2 thereof, available at: http://fmlc.org/wp-content/uploads/2020/03/FMLC_UP_11706611_v_1_Part-I-Response-to-EC-Consultation-on-regulating-cryptoassets-taxonomy.pdf, which provides of synopsis of the European institutions positions, e.g., U.K. FCA, ESMA, BIS, etc.

[33] See note 2, in particular Durand, D. and Dorweiler, D., "*Don't Block The Blockchain: How Canada Can Guard Against Money Laundering While Maintaining Global Competitiveness*" (July 2018), available at: https://www.ourcommons.ca/Content/Committee/421/FINA/Brief/BR10007367/br-external/IJWAndCoLtd-2018-09-17-Updated-Final-e.pdf. Further reference can also be made to Hossein Nabilou (2020) The dark side of licensing cryptocurrency exchanges as payment institutions, *Law and Financial Markets Review*, 14:1, 39-47, DOI: 10.1080/17521440.2019.1626545. Also, available at : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3346035, as it pertains to hybrid nature of cryptocurrencies, displaying the features of both commodities and curencies.

[34] However, in a 2019 publication regarding payments and market infrastructures, the ECB indicated:

> "Under the current regulatory framework, cryptoassets cannot be used to conduct money settlements in financial market infrastructures. The Principles for financial market infrastructures as defined by the international standard-setting bodies, the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions, and as transposed into EU legislation require the use of central bank money for settlement where practicable and available, and commercial bank money in all other cases. Therefore, being neither central bank money nor commercial bank money, cryptoassets cannot be used to carry out settlement in financial market infrastructures. Moreover, cryptoassets, as defined by the ECB CryptoAssets Task Force, cannot be settled by central securities depositories because they do not qualify as transferable securities under the European Central Securities Depositories Regulation.
>
> An operator of a financial market infrastructure has the flexibility to revise its risk-based participation requirements in the event that a participant involved in crypto-asset activities poses a threat to the system and its other participants. For instance, the Eurosystem, as an operator of TARGET2, is in a position to revise the TARGET2 Guidelines and to terminate participation on grounds of prudence. Should participants engage in crypto-assets activities to the point of raising concerns about the safety of the market infrastructure, this mechanism would allow the Eurosystem to keep it safe and sound.

(b) it confers a right to use a predefined product or service; (c) it is transferable (e.g., transferability of the GSC), (d) level of decentralization, (e) *etc.*;

(iii) network effect, including the potential for the issuer to scale;

(iv) whether the stablecoin ecosystem involves a wide range of market participants such as market maker, liquidity providers, custodians, VASPs (exchanges), *etc.*;

(v) the potential impact of the stablecoin arrangement on financial stability, monetary sovereignty and market integrity of the jurisdictions in which it operates;

(vi) Amongst other considerations identified the Consultation's participants.

2. Are there stabilisation mechanisms[35] other than the ones described, including emerging ones, that may have implications on the analysis of risks and vulnerabilities? Please describe and provide further information about such mechanisms.

No comment.

3. Does the FSB properly identify the functions and activities[36] of a stablecoin arrangement? Does the approach taken appropriately deal with the various degrees of decentralisation of stablecoin arrangements?

No comment.

4. What criteria or characteristics differentiate GSC arrangements from other stablecoin arrangements?

See our response to Question #1.

Cryptoassets in the clearing layer

At the moment, central counterparties (CCPs) based in the EU cannot provide clearing services for cryptoasset based products because they are not qualified as financial instruments either by the national competent authorities or the European Securities and Markets Authority. Even if CCPs were authorised to clear cryptoasset based products, they would need to comply with the demanding risk management requirements set out in the European Market Infrastructure Regulation, which would make it difficult or impracticable. Furthermore, CCPs are not permitted to use crypto-assets as collateral because they are not on the list of eligible collateral under the Commission Delegated Regulation (EU) 2016/2251."

Source : ECB - Crypto-assets – trends and implications (June 2019), available at : https://www.ecb.europa.eu/paym/intro/mip-online/2019/html/1906_crypto_assets.en.html.

[35] Section 1.1 of the FSB Consultative Document.
[36] Section 1.2 of the FSB Consultative Document and Table 1 thereof.

5. Do you agree with the analysis of potential risks to financial stability[37] arising from GSC arrangements? What other relevant risks should regulators consider?

In support of the FSB's position that "financial stability risks from the current use of stablecoins are currently contained", we draw your attention to :

- Paragraph 29 the *FATF Report to G20 on So-Called Stablecoins*, wherein it is stated "[w]hile the FATF has concluded that stability of value, on its own, does not pose a specific ML/TF risk, there may be ML/TF risks associated with the stabilisation mechanism specific to so-called stablecoins (e.g., by creating new mechanisms for market manipulation). Such risks remain theoretical at this point, but could be subject of more detailed analysis in the future should they emerge." (Our underlining);

- In *IMF FinTech Note 19/03 - Regulation of Crypto-assets* (December 2019)[38], wherein it is stated that cryptoassets do not pose a material risk to global financial stability at that time (*cf.* Page 6, right hand column) through page 7, left hand column);

- ECB Cryptoassets task force – Occasional Paper Series – *Cryptoassets : Implications for financial stability, monetary policy, and payments and market infrastructures* (#223/May 2019)[39], wherein it is written that cryptoassets' risks are limited or manageable (at the bottom of page 4 thereof).

We also wish to draw the FSB's attention to a recent *Cointelegraph* article, entitled *How Global Stablecoins Can Promote Financial Stability in the World* (published on June 27, 2020)[40], wherein the author argued that:

> "[…] Global stablecoins provide sophisticated market participants with cost-efficient means to quickly shift and rebalance their capital across global markets. This reduced friction promotes active market participation and more healthy price discovery mechanisms, which are the best defence against financial systemic risk.
>
> Included within these oversight bodies' notion of financial stability is the profitability and solvency of traditionally incumbent financial institutions. They worry that widespread adoption of global stablecoins could "further reduce bank profitability, potentially leading banks to take on more risks." But what domestic policymakers must recognize is that incumbent financial institutions are not synonymous with the broader financial system.

[37] Section 2 of the FSB Consultative Document, at p. 11.
[38] https://www.imf.org/~/media/Files/Publications/FTN063/2019/English/FTNEA2019003.ashx
[39] Manaa, Mehdi & Chimienti, Maria Teresa & Adachi, Mitsutoshi & Athanassiou, Phoebus & Balteanu, Irina & Calza, Alessandro & Devaney, Conall & Diaz Fernandez, Ester & Eser, Fabian & Ganoulis, Ioannis & , 2019. "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures," Occasional Paper Series 223, European Central Bank, available at: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf.
[40] https://cointelegraph.com/news/how-global-stablecoins-can-promote-financial-stability-in-the-world

DAVID DURAND, ATTORNEYS CORPORATION INC.
1255, Blvd. Robert-Bourassa, Suite 1500,
Montréal, Québec H3B 3X2
T. +1 (877) 490-1725 ext. 101 | F. +1 (877) 500-2520
info@durand-lex.com | www.durand-lex.com

The stability of bank profits cannot be synonymous with global financial stability. For many millions of people around the world, cryptoassets are a welcome addition to the global financial system. Regardless of these oversight bodies' concerns, the potential of global stablecoins and other crypto assets to enhance financial stability — and mobility — at the individual and household levels is of considerable social importance. Domestic policy makers should not overlook this."

Potential risks related to the cryptoasset space, including GSCs, include but are not limited to :

- localized disruptions to power supply, such as the operation of computer systems that require an abundance of electricity to operate;

- recurrence of pandemics[41] (and corresponding disruption to supply chain);

- Use of cryptoassets as payment instrument; of which reference can be made to the following extracts[42] : (i) "For example, the risks in the retail payments stems largely from information asymmetry and certain externalities that give rise to issues such as consumer protection"; and "[at] the moment, the risks of using cryptocurrencies as a payment instrument for large value payments (e.g., interexchange payments) include operational risks, liquidity risks, and legal risks. The sources of such risks lie in two idiosyncratic aspects of cryptocurrencies such as bitcoin. One is the settlement finality risk stemming from the probabilistic finality of settlements and risks of fork formation leading to possible double-spends. The second risk stems from the fact that bitcoin and other cryptocurrencies might not be sufficiently liquid to pass muster with the liquidity standards applicable to assets playing the role of settlement asset in sophisticated Large Value Payment System (LVPS)".

6. **Do you agree with the analysis of the vulnerabilities[43] arising from various stablecoin functions and activities (see Annex 2)? What, if any, amendments or alterations would you propose?**

"*Because fraud is as old as time, attempts to deter fraud are virtually as old*"[44]

[41] On June 15, 2020, the Cambridge Centre for Alternative Finance (CCAF), the World Bank Group and the World Economic Forum launched a global Covid-19 FinTech Market Rapid Assessment Survey so to understand Covid-19's impact on the FinTech markets and how the global FinTech industry has responded and some of the immediate regulatory and policy implications, available at: https://www.finextra.com/pressarticle/82889/ccaf-world-bank-and-the-world-economic-forum-investigate-covid-19s-impact-on-global-fintech.

[42] Hossein Nabilou (2020) The dark side of licensing cryptocurrency exchanges as payment institutions, *Law and Financial Markets Review*, 14:1, 39-47, DOI: 10.1080/17521440.2019.1626545. Also, available at : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3346035.

[43] Section 2.2 of the FSB Consultative Document, at p. 12.

[44] Cendrowski, H., The Handbook or Fraud Deterrence" (2015), available at: https://books.google.ca/books?id=qTXhe87o3OAC&pg=PA15&lpg=PA15&dq=%22fraud+is+as+old+as+%22&source=bl&ots=cYN3nGhz5H&sig=ACfU3U3wlW3amVh6g7H6kINlke3X5D0AAw&hl=en&sa=X&ved=2ahUKEwiK6IqznMDqAhUfknIEHaBfBcsQ6AEwAXoECAoQAQ#v=onepage&q=%22fraud%20is%20as%20old%20as%20%22&f=false.

All forms of assets suffer of traditional risks and vulnerabilities, and usually occur at the **convertibility mechanism (or point of conversion)**, as referred to at page 29 and *ff.* of our submission before the Canadian Standing Commitee of Finance[45]. In addition to the vulnerabilities stated in section 2.2 and Annex 2 of the *FSB Consultative document*, other vulnerabilites include, for example:

(i) market manipulation, including trading volumes, asset prices (via system shut-downs, asset freezes, wash-trading[46], and whale manipulation)[47];

(ii) the value of the GSC, which may have a price difference (or fluctuation) in on one or markets, or VASPs; thereby giving rise to *arbitrage*, "a type of trading capitalizes on imbalances in prices between markets."[48] In this regard, consideration should be given to price stabilisation mechanisms, or perhaps the notion of *tâtonnement* (supply and demand) as a process by which equilibrium prices are determined[49];

(iii) Anonymity and use of anonymous P2P transactions with no intermediaries (or unhosted wallets), especially if they have no ML/TF controls in place, *cf.* paras. 30 and *ff.,* 70 and *ff.* of the *FATF Report to G20 on so-called Stablecoins*; and

(iv) Risks from weak or non-existent AML/CFT regulation by some jurisdictions (cf. Para. 74 and *ff.* of the *FATF Report to G20 on so-called Stablecoins*).

Considering the involvement of financial institutions and/or intermediaries, it would also be prudent to await the BIS's position with respect to its December 2019 Consultation entitled "Designing a prudential treatment for crypto-assets"[50]; of which comments were due on March 13, 2020.

In light of the foregoing, guidance should be provided with respect to the ways risk can be mitigated by addressing :

- Adoption of appropriate technological solutions and standards for the implementation of the FATF "travel rule" as described in section 4 of the *12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers*, with particular regard to paragraphs nos. 56, 57 ("residual risks relating to anonymous peer-to-peer transactions via unhosted wallets, jurisdictions with weak or non-existent AML/CTF regulation and so-called stablecoins with dectralised governance"), 58 (e.g., identification of counter-party VASPs), 63

[45] https://www.ourcommons.ca/Content/Committee/421/FINA/Brief/BR10007367/br-external/IJWAndCoLtd-2018-09-17-Updated-Final-e.pdf.
[46] https://cointelegraph.com/news/coinsquare-ceo-accused-of-orchestrating-wash-trades ("Leaked documents reportedly show the CEO of Canadian crypto exchange Coinsquare orchestrating wash trades to [sic. bolster] volume.")
[47] https://bitcoinke.io/2020/04/crypto-market-manipulation/.
[48] https://cointelegraph.com/explained/arbitrage-trading-in-crypto-explained, "
[49] Wallrabenstein, John Ross, Clifton, Chris, Privacy Preserving Tâtonnement: A Cryptographic Construction of an Incentive Compatible Market, DOI: 10.1007/978-3-662-45472-5_26, Issn: 0302-9743, available at: https://www.researchgate.net/publication/284188854_Privacy_Preserving_Tatonnement_A_Cryptographic_Construction_of_an_Incentive_Compatible_Market; https://economics.stackexchange.com/questions/30501/whats-the-math-behind-calculating-the-price-of-cryptocurrency-through-supply-and.
[50] https://www.bis.org/bcbs/publ/d490.htm.

(P2P transactions via private / unhosted wallets; further requiring blockchain analytical tools can be used in complying with travel rule requirements), 64 (Batch and post facto submission and past transfers; in other words length of time required to report originator and beneficiary data), and 65 (Interoperability of systems so as to address data sharing, storage and security); and

- Data sharing, storage and security (cybersecurity), as well as compliance to cross-border data transfer requirements in light of GDPR and national privacy legislation; of which Canada's legislation is "subject to modernization[51].

Indeed, the issue of cybersecurity and data privacy (cross-border data transfers) appears to have been excluded by the FSB and other institutions studying cryptoassets. These important issues should be addressed by the FSB.

7. **Do you have comments on the potential regulatory authorities and tools and international standards applicable to GSC activities presented in Annex 2?**

We agree in large part with the issues cited in the FSB Consultative document, but have noted that the issues of : (1) cybersecurity, (2) data privacy (and cross-border data transfers), and (3) means of digital identification do not appear to have been addressed by the FSB.

8. **Do you agree with the characterisation of cross-border[52] issues arising from GSC arrangements?**

We agree in large part with the issues cited in the FSB Consultative document, but have noted that the issues of : (1) cybersecurity, (2) data privacy (and cross-border data transfers), and (3) means of digital identification do not appear to have been addressed by the FSB.

9. **Are the proposed recommendations appropriate and proportionate with the risks? Do they promote financial stability, market integrity, and consumer protection without overly constraining beneficial financial and technological innovation?**

    a. **Are domestic regulatory, supervisory and oversight issues appropriately identified?**

We refer the FSB to our submission before the Canadian Standing Commitee of Finance[53], as well as the Government Response thereto.

    b. **Are cross-border regulatory, supervisory and oversight issues appropriately identified?**

[51] https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html (released June 5, 2020).
[52] Section 4 of the FSB Consultative document, at page 20.
[53] https://www.ourcommons.ca/Committees/en/FINA/StudyActivity?studyActivityId=9933703; Durand, D. and Dorweiler, D., "*Don't Block The Blockchain: How Canada Can Guard Against Money Laundering While Maintaining Global Competitiveness*" (July 2018), available at: https://www.ourcommons.ca/Content/Committee/421/FINA/Brief/BR10007367/br-external/IJWAndCoLtd-2018-09-17-Updated-Final-e.pdf. The Government of Canada's Response is available at: https://www.ourcommons.ca/DocumentViewer/en/42-1/FINA/report-24/response-8512-421-468.

No, as the issues of (1) cybersecurity, (2) data privacy (and cross-border data transfers), and (3) means of digital identification do not appear to have been addressed by the FSB.

c. Do the recommendations adequately anticipate and address potential developments and future innovation in this sector?

No comment.

10. Do you think that the recommendations would be appropriate for stablecoins predominately used for wholesale purposes and other types of crypto-assets?

No comment.

11. Are there additional recommendations that should be included or recommendations that should be removed?

- *Cross-border data transfers & potential conflict of national data privacy laws*

Considering the global outreach of cryptoassets, and GSCs, it will necessarily involve **cross-border data transfers**, which need to be compliant with **national data privacy laws** (GDPR, *etc.*) governed by the respective **national data privacy authorities**[54]. This will require an understanding of the datasets derived from cryptoasset activities, from its source (originating data, including KYC information) all the way to its "end point" (e.g., point of conversion), which may further pass through "off-shore" processing centers (e.g., in the cloud). By way of example, if data originated from Europe and was being processed in Canada, one would have to comply with the GDPR and the Canadian[55] and provincial privacy laws; further reviewing the applicability and validity of : (i) standard contractual clauses, (ii) adequacy decisions, (iii) terms and conditions of user agreements, with particular respect to consent, collection, storage, use and processing of data, either domestically or in a foreign jurisdicition (e.g., in the cloud, "off-shore", or in foreign jurisdiction), (iv) amongst other considerations.

Indeed, it is respectfully submitted that the **FSB should address issues of GSC data privacy compliance** so as to avoid inconsistent oversight, as well as application of national data privacy law(s), which may be in conflict.

- *KYC - Digital identification*

The World Bank and other firms[56] have explored the issue of digital identification[57]. One of the key factors building trust.[58] The FATF has released it Guidance on Digital ID[59].

[54] A list of National Data Privacy Authorities. https://en.wikipedia.org/wiki/National_data_protection_authority
[55] Reference can be made to our submission to the Office of the Privacy Commissioner of Canada, available at: https://www.durand-lex.com/privacy-and-data-security-law, and the result of its consultation, available at: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2019/an_190923/.
[56] https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

12. Are there cost-benefit considerations that can and should be addressed at this stage?

No comment.

CONCLUDING REMARKS

Once again, we would like to commend the FSB for its call for public commentary on cryptoassets, in particular GSCs, and hope that the above submissions will be considered in its deliberations. Of course, the undersigned will make himself available for any further discussion, if called upon to do so.

Per : *David Durand*

Me David Durand
DURAND LAWYERS

[57] http://documents.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf, and the ID4D initiative, available at: https://id4d.worldbank.org.
[58] https://www.pymnts.com/news/security-and-risk/2019/digital-identity-sharing-economy-authentication/ and https://www.acamstoday.org/digital-identity-the-integrity-of-information/.
[59] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html.

DAVID DURAND, ATTORNEYS CORPORATION INC.
1255, Blvd. Robert-Bourassa, Suite 1500,
Montréal, Québec H3B 3X2
T. +1 (877) 490-1725 ext. 101 | F. +1 (877) 500-2520
info@durand-lex.com | www.durand-lex.com

SCHEDULE 1
FINA SUBMISSION

Don't Block The Blockchain: How Canada Can Guard Against Money Laundering While Maintaining Global Competitiveness

DAVID DURAND, ATTORNEYS CORPORATION INC.
1255, Blvd. Robert-Bourassa, Suite 1500,
Montréal, Québec H3B 3X2
T. +1 (877) 490-1725 ext. 101 | F. +1 (877) 500-2520
info@durand-lex.com | www.durand-lex.com

DON'T BLOCK THE BLOCKCHAIN: HOW CANADA CAN GUARD AGAINST MONEY LAUNDERING WHILE MAINTAINING GLOBAL COMPETITIVENESS

EXECUTIVE SUMMARY

Our study examines the current environment in Canada surrounding cryptoassets with a dual objective: how might the Government of Canada contribute to enhancing public trust in the financial system by securing it against money laundering and terrorism financing while fostering a domestic climate enabling participants in the cryptoasset/blockchain sector to thrive and compete favourably on an international basis?

