SMARTBLOCK LAW

PROFESSIONAL CORPORATION

https://smartblocklaw.com

Cyber Tech Law Firm in Toronto

Blockchain. Data Privacy. IT Contracts. Litigation.

We navigate complex legal frameworks and fight for your interests.

Ontario Bar
New York State Bar
Massachusetts Bar

Last updated April 10, 2019

SMARTBLOCK LAW

PROFESSIONAL CORPORATION

https://smartblocklaw.com

Overview

We provide legal advice on **blockchain**, **cryptocurrency**, **data privacy**, **artificial intelligence**, and **cloud service contracts**.

We also litigate cases in court involving **commercial disputes**, **corporate law**, **regulatory investigations**, **online defamation & freedom of speech**, **professional negligence**, and various **insurance claims including cyber insurance**.

Chetan Phull, Principal Lawyer at Smartblock Law, is a speaker on cross-border legal management of blockchain operations, including data privacy issues. He has delivered blockchain law seminars for the Ontario Bar Association and Dubai government, and has upcoming seminars in Canada, Europe, UAE, and India.

Chetan is a blockchain law instructor with York University and Osgoode PD, and an expert legal panelist at various industry events. He has recorded podcasts on various aspects of cyber regulation, and has been interviewed by numerous lawyer magazines and news outlets.

Last updated April 10, 2019

SMARTBLOCK LAW

PROFESSIONAL CORPORATION

https://smartblocklaw.com

Expertise

- Blockchain & Cryptocurrency
- Data Privacy & Artificial Intelligence
- IT, Software & Internet Contracts
- Litigation & Arbitration

Last updated April 10, 2019

Legal Resources

Smartblock Law Guide to Data Privacy and Cybsersecurity

Smartblock Law Guide to Security Tokens, OTC Trades, Prospectus Exemptions, and Registration

Smartblock Law Guide to Cryptocurrency Contracts, Litigation, Monetary Instruments, and Financial Institution Regulations in Canada

Smartblock Law Crypto-Tax Primer

Other Articles

Last updated April 10, 2019

Legal Resources

Smartblock Law Guide to Data Privacy and Cybsersecurity

Anticipated publication date: late April / early May 2019

Smartblock Law Guide to Security Tokens, OTC Trades, Prospectus Exemptions, and Registration

- ***Part 1:*** *Overview of Securities Regulation in Canada*;
- ***Part 2:*** *"Security Tokens" – A Developing Concept*;
- ***Part 3:*** *Foreign Issued Tokens Traded Over-the-Counter in Canada*;
- ***Part 4:*** *Prospectus Exemption Options for Blockchain Businesses*; and
- ***Part 5:*** *Securities Registration Requirements for Blockchain Businesses*.

Smartblock Law Guide to Cryptocurrency Contracts, Litigation, Monetary Instruments, and Financial Institution Regulations in Canada

- ***Part 1:*** *Cryptocurrency Can't Be "Money" in Canadian Commercial Law*;
- ***Part 2:*** *Enforcing Cryptocurrency Contracts*;
- ***Part 3:*** *Cross-Border Crypto Related Litigation*;
- ***Part 4:*** *Cryptocurrency and Monetary Instruments*; and
- ***Part 5:*** *Financial Institution Regulations*

Smartblock Law Crypto-Tax Primer

- ***Part 1:*** *the CRA's Present Position on Crypto-Tax*;
- ***Part 2:*** *Crypto as Specified Foreign Property*;
- ***Part 3:*** *Crypto-Exchange/Wallet Tax Issues*; and
- ***Part 4:*** *What's Next in Crypto-Tax?*

Other Articles

- *Crypto-KYC in Canada* (Feb 8/18)
- *Virtual Currency Regulations in Canada: Will Your Blockchain Business Be Affected?* (Feb 8/18)
- *The Law of ICOs/ITOs: Simplified* (Jan 25/18)
- *Toronto May Soon Drive Virtual Currency Laws Across Canada* (Jan 16/18)
- *Your Blockchain Business Needs a Blockchain Lawyer* (Jan 4/18)

Last updated April 10, 2019

Blockchain Law Podcast #1: ICOVisions featuring Chetan Phull on blockchain law (Jun 8/18, 70 mins total): Part 1 | Part 2 | Part 3 | Part 4.

Blockchain Law Podcast #2: LSEAAL Law 2.0 Podcast featuring Chetan Phull on blockchain regulatory insights (Nov 18/18, 30 mins).

In the works:

- *Smartblock Law Guide to Data Privacy & Cybersecurity*.
- Upcoming article on forthcoming CSA/IIROC rules respecting digital asset securities.
- Blog series on virtual currency AML regulations, after Canada's new draft AML regulations are finalized and passed as law.

Speaking Engagements

List is constantly changing. Click here for an update.

Quotes in the News, Magazines, Radio, etc.