1. INTRODUCTION

In today's digital world and economy, in which transactions know few borders, vigilance against money laundering and terrorism financing activities requires heightened international cooperation, including interoperability[1] and data exchanges amongst various domestic stakeholders. Such interoperability is required to involve Canada both domestically and as a founding member of the Financial Action Task Force ("FATF")[2] within the international community. To combat these threats, the Government of Canada enacted an anti-money laundering ("AML") and anti-terrorism financing ("ATF") legislative framework, including the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (*PCMLTFA*),[3] which is currently under statutory review.[4] In this connection, the Government of Canada concurrently released a series of proposed amendments to the regulations made under the *PCMLTFA*, 2018[5] on June 9, 2018 to "strengthen Canada's AML/ATF Regime, and ensure its measures are aligned with the FATF standards,"[6] therefore meeting its international commitments (hereinafter the "Proposed Amendments"). According to the June 9, 2018 Regulatory Impact Assessment Statement of the Proposed Amendments [emphasis added]:

---

[1] "Interoperability" is defined as "the ability of the federal government's numerous security information systems to work together technically, legally, semantically (through standard terminology), and culturally (through the willingness of organizations to share information)," as set forth in chapter 1 of the 2009 March Status Report of the Auditor General of Canada, <http://www.oag-bvg.gc.ca/internet/English/parl_oag_200903_e_32304.html>.

[2] Canada, Government of Canada, *Money Laundering* (Ottawa: 2017) <http://international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/money_laundering-blanchiment_dargent.aspx?lang=eng> accessed 02 July 2018.

[3] SC 2000, c 17 [*PCMLTFA*].

[4] Canada, Department of Finance, *Reviewing Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime*, (Ottawa: Department of Finance, 2018) < https://www.fin.gc.ca/activty/consult/amlatfr-rpcfat-eng.asp> accessed 01 July 2018.

[5] Gazette, Part I, Volume 152, Number 23: Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2018, <http://www.gazette.gc.ca/rp-pr/p1/2018/2018-06-09/html/reg1-eng.html> accessed 04 July 2018 [Canada Gazette].

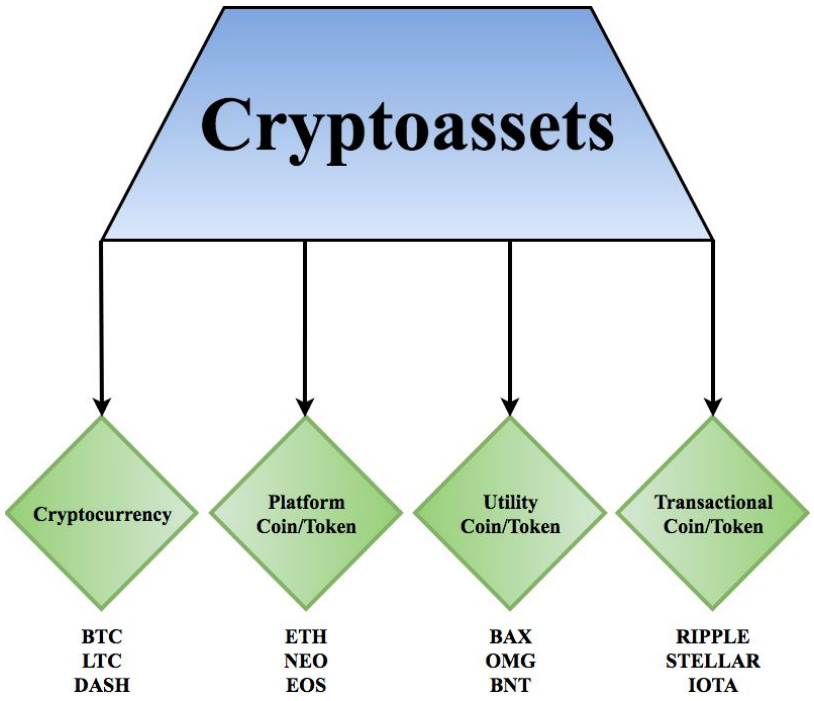
[6] *Ibid*.

> The proposed amendments to the regulations would strengthen Canada's AML/ATF Regime by updating customer due diligence requirements and beneficial ownership reporting requirements; regulating businesses dealing in virtual currency; updating the schedules to the regulations; including foreign money service businesses (MSB) in Canada's AML/ATF Regime; clarifying a number of existing requirements; and making minor technical amendments.[7]

2. WHAT ARE CRYPTOASSETS?

Bitcoin, Ether and Ripple have often been referred to as virtual currencies, which can be somewhat of a misnomer, as these "units" do not comprise currency. We shall define these units as "cryptoassets." Within the Proposed Amendments[8] put forth by the Department of Finance, as the term "virtual currency" is utilized, it creates judicial gaps, being that neither the said term, nor the often-used synonyms "digital currency" and "electronic money" are defined in Canadian legislation. Furthermore, the words "money" and "currency" do not accurately describe the inherent characteristics of a cryptoasset; *viz*., a cryptoasset is not a store of value. Moreover, such units should not be considered to be commodities or securities, as will be outlined hereinbelow. For the purpose of harmonization and ease of use, the term cryptoassets has been used hereinafter. A visual representation of cryptoassets appears in Figure 1.

Figure 1: Cryptoasset Categories[9]



[7] *Ibid*.
[8] Canada Gazette, *supra* note 5.
[9] Adam Haeems, "What is a crypto-asset" (27 April 2018), *Medium* (blog), online: <https://medium.com/babb/what-is-a-crypto-asset-1f0fcc517887>.

The term cryptoasset is a relatively new term describing digital assets that are recorded on a distributed public ledger. "Cryptoassets facilitate the decentralization of industries, removing the middlemen through the use of and peer-to-peer networking, reducing costs"[10] and improving efficiency and accuracy. While various terms such as cryptocurrency, virtual currency, utility token, transactional token and platform token are often used synonymously, these all fall under the umbrella of cryptoassets.

In the Canadian regulatory sphere, various Canadian regulatory bodies have been struggling with the definition of "virtual currencies," including cryptoassets, under the headers of currencies, securities and commodities. Under the regulatory regime of the United States, Americans have been facing similar problems. In July 2017, the U.S. Securities and Exchange Commission ("SEC") stated that cryptoassets or, in the SEC's terminology, "digital assets," would be subject to securities law under this regulatory body.[11] Less than one year later, in June 2018, during the *Yahoo! All Markets Summit: Crypto* event, the SEC's Director for Corporate Finance stated in a presentation that the SEC no longer considered Bitcoin and Ether to constitute securities.[12]

Moreover, the U.S. Financial Crimes Enforcement Network ("FinCEN") settled with Ripple Labs Inc., and its subsidiary XRP II, LLC in a $700,000 civil suit, where it was made clear the FinCEN had considered XRP to constitute the "currency of the Ripple network" based on the statement of facts in the settlement agreement.[13] Furthermore, since September 17, 2015, the Commodity Futures Trading Commission ("CFTC") has considered Bitcoin and other virtual currencies to be commodities, as determined in the matter of *Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan*.[14] This decision was re-affirmed during the granting of CFTC's preliminary injunction against Patrick K. McDonnell and CabbageTech, Corp. d/b/a Coin Drop Markets in March 2018 when a federal judge ruled that virtual currencies like Bitcoin will be regulated as commodities by the CFTC.[15]

---

[10] *Ibid*.
[11] Securities and Exchange Commission, Release No 81207, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (25 July 2017), online: Securities and Exchange Commission <https://www.sec.gov/litigation/investreport/34-81207.pdf>.
[12] William Hinman, "Digital Asset Transactions: When Howey Met Gary (Plastic)" (June 14 2018), online: SEC <https://www.sec.gov/news/speech/speech-hinman-061418>.
[13] U.S. Department of Justice, United States Attorney Northern District of California, *Settlement Agreement,* (between United States Attorney's Office in the Northern District of California v Ripple Labs Inc.) online: DOJ <https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/05/05/settlement_agreement.pdf>.
[14] *Commodity Futures Trading Commission v Coinflip, Inc., Derivabit, and Francisco Riordan* (17 September 2015), CFTC Docket No 15-29, online: Commodity Futures Trading Commission <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf>.
[15] *Commodity Futures Trading Commission v Patrick K. McDonnell, and CabbageTech Corp. d/b/a Coin Drop Markets* (6 March 2018), 18-CV-361, online: Commodity Futures Trading Commission <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoindroporder030618.pdf> [*CabbageTech*].

3. WHAT IS BLOCKCHAIN?

In order to understand cryptoassets, we must begin with an introduction of the underlying technology through which cryptoassets are created. One of the features of cryptoassets is the use of blockchain technology, which provides users anonymity, and a payment system structure.[16] Blockchain is a "distributed ledger that is usually managed by a peer-to-peer network."[17] In a blockchain, each transaction is separated into various blocks that are attached to one another using the "hash value of the previous block" which is referred to as that block's "parent."[18] Each block contains several transactions. As blocks are hashed together, the ensuing structure creates a blockchain. New blocks are added to the chain through a process known as mining, wherein miners are rewarded with an amount of a cryptoasset for solving mathematical equations through computation.[19] A timestamp, and a nonce, which is a pseudo-random number for verifying the hash, are also included on each block.

Blockchain is a unique means which can be used to prevent fraud, since any change in a block would alter the hash value of the block. In order for a block to be added to the blockchain it must first be validated. "A majority of nodes [a computer which is connected to the cryptoasset network] in the network agree by a consensus mechanism on the validity of transactions in a block and on the validity of the block itself"[20] before a particular block will be added to the blockchain. Once the information has been entered onto the blockchain, it can never be erased, creating a public and verifiable ledger through which every single transaction ever made on this blockchain can be observed.[21] A copy of the blockchain is automatically downloaded to every computer that is connected to the cryptoasset network.[22]

4. WHAT IS CURRENCY?

In Canada, "currency" is defined and regulated by statute under the *Currency Act.*[23] The *Currency Act* established that the monetary unit in Canada shall be measured in Canadian dollars ("CAD"), and the denominations of money will be in dollars and cents.[24] Under section 13 of the *Currency Act*, it is stipulated that [emphasis added]:

> Every contract, sale, payment, bill, note, instrument and security for money and every transaction, dealing, matter and thing relating to money or involving the payment of or the liability to pay money shall be made, executed, entered into, done or carried out in the currency of Canada, unless it is made, executed, entered into, done or carried out in

[16] United States, Press Release, "IBM Announces Major Blockchain Solution to Speed Global Payments" (16 October 2017), online IBM: < https://www-03.ibm.com/press/us/en/pressrelease/53290.wss>.
[17] Yan Chen, "Blockchain Tokens and the Potential Democratization of Entrepreneurship and Innovation" (2017) 61:4 Business Horizons 567.
[18] M. Nofer et al., "Blockchain" (2017) 59:3 Bus Inf Syst Eng 183.
[19] Oleg Straitev, "Crypto-currency and Blockchain: How to Regulate Something We Do Not Understand" (2018) 33:2 BFLR 90.
[20] Nofer, *supra* note 18 at 184.
[21] Steve Mitch, "Crypto Currency & Block Chain Technology: A Decentralized Future, RBC Capital Markets" (January 3 2018) at 1. online: RBC Capital Markets <https://ca.rbcwealthmanagement.com/documents/616937/616953/Crypto+Currency+%2B%20Blockchain+-+RBC+-+2018+01+03.pdf/6f959d80-b77b-43c4-80cb-38e1187793a1>.
[22] Investopedia, Blockchain, *Investopedia* (blog), online: <https://www.investopedia.com/terms/b/blockchain.asp>.
[23] RSC, 1985, c C-52.
[24] *Ibid* at s 3 and s 7.

> (a) the currency of a country other than Canada; or
>
> (b) a unit of account that is defined in terms of the currencies of two or more countries.

The *Currency Act* also states that the only coins which may be used as currency of Canada must be minted by the Royal Canadian Mint or have been issued by the "Crown in any province of Canada before it became part of Canada and if the coin was, immediately before October 15, 1952, current and legal tender in Canada."[25] The value of currency as a payment of money "derives solely from the quality of being legal tender which is conferred to them by section [8](1) of the *Currency Act*."[26]

5. ARE CRYPTOASSETS CURRENCIES?

If cryptoassets are to be defined as a currency, it would mean that they could be used to purchase goods and services. It could also be argued that cryptoassets are not currencies *per se*, as a currency by general definition consists of "notes and coins that are of fixed nominal values and are issued or authorized by the central bank or government."[27] By way of example, it has been mentioned that Bitcoin "operates without a centralized steering-mechanism and without direct intervention of central private regulator."[28]

As the *Currency Act* is the statutory basis for currency regulation in Canada, it requires that money[29] or currency must serve three primary functions:[30]

(i) It is a generally accepted medium of exchange;
(ii) It serves as a unit of account; and
(iii) It can be used as a store of value.

For cryptoassets to be considered money under the Bank of Canada's guidelines, they would need to satisfy all three of these criteria. We do not contend that cryptoassets cannot serve as a unit of account; however, they currently appear to fall short in terms of being viewed as a generally-accepted medium of exchange or as a store of value. Nevertheless, potential exists for success in this area as there are vendors throughout Canada that allow for transactions to be conducted in Bitcoin and/or other cryptoassets. One of the issues in the legitimization of cryptoassets as a currency is that a large number of the vendors that accept cryptoassets continue to base the "underlying value of transactions… in terms of national currencies such as the U.S. or Canadian dollar"[31] instead of denominating such transactions in cryptoasset units.

---

[25] *Ibid* at s 7(1)(b).
[26] Guy David, "Money in Canadian Law" (1986) 65 Can Bar Rev 192 at 200.
[27] Public Sector Debt, p. 1-6, online: OECD statistics <https://www.oecd.org/statistics/data-collection/Public%20sector%20Debt_guidelines.pdf>.
[28] Rainer Kulms, "Bitcoin – a Technology and a Currency" Central Bank Journal of Law and Finance, No. 1/2016.
[29] Straitev, *supra* note 19 at 199.
[30] Johnson Grahame, Pomorski Lukasz, *Briefing on Digital Currencies*, Senate of Canada, Ottawa Ontario, (2, April 2014), online: Bank of Canada <https://www.bankofcanada.ca/wp-content/uploads/2014/04/Senate_statement.pdf> at 8.
[31] *Ibid*.

Many major Canadian financial institutions currently ban "credit and debit card customers from participating in [cryptoasset] purchases with their cards,"[32] including BMO Financial Group and TD Bank, while Royal Bank of Canada accepts cryptoasset transactions in only very limited circumstances. In a leaked memo, BMO apparently restated its decision to ban these transactions was "due to the volatile nature of cryptocurrencies and to better protect the security of our clients and the bank."[33]

The current prevailing climate indicates that the majority of the financial institutions in Canada are hesitant to deal with any business related to cryptoassets, including cryptoasset exchanges. Such reluctance is not strictly a Canadian initiative. The Commonwealth Bank of Australia stated that it will no longer allow its customers to acquire cryptoassets with credit cards, stating, "we have made this decision because we believe virtual currencies do not meet a minimum standard of regulation, reliability, and reputation when compared to currencies that we offer to our customers. Given the dynamic, volatile nature of virtual currency markets, this position is regularly reviewed."[34]

It is difficult to argue that cryptoassets should be characterized as a currency when the institutions that are most closely connected to the exchange of currency are hesitant in allowing their customers to purchase cryptoassets with their credit and debit card payment systems. As in the case of the newly-regulated cannabis regime in Canada, it appears that financial institutions may be less reluctant to facilitate cryptoasset transactions once proper regulatory practices and procedures are established, as illustrated by the recent $250 million loan facility granted by BMO Financial Group, one of the "big-six" Canadian banks, to Aurora Cannabis Inc.[35]

[32] Nathan Reiff, "Canada Banks Ban Users from Buying Cryptocurrency" (11 April 2018), *Investopedia* (blog), online < https://www.investopedia.com/news/canada-banks-ban-users-buying-cryptocurrency/>.
[33] Aziz Abdel-Qader, "Cryptocurrency Ban Expands Across Canadian Banks as BMO Joins Crackdown", *Finance Magnates* (30 March 2018), online: Finance Magnates <https://www.financemagnates.com/cryptocurrency/news/cryptocurrency-ban-expands-across-canadian-banks-bmo-joins-%E2%80%8Ecrackdown/>.
[34] Commonwealth Bank of Australia, "Commonwealth Bank Blocks Credit Card Purchases of Virtual Currencies" (14 February 2018), online: On the Record < https://www.commbank.com.au/cs/newsroom/virtual-currency-credit-card-block-201802.html?ei=card-view>.
[35] The Canadian Press, "Aurora Cannabis signs loan deal for up to $250-million with Bank of Montreal", *The Globe and Mail* (26 June 2018), online: The Canadian Press < https://www.theglobeandmail.com/business/article-aurora-cannabis-signs-loan-deal-for-up-to-250-million-with-bank-of/>.

While it has been argued that cryptoassets may be utilized as a store of value, the observed high levels of volatility make them a less-than-ideal medium to be used as a currency. Examples of cryptoasset volatility include Bitcoin growing by 1,318% in 2017 while ranking 14th among the fastest-growing cryptoassets of the year. Ripple was the top performer in 2017 due to its value rising 36,018%, followed by NEM and Ardor which grew 29,842% and 16,808%, respectively.[36] Ethereum also rose 9,162% in 2017.[37]According to Gangwal *et al*, the daily volatility of Bitcoin is calculated at 7.18%, which is approximately ten times higher than the volatility of fiat currencies backed by central banks or governments.[38] In order to be a legitimate store of value, "economic agent[s] should be able to transfer his/her purchasing power over time, especially on the short term."[39] This extreme price volatility experienced significantly contributes to the rejection of the argument that cryptoassets should be considered as a store of value and, hence, regulated as a currency.

Thus, for cryptoassets to fall within the category of currency, the *Currency Act* would have to be amended by the Canadian legislature. Based on the foregoing, it would be incorrect to equate cryptoassets to currency *stricto sensu*.

[36] Wong, Ian Joon, "2017's biggest cryptoassets ranked by performance", online: The Atlas <https://www.theatlas.com/charts/B1pWqcDQM>.
[37] *Ibid*.
[38] Sashwat Gangwal and Fançois Longin, "Extreme Movements in Bitcoin prices: A study based on extreme value theory" (2017) at 5 online: Longin Inside <https://www.longin.fr/Recherche_Publications/Resume_pdf/Gangwal_Longin_Extreme_movements_Bitcoin_prices.pdf>.
[39] *Ibid* at page 6.