- Amy Castor interviewing Chetan Phull, "*Quadriga's representative withdraws from CCAA hearings over 'potential' conflict of interest*" (Mar/19)
- *Canadian Lawyer Magazine*, Aidan Macnab quoting Chetan Phull, "*Will Quadriga CX spur regulatory oversight for crypto exchanges?*" (Feb/19)
- *GeekForge Academy*, Kirill Shilov interviewing Chetan Phull, "STO Registration Procedures in Canada" (Feb/19)
- *Bitcoin Magazine,* Colin Harper quoting Chetan Phull, "Judge Delays Decision to Appoint Legal Counsel for QuadrigaCX Creditors" (Feb/19)
- *Bitcoin Magazine*, Colin Harper quoting Chetan Phull, "QuadrigaCX Sent Deposits Allegedly Linked to CEO's Widow, Mailed Withdrawals in Cash" (Feb/19)
- *Vancouver Sun*, Randy Shore quoting Chetan Phull, "Troubled Bitcoin trader QuadrigaCX takes another bizarre turn" (Feb/19)
- *Bitcoin Magazine*, Jessie Willms quoting Chetan Phull, "*Elections Canada Consults With Political Parties on Crypto Donations*" (Jan/19)
- *Canadian Lawyer Magazine*, Luis Millan quoting Chetan Phull, "*Blockchain justice*" (Jan/19)
- *Law Times*, Anita Balakrishnan quoting Chetan Phull, "*Decision confronts challenges in valuing Bitcoin*" (Sep/18)
- Canadian Bar Association National Magazine, "*Parliament should formally legalize cryptocurrency as 'money'*" (May/18)

SMARTBLOCK LAW
PROFESSIONAL CORPORATION

Chetan Phull

Principal Lawyer

- ***Called to the Bars of Ontario, New York State and Massachusetts (2013)***
- ***Clerkship, Nova Scotia Court of Appeal (2011-2012)***
- ***LL.M., University College London (2010-2011)***
- ***J.D., Queen's University (2007-2010)***
- ***B.Mus., University of Toronto (2003-2007)***

Chetan Phull is a lawyer in his 7th year of practice. He is the principal of Smartblock Law Professional Corporation, a cyber tech law firm in Toronto.

Chetan has a regulatory and advisory focus in blockchain & cryptocurrency, data privacy & artificial intelligence, and IT contracts inclusive of cloud contracts.

He also practices litigation involving commercial disputes, corporate law, regulatory investigations, online defamation & freedom of speech, professional negligence, and various insurance claims including cyber insurance.

Prior to founding Smartblock Law in 2017, Chetan worked for five years in Toronto as a litigator and corporate counsel, for large private corporations and institutional clients including TD Insurance. His corporate counsel experience includes regulatory compliance, governance, high-value contracts, and contentious corporate meetings. He has trial, application, and motion experience in the Superior Court and Commercial List, as well as experience preparing materials for appeal before the Ontario Court of Appeal.

Chetan is also a speaker on legal management of cross-border blockchain operations. He is the sole speaker for such a seminar series in Europe and the UAE run by *Forte Markets*, and in India run by *KnowledgeHut*, with additional Canadian and U.S. speaking dates in 2019. To date, Chetan has taught blockchain law seminars for the *Ontario Bar Association*, *Osgoode Professional Development*, the *BlockchainHub at York University*, and the *Government of Dubai Legal Affairs Department*.

He has also authored numerous blockchain law compilations (see *here*), and has been published on cryptocurrency issues in the *Canadian Bar Association National Magazine*, and quoted in the *Law Times*, *Canadian Lawyer Magazine*, *Bitcoin Magazine* (three times), and the *Vancouver Sun*. Chetan has also been featured in a 4-part podcast on blockchain law by *ICOVisions*, and an *LSEAAL* on blockchain regulatory strategies.

Chetan's peer-reviewed publications appears in the *Journal of International Arbitration*, and the *Journal of International Banking Law & Regulation*. His publication in the former law journal was *translated into Thai* by the Thai Arbitration Institute.

Last updated April 10, 2019

Idan Levy

Student-At-Law

- ***Passed the Ontario Bar exams and NCA exams (2017)***
- ***J.D., Bond University (2013-2016)***
- ***B.A. (Hons) Humanities., UWO & York University (2006-2010)***

Idan works as an articling student in all practice areas of Smartblock Law tailored to blockchain and cryptocurrency clients. He regularly attends lawyer education seminars on blockchain law involving the firm, including one recent event held by the Ontario Bar Association.

Idan has over two years' experience in software marketing with Spar Group Inc., where he designed and implemented guerilla marketing campaigns for large software and technology brands, including Fitbit, Nest, August Smart Lock, and Electronic Arts. In this role he also designed and led in-house seminars on brand strategies.

During law school, Idan worked part-time for a wholesale nutrition company in Australia. That experience exposed him to various issues in the law of corporations, commercial contracts, consumer protection, and KYC. In this role he also gained valuable experience drafting legal documents and submissions, and managing client relationships. Idan also took practicums in Alternative Dispute Resolution, where he navigated complex legal problems, and prioritized the business and legal interests of his clients.

Idan has a J.D. from Bond University Law School, and a B.A. (Honours) from York University. He is fluent in French and Hebrew.

Disclaimer

- The material shared during this seminar is offered as general information only, not legal advice.

- Chetan Phull, Smartblock Law Professional Corporation, and its employees, contractors, and agents, as well as the event organizers, are ***not*** responsible for your reliance on the information shared during this presentation.

- You should obtain formal legal advice particular to your situation.

Copyright

Data Privacy & Cybersecurity: Overview

- Introduction: Legislative Landscape
- Proactive Planning for Breaches
- Reacting to Breaches:
  - Breach Record Keeping Obligations;
  - Breach Notification Obligations; and
  - Breach Reporting Obligations.

Data Privacy & Cybersecurity: Overview (Cont’d)

- Cybersecurity Standards and Management of Third Party Risk
- Defending Against or Prosecuting a Breach
- Digital Authentication
- Data Residency

Data Privacy & Cybersecurity: Overview (Cont'd)

- Privacy and Artificial Intelligence
- CASL

Data Privacy & Cybersecurity: Legal Framework

- Privacy Law in Canada is covered, first by a patchwork of regulations covering:
  - Different jurisdictions
    - PIPEDA is federal;
    - BC has a provincial *Personal Information Protection Act*;
    - AB has a provincial *Personal Information Protection Act*;
    - QB has *An Act Respecting the Protection of Personal Information in the Private Sector;*
    - *Municipal Freedom of Information and Protection of Privacy Act* (ON);
    - Various international treaties (discussed later).