6. WHAT IS A SECURITY?

In order to determine whether a cryptoasset should fall under the purview of provincial and territorial securities legislation, it is vital to understand what a security is, pursuant to the applicable legislative enactment. Generally, securities are financial instruments or claims issued by businesses or financial organizations to investors with the objective of raising capital for enterprises. Though not defined in each provincial and territorial securities legislation, the Ontario *Securities Act*, by way of example, defines a security.[40]

Securities in Canada are regulated by provincial or territorial regulators, who are "organized and coordinated"[41] by the Canadian Securities Administrators ("CSA"). Their aim is to create some sense of conformity and uniformity across the thirteen (13) Canadian jurisdictions. From time-to-time, the provincial and territorial regulators release policies that provide some insight into the interpretation of existing securities legislation.[42] Staff Notices, which are released by the CSA, also provide insight on potential future policies created by provincial and territorial regulators. The objectives of the securities regulators are fairly consistent, as they are focused on the idea that "investors pay enormous amounts of money to strangers for completely intangible rights, whose value depends entirely on the quality of the information that the investor receives and on the seller's honesty."[43]

The purpose of provincial and territorial securities legislation is fairly standardized. For example, under the Ontario *Securities Act*, it is stated at section 1.1 thereof that:

---

[40] RSO 1990, c S.5, at s 1(1) [*Securities Act*], wherein security is defined as:

> (a) any document, instrument or writing commonly known as a security,
> (b) any document constituting evidence of title to or interest in the capital, assets, property, profits, earnings or royalties of any person or company,
> (c) any document constituting evidence of an interest in an association of legatees or heirs,
> (d) any document constituting evidence of an option, subscription or other interest in or to a security,
> (e) a bond, debenture, note or other evidence of indebtedness or a share, stock, unit, unit certificate, participation certificate, certificate of share or interest, preorganization certificate or subscription other than,
> (i) a contract of insurance issued by an insurance company licensed under the *Insurance Act*, and
> (ii) evidence of a deposit issued by a bank listed in Schedule I, II or III to the *Bank Act* (Canada), by a credit union or league to which the *Credit Unions and Caisses Populaires Act, 1994* applies, by a loan corporation or trust corporation registered under the *Loan and Trust Corporations Act* or by an association to which the *Cooperative Credit Associations Act* (Canada) applies,
> (f) any agreement under which the interest of the purchaser is valued for purposes of conversion or surrender by reference to the value of a proportionate interest in a specified portfolio of assets, except a contract issued by an insurance company licensed under the *Insurance Act* which provides for payment at maturity of an amount not less than three quarters of the premiums paid by the purchaser for a benefit payable at maturity,
> (g) any agreement providing that money received will be repaid or treated as a subscription to shares, stock, units or interests at the option of the recipient or of any person or company,
> (h) any certificate of share or interest in a trust, estate or association,
> (i) any profit-sharing agreement or certificate,
> (j) any certificate of interest in an oil, natural gas or mining lease, claim or royalty voting trust certificate,
> (k) any oil or natural gas royalties or leases or fractional or other interest therein,
> (l) any collateral trust certificate,
> (m) any income or annuity contract not issued by an insurance company,
> (n) any investment contract,
> (o) any document constituting evidence of an interest in a scholarship or educational plan or trust, and
> (p) any commodity futures contract or any commodity futures option that is not traded on a commodity futures exchange registered with or recognized by the Commission under the *Commodity Futures Act* or the form of which is not accepted by the Director under that Act,

[41] Canadian Securities Administrators, *About CSA: Overview* (Montreal: Canadian Securities Administrators, 2009) <https://www.securities-administrators.ca/aboutcsa.aspx?id=45>.

[42] *Securities Act*, *supra* note 40 at s 143.8.

[43] Bernard Black, "The Legal and Institutional Preconditions for Strong Securities Markets", (2001) 48:4, UCLA Law Review, online: Northwestern Scholars <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=182169>.

> The purposes of this Act are:
>
> (a) to provide protection to investors from unfair, improper or fraudulent practices;
> (b) to foster fair and efficient capital markets and confidence in capital markets; and
> (c) to contribute to the stability of the financial system and the reduction of systemic risk.[44]

The issue of regulating of cryptoassets as securities arose following a 2016 U.S. incident in which there was an attempt at a cryptocurrency heist after an Initial Coin Offering ("ICO"), which had raised $150 million USD, became the largest crowdfunding project in history.[45] Through an anomaly in the system, a hacker was able to divert approximately $50 million USD worth of assets from the ICO into another account.[46] While the hacker was unable to receive the assets and the transaction was cancelled, this attack led critics to question under which particular regime such ICOs should be regulated.[47] In response to this attack, the SEC released a report to determine whether the ICO in the aforementioned attack, as well as other cryptoassets, should fall under the auspices of U.S. federal securities laws.[48] The SEC was of the opinion that various cryptoassets fall within the scope of the *Securities Act*.[49] More specifically, the SEC concluded that many cryptoassets may be considered *prima facie* to constitute an "investment contract" pursuant to section 2(a)(1) of the U.S. *Securities Act*.[50]

[44] *Securities Act*, *supra* note 40.
[45] David Siegel, "Understanding the DAO Attack" Coindesk (blog) (25 June 2016), online: <www.coindesk.com/understanding-dao-hack-journalists/>.
[46] *Ibid*.
[47] *Ibid*.
[48] United States, Securities and Exchange Commission, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (Release No 81207) (Washington, DC: US Government Printing Office, 2017).
[49] 15 U.S.C. § 77a.
[50] *Ibid*.

In response to the SEC finding above, the CSA released Staff Notice 46-307[51] ("Staff Notice 46-307") on August 24, 2017, in which the CSA warned that many "cryptocurrency offerings, such as initial coin offerings (ICO), initial token offerings (ITO) and sales of securities of cryptocurrency investment funds" would fall under the securities laws of Canada, as they would be considered investment contracts (similar to the status thereof in the United States). To support its position, the CSA refers to the four-prong test set forth in *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*[52] ("*Pacific Coast*") to determine whether a coin or token would be considered to be an investment contract. The *Pacific Coast* four-prong test reads:[53]

(1) Does the scheme involve an investment of money?
(2) Is the scheme in a common enterprise?
(3) Has an investment of money been made with the intention of profit?
(4) Are the profits to come solely from the efforts of others?

In order for a cryptoasset to be considered an investment contract under the current judicial precedent, each component of this test must be answered in the affirmative. Only then would a cryptoasset be considered a security and therefore subject to Canadian securities laws.

Interestingly, on June 11, 2018, the CSA released Staff Notice 46-308,[54] in which it outlined fourteen (14) situations that impact the presence of one or more of the elements of an investment contract. In Staff Notice 46-308, the CSA referred to its own publication, Staff Notice 46-307, writing [emphasis added]:

---

[51] Canadian Securities Administrators, "CSA Staff Notice 46-307: Cryptocurrency Offerings", 40 OSCB 7233 at 7321 (Toronto: OSCB, 24 August 2017), online: Canadian Securities Administrators <http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency-offerings.htm>.

[52] [1978] 2 SCR 112, 1977 CarswellOnt 50, 2 BLR 212 [*Pacific Coast*]. The majority held at page 113-114:

> *Per* Martland, Judson, Ritchie, Spence, Pigeon, Dickson, Beetz and de Grandpré JJ.: Section 35 of the Act prohibits anyone trading in a security in the absence of a prospectus and section 1(1) (22) xiii defines security as including "any investment contract, other than an investment contract within the meaning of *The Investment Contracts Act"*. [The contract in question was not one covered by *The Investment Contracts Act*]. While the term investment contract is not defined, the policy of the legislation is clearly the protection of the public through full, true and plain disclosure of all material facts relating to securities being issued. The fourteen subdivisions of the definition encompass practically all types of transactions and indeed the definition had to be narrowed down by the long list of exceptions in s. 19. The categories in the definition are not mutually exclusive and are in the nature of 'catchalls'. Such remedial legislation should be construed broadly. Substance, not form, is the governing factor. The legislation is not aimed solely at schemes that are actually fraudulent but rather relates to arrangements that do not permit the customers to know exactly the kind of investment they are making.
>
> The Supreme Court of the United States in *SEC v. W.J. Howey Co.,* 328 U.S. 293 (1946), with the foregoing in mind laid down the test "Does the scheme involve 'an investment of money in a common enterprise, with profits to come solely from the efforts of others'?" In the case at bar all aspects of this test can be answered in the affirmative. Clearly an investment of money was involved; as to the common enterprise aspect the only commonality necessary for an investment contract is that between the investor and promoter; and as to the dependence of the customer for the success of the enterprise the end result of the investment by each customer was dependent upon the quality of the expertise brought to the administration of the funds obtained by appellant from its customers. The test to determine the economic realities of a securities transaction based on "the risk capital approach" adopted by the Supreme Court of Hawaii in *State of Hawaii v. Hawaii Marker Center, Inc.,* 485 P. 2d 105, results in the same conclusion that the agreement in question is an investment contract.
>
> The facts were examined in the sole light of the *Howey* and *Hawaii* tests at the invitation of the parties. A broader approach could however have been taken. The clear legislative policy was to replace the harshness of *caveat emptor* in security related transactions and the courts should seek to attain that goal even if tests formulated in prior cases prove ineffective and have to be broadened in scope.

[53] *Ibid* at pg 128.

[54] Canadian Securities Administrators, "CSA Staff Notice 46-308 Securities Law Implications for Offerings of Tokens", (Toronto: OSCB, 11 June 2018), online: Canadian Securities Administrators <http://www.osc.gov.on.ca/documents/en/Securities-Category4/csa_20180611_46-308_implications-for-offerings-of-tokens.pdf>.

> […] As 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 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 an 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" [FN1], including considering whether the offering involves:
>
> 1. An investment of money
> 2. In a common enterprise
> 3. With the expectation of profit
> 4. Derived 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. […][55]

[55] *Ibid*.

> [FN1]: 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.

In Staff Notice 46-308, the CSA also refers to its Regulatory Sandbox,[56] the purpose of which is to allow:

> […] firms to register and/or obtain exemptive relief from securities laws 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 on a time-limited basis.
>
> The CSA Regulatory Sandbox is part of the CSA's 2016-2019 Business Plan to gain a better understanding of how technology innovations are impacting capital markets, assess the scope and nature of regulatory implications and what may be required to modernize the securities regulatory framework for fintechs.[57]

Moreover, the CSA has published a list of decisions[58] granted through the CSA Regulatory Sandbox, as well as the terms and conditions of registration of the firms authorized to participate in the CSA Sandbox.

7. ARE CRYPTOASSETS SECURITIES?

In Staff Notice 46-307, the CSA made it clear that "in many instances [the CSA] found that the coins/tokens in question constitute securities for the purposes of securities laws."[59] If cryptoassets are to be considered investment contracts, many extraneous securities law obligations would arise that are not present in the current regulatory sphere. Included in these obligations would be the prospectus requirement (or corresponding exemption) and the registration requirement (and/or its corresponding exemption).[60] These obligations would be much more onerous than the current requirements put forth by the various regulatory bodies that are trying to regulate this space. When considering whether or not securities law is going to apply to a cryptoasset, the CSA has mentioned it will "consider substance over form" when determining whether or not that particular asset should be considered a security. For example, the SEC is under the impression that neither Bitcoin nor Ether should be considered a security under the current securities regulations.[61]

---

[56] *Ibid*.
[57] *Ibid*.
[58] Canadian Securities Administrators, *CSA Regulatory Sandbox* (Montreal: Canadian Securities Administrators, 2009) < https://www.securities-administrators.ca/industry_resources.aspx?id=1626>.
[59] Canadian Securities Administrators, *supra* note 51.
[60] *Ibid*.
[61] Hinman, *supra* note 12.

Currently, the CSA appears to be of the view that many cryptoassets should be treated as securities and consequently become subject to stringent regulatory obligations, despite the SEC's reversal on its classification of cryptoassets as securities. Indeed, the SEC recently announced in a June 14, 2018 statement[62] *that it no longer considered Ether or Bitcoin to be securities*. In this statement, the SEC reviewed whether cryptoassets would be deemed securities according to *SEC v Howey*,[63] one of the U.S. Supreme Court decisions that the Supreme Court of Canada ("SCC") refers to in *Pacific Coast* regarding the above four-prong test for investment contracts.[64] Through its application of the four-prong test, the SEC expressed concern that purchasers of a cryptoasset would "no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts."[65]

In these cases, when a cryptoasset reaches the level where it is so decentralized that any third-party activity no longer influences its success, the identification of such third parties no longer plays a vital role in protecting the rights and interests of the users of the cryptoassets. When these third parties lose their influence to exert any influence on these decentralized networks, specific information regarding their "background, financing, plans, financial stake and so forth"[66] become minimally relevant to the efficient functioning of the market for the cryptoasset.

Bitcoin was supposedly created by someone under the pseudonym Satoshi Nakamoto, who released a paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System"[67] on October 31, 2008, which detailed a system of decentralized peer-to-peer electronic transactions. The Bitcoin network was established on January 3, 2009, when Mr. Nakamoto mined the first Bitcoin block and was rewarded with 50 bitcoins.[68] As the Bitcoin network has been decentralized since its creation,[69] attempting to regulate Bitcoin as a security in Canada would be highly ineffective from an enforcement perspective.

[62] *Ibid*.
[63] *SEC v W.J. Howey Co.*, 328 U.S. 293 (1946).
[64] *Pacific Coast*, *supra* note 52 at 128.
[65] Hinman, *supra* note 12.
[66] *Ibid*.
[67] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", (31 October 2008), online: <https://bitcoin.org/bitcoin.pdf>.
[68] Benjamin Wallace, "The Rise and Fall of Bitcoin", *Wired* (blog) (23 November 2011), online: <https://www.wired.com/2011/11/mf_bitcoin/>.
[69] Hinman, *supra* note 12.

In late 2013, a Canadian by the name of Vitalik Buterin proposed the development of the Ethereum network; the pre-sale of Ether tokens began on July 22, 2014 and raised over $14 million USD by August 6, 2014.[70] Subsequently, the network has grown exponentially, with Ether currently ranking second behind Bitcoin in market capitalization.[71] The SEC has proposed a similar treatment for Ether and Bitcoin: based on the decentralization of the current Ethereum network, Ether transactions should not be subject to disclosure requirements under U.S. securities laws.[72] Requiring securities disclosure for such cryptoassets, where the distributed network is functional and efficient without any significant influence exerted by a third-party, provides little benefit. While securities regulations are intended to protect investor rights, as well as those of other stakeholders, in decentralized systems such as those underpinning cryptoassets, there is very little that securities regulatory bodies need do to protect its users, as no single participant is able to manipulate the network.

While the SEC has remained silent recently on the status of cryptoassets other than Bitcoin and Ethereum, it is reasonable that the CSA should re-evaluate its identification of various coins as investment contracts, and thus as a security. Proposing overreaching securities regulation on the cryptoasset regime would likely create a system where onerous requirements are placed on users of such assets, with an end result of suppressing innovation in financial technology and motivating human and financial capital to leave Canada seeking more favourable environments.

Given the nature of cryptoassets, they do not fit the definition of a security. The fact that securities regulations would have scant effect in protecting users on decentralized networks makes it evident that defining cryptoassets as a security would provide ineffective regulatory enforcement in this respect.

Thus, it could be postulated that a divergence of position and legislative interpretation has formed between various jurisdictions with respect to the characterization of cryptoassets as a security.

8. DIVISION OF POWERS - A LOOMING CONFLICT FOR REGULATORY OVERSIGHT OF CRYPTOASSETS

During June 2018, both the provincial and federal levels of government were active in releasing numerous documents regarding cryptoassets, including Proposed Amendments, Staff Notices, studies and other documents; the latest of which was published by the Ontario Securities Commission ("OSC") on June 28, 2018.[73]

[70] Investoo Group, "History of Ethereum: How it's set to overtake Bitcoin by 2018", (June 26 2017), online: Investoo Group (blog), online: Mining < http://www.mining.com/web/history-ethereum-set-overtake-bitcoin-2018/>.
[71] "Top 100 Cryptocurrencies By Market Capitalization", online: CoinMarketCap: <https://coinmarketcap.com/coins/> [Top 100].
[72] Hinman, *supra* note 12.
[73] Ontario, Ontario Securities Commission, *Taking Caution: Financial Consumers and the Cryptoasset Sector* (Toronto: Ontario Securities Commission, 2018) <https://www.osc.gov.on.ca/documents/en/Investors/inv_research_20180628_taking-caution-report.pdf>.

In this publication entitled *Taking Caution: Financial Consumers and the Cryptoasset Sector*, the OSC claims that "most ICOs are subject to securities regulations,"[74] referring to their own studies, without disclosing the methodology or the sample set, as well as to other reports. Throughout this publication, the OSC provides various statistics from a survey of Ontarians who own or have owned cryptoassets relating to motives and methods of purchase, as well as various other pieces of information. At one point, the OSC comments that many users of cryptoassets are unsure of whether cryptoassets are subject to regulation and, if so, who the regulatory authority might be. In response to their finding, the OSC asserts "this belief is incorrect. The OSC regulates ICOs that constitute securities offerings."[75] CSA Staff Notice 46-308 is mentioned as the authority from where this regulatory power is derived.

However, as stated in section 143.8 of the *Securities Act* of Ontario, even when a Staff Notice becomes a policy, it "is not of a legislative nature."[76] Furthermore, the *Securities Act* is clear that before a Staff Notice becomes a policy, the public must be provided "reasonable opportunity to interested persons and companies to make written representations with respect to the proposed policy within a period of at least 60 days after the publication."[77] Thus, review of a Staff Notice is necessary before it becomes policy; while the OSC may be able to provide "guidance on the potential application of, and possible approaches required to comply with, securities legislation," its current role in regulating ICOs has not been defined by either Canadian or Provincial regulators or legislation.

Interestingly, CSA Staff Notice 46-308 further refers the reader to *Reference Re Securities Act (Canada)*[78] ("*Re Securities Act*"), consisting of an opinion rendered by the SCC in which it analyzed the extent of the ability of the Parliament of Canada to use its trade and commerce power under the section 91 of the *Constitution Act, 1867*.[79] At paragraph 45 of *Re Security Act*, the Supreme Court of Canada wrote:

> [45] The provincial power over securities extends to impacts on market intermediaries or investors outside a particular province (*Global Securities*, at para. 41; *R. v. W. McKenzie Securities Ltd.* (1966), 56 D.L.R. (2d) 56 (Man. C.A.), leave to appeal refused, [1966] S.C.R. ix (*sub nom. West & Dubros v. The Queen*); *Gregory & Co. v. Quebec Securities Commission*, [1961] S.C.R. 584). The case law also recognizes provincial jurisdiction where the province's capital markets are engaged (*Québec (Sa Majesté du Chef) v. Ontario Securities Commission* (1992), 10 O.R. (3d) 577 (C.A.), leave to appeal refused, [1993] 2 S.C.R. x (*sub nom. R. du chef du Québec v. Ontario Securities Commission*); *Bennett v. British Columbia (Securities Commission)* (1992), 94 D.L.R. (4th) 339 (B.C.C.A.)).

In other words, the SCC "[…] sank the federal government's attempt to create a national securities regulator. The Court ruled that the proposed Canadian *Securities Act* (Act), as presently drafted, is *ultra vires* the federal government."[80] The SCC further noted:

---

[74] *Ibid* at 1.
[75] *Ibid* at 5.
[76] *Securities Act*, *supra* note 40 at s 143.8(1).
[77] *Securities Act*, *supra* note 40 at s 143.8(5).
[78] 2011 SCC 66, [2011] 3 SCR 837 [*Re Securities Act*].
[79] (UK), 30 & 31 Vict, c 3, reprinted in RSC 1985, App II, No 5 [*Constitution Act*].
[80] Wayne Gray and Stephen Genttner, "Supreme Court's Unanimous Ruling Sinks Canadian *Securities* Act (But Leave Much to be Salvaged" (23 December 2011), *McMillan LLP* (blog), online: <https://mcmillan.ca/Supreme-Courtss-Unanimous-Ruling-Sinks-Canadian-Securities-Act-But-Leaves-Much-to-be-Salvaged>.

> To determine the constitutional validity of legislation from a division of powers perspective, the pith and substance analysis requires the courts to look at the purpose and effects of the law. The inquiry then turns to whether the legislation falls under the head of power said to support it. If the pith and substance of the legislation is classified as falling under a head of power assigned to the adopting level of government, the legislation is valid. When a matter possesses both federal and provincial aspects, the double aspect doctrine may allow for the concurrent application of both federal and provincial legislation.