Data Privacy & Cybersecurity: Legal Framework

- Privacy Law in Canada is covered, first by a patchwork of regulations covering:
  - Different industries – for example, health
    - ON has *Personal Health Information Protection Act*;
    - NB has *Personal Health Information Privacy and Access Act*;
    - NS has *Personal Health Information Act*;
    - Nfld has *Personal Health Information Act.*

Data Privacy & Cybersecurity: Legal Framework

- Privacy Law in Canada is covered, first by a patchwork of regulations covering:
  - Different industries – for example, the financial and investment sectors
    - *Bank Act* (federal);
    - *Trust and Loan Companies Act* (federal);
    - *Insurance Act* (ON);
    - *OSFI Guidelines;*
    - *CSA, IIROC, and MFDA for the capital markets.*

Data Privacy & Cybersecurity: Legal Framework

- Privacy Law in Canada is covered, first by a patchwork of regulations covering:
    - Public vs. Private sectors
        - PIPEDA covers employee information of federally regulated organizations (e.g. banks and telecom companies), and ***personal information in the course of commercial activities that do not have substantially similar legislation (i.e. all provinces except AB, BC, and QC).***
        - Federal public sector is covered by the *Privacy Act* (federal).

Data Privacy & Cybersecurity: Legal Framework

- There are also Criminal Code provisions to keep in mind:
  - **Criminal Code, s. 184:** using a device willfully to intercept a private communication without the express or implied consent of the originators or intended recipient; and
  - **Criminal Code, at s.342.1:** intercepting fraudulently and without colour of right any function of a computer system.

Data Privacy & Cybersecurity: Legal Framework

- Privacy Law in Canada is next covered by statutory torts for breach of privacy without damages:
    - Only in British Columbia, Manitoba, Newfoundland and Saskatchewan.
- Let’s not forget CASL:
    - Several prohibitions against installing computer programs without consent.

Data Privacy & Cybersecurity: Legal Framework

- Finally, private common law rights of actions in:
  - tort;
  - negligence;
  - breach of contract;
  - breach of consumer protection legislation;
  - breach of trust/fiduciary duty;
  - breach of privacy;
  - intrusion upon seclusion; and
  - unjust enrichment.

Data Privacy & Cybersecurity: Proactive Planning for Breaches

- The question is not *if* you are breached.

- The question is when you are breached.

- Protection from data breaches is rooted in training, proactive network monitoring, and continuous system reinforcement through upgrades/patches.

- A formal breach plan focuses these measures according to legal standards and industry best practices.

Data Privacy & Cybersecurity: Proactive Planning for Breaches

- The immediate objectives of a breach plan are:
  - identify and document operational risk tolerance specific to your organization within its industry; and
  - develop risk-mitigated approaches to data collection, use, disclosure, retention, accuracy, security and disposal.

Data Privacy & Cybersecurity: Proactive Planning for Breaches

- The ultimate purposes of a breach plan are:
  - minimize delay to react to breaches;
  - maximize effectiveness of the reaction to breaches;
  - minimize liability for breaches; and
  - minimize damage caused by breaches.

Data Privacy & Cybersecurity: Proactive Planning for Breaches

- Breach plans should be drafted according to regulation, case law, privacy-by-design and other industry best practices.

- Consider also appropriate safeguards in IT contracts with customers (i.e. users), and third party vendors (i.e. arm's length data processors).

- Consider options for multi-jurisdictional breach-plan compliance through operational analysis and working with third party counsel re foreign privacy law frameworks.

Data Privacy & Cybersecurity: Reacting to Breaches

- New rule as of November 2018:

  Private organizations must keep records of all security breaches exposing personal information, for 2 years after each breach is discovered.

- This rule stems from PIPEDA (federal legislation).

- Failure to report can result in a fine upwards of $100,000.

Data Privacy & Cybersecurity: Reacting to Breaches

- When do the breach requirements kick in?

- Think RROSH: “real risk of significant harm” to an individual

Data Privacy & Cybersecurity: Reacting to Breaches

- For any breach that creates a RROSH to an individual:
  - the individual must be notified in a specified form as soon as feasible upon discovery of the breach;
  - notification must be given to any organization or government institution that could reduce the risk of harm;
  - the breach must be reported to the Privacy Commissioner in a specified form; and
  - the breach record must be disclosed to the Privacy Commissioner upon request.

Data Privacy & Cybersecurity: Reacting to Breaches

- Unsurprisingly, breach records must contain information to assess compliance with breach reporting requirements.

- **Key Takeaway:** Build a detailed breach-logging system to ensure the integrity of legal “breach files”.

Data Privacy & Cybersecurity: Cybersecurity Standards and Management of Third Party Risk

- PIPEDA states:

“Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

…

“The methods of protection shall include

…

“(c) technological measures, for example, the use of encryption.”

(See ss.4.7 and 4.7.3(c).)

Data Privacy & Cybersecurity: Cybersecurity Standards and Management of Third Party Risk

- Data privacy breaches can spawn common law claims in tort, negligence, breach of contract, breach of consumer protection legislation, breach of trust/fiduciary duty, breach of privacy, intrusion upon seclusion, and unjust enrichment.

- In certain cases, a breach can also invoke criminal liability, and/or liability under various statutes within the Canadian privacy law framework.

- Organizations are generally also responsible for Privacy Commissioner reporting in respect of breaches that occur with third party data processors.

Data Privacy & Cybersecurity:
Cybersecurity Standards and Management of Third Party Risk

- A proactive approach to avoid such liability—before it accrues—is the best approach.