Though Parliament's power over the regulation of trade and commerce under s. 91(2) of the *Constitution Act, 1867* has two branches – the power over interprovincial commerce and the general trade and power – "[…] it cannot be used in a way that denies the provincial legislatures the power to regulate local matters and industries within their boundaries. Nor can the power of the provinces deprive the federal Parliament of is powers under s. 91(2) to legislate on matters of genuine national importance and scope – matters that transcend the local and concern Canada as a whole." As the Supreme Court of Canada further stated in the summary of in *Re Securities Act* [emphasis added]:

> As held in *General Motors of Canada Ltd. v. City National Leasing*, [1989] 1 S.C.R. 641, to fall under the general branch of s. 91(2), legislation must engage the national interest in a manner that is qualitatively different from provincial concerns. Whether a law is validly adopted under the general trade and commerce power may be ascertained by asking (1) whether the law is part of a general regulatory scheme; (2) whether the scheme is under the oversight of a regulatory agency; (3) whether the legislation is concerned with trade as a whole rather than with a particular industry; (4) whether it is of such a nature that provinces, acting alone or in concert, would be constitutionally incapable of enacting it; and (5) whether the legislative scheme is such that the failure to include one or more provinces or localities in the scheme would jeopardize its successful operation in other parts of the country. These indicia of validity are not exhaustive, nor is it necessary that they be present in every case.[81]

The inherent conflict between federal and provincial powers to regulate various aspects of (i) trade and commerce under s. 91(2) [federal jurisdiction], (ii) civil rights under s. 92(13) [provincial jurisdiction] and matters of merely local or private nature under s. 92(16) [provincial jurisdiction] of the *Constitution Act, 1867*[82] is well known, and is indicative of a brewing conflict that may occur between the federal and provincial levels of government with respect to the regulation of cryptoassets, especially considering provincial securities regulators, such as the OSC[83] have characterized them as securities, whilst others (such as Quebec's Autorité des Marchés Financiers) have not,[84] and the Canadian Parliament has released its Proposed Amendments.

[81] *Re Securities Act, supra* note 78 at page 839.
[82] *Constitution Act*, *supra* note 79.
[83] Ontario Securities Commission, *supra* note 73.
[84] Jacob Serebrin, "Virtual currencies like Bitcoin fall into a cryptic regulatory gap in Quebec", *Montreal Gazette* (11 January 2018), online < https://montrealgazette.com/business/amf-on-bitcoin>.

As applied to the regulation of cryptoassets, it could be argued that the federal government has the authority to regulate cryptoassets; such through the application of section 91 of the *Constitution Act, 1867*[85] and application of the national concern doctrine.

The first mention of the national concern doctrine was asserted in *Attorney-General for Ontario vs. Attorney-General for the Dominion and The Distillers and Brewers' Association of Ontario*:

> [13] […] Their Lordships do not doubt that some matters, in their origin local and provincial, might attain such dimensions as to affect the body politic of the Dominion, and to justify the Canadian Parliament in passing laws for their regulation or abolition in the interest of the Dominion. But great caution must be observed in distinguishing between that which is local and provincial, and therefore within the jurisdiction of the provincial legislatures, and that which has ceased to be merely local or provincial, and has become matter of national concern, in such sense as to bring it within the jurisdiction of the Parliament of Canada. […][86]
>
> Fifty years after this decision, the doctrine was given its modern interpretation through the *Reference re Canada Temperance Act* decision, wherein it was acknowledged that:
>
> […] if [the subject matter of the legislation] is such that it goes beyond local or provincial concern or interests and must from its inherent nature be the concern of the Dominion as a whole […] then it will fall within the competence of the Dominion Parliament as a matter affecting the peace, order and good government of Canada. […][87]

The modern-day interpretation was affirmed through *Johannesson v. West St. Paul*, wherein it was held:

> [19] […] the true test must be found in the real subject matter of the legislation: if it is such that it goes beyond local or provincial concern or interests and must from its inherent nature be the concern of the Dominion as a whole . . . then it will fall within the competence of the Dominion Parliament as a matter affecting the peace, order and good government of Canada, though it may in another aspect touch on matters specially reserved to the provincial legislature. […][88]

This was re-affirmed in *Munro v. National Capital Commission*, wherein it was held:

[85] *Supra* note 79.
[86] 1896 CarswellNat 45, [1896] AC 348, 5 Cart BNA 295.
[87] 1946 CarswellOnt 100 at 205-206, [1946] 2 WWR. 1, [1946] 2 DLR 1.
[88] [1952] 1 SCR 292, [1951] 4 DLR 609.

> […] [24] I find it difficult to suggest a subject matter of legislation which more clearly goes beyond local or provincial interests and is the concern of Canada as a whole than the development, conservation and improvement of the National Capital Region in accordance with a coherent plan in order that the nature and character of the seat of the Government of Canada may be in accordance with its national significance. Adopting the words of the learned trial judge, it is my view that the Act "deals with a single matter of national concern. […][89]

For the point of this discussion, reference can be made to paragraph 33 of *R v. Crown Zellerbach Canada Ltd.*[90] ("*Zellerbach*"), wherein it was established that [emphasis added]:

> […]
>
> 1. The national concern doctrine is separate and distinct from the national emergency doctrine of the peace, order and good government power, which is chiefly distinguishable by the fact that it provides a constitutional basis for what is necessarily legislation of a temporary nature;
>
> 2. The national concern doctrine applies to both new matters which did not exist at Confederation and to matters which, although originally matters of a local or private nature in a province, have since, in the absence of national emergency, become matters of national concern;
>
> 3. For a matter to qualify as a matter of national concern in either sense it must have a singleness, distinctiveness and indivisibility that clearly distinguishes it from matters of provincial concern and a scale of impact on provincial jurisdiction that is reconcilable with the fundamental distribution of legislative power under the Constitution;
>
> 4. In determining whether a matter has attained the required degree of singleness, distinctiveness and indivisibility that clearly distinguishes it from matters of provincial concern it is relevant to consider what would be the effect on extra-provincial interests of a provincial failure to deal effectively with the control or regulation of the intra-provincial aspects of the matter.

[89] [1966] SCR 663.
[90] [1988] 1 SCR 401 at para 33, 1988 CarswellBC 137, [1988] SCJ No [*Zellerbach*].

The *Zellerbach* decision presented the modern-day interpretation of the national concern doctrine, which will show how the cryptoasset regime would be best regulated through federalism. The national concern doctrine is concerned with matters that did, (a) not exist before Confederation, and (b) which have become a matter of national concern. It is clear that the first requirement of the test has been passed. The analysis will focus on whether or not the cryptoasset regime has become a matter of national concern. *Zellerbach* makes it clear that in order for the cryptoasset regulatory regime to have reached the level of a matter of national concern it must attain the levels of "singleness, distinctiveness and indivisibility that clearly distinguishes it from a matter of provincial jurisdiction."[91] The *A.G. Canada v Hydro Quebec et al* ("*AG Canada*") decision made distinctive that "the test for singleness, distinctiveness and indivisibility is a demanding one. Because of the high potential risk to the Constitution's division of powers presented by the broad notion of national concern, it is crucial that one be able to specify precisely what it is over which the law purports to claim jurisdiction."[92] *Zellerbach* extends the definition of a national concern where it states that what classifies singleness, distinctiveness and indivisibility is to "consider what would be the effect on extra-provincial interests of a provincial failure to deal effectively with the regulation or control or regulation of the intra-provincial aspects of this matter."[93]

On January 7, 2018, the twenty-four (24) hour volume of cryptoasset trading reached a high of over $80 billion USD a day.[94] Millions of dollars are being converted into and out of Canadian fiat currency and cryptoassets while hundreds of millions of dollars are being converted into USD daily on cryptocurrency exchanges.[95] Fortunes have been made and cryptoassets have become a global phenomenon. While different regulatory bodies in Canada struggle to determine who should be in charge of regulating this growing marketplace, it should be recognized that cryptoassets are potentially much "too important and impactful"[96] and the social benefits far too large for Canada to stifle the potential to become a global leader in this market.

[91] *Ibid*.

[92] [1997] 3 SCR 213 at para 673.

[93] *Zellerbach*, *supra* note 90 at para 3.

[94] Coinmarketcap, "Total Market Capitalization", online: Coinmarketcap <www.coinmarketcap.com/charts> [Total Market].

[95] "CryptoCompare Index: BTC", online: Cryptocompare <https://www.cryptocompare.com/coins/btc/analysis/CAD>.

[96] William Michael Cunningham, "Cryptocurrency Regulation is a job for treasury" *American Banker* 183:37 (23 February 2018), online: <https://www.americanbanker.com/opinion/cryptocurrency-regulation-is-a-job-for-treasury>.

Considering the objectives[97] of the *PCMLTFA*, the most effective and the most important areas of regulation are to prevent money laundering, terrorist financing and tax evasion. These new technologies "threaten existing approaches to regulation, and empower groups and individuals – including criminals and terrorists – seeking to skirt regulations for nefarious purposes."[98]

Under section 91(27) of the *Constitution Act*, *1867*,[99] criminal law will be regulated by the Parliament of Canada. Currently the AML and ATF regime are federally regulated under *Proceeds of Crime (Money Laundering and Terrorist Financing Act*, [100] ("*PCMLTFA*"). Money laundering has and will continue to be a threat to Canada's financial institutions.[101] Without the proper resources and appropriate authority that stems from federal legislation, this problem will continue to grow.

In addition to this consideration, the *PCMLTFA* also relates to section 91(7) of the *Constitution Act, 1867*,[102] which focuses on the defense and military of Canada, including preventing any threats of terrorism. It is extremely important to have effective measures to prevent terrorism; this effort begins with the obstruction of terrorist financing which can lower the risk of terrorist attacks on Canadian citizens both at home and abroad. We see no reason why such endeavours should be regulated provincially. The resources and the current legislation that would be provided by federal regulation will be the most effective process in preventing money laundering and terrorist financing.

The regulation of the convertibility mechanism where cryptoassets are transferred into fiat currency (and vice versa) through a cryptoasset exchange is the stage of the cryptoasset transaction that will be able to most effectively protect Canada against these threats.

---

[97] The objective of the *PCMLTFA* is to:

- implement specific measures to detect and deter money laundering and the financing of terrorist activities to facilitate the investigation or prosecution of money laundering and terrorist financing offences, including:
    - establishing record keeping and client identification requirements for financial services providers and other persons that engage in businesses, professions or activities that are susceptible to being used for money laundering, and the financing of terrorist activities, […];
    - requiring the reporting of suspicious financial transactions and of cross-border movements of currency and monetary instruments, and
    - establishing an agency that is responsible for dealing with reported and other information;
- respond to the threat posed by organized crime by providing law enforcement officials with the information they need to investigate and prosecute money laundering or terrorist financing offences, while ensuring that appropriate safeguards are put in place to protect the privacy of persons with respect to personal information about themselves; and
- assist in fulfilling Canada's international commitments to participate in the fight transnational crime, particularly money laundering and the fight against terrorist activities […].

[98] Alex Wilner & Evangeline Ducas, "The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada" (2017) 72:4 Intl J 539.

[99] *Constitution Act*, *supra* note 79.

[100] *PCMLTFA*, *supra* note 3.

[101] Nicolas W. R. Burbidge, "International anti-money laundering and anti-terrorist financing: the work of the Office of the Superintendent of Financial Institutions in Canada" (2004) 7:4 Journal of Money Laundering Control 320.

[102] *Constitution Act*, *supra* note 79.

Blockchain and related technologies also provide opportunities for innovation and profit on a large scale. On January 7, 2018 the global market capitalization for cryptoassets reached a value of over $810 billion USD.[103] This market is much too large to be regulated by individual provinces. Under section 91(2) of the *Constitution Act, 1867*[104] it shall be within the power of the Parliament of Canada to regulate Trade and Commerce throughout the country. It is therefore important for the Federal Parliament to create legislation that finds the balance between a prohibitive regulatory environment and a lax AML and ATF regime without stifling innovation and favouring a competitive Canadian cryptoasset industry within a global economy; such being within its powers.

Currently, Canada has assumed a "watchful approach."[105] They are watching the global regulation and weigh the risks and commensurate opportunities in the cryptoasset environment. Other jurisdictions (such as Singapore and Switzerland) have adopted a more "facilitative approach,"[106] electing to become attractive destinations in the growing cryptoasset market. They have chosen to "regulate blockchain technologies in order to both capitalize on potential opportunities that emerge, while minimizing identified risks."[107] These foreign jurisdictions are slowly becoming the global FinTech leaders; Canada needs to ensure that it does not fall behind in this respect. "Canada risks losing its competitive advantage in developing and profiting from blockchain technologies."[108] In the future, jurisdictions that have benefited from facilitative cryptoasset regulation shall benefit from the lessons they learned during the progression of this technology.[109] It is therefore imperative for Canada to become one of the jurisdictions that is a global leader in this space.

A failure of the provinces to implement proper regulation for cryptoassets intra-provincially would likely have extra-provincial effects that would be felt on a national and potentially global level. The level of impact that improper regulation of this technology could have regarding money laundering and terrorist financing is a matter that falls directly within the "pith and substance" of the federal legislation. Additionally, the necessity to promote Canada as an emerging global leader in this space falls within the areas of trade and commerce as regulated by section 91(2) of the *Constitution Act, 1867*.[110]

In addition to the desirability of the creation of a viable national cryptoasset regulatory framework, such a framework, under the federal regime, would:

---

[103] Coinmarketcap, *supra* note 94.
[104] *Constitution Act*, *supra* note 79.
[105] Wilner et al., *supra* note 98.
[106] *Ibid*.
[107] *Ibid*.
[108] *Ibid*.
[109] United States, *Foundation for Defense of Democracies*, *An Analysis of Illicit Flows into Digital Currency Services*, Yaya J Fanusie & Tom Robinson, (Washington D.C, January 2018) at 11.
[110] *Constitution Act*, *supra* note 79.

- allow FINTRAC[111] to fulfil its mandate, which is "to facilitate detection, prevention and deterrence of money laundering and the financing of terrorist activities, while ensuring the protection of personal information under its control," as well as respect Canada's international commitments to its partners;[112]

- Enable the use of an existing and highly functional AML/ATF federal framework to regulate cryptoassets, with known requirements (i.e., reporting requirements, money services business ("MSB") reporting requirements, etc.), under an existent set of laws and rules designed to permit uniform regulation and enforcement on a national basis, thus fostering the integrity and stability of Canada's financial system, among other considerations;

Moreover, given the nature of cryptoassets described in this paper, they are impacted by other forms of federal legislation, including, but not limited to (i) the *Clearing and Settlement Act*, (ii) the *Bank Act*, and (iii) the *Payment Act*;[113] especially if cryptoassets are used in financial institutions on a day-to-day, as well as mainstream basis. Furthermore, technological innovation is federally regulated under the *Patent Act* and Constitution. In light of the foregoing, it could be argued that the cryptoasset regulatory regime is *intra* vires of the Parliament of Canada to regulate.

[111] Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is Canada's financial intelligence unit (FIU). According to its website, "the Centre assists in the detection, prevention and deterrence of money laundering and the financing of terrorist activities. FINTRAC's financial intelligence and compliance functions are a unique contribution to the safety of Canadians and the protection of the integrity of Canada's financial system. FINTRAC acts at arm's length and is independent from the police services, law enforcement agencies and other entities to which it is authorized to disclose financial intelligence. It reports to the Minister of Finance, who is in turn accountable to Parliament for the activities of the Centre", available at: http://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng.asp.

[112] Canada, Financial Transactions and Reports Analysis Centre of Canada, *Who we are* (Ottawa: 2017) < http://www.fintrac-canafe.gc.ca/fintrac-canafe/1-eng.asp>.

[113] *Re Securities Act, supra* note 78 at para 46. The Constitution gives Parliament powers that enable it to pass laws that affect aspects of securities regulation and, more broadly, to promote the integrity and stability of the Canadian financial system. These include Parliament's power to enact laws relating to criminal law (s. 91(27)), banks (s. 91(15)), bankruptcy (s. 91(21)), telecommunications (ss. 91 and 92(10) (*a*)), and peace, order and good government (s. 91) (*Multiple Access*; *Bell Canada v. Quebec (Commission de la santé et de la sécurité du travail)*, [1988] 1 S.C.R. 749, at pp. 765-66; *Smith v. The Queen*, [1960] S.C.R. 776, at p. 781). Parliament has exercised its powers by enacting, for example, the following statutes and provisions: the *Canada Business Corporations Act*, R.S.C. 1985, c. C-44 ; the *Criminal Code*, R.S.C. 1985, c. C-46, ss. 380(2) , 382 , 382.1 , 383 , 384 and 400 ; the *Bank Act*, S.C. 1991, c. 46 ; the *Investment Canada Act*, R.S.C. 1985, c. 28 (1st Supp .); the *Payment Clearing and Settlement Act*, S.C. 1996, c. 6, Sch .; the *Telecommunications Act*, S.C. 1993, c. 38 ; the *Bankruptcy and Insolvency Act*, R.S.C. 1985, c. B-3, Part XII. Finally, s. 91(2) of the *Constitution Act, 1867* gives Parliament power over the regulation of trade and commerce. This power has two branches: the power over interprovincial and international commerce (*Citizens Insurance Co. of Canada v. Parsons* (1881), 7 App. Cas. 96 (P.C.) ("*Parsons*")) and the general trade and commerce power that authorizes laws where the national interest is engaged in a manner that is qualitatively different from provincial concerns, as discussed more fully later in these reasons.

9. WHAT IS A COMMODITY?

It has been argued that the currency and securities regulatory bodies may not be the most effective authorities to regulate cryptoassets. It has also been suggested by both the United States Federal Court[114] and by the Canadian Revenue Agency[115] that cryptocurrencies should be treated as commodities.

The Law Library defines a commodity as "a good that is sold freely to the public. It can be agriculture, fuel or metals. It is traded in bulk in the commodity or spot market."[116] Canadian jurisprudence defines a commodity as "anything produced for use or sale, article of commerce or object of trade,"[117] or "in its ordinary business and derivative sense, it means anything moveable that is a subject of trade of acquisition, a kind of thing produced from a sale, an article of commerce, an object of trade."[118] Statutes define commodities in several places, most prevalently in the Alberta *Securities Act* under section 1(h), which defines a commodity too as: "(i) any good, article, service, right or interest of which any unit is, from its nature or by mercantile custom, treated as the equivalent of any other unit, (ii) the currency of any jurisdiction, (iii) any gem, gemstone or other precious stone."[119] The *Commodity Futures Act* defines commodity in section 1(1) as: "whether in the original or a processed state, any agricultural product, forest product, product of the sea, mineral, metal, hydrocarbon fuel, currency or precious stone or other gem, and any goods, article, service, right or interest or class thereof, designated as a commodity under the regulations."[120]

While the definitions are not entirely consistent in their interpretations of a "commodity" in the Canadian regulatory sphere, they do provide guidelines to assist in helping us determine whether cryptoassets would fall under this definition, and therefore be regulated as such.

---

[114] *CabbageTech, supra* note 16 at 27.
[115] Canada, Canadian Revenue Agency, *What you should know about digital* currency, (Ottawa: Canadian Revenue Agency, 2013) <https://www.canada.ca/en/revenue-agency/news/newsroom/fact-sheets/fact-sheets-2015/what-you-should-know-about-digital-currency.html>. Further reference can be made to Schedule 1.
[116] *Black's Law Dictionary*, 10th ed, *sub verbo* "commodity".
[117] Enron Capital & Trade Resources Canada Corp. v Blue Range Resource Corp., 2000 ABCA 239 at para 39, 192 DLR (4th) 281, [2001] 2 WWR 454 [*Enron*].
[118] *Canadian Pacific Railway v Ottawa Fire Insurance Company*, 1906 CarswellOnt 143, 7 OWR 353, aff'd 1905 CarswellOnt 143.
[119] *Securities Act*, RSA 2000, c S-4 at s 1 [*ASA*].
[120] RSO 1990, c C.20 at s 1(1) [*CFA*].

10. ARE CRYPTOASSETS COMMODITIES?

Perhaps the most relevant argument to cryptoassets being defined as a commodity in Canada comes from the U.S. decision in *Commodity Futures Trading Commission v. Patrick K. McDonnell and CabbageTech, Corp. d/b/a Coin Drop Markets*[121] ("CabbageTech") where Federal Judge Jack B. Weinstein ruled that he agreed with the CFTC and the Chicago Mercantile Exchange Inc. that cryptoassets (or, as they defined therein, "virtual currencies") should be considered commodities pursuant to the *Commodity Exchange Act* ("CEA"). In CabbageTech, the plaintiffs were granted a preliminary injunction due to Justice Weinstein's ruling that without it, there was a "reasonable likelihood that defendants will continue to violate the CEA"[122] without the injunction. The U.S. courts agreed with the plaintiffs that virtual currency should be regulated as a commodity and therefore the CFTC would have proper standing in this decision.[123]

CabbageTech cited various sources why they believed that it was likely that a virtual currency would be best regulated as a commodity under the CFTC, as defined in American legislation and jurisprudence. Prentis wrote in his 2015 article that:

> "It would make sense for regulators to treat Bitcoin as a commodity. Commodities are generally defined as 'goods sold in the market with a quality and value uniform throughout the world.' This categorization would be appropriate because it realistically reflects the economic behavior of Bitcoin users and squares with traditional economic concepts of exchange."[124]

Prentis elaborates, discussing how participants in the Bitcoin community use the asset in exchange for property or currency, and how Bitcoin actually behaves very similarly to traditional commodities when considered in a supply and demand framework. As more Bitcoin are released into the market, and the difficulty in mining the Bitcoin is heightened, the value rises; in a manner similar to gold or other precious metals, a Bitcoin "is worth whatever someone is willing to pay for it.[125]

Critics of this analysis have argued that where Bitcoin may fail to conform to the commodity analysis is the "lack of inherent use value that is often included in the definition of a Bitcoin."[126] It is through this argument that Bitcoin may face its strongest resistance as to whether it should be defined as a commodity. It is evident on the surface that Bitcoin does not comprise the traditional functions of a commodity that grain, energy or livestock may have when viewed from a high-level perspective.

---

[121] *Commodity Futures Trading Commission v Patrick K. McDonnell, and CabbageTech Corp. d/b/a Coin Drop Markets* (18 January 2018), 18-CV-361, online: Commodity Futures Trading Commission <https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcdmcomplaint011818.pdf> [*CabbageTech* Complaint].

[122] *CabbageTech, supra* note 15 at 27.

[123] *CabbageTech* Complaint, *supra* note 121.

[124] Mitchell Prentis, "Digital Metal: Regulating Bitcoin As A Commodity" (2015) 66:2 Case W Res L Rev 609. s

[125] *Ibid* and from Brad Jacobsen & Fred Pena, *"What Every Lawyer Should Know About Bitcoins"* (2014), Utah B.J, 40.

[126] Nicholas Godlove, "Regulatory Overview of Virtual Currency" (2014) 10:1 Okla J. L. & Technology 70 1.

While Bitcoin cannot be used for consumption and its intrinsic value may be difficult to quantify or value, Prentis states that its intrinsic value would benefit from its ability to decrease transaction fees online.[127] In a comparison between PayPal and other electronic transaction operators or payment services (i.e. payment processing), Bitcoin transaction fees are much lower. It may be evident that this is where Bitcoin's intrinsic value lies; however, this argument only takes into account direct peer-to-peer transactions of Bitcoin, which are declining in popularity as various cryptocurrency exchanges are increasingly facilitating these transactions and charging similar, if not higher transaction fees than PayPal or other intermediaries had previously been demanding.[128]

Based on this analysis, it could be argued that Bitcoin's intrinsic value would be minimal unless a majority of transactions were performed without the use of an exchange or intermediary to facilitate the transaction.

Jeff Currie, who was also cited in CabbageTech, commented as follows regarding the "store of value" function that commodities may contain:

> A commodity is any item that "accommodates" our physical wants and needs. And one of these physical wants is the need for a store of value. Throughout history humans have used different commodities as a store of value – even cocoa beans – but, more persistently, gold. In contrast, a security is any instrument that is "secured" against something else. As a currency is usually secured by a commodity or a government's ability to tax and defend, it is considered to be a security. By these definitions, bitcoin with a lower case "b," is a commodity, and not a currency, while Bitcoin with a capital "B" is the technology, or network, that bitcoin moves across. The analogy would be Shale technology versus shale oil.[129]

While Currie is correct in his argument that Bitcoin and other cryptoassets may comprise some store of value, it is also consistent with our above discussion of whether cryptoassets should be defined as a currency. Though cryptoassets do, inherently, contain a "store of value" element, it would be inaccurate to argue that such element is a defining factor of a Bitcoin. With its extremely high rate of volatility that is approximately ten (10) times higher than a traditional currency,[130] the argument that Bitcoin facilitates market demand for a commodity that stores value appears to be inherently flawed, as such "want and need" is already served by traditional currencies, as well as other commodities (such as precious metals), both of which feature far lower volatility.

While the CFTC has made it clear that cryptoassets fit into the definition of a commodity under Title 7 U.S.C. § 1(a)(9) as, "all other goods and articles… and all services, rights, and interests… in which contracts for future delivery are presently or in the future dealt in,"[131] the definitions are not consistent under Canadian jurisprudence and legislation. For example, under section 1(h)(a) of the Alberta *Securities Act*, a commodity is defined as "any good, article, service, right or interest of which any unit is, from its nature or by mercantile custom, treated as the equivalent of any other unit."[132]

---

[127] Prentis, *supra* note 124.
[128] Finder "Bitcoin vs. PayPal" (27 April 2018), online : Finder <https://www.finder.com/bitcoin-vs-paypal>.
[129] Jeff Currie, "Bullion Bests bitcoin, Not Bitcoin" *Goldman Sachs Global Macro Research* 21 (11 March 2014) <https://www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-Bit-Coin.pdf>.
[130] Gangwal *et al*, *supra* note 38.
[131] *CabbageTech* Complaint, *supra* note 121.
[132] *ASA, supra* note 119.

While the value of a cryptoasset might measure its value in U.S. dollar terms, similar to other commodities, the value of each of these assets will be uniform. Based on this definition, a cryptoasset may be considered a commodity. Section 1(1) of the *Commodity Futures Act* provides itself with a proverbial catch-all clause, wherein a commodity is defined as "… any goods, article, service, right or interest or class thereof, designated as a commodity under the regulations."[133] In this sense, amendments to this Act or relevant jurisprudence to designate a cryptoasset as a commodity under this act may be necessary.

A commodity may also fit into the definition provided in *Enron Capital & Trade Resources Canada Corp v. Blue Range Resource Corporation* wherein it was held that a commodity should be defined as "anything produced for use or sale, article of commerce or object of trade."[134] The majority of cryptoasset users are deploying their assets strictly as an "object of trade," either in exchange for other cryptoassets or for fiat currency.[135] Per *CPR v. Ottawa Fire Insurance Company* decision, a cryptoasset could also fit under the definition of a commodity as "… anything moveable that is a subject of trade or acquisition, a kind of thing produced from a sale, an article of commerce, an object of trade."[136] Thus, a cryptoasset generally seems to fit under this broad and traditional definition of a commodity, as its technological sophistication is much greater than any other commodity defined as such under Canadian legislation. In that sense, we contend that labelling and regulating cryptoassets as commodities would be both ineffective and inconsistent with the goals of the Canadian government and associated various regulatory bodies.

The potential multiple characterizations of cryptoassets under different heads of currencies, securities, commodities, etc. could create regulatory chaos, as competing authorities could lay claim to governing power, creating conflicting jurisdictional approaches, ineffective regulation and enforcement and divergent regulation. It appears that regulators of cryptoassets would best be served by a single federal authority in Canada under the AML/ATF framework.

---

[133] *CabbageTech* Complaint, *Supra* note 120.
[134] *Enron, supra* note 117 at para 39.
[135] Christine Lagarde, "Addressing the Dark Side of the Crypto World" (13 March 2018), online: IMFBlog (blog) <https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/>.
Spencer Applebaum, "Analysis of the Cryptocurrency Landscape" (31 December 2017), online: Medium (blog) <https://medium.com/@MUBC/analysis-of-the-cryptocurrency-exchange-landscape-948752318fae>.
[136] *ASA, supra* note 119.

11. RECOMMENDATION

Indeed, rather than instructing regulatory bodies to implement resource-heavy policies restricting decentralized cryptoasset networks that would ultimately offer little protection for the users of these networks, it would be most prudent for Canada to concentrate its regulatory efforts on the area where the government could provide greater public benefit: cryptoasset exchanges. This approach to concentrate regulatory efforts at the locus of cryptoasset transactions – the convertibility mechanism - is imperative as cryptoasset exchange users are theoretically able to transact in almost complete anonymity in terms of identity, location or source of income. In the absence of some degree of regulatory oversight, cryptoasset transactions may be used by innominate parties to swiftly move large amounts of wealth across borders.

The implications of this structure from an AML perspective are of obvious concern. Essentially, the only effective method to ascertain the identity of parties to a cryptoasset transaction would be to ensure that sufficient "know-your-client" ("KYC") information is collected with respect to the parties opening accounts (known as "wallets") at cryptoasset exchanges, as well as their sources of funds (e.g., fiat currency that is exchanged into cryptoassets) that are deposited into the wallets to be used in transactions.[137] *Details supporting our foregoing recommendations appear in the remainder of our brief.*

12. WHAT IS AML/ATF AND HOW ARE CRYPTOASSETS RELEVANT TO THE DISCUSSION?

Though Canadian law does not define "money laundering" *per se*,[138] it can be described in different ways, such as, *inter alia*:

(i) "a form of financial crime in which the proceeds from criminal activity are made to appear legitimate. The goal of many criminal acts is to make a profit for the individual or group that commits the crime. A strategy to fight money laundering seeks to reduce crime by making it harder for criminals to keep and use their profits";[139]

(ii) "the process of concealing illicit gains that were generated from criminal activity";[140]

(iii) "the processing of these criminal proceeds to disguise their illegal origin."[141]

In addition, money laundering is often referred to as a three-stage process involving:

(1) placement of proceeds of crime into the financial system;

[137] Perri Reynolds & Angela S.M. Irwin, "Tracking digital footprints: anonymity within the bitcoin system" (2017) 20: 2 J Money Laundering Control 172.
[138] Canada, Office of the Auditor General of Canada, *2003 April Report of the Auditor General of Canada*, (Ottawa: Office of the Auditor General of Canada) at s 3.20.
[139] *Ibid* at s 3.6.
[140] Organization for Economic Co-operation and Development, "Money Laundering", online: OECD <https://www.oecd.org/cleangovbiz/toolkit/moneylaundering.htm>.
[141] Financial Action Task Force on Money Laundering, "What is Money Laundering", online: FATF <http://www.fatfgafi.org/faq/moneylaundering/#d.en.11223>.

(2) creation of layers (i.e., *layering*) of financial transactions to disguise their origins, and

(3) moving the laundered funds back into the legitimate economy (i.e., *integration*).[142]

On the other hand, "terrorist financing" consists of the provision of funds for terrorist activity[143] and/or as "[…] the financing of terrorist acts, and of terrorists and terrorist organisations."[144] Chapter 3 of the 2003 *Report of the Auditor General of Canada to the House of Commons*[145] describes the relationship between money laundering and terrorist financing as follows:

> [3.25] Money laundering involves the processing of the profits of crimes that were committed in the past so as to disguise their illegal origin. The financing of terrorism, however, involves the processing of funds—whether obtained legally or illegally—to be used in future crimes.
>
> [3.26] Following the terrorist attacks of 11 September 2001, Canada has taken a number of steps to combat terrorist financing. They are aimed at assisting the police to detect and deter the financing of terrorist activities and to investigate and prosecute offences that are related to terrorist financing.
>
> [3.27] Terrorist groups differ from large criminal organizations in several important ways.
>
> - **Motivation.** While drug traffickers and organized crime groups seek primarily monetary gain, terrorist groups usually have non-financial goals that motivate them. According to one definition, the primary goal of terrorism is "to intimidate a population or to compel a government to do something, or abstain from doing any act."
>
> - **Source of funds.** The financial dealings of a terrorist organization are difficult to investigate since its funds may come from legitimate businesses that the terrorists may own and donations they have received from sympathizers. The apparently legal sources of funds may mean there are few, if any, indicators that would make one or a series of transactions stand out.
>
> - **The size and nature of financial transactions.** Individual financial transactions tied to terrorist operations may involve amounts that are not large enough to trigger existing reporting thresholds. An FBI analysis of the events surrounding 11 September 2001, for example, indicates that the hijackers each opened accounts with a single cash or wire transfer deposit in the average amount of US $3,000 to $5,000. The analysis also showed that they made numerous withdrawals in small amounts using mostly debit cards.

---

[142] Canada, *supra* note 138 at s 3.34.
[143] Canada, Financial Transactions and Reports Analysis Centre of Canada, *What is terrorist financing?* (Ottawa: 2015) < http://www.fintrac-canafe.gc.ca/fintrac-canafe/definitions/terrorist-terroriste-eng.asp>.
[144] Financial Action Task Force on Money Laundering, "International Standard on Combatting Money Laundering and the Financing of Terrorism and Proliferation" (February 2018) at 123, online: FATF < http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>.
[145] Canada, *supra* note 138.

- **Transfers of money outside the traditional financial system.** There are ways to transfer money from one person or country to another other than using banks or financial institutions. *Hawala* and similar methods of transferring money such as the *Fei ch'ien* and *Hundi* systems have also played a role in moving terrorist funds. In the *Hawala* system, a person gives money to an agent in one country, who tells an agent in another country to give money to a specific person. The transfer is all handled through word of mouth. Funds moved this way do not leave a paper trail similar to one that would be left if the person used a traditional financial setting like a bank.

3.28 As a result, it is difficult to follow terrorist money trails. For the three-year period ending 2003-04, the government has allocated a total of $34 million to the Financial Transactions and Reports Analysis Centre to detect and deter terrorist financing. Regulations have been developed for reporting transactions that appear to be related to terrorist financing.

One of the rationales or concerns as to why cryptoassets may pose a specific risk in the area of money laundering and terrorist financing,[146] or as a vehicle thereof,[147] may be related to the anonymous nature of cryptoassets and the source of funds thereof. Other concerns (amongst others) relate to:

(i) "[…] degree of anonymity that can potentially be exploited by money launderers or terrorist activity financiers,"[148] especially in transactions conducted through the Internet;

(ii) the "origins of funds are difficult to trace and it is difficult to ascertain whether or not the money is from a legitimate source (e.g. some cards can be anonymously loaded with cash at a third party reseller location, such as a Canada Post office)";

(iii) "convertible virtual currencies are vulnerable to abuse for money laundering and terrorist activity financing purposes because they allow greater levels of anonymity, or in some cases complete anonymity, when compared to traditional non-cash payment methods."

[146] Banque de France, "The emergence of bitcoin and other crypto-assets: challenges, risks and outlook" (5 March 2018) 16, online: Focus <https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_en.pdf>.
[147] Christine Lagarde, "Addressing the Dark Side of the Crypto World" (13 March 2018), online: IMFBlog (blog) <https://blogs.imf.org/2018/03/13/addressing-the-dark-side-of-the-crypto-world/>.
[148] Canada Gazette, *supra* note 5.

Figure 2: At Which Point Should Cryptoassets Be Regulated?

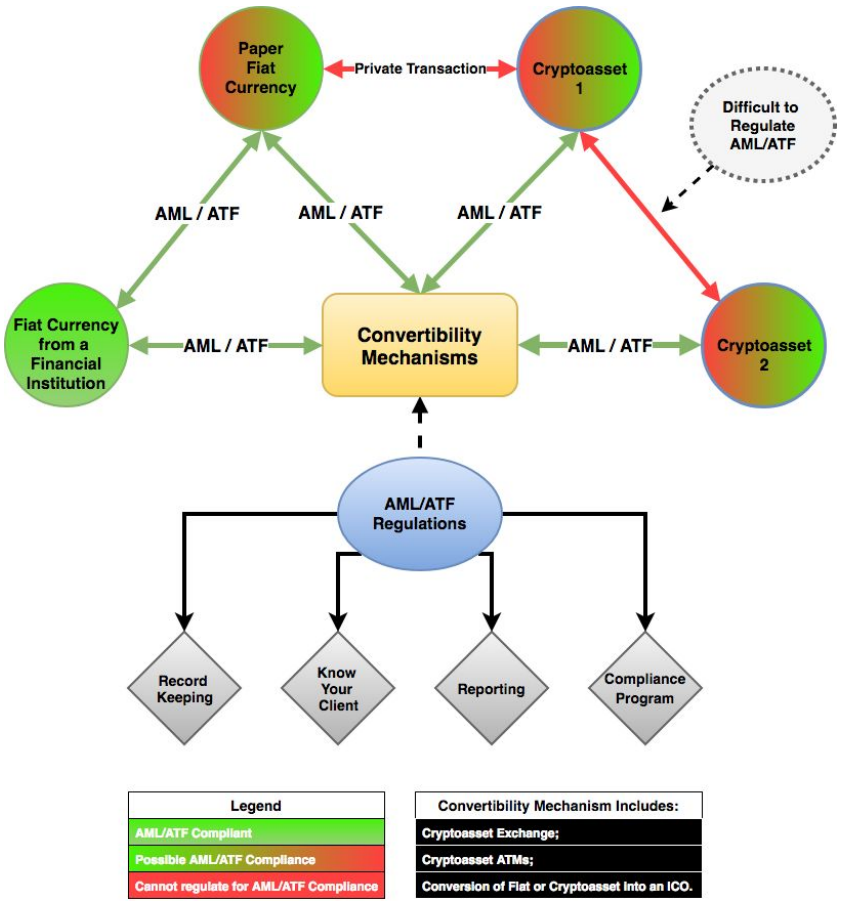


Figure 2 highlights the proposed method we recommend as the most effective way to regulate cryptoassets under a Canadian regulatory framework.

The three main methods of entry into the cryptoasset network are through (i) physical fiat currency, (ii) fiat from a financial institution, and (iii) by exchanging a currently-owned cryptoasset for another cryptoasset. In addition to these methods of entry, there exist convertibility mechanisms that are operated as a method for conversion from currency into cryptoassets and *vice versa*. Our proposal theorizes that the best area wherein the Federal government will be able to effectively and efficiently monitor this space is at the **convertibility mechanism** point. The convertibility mechanisms have been divided into three categories:

1) cryptoasset exchanges, which are operations that allow their users to exchange cryptoassets for fiat currency or for other types of cryptoassets and *vice versa*;
2) cryptoasset ATMs, which are machines that allow users to exchange cryptoassets for fiat currency and *vice versa*; and
3) conversion of fiat or cryptoasset into an ICO, which is the method by which a user would exchange fiat currency or another cryptoasset for ICO tokens or coins issued by a start-up business.