- Internal cybersecurity standards should be set and adhered to, and such standards should be entrenched in contracts with third party data processors.

Data Privacy & Cybersecurity: Cybersecurity Standards and Management of Third Party Risk

- In Canada, the applicable legal standard for cybersecurity is informed by various Ontario Privacy Commissioner (“OPC”) decisions.

- Those decisions have found inadequate cybersecurity measures with respect to the following:

  - documented security policies and practices; password administration; key and password management; multi-factor authentication; encryption measures; security monitoring and logging; audit trails; appropriate VPN use; network segmentation including with firewalls; network activity logging; virus protection; timely upgrading and patch implementation; accountability of third party data processors; inconsistent security measures applied between pools of redundant data; backup system testing.

Data Privacy & Cybersecurity:
Cybersecurity Standards and Management of Third Party Risk

- Further guidance regarding cybersecurity standards are available from:
  - the Office of the Privacy Commissioner (federal), provincial privacy commissioners, other Canadian regulators (e.g. OSFI, MFDA, CSA, IIROC), and through other compliance frameworks (e.g. PCI DSS, NIST, ISO27000, SOC1 & 2, COBIT, OWASP, Privacy By Design, NIS Directive).

Data Privacy & Cybersecurity: Cybersecurity Standards and Management of Third Party Risk

- See also Microsoft's "10 Immutable Laws of Security" (Microsoft Security Response Center, 2000):
  - Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore
  - Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore
  - Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore
  - Law #4: If you allow a bad guy to upload programs to your website, it's not your website any more
  - Law #5: Weak passwords trump strong security
  - Law #6: A computer is only as secure as the administrator is trustworthy
  - Law #7: Encrypted data is only as secure as the decryption key
  - Law #8: An out of date virus scanner is only marginally better than no virus scanner at all
  - Law #9: Absolute anonymity isn't practical, in real life or on the Web
  - Law #10: Technology is not a panacea

Data Privacy & Cybersecurity: Defending Against or Prosecuting a Breach

- A lawsuit generally requires the Plaintiff to prove “liability” and “damages” to have any chance at recovery.

- Liability and damages flowing from a data breach can involve complicated questions of law, and contentious questions of fact.

Data Privacy & Cybersecurity: Defending Against or Prosecuting a Breach

- Cyber insurance coverage may also be disputed, depending on the organization’s systemic practices relating to data privacy.

- Disputes may also extend to foreign jurisdictions on matters of data residency and disclosure of source code.

Data Privacy & Cybersecurity: Digital Authentication

- The federal and provincial governments, with the Digital ID & Authentication Council of Canada (“DIACC”), are working with the private sector to manage and deliver digital ID services across government and commercial platforms.

- As of June 2018, fintech legislative reform has permitted various types of financial entities to “provide identification, authentication or verification services”.

Data Privacy & Cybersecurity: Digital Authentication

- Moreover, we note that the Canadian Bankers Association ("CBA") has recommended a blockchain-type solution to digital identity through a "federated system".

- we expect that digital identify verification will become a commonly outsourced service to Canadian financial institutions and foreign affiliates.

Data Privacy & Cybersecurity: Digital Authentication

- These developments are expected to extend to the cryptocurrency industry, specifically with regard to crypto-wallet ownership and control.

- In light of the recent QuadrigaCX debacle, we also anticipate that digital ID requirements for crypto wallets will extend to securities dealers.

Data Privacy & Cybersecurity: Digital Authentication

- Meanwhile, preliminary legal clarification for digital authentication operations across organizations is provided by DIACC in its Pan-Canadian Trust Framework. The framework provides common terms, expectations, and defined processes to assist with contract drafting in this space.

- There are no model contracts involving interaction with the DIACC's Pan-Canadian Trust Framework.

- For digital authentication issues, get legal counsel familiar with the status of digital authentication policy and direction.

Data Privacy & Cybersecurity: Data Residency

- Data residency requirements are generally meant to control the locality of data at rest, and the channels of data flow.
- The nature of this area of law is necessary international in scope.
- There is no Canadian federal or Ontario data localization requirement for personal information.

Data Privacy & Cybersecurity: Data Residency

- The data residency provisions in the USMCA (pending ratification), and *Comprehensive and Progressive Trans-Pacific Partnership* (U.S. did not ratify), suggest a free-flow of data between the U.S. and Canada.

- In both treaties, a Party cannot require localized computing facilities in order to do business within its borders.

- **Important note:** In the CPTPP, this provision is limited by a legitimate policy objective.

- However, in the USMCA this provision is <u>not</u> limited by a legitimate public policy objective.

- **This means that when a Canadian entity enters into contract with a U.S. data processor, the Canadian entity has no right to insist that a foreign company operating within its boarders use local computing facilities.**

Data Privacy & Cybersecurity: Data Residency

- In the E.U., the GDPR requires the Commission to issue an “adequacy decision” before data can be transmitted to a non-E.U. country.

- Fortunately, the E.U. has issued favourable adequacy decisions for both Canada and the U.S.

- This means personal data can be transmitted between Canada, the E.U., and the U.S. largely without data localization impediments.

Data Privacy & Cybersecurity: Data Residency

- However, many jurisdictions have data residency requirements:

> "Data localization requirements are popping up around the world with European requirements in countries such as Germany, Russia, and Greece; Asian requirements in Taiwan, Vietnam, and Malaysia; Australian requirements for health records, and Latin America requirements in Brazil." (See Michael Geist, "The Sharing Economy and Trade Agreements: The Challenge to Domestic Regulation" appearing as Chapter VII in Derek McKee, Finn Makela, Teresa Scassa, eds., "Law and the 'Sharing Economy' – Regulating Online Market Platforms" [UOP 2018] at 245).

Data Privacy & Cybersecurity: Data Residency

- Consider:
  - British Columbia and Nova Scotia have local data storage and access requirements applicable to the provincial public sector; and
  - the Business Council of Canada has recognized the rare need to control data "to protect the public interest".

Data Privacy & Cybersecurity: Data Residency

- When dealing with a treaty Party outside the U.S. and E.U., need to consider Canada’s treaty obligations to other countries.

- Consider:
  - Minimum standards;
  - Most favoured nation;
  - National standard.

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- Issues for consumers in AI and data collection/processing:
  - The processing of data, through computer code embedded in “smart devices” or pushed to a back-end, is not visible or otherwise tangible for consumers.
  - Users may not have control over data collection, data processing, or decision logic run by their mobile or IoT devices.

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- Canada is a member of the "Digital 9" group of countries who value artificial intelligence and improved access to services (see here). The U.S. is conspicuously absent from this list.

- Artificial intelligence policy frameworks are being developed through the "Digital 9" group of countries, and the International Panel on Artificial Intelligence ("IPAI").

- The G7 have committed to ensuring that AI design and implementation respect, promote, develop and enforce applicable frameworks for privacy and personal data protection. (See the "Charlevoix Common Vision for the Future of Artificial Intelligence".)

Data Privacy & Cybersecurity:
Privacy and Artificial Intelligence

- In October 2018, the “Declaration on Ethics and Data Protection in Artificial Intelligence” was issued at the International Conference of Data Protection & Privacy Commissioners.

- The declaration contained six guiding principles as core values to preserve human rights in the development of artificial intelligence which we have paraphrased:

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

1. AI should be designed, developed and used in respect of fundamental human rights in accordance with the fairness principal;
2. Continued attention, vigilance, and accountability for AI should be ensured;
3. AI systems should be transparent and intelligible.
4. AI should be designed in accordance with ethics by design, privacy by default, and privacy by design.
5. Empowerment of every individual should be promoted.
6. Possible biases and discrimination related to the use of AI should be reduced and mitigated

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

1. As of April 1, 2019, Canada's Directive on Automated Decision-Making will take effect.

2. It emphasizes "core administrative law principles such as transparency, accountability, legality, and procedural fairness", and is anticipated to evolve in order to stay relevant.

Data Privacy & Cybersecurity: Privacy and Artificial Intelligence

- How will the courts handle AI?

- Ontario courts have promoted the use of artificial intelligence, at least with respect to lowering legal costs.

  - *Cass v. 1410088 Ontario Inc.*, 2018 ONSC 6959 at para 34 (CanLII):

> [10] My own view is that the hours spent on legal research is recoverable both as a component of counsel fee and as a disbursement. The reality is that computer-assisted legal research is a necessity for the contemporary practice of law and computer assisted legal research is here to stay with further advances in artificial intelligence to be anticipated and to be encouraged. Properly done, computer assisted legal research provides a more comprehensive and more accurate answer to a legal question in shorter time than the conventional research methodologies, which, however, also remain useful and valuable. Provided that the expenditure both in terms of lawyer time and computer time is reasonable and appropriate for the particular legal problem, I regard computer-assisted legal research as recoverable counsel fee item and also a recoverable disbursement.

Data Privacy & Cybersecurity:
Privacy and Artificial Intelligence

- How will the courts handle AI?

- Ontario courts have promoted the use of artificial intelligence, at least with respect to lowering legal costs.

  - *Drummond v. The Cadillac Fairview Corp. Ltd.*, 2018 ONSC 5350 at para. 10 (CanLII):

> [34] All in all, whatever this "research" was would be well within the preparation for the motion. There was no need for outsider or third party research. If artificial intelligence sources were employed, no doubt counsel's preparation time would have been significantly reduced.

Data Privacy & Cybersecurity: CASL

- **Question:** What is CASL for?

- **Response (in part):** to enable Canadians to make more informed decisions about what they allow to be installed on their computers, tablets, phones.

Data Privacy & Cybersecurity: CASL

- CASL is enforced by:
  - Canadian Radio-television and Telecommunications Commission;
  - Competition Bureau;
  - Office of the Privacy Commissioner of Canada.
- No private rights of action presently available, i.e. no Plaintiff class action law suits possible under CASL (yet).

Data Privacy & Cybersecurity: CASL

- CASL applies to:
  - a commercial electronic message ("CEM"), that is
  - sent to an "electronic address".
- The definition of "electronic address" includes SMS and other messaging to mobile phones and devices.
- CASL does not apply to unsolicited telecommunications, including live voice and automated telemarketing calls, to telephone numbers, which are regulated under the Unsolicited Telecommunications Rules.

Data Privacy & Cybersecurity: CASL

- If a computer program performs one or more of the following functions, the installer must make this clear when seeking the user’s consent:

1. collects personal information (such as accessing a mobile phone's GPS to track the location of the phone);
2. interferes with the user's control of the device (for example, preventing someone from using the Wi-Fi on his or her mobile phone);
3. changes or interferes with the user's settings, preferences or commands without his or her knowledge (for example, changing the default web browser on a computer);
4. changes or interferes with the data stored on the device in a way that obstructs, interrupts or interferes with the user's access to the data (for example, encrypting data on a computer so that the owner can't access it);
5. causes the computer system to connect to or send messages to other computer systems without the user's authorization (for example, causing a computer to automatically send out email messages to an individual's list of contacts); or
6. installs a program that may be activated by a third party without the user's knowledge..

Data Privacy & Cybersecurity: CASL

- CASL punishes the direct sending of unsolicited CEMs.