We recommend that these three entry points comprise the space where the Canadian regulators are going to be able to most effectively regulate cryptoassets. As illustrated in Figure 2, there are two methods of convertibility where it will be difficult or impossible to regulate the transfer of cryptoassets and fiat currency. The first of these methods constitute private transactions made between cryptoassets and paper fiat currency. If users wish to purchase cryptoassets with physical fiat currency or if they wish to exchange their cryptoassets for physical fiat currency in a private transaction without the use of a convertibility mechanism, it is going to be extremely difficult to monitor whether this transaction was completed without a criminal element involved. In the same manner in which a person may sell any type of physical asset with paper fiat currency, this type of transaction will be very difficult to monitor in terms of its legality.

The second convertibility situation occurs when users trade cryptoassets among each other without the use of a convertibility mechanism. Similar to the previous transaction category, the legality of these transactions will also be difficult to regulate, given the degree of anonymity involved in this exchange. Fortunately, the large majority of transactions are conducted in the cryptoasset network using convertibility mechanisms. Hence, just as it is impossible for authorities to monitor every transaction occurring in fiat currency, the government's regulatory framework should focus on the preponderance of transactions that can be monitored, being those transactions completed at the point in which convertibility mechanisms exist.

In Figure 2, the green arrows represent the areas through which AML/ATF compliance can be effectively monitored. The green circle, "Fiat Currency from a Financial Institution", represents any fiat currency that is being stored in a financial institution. This green circle indicates that this currency should already have undergone the proper practices and procedures imposed by the financial institution to ensure that the currency is compliant with AML/ATF requirements promulgated by Canadian legislation. Thus, it can be securely concluded that the financial institution has already performed its KYC obligations to ensure that this currency is "clean" and does not originate from proceeds of crime or terrorist financing.

The other three circles in Figure 2, Paper Fiat Currency, Cryptoasset 1 and Cryptoasset 2, all have a possibility of not being "clean" from an AML/ATF standpoint. It is often difficult to accurately identify the source through which paper fiat currency and cryptoassets originated from. It is therefore vital to ensure that these methods of entry into the cryptoasset regime have gone through the proper AML/ATF scrutiny, including record keeping, KYC, reporting of suspicious transactions and compliance program requirements. When physical fiat currency is used in a transaction at a financial institution, the said transaction must already undergo proper AML/ATF regulatory compliance in order to be accepted at the institution. It is vital for the protection of Canada's AML/ATF regime that we also ensure that proper AML/ATF compliance occurs at the convertibility mechanism stage for cryptoassets.

Furthermore, if Canada can properly regulate the convertibility mechanisms, which is the point of entry for a large majority of these transactions, then the Federal government will be able to effectively monitor the only point in cryptoasset transactions where the identity of users and source of funds can be accurately determined.

It is important to bear in mind that regardless of the regulations implemented into this space by the Canadian legislators, there are always going to be areas where proper enforcement of these regulations is going to be difficult, such as the exchange of one cryptoasset to another without the use of a convertibility mechanism. However, by focusing regulatory efforts on the convertibility mechanisms using an AML/ATF framework, Canada will be able to minimize the risk of money laundering and terrorist financing in this space.

13. AT WHAT POINT SHOULD CRYTOASSETS BE REGULATED?

As set forth above, we suggest that the key point of regulation should occur at the coverability mechanism. Governments and international organizations have struggled with the details of how cryptoassets should be regulated in this rapidly-growing space. An important aspect of this debate focuses on the Canadian government balancing protection of cryptoassets users with ensuring Canadian competitiveness of its financial technology. Other points of this debate include seeking regulatory equilibrium among innovation, privacy and protection of stakeholders. Ms. Christine Lagarde, Director of the International Monetary Fund, has stated that regulators need to respond to these cryptoasset-driven issues in order to "combat tax evasion, money laundering, and the financing of terrorism, ensuring that risks are thoroughly understood and managed."[149]

In this regard, the initial popularity of decentralized cryptoassets was due to their high degree of anonymity and lack of government regulation.[150] These cryptoasset attributes created an environment that could be used by criminals to facilitate money laundering and terrorist financing with a high degree of anonymity. Brown discusses the benefits of anonymity in the cryptoasset space as follows:

> In money laundering investigations, a main strategy has always been 'to follow the money'. Given that the details of all Bitcoin transactions are distributed to all account holders in the ledger, analysis of transaction flows and values against the timing of criminal activities should make it possible to spot the Bitcoin pseudonyms involved and to follow their transaction history. The challenge then would be to link the pseudonym to a real person and, as mentioned already, the decentralised nature of Bitcoin makes this particularly difficult.[151]

[149] Christine Lagarde, "A Regulatory Approach to Fintech", (March 2018) online: *Finance & Development* 55:2 < http://www.imf.org/external/pubs/ft/fandd/2018/06/how-policymakers-should-regulate-cryptoassets-and-fintech/straight.pdf>.
[150] Steven David Brown, "Cryptocurrency and criminality: the Bitcoin opportunity" (2016) 89:4 The Police Journal: Theory, Practice and Principals 327.
[151] *Ibid*.

Such anonymity makes it highly improbable that any modern tool or mechanism would be able to track any direct exchange of cryptoassets when they are strictly peer-to-peer transactions from one user to another (e.g., over-the-counter transactions). Attempting to regulate this segment of cryptoasset transactions will ultimately generate little value for the regulators, as this activity will expend significant resources on the incorrect aspect transaction. This concept is similar to two criminals exchanging large amounts of physical fiat currency (cash) between one another without the use of a financial institution intermediary. In both examples, effective monitoring will be both costly and highly ineffective, as attempting to regulate every aspect of a cash or a cryptoasset transaction will largely be futile. Sharma effectively explains this concept:

> It is important to note that all of the money laundering and illegal activities that Bitcoins can be used for, can also be done cash. That is, cash has been the primary mode of payment for drug dealers, money launderers, and other violent criminals. But since so many ordinary citizens also rely on cash for everyday payments, governments cannot ban cash. Similarly, even though a small fraction of Bitcoin transactions may be used for illegal activities, it is counterproductive to ban all of cryptocurrencies as that they have potential to improve the current banking system by a lot. Instead, governments should focus their energies on using this revolutionary technology to bring more transparency into their function.[152]

One option for regulation would be a complete and outright ban on cryptoassets, which has been the method pursued by the People's Bank of China[153] and the State Bank of Vietnam,[154] both of which have enacted laws banning any financial institution from handling or conducting any cryptoasset transaction. We concur with Sharma's comments above that such prohibition seems counter-intuitive, as an intrusive degree of regulation or an outright ban may even result in negative externalities through the creation of an underground network, eventually leading these states to reverse their bans and focus instead on how to best regulate cryptoassets.[155] Such extensive regulation would hence be counter-productive to protecting the AML/ATF regimes of Canada.

---

[152] Toshendra Kumar Sharma, "How does Bitcoin Money Laundering Work" (27 January, 2018), Blockchain Council (blog), online: <www.blockchaincouncil.org>.
[153] Xie Yu, "China orders banks to stop financing cryptocurrencies as noose tightens around disrupter", *South China Morning Post* (19 January 2018), online: < https://www.scmp.com/business/banking-finance/article/2129645/pboc-orders-banks-halt-banking-services-cryptocurrency>.
[154] Bank Indonesia Communication Department, Press Release, 20/50/DKom, "Trade Balance Deficit Decreases" (25 June 2018), online: <https://www.bi.go.id/en/ruang-media/siaran-pers/Pages/sp_205018.aspx>.
[155] Gilly Wright, "Cryptocurrencies Face Bans, More Regulation", *Global Finance magazine* 32:2 (2 February 2018) 10, online: < https://www.gfmag.com/magazine/february-2018/cryptocurrencies-face-bans-more-regulations>.

Again, these considerations favour a regulatory focus on convertibility mechanisms. A convertibility mechanism constitutes the exchange mechanism or processor through which users are able to convert their cryptoasset into fiat money (or *vice versa*). The French Ministry of Finance stated that "assessing the risks associated with virtual currencies must factor in how these currencies are issued, how they are used and in particular transparency of flows, issues of liquidity and their convertibility to legal tender."[156] Initial concerns expressed by the French Ministry of Finance related to the potential lack of transparency required when setting up a cryptoasset wallet and the total anonymity underlying cryptoasset transactions, rendering critical the necessity to "address the issues of the identities of the principal and effective beneficiary."[157] The French Ministry of Finance was also concerned with the extraterritoriality aspect of cryptoassets, given the ability of the cryptoasset transactions to be rapidly and discreetly conducted across international borders.

While attempting to regulate peer-to-peer cryptoasset transactions is largely futile, it would be far more effective to instead place the regulatory burden on cryptoasset exchanges that are the primary convertibility mechanism used in order to convert the value of fiat currency into cryptoassets. While this structure would still permit certain cryptoasset transactions to be executed through trades between cryptoassets and physical cash in an "underground" market, while the preponderance of transactions are completed on cryptoasset exchanges, these exchanges constitute the area where regulatory bodies should concentrate their AML/ATF efforts. For this reason, certain exchanges have voluntarily registered themselves in Canada to be MSBs to be compliant with the current AML/ATF framework, prior to the Proposed Amendments, with the intent to gain the public trust.

14. KYC

The term KYC describes the process of a business verifying the identity of its potential clients and assessing potential risks of illegal activities underlying the business relationship. KYC is one of the key measures which can be implemented to reduce the risk of money laundering and terrorist financing. Indeed, as noted in the summary of the Supreme Court of Canada's decision in *Canada (A.G.) v. Federation of Law Societies*:[158]

> There is a risk that financial intermediaries — those who handle funds on behalf of others — may facilitate money laundering or terrorist financing. To reduce that risk, Canada's anti-money laundering and anti-terrorist financing legislation imposes duties on financial intermediaries, including lawyers, accountants, life insurance brokers, securities dealers and others. They must collect information in order to verify the identity of those on whose behalf they pay or receive money, keep records of the transactions, and establish internal programs to ensure compliance. The legislation also subjects financial intermediaries, including lawyers, to searches and seizures of the material that they are required to collect, record and retain.

[156] Virtual Currencies Working Group, "Regulating Virtual Currencies – Recommendations to prevent virtual currencies from being used for fraudulent purposes and money laundering" (June 2014), online: Docplayer <https://www.economie.gouv.fr/files/regulatingvirtualcurrencies.pdf>.
[157] *Ibid* at 4.
[158] 2015 SCC 7, [2015] 1 SCR 401.

The Auditor General of Canada identified the best point to combat money laundering and terrorist financing as occurring with the "front-line employees – who deal with customers on a day to day basis."[159] These employees are in the ideal position to be able to identify transactions that may be categorized as unusual or suspicious. It is important for employees who are positioned on the "front-line" to be able to recognize what constitutes an unusual or suspicious transaction, which define the triggering events leading to suspicious transactions, as they are the gatekeepers for preventing money from being laundered through the organization by which they are employed.

KYC is guided in Canada by FINTRAC, which updated its guidelines in June 2017, expanding and further defining the accepted methods for identifying a client in order to ensure compliance with AML/ATF objectives. FINTRAC has outlined various types of transactions or activities required to identify individuals and confirm the existence of entities. Included in this list of transactions and activities are casinos, financial entities, real estate, securities dealers and money services businesses ("MSBs"). The various KYC requirements for these occupations are detailed under the *PCMLTFA,* including those relating to business relationships, ongoing monitoring processes, beneficial ownership guidelines, third-party determination and regulations relating to politically-exposed persons and heads of international organizations.

In relation to cryptoasset transactions, KYC requirements will most easily and efficiently be completed at the point of a cryptoasset convertibility mechanism. **We recommend that entities operating as convertibility mechanisms would ideally be required to register as MSBs for purposes of AML/ATF enforcement.** As discussed hereinabove, it is at the convertibility mechanism level where government regulation would be most effectively able to implement a KYC-based strategy.

15. CRYPTOASSET EXCHANGES UNDER MSB

In Canada, the law that establishes the AML/ATF framework, Bill-31, *An Act to Implement Certain Provisions of the Budget Tabled in Parliament on February 11, 2014 and Other Measures*[160] ("Bill C-31") was given Royal Assent on June 19, 2014. Despite the fact that the Governor in Council was conferred the right in subsection 73.1(a) of the *PCMLTFA*[161] to make any regulations with respect to "*dealing in virtual currencies*," the *PCMLTFA* was never amended to include a definition of "dealing in virtual currencies," therefore creating a legislative gap. If "virtual currencies" are not to be clearly defined, this situation has the potential to create an over-reaching regime wherein every person who is involved in the cryptoasset sphere be required to register as an MSB.

---

[159] Canada, *supra* note 138.

[160] Bill C-31, *An Act to implement certain provisions of the budget tabled in Parliament on February 11, 2014 and other measures*, 2nd Sess, 41st Parl, 2014, cl 256(2) (assented to 19 June 2014), SC 2014, c 20.

[161] *PCMLTFA*, *supra* note 3. Indeed, under the Section entitled "AMENDMENTS NOT IN FORCE" of the *PCMLTFA*, it is expressly written:

> AMENDMENTS NOT IN FORCE
> — 2014, c. 20, s. 256(2), as amended by 2017, c. 20, s. 436
> 2006, c. 12, s. 3(1)
> 256 (2) Paragraph 5(h) of the Act is replaced by the following:
> (h) persons///' and entities that have a place of business in Canada and that are engaged in the business of providing at least one of the following services:
> […]
> (iv) dealing in virtual currencies, or
> (v) any prescribed service;
> […]

In addition to this problem, the legislators, for reasons unknown to us, did not replace paragraph 5(h) of the *PCMLTFA* to include those persons "dealing in virtual currencies." Accordingly, there is no regulatory requirement for such persons to fall under the auspices of "money services businesses," obligating them to comply with the various requirements of the *PCMLTFA*, including: (a) record keeping, (b) verifying identity, (c) reporting of suspicious transactions, and (d) registration, as set forth in the FINTRAC Advisory regarding Money Services Businesses dealing in virtual currency.[162] The legislation also does not appear to explore any of the mechanisms relating to the convertibility of cryptoassets into fiat currency (and *vice versa*), which should trigger the application of the *PCMLTFA*. FINTRAC also appears to have given conflicting policy interpretations[163] as to how cryptoasset businesses must be treated under the PCMLTFA and whether they would be defined as an MSB, which can be observed in Schedule A thereof (Schedule A is appended to our report).

When Bill C-31 was given Royal Assent in 2014, it is curious that the legislators never defined "dealing in virtual currencies" in the *PCMLTFA*. It is also perplexing why this phrase was never amended into paragraph 5(h) of the Act in order to regulate certain cryptoasset businesses as MSBs. In this connection, it is important for the legislators to enact legislation that strikes a balance between an effective AML/ATF regime and one that does not stifle innovation in Canadian financial technology, preventing it from becoming a global leader in this space.

> (h.1) persons and entities that do not have a place of business in Canada, that are engaged in the business of providing at least one of the following services that is directed at persons or entities in Canada, and that provide those services to their clients in Canada:
> […]
> (iv) dealing in virtual currencies, or
> (v) any prescribed service;
> […]

[162] Canada, Financial Transactions and Reports Analysis Centre of Canada, *Register your money services business (MSB)* (Ottawa: 2017) < http://www.fintrac-canafe.gc.ca/msb-esm/register-inscrire/reg-ins-eng.asp>.

[163] Canada, Financial Transactions and Reports Analysis Centre of Canada, *FINTRAC Policy Interpretations* (Ottawa: 2017) <http://www.fintrac-canafe.gc.ca/guidance-directives/overview-apercu/FINS/2-eng.asp?s=12>.

16. AN EXAMINATION OF REGULATORY MODELS FROM SWITZERLAND AND SINGAPORE

16.1. SINGAPORE[164]

I. Introduction

Singapore has comfortably settled into its position as one of the world's cryptohavens, as it continues to be a magnet for blockchain ecosystem operations and capital raises, amidst the ups and downs of some of the most popular virtual currencies, such as Ethereum. We examine and analyse below some of the key components of Singaporean legal and regulatory aspects, including legal documentation, data protection, KYC and AML considerations, as well as intellectual property.

II. The Bedrock is the "Solution"

In a typical blockchain cryptocurrency ecosystem, a community exists whose members all have roles to play in the implementation of a solution to an identified problem. Alternatively referred to as a protocol or platform, the solution is the crucial bedrock, as without a viable, practical solution, irrespective of capital raised or number of supporters, the ecosystem is unlikely to succeed. In addition to the technology, thought processes and sophistication behind some of the solutions, the same simplistic market feasibility exercises of the past could work in determining the predicted success or not of a solution, in terms of its usefulness, practicality and sustainability. So, before even starting, the critical question to be considered is "is our solution useful, practical and desirable, and does it make business sense?"

There are, however, some founders who create a new virtual currency on the pretense of a solution, but whose main goal is to see it trade on an exchange, hopefully increase in its value, and gain quick wealth. These participants are not concerned at all about the development or use of the ecosystem and building a community, but only in creating an asset that is driven by speculation. Further to this extent, some participants do not mind that they are engaging in a speculative activity, as long as they ultimately profit, as they never intended on being a long-term part of a cryptoasset ecosystem.

III. Why is Singapore an Attractive Option?

Singapore has been described by many as a conducive landscape for cryptocurrencies and blockchain technology to flourish due to its superb communications network, its global reputation as a financial hub, characterized by non-interference and a balanced approach by regulators, and growing interest in FinTech.

[164] Franca Ciambella *et al.*, *Blockchain Cryptocurrency & the Legal Environment in Singapore* (Singapore: Consilium Law Corporation, 2017).

Unlike some other countries, Singapore has taken a liberal approach and opted for a more balanced view – it has embraced cryptoasset start-ups - and the government has set into motion large-scale initiatives to drive FinTech growth and innovation. The challenge faced by the Singaporean regulator, the Monetary Authority of Singapore ("MAS") is in ensuring the retail investor and the greater public are adequately protected from "scam" offerings and to instill proper safeguards. Importantly, a key objective of the MAS is to not adopt too many restrictions so as to stifle the crypto environment.

The great interest in the cryptocurrency space in Singapore is from investors and corporations (both local and foreign) alike. The individual investors or token purchasers want to invest in the various cryptocurrencies being issued, while corporations are interested in conducting a token-generation event ("TGE") related to the issue of digital tokens in Singapore and raising capital (the terms ICO and TGE are used herein interchangeably).

Singapore is viewed as an attractive jurisdiction to conduct a TGE because, among other things; (1) it is easy to incorporate an entity in Singapore; and (2) the MAS has taken the position (as of August 1, 2017) that it will not regulate the offer or issue of digital tokens provided the digital tokens do not constitute products that are regulated under the *Securities and Futures Act* (Cap. 289) ("SFA") in Singapore. The lack of express prohibition on the issuance of digital tokens and the perception that decentralised cryptocurrencies are considered unregulated assets is therefore the reason Singapore, along with Switzerland, has been identified by many as a "crypto-haven."

Having said that, it must be noted that more recently, after the publication of "The DAO Report" in July 2017 by the SEC, MAS issued "A Guide to Digital Token Offerings" on November 15, 2017. The guide elaborated that the offering of digital tokens must comply with the SFA only if the digital token constitutes a product regulated under the SFA.

In its guide, MAS also provides several hypothetical case studies of digital tokens that would be regulated in Singapore and others that would fall outside the ambit of its regulatory framework. There is now a clearer picture for potential offerors on which of their offerings may be caught by MAS' regulatory framework.