- CASL also punishes anyone who aids, induces, procures, or causes to be procured the direct sending of unsolicited CEMs.

- This means there can be indirect liability under CASL.

Data Privacy & Cybersecurity: CASL

- With regard to consent, the onus of proof is on the person who alleges that they have consent to send a CEM (typically, the person who sends the CEM), either implied or express, to send each message.

- But the test for consent appears to be malleable...

Data Privacy & Cybersecurity: CASL

- The test appears to be malleable:

  - “The Commission recognizes that each organization is different. … [M]easures to ensure compliance with CASL may vary, particularly in the case of small- to medium-sized businesses.” (CRTC 2018-415, Nov 5/18, para. 3.)

  - The Commission will consider level of control, degree of connection, and reasonable steps taken to prevent CASL violations. (CRTC 2018-415, Nov 5/18, para. 8.)

Data Privacy & Cybersecurity: CASL

- Other notable “CASL law” propositions:

  - CASL violations are determined on the balance of probabilities (CRTC 2017-65 at para. 30).

  - CASL violations are not criminal proceedings (CRTC 2017-65 at footnote #3).

  - Penalty is meant to promote compliance and not to punish. In one case, an individual was fined $15,000 (CRTC 2017-65 at paras. 38, 43).

Blockchain Legal Issues

- A (very) brief introduction to blockchain technology: click here.

Introduction

- We are primarily concerned today with digital assets and blockchain operations.

- Blockchain networks, or distributed ledgers, require nodes.

- Proliferation of data across 2+ of nodes involves the transfer of data – often across borders.

Introduction

- The internet until now has involved the transfer of information.

- Information transferred across borders in certain cases can be problematic.

  - Examples: privacy laws, cyber defamation and free speech.

Introduction

- Blockchain technology sits on top of the internet, and facilitates a transfer of value.

- Value transfer is governed differently within numerous areas of regulation, and between jurisdictions.

- On this basis, developing an operational strategy for cross-border blockchain operations can seem like you’re playing “whack a mole”.
  - Example: a “sufficiently decentralized network” can be an advantageous feature in U.S. securities law, but may present hurdles in E.U. privacy law.

Overview

- Various bodies are in the process of formulating blockchain regulatory frameworks.
- However, there is no international framework in place for blockchain activities yet.
- Blockchain activities are presently governed by a patchwork of varying—and possibly conflicting—national and regional regulatory regimes.

Overview

- Any blockchain venture seeking early market share should be aware of the major legal issues invoked by blockchains across jurisdictions.

- **Key Take-Away #1:** it is impossible right now to optimize both early market share and regulatory compliance.

Overview

KEY TAKEAWAY #2:

- Be prepared to assume risk.
- Make sure you know your risk in all concerned jurisdictions.
- Optimize your legal risk across borders.

Overview

- Understanding your venture's risk profile requires an understanding of the primarily blockchain law issues applicable across borders.

- This presentation will address some of the primary blockchain law issues that will need to be handled across jurisdictions.

- We will sample primarily from Canada and the U.S.

- The information shared will comprise a general base, to be further developed and refined by lawyers across jurisdictions in respect of any given blockchain venture or operation.

Overview

- "Blockchain law" is an umbrella term consisting of three primary sub-groups:

1. Corporate Funding by ICO/ITO/STO (Initial Coin/Token Offerings, or Security Token Offerings);

2. Ongoing Blockchain Operations; and

3. Enforcement/Litigation.

Road Map

I. A Love-Hate Story: Blockchain and the Law

II. Corporate Funding by ICO/ITO/STO

- digital tokens in the context of securities issues, distributions, and registration;
- persuasive “soft law” released by the U.S. Securities Exchange Commission, and the Commodity Futures Trading Commission;
- the latest statements by the Ontario Securities Commission;
- local compliance is not the same as global compliance;
- secondary market trading issues;
- sandbox regimes;
- practical strategies to work within the rules;

Road Map

III. Ongoing Blockchain Operations

- ongoing issues in securities law, and over-the-counter trades;
- anti-money laundering and anti-terrorist financing regimes;
- income tax and tax classification of digital assets;
- VAT on digital tokens as goods or services;
- contracting in cryptocurrency and the definitions of “money” and “funds”;
- division of legislative powers and in the context of government blockchain operations;
- payments system issues;

Road Map

III. Ongoing Blockchain Operations (cont’d)

- financial institutions;
- fiduciary issues;
- monetary/financial instruments;
- IT contracts including;
- data privacy and use of a distributed ledger to point to centrally managed cloud storage;
- AI & algorithmic governance in smart contracts;
- insurance considerations;
- optimistic outlook for blockchain and cryptocurrency regulations in the UAE.

Road Map

IV. Enforcement/Litigation

- local and cross-border market manipulation offences;
- local and cross-border regulatory litigation;
- domestic rights when a foreign exchange goes bankrupt;
- private disputes over tokens in the context of public and private international law.

Road Map

V. Final Thoughts

- Market opportunity and cross-jurisdictional regulatory risk;
- “Sharding” as a potential response to conflicting rules across jurisdictions.
- Some hope for the future provided by the SCOTUS.

I. A Love-Hate Story: Blockchain and the Law

- Blockchain facilitates a transfer of value over the internet.
- Value transfer invokes various areas of law.
- Examples:
  - Securities law (protects investors in the capital markets);
  - Anti-money laundering and anti-terrorist financing law (aims to prevent illicit proceeds of sale);
  - Tax law (governs public revenue generation);
  - Cryptocurrency contracts (invokes legal definition of “money”);
  - Financial institutions and fiduciary issues (invokes legal definition of “banking”, and obligations to customers/users);
  - Etc.