MAS has said that it will carefully assess the nature, composition and specifications of the digital token, and has created a "Sandbox" approach in doing so, in an effort to provide speedy replies.

Notwithstanding regulation, an investor must take into account that there will always be inherent commercial risks in the investment, largely due to the success of the solution as discussed above, which could result in an investor losing all or a substantial portion of its investment. This brings us to the second step in the regulatory analysis: It could very well be that the token itself is not regulated, but that the solution or activity of the platform is regulated. For example, if tokens are used for a protocol whose activity is regulated in Singapore, such as insurance or moneylending, then the licenses required by these activities would need to be procured.

IV. Typical Legal Documentation Used for TGE/ICO

The practical reality then is that the only recourse available to a supporter or investor investing or buying into an unregulated digital token or coin offering may be the legal provisions found in the commercial agreements entered into between an investor or supporter and the Token/Coin Generator.

In terms of structuring a TGE or ICO, one way might be for the actual Generator to be set up as a foundation, which is usually in the form of a company limited by a guarantee, as this company is meant to carry out non-profit making activities that have some basis of national or public interest. The actual platform may be operated by a separate operating company. This can be a private limited company which should ideally be responsible for the on-boarding of the users and platform development. The agreements typically involved in such a structure are both a development and service contract.

We set out below some of the other documentation and agreements typically used in digital token or coin offerings in Singapore:

(1) *White Paper*

The "White Paper" is a document that provides an investor with a preliminary understanding of the intent of the Token or Coin Generator, objectives of the offering, technology behind the project (for example if it is underpinned by blockchain technology), type of corporate structure used in a potential offering and also the financial modelling of the token generation.

The White Paper is often the first document published on the website of the Token Generator and serves as an "expression of interest" to the potential investor. It is imperative for a potential investor to review the information in the White Paper carefully and ask the right questions so that he or she understands the technology behind the digital tokens issuance for example, prior to making an investment.

(2) *Legal Opinion*

The "Legal Opinion" is an essential first step in Singapore, as its purpose is to analyse the characteristics of the token and determine whether its "behaviour" falls within the scope of the SFA, and any other legislation pertaining to securities law. It would provide advice on any licenses or disclosure requirements required for an ICO. The Legal Opinion would also typically include advice on any other laws that would apply to the operation of the platform.

(3) *Pre-Sale Agreement*

The Pre-Sale Agreement ("**PSA**"), as its name implies, is an agreement that is entered into between selected investors and the Generator ahead of the "crowd-sale."

The pre-sale is usually convened prior to the main TGE or ICO process in order for the Generator to pre-sell the digital tokens or coins to a select group of potential supporters or investors (such as family, friends and selected investors) at discounted prices and for a limited period of time as determined by the Generator. The pre-sale is also a useful way for the Generator to gauge interests in the digital token offering ahead of the crowd-sale with the TGE/ICO. It must also be emphasized that selling too many tokens at a pre-sale may not in fact be a good thing because for an ecosystem or a community to be successful, it often needs a large number of supporters. Selling tokens quickly to a small group may limit the number and scope of supporters, and ultimately the success of a community.

In certain cases, Generators offer a localized version of the Sale of Future Tokens Agreement ("SAFT") that is compliant with Singapore law, as a means of a pre-sale document.

In certain transactions, parties may decide to enter into an escrow arrangement ahead of the TGE whereby an escrow agent will hold relevant cryptocurrency in trust for the investor, which will be released to the Token Generator upon certain trigger events occurring.

(4) *TGE Terms & Conditions*

The TGE or ICO Terms & Conditions (the "TGE Documentation") comprise the main documentation used in the "crowd-sale."

The TGE Documentation usually contains, among other things, information about the Token Generator, restrictions on distribution of the tokens, disclaimer, indemnification and self-regulation, features of the tokens, procedures for acquiring and receiving tokens and representations and warranties by investors.

In other words, the TGE Documentation is the main legally-binding agreement between the investor and Token Generator and will clearly set out the liability of the Token Generator to the investor in the event that any risks in the issuance materialize. It is therefore essential for the investor to carefully review the TGE Documentation and understand its implications ahead of the investment.

The TGE Documentation will also contain certain commercial terms which will be specific to each offering and differ, depending on the factual matrix and technological details of the offering.

(5) *Compliance Manual*

The Token Generator would generally have in place a robust compliance manual that will contain information on general compliance of the operating entity (that issues the tokens), relationship with regulators (if applicable), corruption and anti-bribery provisions, record keeping and personal data protection policy and more importantly, anti-money laundering and fraud provisions.

MAS has emphasized that the relevant MAS Notices on Prevention of Money Laundering and Countering the Financing of Terrorism may still apply to digital tokens that fall outside the MAS regulatory framework (especially the obligations to report suspicious transactions with the Suspicious Transaction Reporting Office of the Commercial Affairs Department and prohibitions against dealing with or providing financial services to designated individuals and corporates pursuant to the *Terrorism (Suppression of Financing) Act* (Cap. 325)), as well as any related subsidiary legislation.

It would be prudent for an investor to ask the Token Generator if it has in place a robust compliance manual containing all of the provisions mentioned above and whether the Token Generator is willing to share such compliance manual with the investor at the opportune time.

The MAS has also announced that it will, in due course, establish a new payment services framework to include rules to address money laundering and terrorism financing risks related to the dealing or exchange of virtual currencies for fiat or other virtual currencies. It is advisable that the investors seek clarification from the Token Generator intermediaries on whether MAS has issued those guidelines already and, if so, whether they have put in place the required framework before investing.

V. Personal Data Protection

Section 2(1) of the Personal Data Protection Act ("**PDPA**") states that:

> *"'personal data' means data, whether true or not, about an individual who can be identified —*
> *(a) from that data; or*
> *(b) from that data and other information to which the organisation has or is likely to have access;"*

The personal details of the participants collected online at the time of the ICO will constitute personal data under the PDPA. According to the PDPA, a Generator will have to obtain the consent of the participants in order to collect, use and disclose the personal data, and the collection has to be reasonable to provide the product services. The Generator also has to ensure it has made reasonable efforts to prevent unauthorised access to the data. Once the purpose for having the data is over, then the Generator has to cease retaining the personal data.

Section 26 of the PDPA requires that a Generator refrain from transferring any personal data to a country or territory outside Singapore except to organisations that provide a standard of protection to personal data that is comparable to the protection under the PDPA. This is relevant when an ICO is undertaken over a number of countries.

The recent passage of the General Data Protection Regulation and its extra territorial application also presents certain obligations in Singapore if any of the Participants are from the European Union.

VI. KYC/AML

The KYC and AML considerations, as stated above and as included in the compliance manuals, would also be included in the questionnaires for information on supporters or buyers of tokens. While it is unclear whether the *Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act* (Cap.65A) ("CDSA") may apply to cryptocurrencies, it would be prudent for the Generator to have in place comprehensive questionnaires collecting the identifying information under the CDSA from potential investors, or supporters either at the pre-TGE or TGE stage.

VII. Intellectual Property

In Singapore, copyright is not registrable. Therefore, in order to protect the copyright of the software source codes, the Generator should keep concise records, including dates of creation, of the software source codes for the blockchain protocol.

The Generator should also look into the possibility of registering its patent (if any) for any new processes for its blockchain technology and consider registering any trademarks it has with the Intellectual Property Office of Singapore.

VIII. Conclusion

The decentralised monetary system of cryptocurrencies is likely to be the future of financial transactions in Singapore and will also revolutionise the global financial landscape. It will be interesting to see how MAS attempts to strike a balance between permitting this virtual currency platform to grow and prosper in Singapore and enhancing an already complex regulatory regime with safeguards, with its attempts to protect not only investors, but the public at large. It will also be interesting to see what methods Token or Coin Generators take to ensure their "Solutions" make good commercial sense so that their communities or ecosystems succeed.

16.2 SWITZERLAND[165]

On November 16, 2016, the Swiss Financial Market Supervisory Authority (FINMA) issued its strategic goals for 2017 to 2020. Goal No. 5 is to "*push for the removal of unnecessary regulatory obstacles for innovative business models*,"[166] for crowdfunding in particular and FinTech in general.

On August 1, 2017, the first new FinTech rules entered into force.[167] Moreover, a new banking license (banking license light) is currently being discussed in Switzerland based on a draft of regulations published on June 21, 2018. The objective of this new license is for entities (other than banks) to be able to accept deposits up to CHF 100 million.[168]

Given, in particular, the Swiss political decision to open its regulations to FinTech (as a strategical objective), events are currently moving quite fast in Switzerland.

On February 16, 2018, FINMA has published guidelines on ICOs[169] (the FINMA Guidelines).

This article is based principally on these FINMA Guidelines (as well as on the first FINMA decisions received), given that they provide for a relatively clear definition of the different categories of tokens and of the applicable Swiss regulation.

I. FINMA Guidelines / Categories of Tokens

FINMA bases its approach on the underlying economic function of the token.[170] It distinguishes three types of tokens:

(1) Payment Tokens

Payment tokens (synonymous with cryptocurrencies) are tokens which are intended to be used as a mean of payment for acquiring goods or services or as a means of money or value transfer.[171]

According to Article 3 Para. 2 Let. b, the issuance of means of payment (which includes payments tokens/cryptocurrencies) by a Swiss entity (i.e. one having a physical presence in Switzerland) is subject to the *Swiss Anti-Money Laundering Act* of October 10, 1997.

One of the consequences of this regulation is that the Swiss issuing entity should be affiliated to a self-regulatory organization (SRO) for AML purposes. This being said, the issuer may choose the option to delegate the acceptance of the funds/amounts to be received to a third-party Swiss financial intermediary (itself being subject to AML).

---

[165] Alexandre de Boccard, *Swiss regulatory framework applicable to Token Generating Event (TGE / Initial)*, (Switzerland, Ochsner & Associes, 2018).
[166] Swiss Financial Market Supervisory Authority, "FINMA's strategic goals" <https://www.finma.ch/en/finma/supervisory-objectives/strategy/>.
[167] Switzerland Government, The Federal Council, *Federal Council puts new fintech rules into force* (Bern: 05 July 2017) <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-67436.html>.
[168] Government of Switzerland, Le Chef du Département fédéral des finances DFF, Modification *de l'ordonnance sur les banques (autorisation FinTech) : ouverture de la procédure de consultation* (Switzerland : 21 June 2018) <https://www.admin.ch/ch/f/gg/pc/documents/2967/OB-autorisation-FinTech_Lettre_fr.pdf>.
[169] Swiss Financial Market Supervisory Authority, "FINMA publishes ICO guidelines" (16 February 2018) <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung>.
[170] FINMA Guidance 04/2017, 29 September 2017 (Switzerland), § 3.1, page 3 [FINMA].
[171] *Ibid*.

In case of such delegation, the issuer should not be subject to AML (as this may be confirmed by FINMA in the context of a non-action letter). Several third-party financial intermediaries currently provide for such KYC/AML tasks. In addition, several Swiss banks have agreed to open commercial accounts (denominated in fiat) for companies that have performed an ICO.

(2) Utility Tokens

Utility tokens are tokens which are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure.[172]

For example, the utility token "*has additionally an investment purpose at the time of its issuance*,"[173] in other words, if the proceeds (even part of them) of the ICO are used to develop the main function of the token/platform (blockchain technology), FINMA treats such a token as a security.[174]

However, in the case where the security does not provide for (i) voting rights (such as equity/stocks/shares), and/or (ii) economic rights of the issuer (such as equity, stock, shares or participation rights) and/or (iii) a claim (debt issued by the issuer, such as bonds), the token may qualify as "uncertificated security." The main requirement to issue such uncertificated securities (on the primary market) is to maintain a token and tokenholders' register (which can be accomplished digitally using a blockchain, as this has been confirmed by FINMA).[175] However, based on the same assumption (i.e., no voting or ownership rights granted by the issuer, and/or no outstanding debt of the issuer), no prospectus is required under current Swiss laws (more specifically the *Swiss Code of Obligations*).

(3) Asset Tokens (Securities Tokens)

FINMA uses the term "asset token" instead of "security token." This being said, materially and from a Swiss legal perspective, these concepts are essentially similar.

According to the FINMA Guide, asset tokens represent assets such as a debt or equity of the issuer. In terms of their economic function, these tokens are analogous to equities, bonds or derivatives.[176] To complete the picture, we could add the structured products and the mutual funds.

In case the tokens qualify as equities (including participation rights; i.e., shares without voting rights) or bonds, an issuing prospectus according to Swiss law is required in case the tokens are offered or sold to the public (i.e., not being exclusively offered to a limited circle of investors). However, under the current laws (more specifically the *Swiss Code of Obligations*), no filing or review of the prospectus by the regulator or another official or self-regulated body is required.

In addition, in case the issuance is performed "for own account," no license (as securities trader) is required under Swiss law. In other words, the issuance of share tokens, participation-right tokens or debt tokens for own account is, in principle, not subject to Swiss financial laws, authorization requirements, or prospectus content requirements.

[172] *Ibid*.
[173] *Ibid* at § 3.2.2, page 5.
[174] *Ibid*.
[175] *Ibid* at § 3.2, page 4.
[176] *Ibid* at § 3.1, page 3.

Finally, tokens enabling physical assets to be traded on the blockchain also fall within the category of asset tokens. Such tokens may qualify as "uncertificated securities."

II. Cantons: Zoug, Neuchâtel & Geneva

As in Canada, Switzerland is a federal jurisdiction. The "provinces" are called "Cantons." Several Cantons are very welcoming to blockchain and issuers of tokens, such as Zoug, Neuchâtel & Geneva.

On May 28, 2018, the Canton of Geneva published an ICO guide to provide specific information (including taxation-related matters) and to assist token issuers (whether Swiss or foreign promoters) on all aspects and different steps of an ICO,[177] including post-ICO events.

Thanks to the sophisticated blockchain, crowdfunding and smart contract ecosystem developed promptly and efficiently by the Canton of Geneva, token projects can be presented to the Canton within a short time frame, as well as simultaneously to various experts, such as Swiss banks, Geneva tax authorities, KYC/AML providers, FinTech specialists, as well as tax advisors and lawyers specialized in FinTech (all subject to a non-disclosure agreement and other internal rules).

17. CONCLUSIONS — TOWARDS A NEW CRYPTOASSET REGULATORY REGIME

Through our above comparative examination of the current global regulatory regimes addressing cryptoassets and the complexity of the cryptoasset space, we propose that establishing a new regulatory regime in Canada would constitute the most prudent approach "on the grounds that these offerings are so new and multi-faceted that they cannot be captured satisfactorily by existing regulations."[178] To this extent, "creating a new regulatory regime… is an extremely difficult and resource-consuming task"; realistically, the requisite time required to implement such a framework would necessitate a long-term planning horizon.[179]

[177] Republic and State of Geneva, Department of Security and Economy, *Initial Coin Offerings (ICOs) in the Canon of Geneva* (Geneva: 28 May 2018) <https://www.ge.ch/document/guide-initial-coin-offerings-icos-canton-geneva>.
[178] France, Autorité Des Marches Financiers, *Discussion Paper on Initial Coin Offerings* (Discussion Paper) (2017).
[179] *Ibid*.

As an initial measure, there exists notable support[180] that those "dealing in virtual currencies" should be regulated under Canada's AML/ATF legislative framework, and, more particularly, as domestic and/or foreign MSBs (i.e., reporting entities) that are subject to obligations of: (i) record keeping, (ii) KYC, and (iii) reporting.[181] Furthermore, the Federal Government has appropriately taken the initiative in releasing its Proposed Amendments (on June 9, 2018), containing the *caveat* that cryptoassets might actually be harder to launder than traditional fiat.[182]

Based on the conclusions gleaned from our examination of the current Canadian regulatory landscape, review of the inherent attributes of cryptoassets and analysis of certain international models of cryptocurrency from the United States, Switzerland and Singapore, we offer the following recommendations:

1. **The definition of "virtual currency" (or cryptoasset) should be replaced by "cryptoasset" so as to avoid ambiguity and indefiniteness**

Under the heading "Virtual Currencies" of the Federal Regulatory Impact Assessment Statement, virtual currencies are described therein as:

> The evolving financial services landscape is further influenced by virtual currencies, especially decentralized digital payment systems, like Bitcoin, that operate outside the traditional financial system. A virtual currency is a medium of exchange that allows for value to be held and exchanged in an electronic, non-physical manner, is not a fiat currency (i.e. the official currency of a country), has the intended purpose of being exchanged for real and virtual goods and services, and allows peer-to-peer transfers.
>
> Virtual currencies can be "centralized," in that they are issued and controlled by a single company or entity, or "decentralized," in that there is no central authority that creates or manages it (e.g. Bitcoin). Rather, these tasks are managed collectively by the network of some virtual currency users.

---

[180] See the evidence submitted by:

- **Dominion Bitcoin Mining Company** (available at: http://www.ourcommons.ca/Content/Committee/421/FINA/Brief/BR9977217/br-external/DominionBitcoinMiningCompany-e.pdf);
- **Ms. Annette Ryan (Associate Assistant Deputy Minister, Financial Sector Policy Branch, Department of Finance)** (available at: http://www.ourcommons.ca/DocumentViewer/en/42-1/FINA/meeting-163/evidence#Int-10230587);
- **Mr. Luc Beaudry (Assistant Director, Collaboration, Development and Research Sector, Financial Transactions and Reports Analysis Centre of Canada)** (available at: http://www.ourcommons.ca/DocumentViewer/en/42-1/FINA/meeting-133/evidence#Int-9976970);
- **Mr. Kyle Kemper (Executive Director, Blockchain Association of Canada)** (available at: http://www.ourcommons.ca/DocumentViewer/en/42-1/FINA/meeting-140/evidence#Int-10039264);
- **Stuart Davis, Chief Anti-Money Laundering Officer, AML Enterprise, BMO Financial Group** (available at: http://www.ourcommons.ca/DocumentViewer/en/42-1/FINA/meeting-140/evidence#Int-10039264).

[181] It is worth mentioning that FINTRAC's guidance document, entitled "Guideline 2: Suspicious Transactions" (June 2017), available at: http://www.fintrac.gc.ca/guidance-directives/transaction-operation/Guide2/2-eng.asp, provides, at sections 7 and 8 thereof, good indicators and KYC measures with respect to triggering events of suspicious transactions.

[182] Kai Sedgwick, "Cryptocurrency is Harder to Launder Than Fiat Currency" (2 February 2018) online: Bitcoin.com <https://news.bitcoin.com/cryptocurrency-harder-launder-fiat-currency/> as shown through the quote ("[d]ue to the nature of public blockchains and the need to cash out into fiat, cryptocurrency is easier to monitor").

> In addition, virtual currencies can be "convertible" or "non-convertible," depending on whether they can be exchanged for funds. Convertible virtual currencies are vulnerable to abuse for money laundering and terrorist activity financing purposes because they allow greater levels of anonymity, or in some cases complete anonymity, when compared to traditional non-cash payment methods. Virtual currencies can be accessed globally via online or mobile systems. They allow for the rapid transfer of funds within or across borders, oftentimes without any intermediary, are generally characterized by non-face-to-face customer relationships and can circumvent the physical "brick and mortar" financial system entirely. Due to these characteristics, virtual currencies are increasingly being used to facilitate fraud and cybercrime, and to purchase illicit goods and services on the Dark Web.