I. A Love-Hate Story: Blockchain and the Law

- Three observations:

  1. These areas of law treat blockchain activities differently *within* jurisdictions.
  2. These areas of law are all substantively different *between* jurisdictions.
  3. These areas of law are *constantly changing* in every jurisdiction.

- But blockchain-focused ventures often need to operate across borders, in many different countries.

I. A Love-Hate Story:
Blockchain and the Law

- **Key question:** How does a DLT company devise a consistent set of operations, while being compliant in all jurisdictions that it operates in?

- Best regulatory response is an international treaty.

- Until then, consider the Global Financial Innovation Network ("GFIN"), announced by the U.K. Financial Conduct Authority ("FCA"): see here.

I. A Love-Hate Story: Blockchain and the Law

- Three main functions of the GFIN:
  - act as a network of regulators to collaborate and share experience of innovation in respective markets, including emerging technologies and business models;
  - provide a forum for joint policy work and discussions; and
  - provide firms with an environment in which to trial cross-border solutions.

- The original GFIN membership consisted of the following:
  - Abu Dhabi Global Market (ADGM); **Autorité des marchés financiers (AMF, Quebec)**; Australian Securities & Investments Commission (ASIC); Central Bank of Bahrain (CBB); Bureau of Consumer Financial Protection (BCFP, USA); Dubai Financial Services Authority (DFSA); Financial Conduct Authority (FCA, UK); Guernsey Financial Services Commission (GFSC); Hong Kong Monetary Authority (HKMA); Monetary Authority of Singapore (MAS); **Ontario Securities Commission (OSC, Canada)**; Consultative Group to Assist the Poor (CGAP).

I. A Love-Hate Story: Blockchain and the Law

- GFIN membership has grown to include the Alberta Securities Commission (ASC) and British Columbia Securities Commission (BCSC).

- **Note:** The Securities Exchange Commission (SEC) is conspicuously absent from GFIN membership.

- The latest GFIN membership is posted here, as of January 31, 2019.

I. A Love-Hate Story: Blockchain and the Law

- Until there is more international cooperation and education in this space, we are likely to get more court decisions like *Copytrack Pte Ltd. v. Wall*, 2018 BCSC 1709:
  - Canadian court identified uncertainty as to whether crypto was a good or currency.
  - The court made an order to trace the cryptocurrency while acknowledging that it didn't know what cryptocurrency was.
  - This is likely a case of bad facts making bad law. It seemed that the court was attempting to find a just solution given the complicating factor of a material party's death. The "practical implications" of Wall's death was an unfortunate aspect of this case (paras 18 and 23).

II. Corporate Funding by ICO/ITO/STO

- The purpose of securities law is to:
  - protect investors;
  - foster confidence, fairness, and efficiency in capital markets; and
  - contribute to a stable financial system.

  (See: *Ontario Securities Act*, s.1.1)

- In the specific context of digital asset transactions, securities law regulates “how tokens and coins are being issued, distributed and sold” (SEC Director W. Hinman’s June 14, 2018 speech).

II. Corporate Funding by ICO/ITO/STO

Why is this important to digital asset businesses focused in ledgers distributed across borders?

II. Corporate Funding by ICO/ITO/STO

If the token is a security, ***transferring the token*** will invoke securities laws.

- **Prospectus** required. Exemptions may not be useful according to business objectives, due to hold periods and transfer restrictions.

- **Registration** of broker/dealers and advisors upon “business trigger”. Could be required on the basis of being a “market place” or “alternative trading system”.

- **Operation as an “exchange”** will require a further application.

II. Corporate Funding by ICO/ITO/STO

- As March 14, 2019, blockchain and cryptocurrency regulations from Canadian securities regulators are being drafted.

- The areas of intended regulation include how to address custody and verification of assets, price determination, market surveillance, cybersecurity systems and business continuity planning, conflicts of interest, crypto-asset insurance, and clearing and settlement.

- The CSA and IIROC consultation paper, “Proposed Framework for #Crypto-Asset Trading Platforms,” is here.

- Feedback is requested until May 15, 2019.

II. Corporate Funding by ICO/ITO/STO

What rules apply until the regulations are drafted and brought in force?

II. Corporate Funding by ICO/ITO/STO

- Unlike the U.S., Canada has no federal securities law or regulator. Rather, each province and territory is responsible for its own legislation and regulation of securities.

- The Canadian Securities Association ("CSA") has attempted to create harmony among the individual securities regulators, through national instruments and policies which every regulator can adopt.

II. Corporate Funding by ICO/ITO/STO

- In the fintech space, the CSA Regulatory Sandbox offers a means for businesses to obtain exemptive relief from certain securities law requirements throughout Canada, on a time-limited basis.

- The equivalent sandbox regime in the U.S. is the FinHub, announced in October 2018.

II. Corporate Funding by ICO/ITO/STO

- The threshold question is whether blockchain operations trigger securities laws.
  - If yes, there are various registration and prospectus requirements that must be met, which require significant resources and time. (Discussed later.)
- So, is the blockchain's "token" a "security"?
  - A "token" is simply data, existing in the larger context of a digital ledger. It is a digital object produced and used in connection with one or more blockchains.
  - A "security" includes an "investment contract".
- As recently stated by SEC Director William Hinman, the way tokens are sold most often triggers securities laws, because the sale evidences an "investment contract".

II. Corporate Funding by ICO/ITO/STO

- What’s an “investment contract”?

- Further to the U.S. *Howey case*, and the Canadian *Pacific Coast case*, the sale of a token is an “investment contract” when it involves:
  - an investment of money;
  - in a common enterprise;
  - with profits;
  - to come significantly from the efforts of others.