The Proposed Amendments currently define the term "virtual currency" as:

> (a) a digital currency that is not a fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or
>
> (b) information that enables a person or entity to have access to a digital currency referred to in paragraph (a).[183]

This proposed definition of "virtual currency" is insufficient, as it promotes the perception that it is: (i) a "currency," which it is not (discussed in Section 5 above), (ii) a "digital currency,"[184] which it cannot be considered, as there is no definition thereof under current Canadian legislation for such expression,[185] (iii) a form of "electronic money," similarly for which no definition thereof exists under current Canadian legislation, (iv) or money.[186]

Moreover, it is not possible to ascertain whether the current definition of "virtual currency" would capture ICOs, ITOs and their corresponding tokens, such as transactional, utility and platform tokens. Tokens may not share similar characteristics (or attributes) with traditional currency or cryptocurrencies, such as Bitcoin and/or Ether. [187] Among the unintended negative consequences of using the phrase "dealing in virtual currency" is that it is not possible to determine whether users of the cryptoassets, exchange services, value transfer services, mining services or such other exchanges, all of which may act as convertibility mechanisms, are encompassed by said terminology.

---

[183] Canada Gazette, *supra* note 5 at 1(7), 14, 15, 25, 26, 27, 29, 31, 32, 33, 35, 36, 40, 42, 49, 51, 55, 57, 61, 63, 67, 69, 70, 73, 79, 81, 82, 84, 86, 95, 116, 120, 121, 122, 123, 125, 129, 133, 135, 136, 137, 144, 146, 154, 155, the section as it pertains to Schedule 4 and 5 of the Proposed Amendments.
[184] Government of Canada, Financial Consumer Agency of Canada, *Digital Currency* (Ottawa: 19 January 2018) < https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html>. According to the Government of Canada's website "digital currency" can be considered "electronic money".
[185] As of July 9th, 2018, there is no mention of "digital currency" on the legislation (using 'http://laws-lois.justice.gc.ca/Search/Search.aspx' to search).
[186] Straitev, *supra* note 19.
[187] Haeems, *supra* note 9.

One possible course of action could be to amend the *PCMLTFA* to include the definition of "virtual currencies" or, ideally utilize the term "cryptoasset" in the legislation, which would fall in line with European Union banking authorities and/or FINCEN's definition of same, as there does not currently exist any consensus in Canada[188] as to how a "virtual currency" (or "cryptoasset") should be defined. Specifically, "cryptoasset" could be defined (as per the EU banking authorities) as: "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a [fiat currency], but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically."[189]

2. AML/KYC enforcement pertaining to cryptoassets should occur at the convertibility mechanism nexus

In our view, the existing KYC framework in Canada is sufficient, indeed exemplary, in enforcing AML/ATF provisions relating to cryptoassets. To this extent, FINTRAC released "Guideline 2: Suspicious Transactions" in June 2017, which detail KYC procedures to be followed, as well as "red flags" that are potential indicators of money laundering and/or terrorist financing activities.

Moreover, KYC procedures are highly effective, as they may utilize sophisticated technological advancements to ascertain an individual's identity (e.g., facial recognition, document scanning and authentication). Such procedures may be easily implemented to ensure documents required to verify customer identity constitute those that are "authentic, valid and current"[190] and verifiable by an independent third party.

Such enforcement could occur by obligating those persons "*dealing in virtual currencies*" (or *"dealing in cryptoassets*"), for example, cryptoasset exchanges that would fall into the MSB regime, to adhere to the current *PCMLTFA*-MSB regime. These obligations would have the benefit of compelling compliance with the *PCMLTFA* requirements, including KYC processes to be implemented for the convertibility mechanisms. Moreover, "FINTRAC Guideline 2: Suspicious Transactions," should be continued to be used as a paradigm for KYC compliance.

[188] The Financial Consumer Agency of Canada loosely defines "digital currency" as electronic money that is not available as bills or coins, and are not legal tender in Canada. See: https://www.canada.ca/en/financial-consumer-agency/services/payment/digital-currency.html.
[189] European Banking Authority, "EBA Opinion on 'virtual currencies'" (4 July 2014), online: EBA <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf>.
[190] Canada Gazette, *supra* note 5.

18. AUTHORS AND ACKNOWLEDGEMENTS

AUTHORS

David Durand LL.L., B.Sc. (chem.) is a Founding Partner at Durand Morisseau LLP and is a member of the Québec Bar since 2011. Prior to founding Durand Morisseau LLP, David worked for various intellectual property boutique firms where he focused on technology and IP. David has recently been expanding his international network during his collaboration with firms from Switzerland and Singapore during the writing of this publication, as well as his practice in FinTech and regulatory issues.

Drew Dorweiler FRICS, FCBV, MBA, CPA•ABV, CPA (IL), ASA, CVA, CBA, CFE is a Managing Director of IJW & Co., Ltd. He possesses over 33 years of experience in valuation of hundreds of privately and publicly-held companies in business valuation, corporate finance and litigation support mandates on a global basis. Drew has frequently participated as a financial advisor in corporate mergers and acquisitions, divestitures and start-up businesses and in sourcing financing in North America and internationally. He has testified as expert witness in more than 27 cases before Québec Superior Court, Ontario Superior Court of Justice, U.S. District Court, Tax Court of Canada, Court of Queen's Bench of Alberta and arbitration panels in high-profile, complex financial litigation and valuation matters.

Drew has given numerous interviews featured in international TV, radio and print media on business valuation, financial and sports business matters. He has spoken at myriad conferences and authored many articles in professional publications on business valuation, litigation support and fraud-related topics during the past 28 years. Drew was elected to Board of Trustees of The Appraisal Foundation for 2013-2018 and to Board of Directors of The Canadian Institute of Chartered Business Valuators from 2006-2009 (he was named a Fellow in 2018). He was named a Fellow of Royal Institution of Chartered Surveyors in 2013 and elected President of the Board of Directors of the Montreal Chapter of the Association of Certified Fraud Examiners for 2005-2007. Drew graduated with a Bachelor of Arts, Economics, Dartmouth College. He obtained a dual MBA, Corporate Finance and Accounting, Lubin Graduate School of Business, Pace University.

Franca Ciambella is Managing Director of Consilium Law Corporation. Trained in law and business in Canada, New York and Singapore, Franca has been a member of the Québec Bar since 1990, and in 2010, was one of the first foreign lawyers to gain full admission to the Singapore Bar. Her legal career of over 25 years encompasses 16 years of private practice including being the Managing Partner of the Singapore office of Stikeman Elliott and a Legal Associate at Norton Rose, seven years as General Counsel for Asia Pacific for Tyco International Ltd. (a US based Fortune 500 corporation), acting as a technical advisor on regional economic integration to high levels of government in ASEAN, carrying on a mediation practice and since 2010, being the Managing Director of the Singapore-based international law firm of Consilium Law Corporation ("CLC"). CLC represents clients doing business in emerging economies, including in south-east Asia and Africa, as well as in Canada, in diverse sectors.

Franca's subject areas of legal expertise are in corporate and commercial law, contracts, technology law and FinTech, cross border M&A, foreign investment law and international trade with a focus on Canada, ASEAN and West Africa. Currently she is focusing on a number of technology projects and cutting-edge, multi-jurisdictional legal practice in the area of cryptocurrency and ICOs. She also assists clients in creating compliance programs, including anti-bribery, and trade compliance. Franca is accredited as a mediator with the Singapore Mediation Centre and with the ADR Group in London, UK, and acts as a mediator in various areas including cross-border family law disputes. Having an undergraduate commerce degree and a certificate in business (from the US and Canada), she also serves as an advisor to multinational businesses and as a director on several boards of corporations and non-profit organizations. She has authored numerous legal and business publications including a book entitled "Investments in South-east Asia: Policies and Laws," contributes regularly to various chambers of commerce publications and websites, and guest lectures to MBA students at McGill University and other educational institutions.

Alexandre de Boccard is a Swiss- and US-trained lawyer specialized in financial regulation. He is a partner of the Swiss law firm Ochsner & Associés. Alexandre de Boccard advises financial institutions such as banks, securities dealers, and asset managers on regulatory matters, contract law, corporate law, FinTech regulation, as well as stock exchange law. He also advises companies that are active in FinTech and has been the official legal partner of the Swiss Crowdfunding Association since its incorporation in 2015. Alexandre de Boccard assists clients in obtaining licenses from the Swiss Financial Market Supervisory Authority (FINMA), as well as negative rulings for activities such as crowdfunding, issuance of means of payment, Token Generating Events (TGE) and Initial Coin Offerings (ICOs). Ochsner & Associés is referenced by the Canton of the Geneva as an expert in ICOs.

Alexander Schaefer is entering his third year of law at the University of Windsor and has been working as a Student at Law for Durand Morisseau LLP at its Montréal office since May 2018. He has worked primarily on Regulatory and FinTech law during his time at the firm. Previous to this, Alexander worked as financial analyst at BMO Financial Group at the London, Ontario branch. Alexander graduated from the University of Western Ontario with a bachelor's degree in Political Science with Distinction.

SIGNATORY FIRMS

Durand Morisseau LLP provides various legal services to clients, including litigation, representation in IP prosecution, and business and commercial transactions, both in Canada and abroad. For more information about Durand Morisseau LLP's practice, please visit durandmorisseau.com.

Because of its generality, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. If you wish to make a comment on this publication, please write to: David Durand at Durand Morisseau LLP, 3 Place Ville Marie, Suite 400, Montréal (Québec) Canada, H3B-2E3 or email info@durandmorisseau.com.

IJW & Co., Ltd. is an investment bank providing mergers and acquisitions advisory, business valuation, litigation support (expert witness) and corporate finance services to clients globally. Headquartered in Canada, the firm has offices in the United States, Hong Kong, Singapore and Antigua. For more information on IJW & Co., Ltd.'s practice, please visit www.ijw.ca.

SCHEDULE A

Summary of FINTRAC Policy Interpretations Regarding MSBs (Virtual Currency)

Policy Interpretation	Rendered on	Description	Decision rendered by FINTRAC
PI-5404	2012-05-02	Securities dealer v. MSB - "There is additional clarification in the interpretations notice that states that a business would be exempt from MSB registration if the activity was carried out as part of another regulated activity (purchasing securities is provided as an example here). The question in this regard is whether the MSB definition would apply to a securities dealer that is also conducting foreign exchange transactions outside of the scope of securities related purchases - are they also required to be registered as an MSB?"	"Should a securities dealer provide money services business (MSB) activities, such as foreign exchange, outside of their securities dealer activities, the securities dealer would be required to register as an MSB. Upon registration as an MSB, the registrant would indicate that their business is also another type of reporting entity (i.e., a securities dealer). As an MSB and a securities dealer, the entity would be subject to all applicable sections of the [*PCMLTFA*] and its associated regulations."
PI-5549	2013-05-09	Business engaged in the trade of digital tokens, particularly Bitcoin and Litecoin.	"Based on the information you provided, namely that your 'business is engaged in the trade of digital tokens, particularly Bitcoin and Litecoin', it appears that your entity is not, at this time, engaged as an MSB in Canada as per the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its associated Regulations. In fact, your business doesn't provide the services of remitting and/or transferring funds for the sake of the service. The transfer of funds is simply a corollary of your actual service of trading virtual currency. Therefore, you do not have to register your entity with us."

PI-5550	2013-05-09	Buying and selling Bitcoins directly from customers; bitcoin payment provider; start an exchange.	"Based on the information you provided, namely that your entity 'Buy and Sell Bitcoins directly from customers', it appears that your entity is not, at this time, engaged as an MSB in Canada as per the [*PCMLTFA*] and its associated Regulations. In fact, your entity doesn't provide the services of remitting and/or transferring funds for the sake of the service. The transfer of funds is simply a corollary of your actual service of buying and selling virtual currency. Also, the creation of a 'software for business to accept Bitcoin payments and either keep Bitcoins or automatically convert to CAD' and an 'order book where people can put in an order at x price and hope it gets filled' does not make your entity, at this time, engaged as an MSB in Canada since your entity provides a platform allowing businesses to accept or trade virtual currency."
PI-5551	2013-05-09	Virtual currency – "Company ABC purchases virtual currency such as bitcoins, litecoins, Facebook credits, world of Warcraft coins at bulk discount rates and sells it at physical locations across the country as well as online through cash deposits in banks. In our physical stores we will collect the money from buyers first before sending them the virtual currencies."	Based on the fact pattern, "[…] it appears that your entity is not, at this time, engaged as a [MSB] in Canada as per the [*PCMLTFA*] and its associated Regulations. In fact, your entity doesn't provide the services of remitting and/or transferring funds for the sake of the service. The transfer of funds is simply a corollary of your actual service of buying and selling virtual currency. Therefore, you do not have to register your entity with us."
PI-5554	2013-05-16	Bitcoin exchanges.	"At this time, if the entity buys and sells Bitcoins directly from customers, it appears that this entity is not engaged as an MSB in Canada as per the [*PCMLTFA*] and its associated Regulations. In fact, this kind of entity doesn't provide the services of remitting and/or transferring funds for the sake of the service. The transfer of funds is simply a corollary of their actual service of buying and selling virtual currency."

PI-5561	2013-06-04	Bitcoin exchange – trade of digital tokens	Trade of digital coins is not recognized under the *PCMLTFA* as one of the three MSB activities. "While the remitting or transmitting of funds is an MSB activity, in this specific scenario, the remitting or transmitting of funds that occurs is incidental and only happens as the business carries out its core activity of trading digital token. The remitting and transmitting of funds is the method used by this business to provide its service of trading digital token. In addition, handling Bitcoins, or defining a business as a Bitcoin Exchange, does not automatically make the business exempt from registering as a MSB. The business may perform other activities, which may or may not involve Bitcoins, which would make it subject to the *PCMLTFA*. While the *PCMLTFA* applies to business engaged in 'foreign exchange dealing,' this does not apply to Bitcoin as it is not a national currency of any country."
PI-5573	2013-07-16	Digital cash platform which mints high-encrypted single use digital coins that can be validated and settled in real-time.	If the entity is remitting and/or transmitting funds of merchants and/or consumers for the purpose of carrying out "electronic payments," or more specifically, "P2P payments" or person to business payments, the entity, at this time, is engaged as a MSB.
PI-5598	2013-08-19	Bitcoin/fiat currency transactions in Canada, wherein the transaction occurs as follows: (1) log into Exchange account and selects add CAD100 credit, (2) transfers CAD100 from personal account into Exchange's bank account, quoting on-off payment reference, (3) buys CAD100 of BTC from the Exchange at a quoted rate based on the Exchange's bid/ask spread, (4) uses BTC balance to buy GBP from the Exchange at a quoted rate based on the Exchange's bid/ask spread, (5) withdraws GBP from the Exchange to personal GBP bank account. - "Even where users think they are making a straight conversion from, for instance, CAD to GBP, the actual Back-office transaction will include Bitcoin as a mid-way currency […]" and that "[t]he Exchange will hold bank accounts with a major bank in each jurisdiction in whose currency we trade – e.g. CAD bank account in Canada & GBP bank in the UK."	The entity will be engaged in foreign exchange dealing and as such, will be a MSB per the Act and its associated Regulations.

PI-5601	2013-08-22	Company ABC provides real time purchasing of small amounts of crypto-currency using an INTERAC debit card. It also facilitates online checkouts where merchants accept Bitcoin while consumers hold debit card balances.	The business is not engaged as a MSB.
PI-5603	2013-08-27	Consumer will scan a digital wallet and specify the amount being sold to the ATM. The ATM will then calculate the market price of Bitcoin and subtract the transaction fee (a pre-set percentage) from the total amount to be received in fiat. The Bitcoins purchased from the consumer will then be transferred to Company ABC's online exchange account and an amount in Canadian dollars will be dispensed to the consumer.	Based on the summary of Company ABC, it appears that your entity is not, at this time, engaged as an MSB.
PI-5685	2014-01-21	Selling a pre-paid bitcoin card at retail locations and that "those cards have activation codes on them. The activation codes can be redeemed only on our website for credit."	The entity is not, at this time, engaged as an MSB in Canada.
PI-6095	2014-02-17	Virtual currency exchange not covered – clarifications	*PCMLTFA* does not apply to virtual currencies because they do not fall within the definition of "funds" under the *PCMLTFA*. The *PCMLTFA* also covers businesses engaged in "foreign exchange dealing," however; this also does not apply to virtual currencies as they are not a national currency of any country. With this in mind, it is important to note that handling virtual currency, or defining a business as a virtual currency exchange, does not automatically make the business exempt from registering as a MSB. The business may perform other activities, which may or may not involve virtual currency, which would make it subject to the *PCMLTFA*.

PI-6110	2014-03-04	Bitcoin – payment for invoices through EFT as an online bill payee – "Company ABC is a convenient and easy option for the small business, entrepreneur or professional to collect and receive payments directly to their bank accounts from their customers through [EFT] as online bill payee" - ABC's clients will have to provide the following during the sign-up process: (1) full legal name of the company; (2) business number incorporation number; (3) existing banking information including a banking reference; (4) type of industry and expected monthly volumes; (5) contact details of at least one director; and (6) all companies using NoCheque need to have been in business for at least 3 years.	The entity is a MSB.
PI-6244	2014-09-30	Using crypto-currency for exchanges – "the client could be depositing $CAD in his account, convert the funds into a crypto-currency and then sell back that currency in exchange of $USD"	The company will be providing a foreign exchange dealing service, and will, therefore, be engaged as an MSB in Canada.
PI-6246	2014-10-01	"Bitcoin as the underlying internal transfer technology that allows users to send remittances online" and "User accounts that hold Canadian dollars send funds through Bitcoin's payment protocol only as a method of simplified monetary movement"	If a user can request the remittance of fiat currency to another individual or entity, then ABC INC. will be considered as engaged as a MSB in Canada, with all of the associated obligations.

PI-6268	2014-12-10	Bitcoin business – "funds will be exchanged at a local Bitcoin exchange and sent to a foreign Bitcoin exchange to be converted back to fiat currency."	"[…] The Government of Canada has made changes to what services make an individual or an entity an MSB in Canada to include virtual currency services; however, these changes are not yet in force. Individuals and entities engaged in the business of dealing solely in virtual currencies will be MSBs, but cannot yet register with FINTRAC. Before these individuals and entities will be subject to [*PCMLTFA*], regulations need to be written to define what it means to be engaged in the business of providing services such as dealing in virtual currency. Based on the information you provided in your business model, namely that 'funds will be exchanged at a local Bitcoin exchange and sent to a foreign Bitcoin exchange to be converted back to fiat currency,' **it appears that your entity is providing fiat to fiat currency remittal services and therefore appears to be, at this time, engaged as an MSB**, as per the *PCMLTFA* and its associated Regulations. As a MSB in Canada, you have legal obligations under Canada's *PCLMTFA* […]."
PI-6367	2015-10-16	Purchase and/or sale of virtual currency from an online virtual currency exchange; matching of buyers and sellers and receipt of funds directly from the individual.	**Not a MSB**, as "changes are not yet in force. Individuals and entities engaged in the business of dealing in virtual currency services will be MSBs, but cannot yet register with FINTRAC. […] Based on the information you provided, it appears you are not providing any of the MSB services identified above, therefore, at this time, you are not engaged as an MSB in Canada as per the [*PCMLTFA*] and its associated Regulations and cannot register with us."
PI-6369	2015-11-09	Transfer of funds from one individual to another using an electronic funds transfer network	You are a MSB as a result of the following summarized scenarios: 1. Pay-out service provided to merchants outside of Canada to pay end recipients in Canada; 2. Pay-out service provided to merchants in Canada with end recipients outside of Canada; Pay-out service provided to merchants in Canada with end recipients in Canada; […]