II. Corporate Funding by ICO/ITO/STO

- Whether the sale of a token is an investment contract, and therefore triggers securities laws, depends on various factors. For example:
  - The blockchain business model, how the tokens will be used, and what the tokens' characteristics are.
  - The stage of development of the blockchain business model. There is a strong argument that most tokens are securities prior to a network's launch, but are probably not securities after this point.
  - Whether the token is anticipated to be traded on a secondary market, for speculation and profit.

II. Corporate Funding by ICO/ITO/STO

- Such factors must be considered and weighed for every individual case.

- They will not always be weighed against the blockchain project.

- See *SEC v. Blockvest* motion, where it was a contentious issue of fact whether the tokens were:

  1. an investment of money; or

  2. were only meant to test the platform without being distributed to the public.

II. Corporate Funding by ICO/ITO/STO

- *SEC v. Blockvest* motion, Southern District of California (Nov 2018) at pages 9-11:
  - In this case, the SEC motioned for a preliminary injunction against Blockvest and others. This required the SEC to show a "primary facie case" that securities laws have been violated.
  - The SEC failed.
  - The Court was uncertain whether there was an investment of money or an expectation of profit in this case.
  - The relevant tokens were arguably only designed for testing the platform, and may never have been distributed to the public.
  - A trial, or discovery at the very least, was required to clarify these factually uncertain issues.
  - The SEC could still win at trial, but this decision demonstrates that the Howey test does not automatically lead to the conclusion that a given token is a security. Evidence matters.

II. Corporate Funding by ICO/ITO/STO

- Around the same time as the *Blockvest* motion, the SEC also stated:

> ...there is a path to compliance with the federal securities laws going forward, even where issuers have conducted an illegal unregistered offering of digital asset securities.
>
> ...
>
> ...the Divisions recommend that those employing new technologies consult with legal counsel concerning the application of the federal securities laws and contact Commission staff, as necessary, for assistance. [See November 16, 2018 Public Statement Statement on Digital Asset Securities Issuance and Trading.]

II. Corporate Funding by ICO/ITO/STO

Key takeaway:

Don’t be intellectually lazy about the *Pacific Coin* & *Howie* test.

II. Corporate Funding by ICO/ITO/STO

- On June 11, 2018, the CSA released its Staff Notice 46-308, which provides numerous helpful examples of when a token is a security under the "investment contract" test in Canada.
- We have distilled this notice into 4 core principles of security tokens.

II. Corporate Funding
by ICO/ITO/STO

1. the objective of investor protection is an important consideration in determining whether a token is a security.

II. Corporate Funding by ICO/ITO/STO

2. a token can be a security notwithstanding its utility. The economic realities of the token offering as a whole will be considered, with a focus on substance over form. Token features, on their own, are not decisive;

II. Corporate Funding by ICO/ITO/STO

3. even freely distributed tokens could be securities, if the overall token distribution is “part of an overall sale of an ancillary or secondary product or service”.

II. Corporate Funding by ICO/ITO/STO

4. the SAFT (discussed here) will not necessarily result in a token that is not a security.

II. Corporate Funding by ICO/ITO/STO

- The same analysis largely applies in the U.S.
- The SEC's Chairman Clayton stated that a cryptocurrency operating as a replacement of sovereign currency is not a security.
- SEC Director William Hinman stated that if a given crypto-asset had become "sufficiently decentralized", there may no longer be any enterprise receiving investment. Therefore, the token would not be a security.
- This was reiterated by SEC Chairman Jay Clayton in March 2018.
- For practical purposes, these statements are "soft law".

II. Corporate Funding by ICO/ITO/STO

- Some new questions:

1. at what point does a given cryptocurrency “replace” a sovereign currency?
2. at what point does a given token become “sufficiently decentralized”?
3. when a token—which originated as a security—replaces a sovereign currency or becomes sufficiently decentralized, do investors lose their rights in securities law?

II. Corporate Funding by ICO/ITO/STO

BUT NOTE:

- according to U.K. securities regulators, a “sufficiently decentralized” network has no bearing on whether a token is a security. (See here.)

II. Corporate Funding by ICO/ITO/STO

- **First Case study:** Blockchain’s Airdrop Program, which is set to give away crypto to drive mainstream adoption. (More on their legal strategy here.)

- **Blockchain's apparent strategy:** if crypto is given away for free until its network is “sufficiently decentralized”, there is minimal chance of that crypto being a security

- The OSC previously has frowned upon this strategy. And the SEC’s *Tomahawk* decision at para 33 states: “a ‘gift’ of a security is a ‘sale’ within the meaning of the *Securities Act* when the donor receives some real benefit.”

- Although the security token in *Tomahawk* was already a security notwithstanding the free gifting, the purpose of the airdrop is clearly to make an indirect profit.

II. Corporate Funding by ICO/ITO/STO

- **Second Case Study:** Why are established points cards (e.g. Aeroplan & Airmiles) not investment contracts?

II. Corporate Funding by ICO/ITO/STO

- Can you avoid Canadian and U.S. securities laws if you raise funds from a token sale outside Canada or the U.S.?

- In other words, is there any regulation of the secondary market?

II. Corporate Funding by ICO/ITO/STO

- Effectively yes, at least in Ontario.

- The OSC can:

  - make various orders to protect the public interest—even where there is no actual breach of securities law;

  - freeze the funds, securities or property of a company or person for the regulation of Ontario’s capital markets; and

  - pursue criminal liability for various fraud offences.

II. Corporate Funding by ICO/ITO/STO

- A New Security Token Standard: the ERC 1400, to track applicable exemptions in any concerned jurisdiction, etc.

- The SEC reportedly plans to clarify when and how cryptocurrencies may be classified as securities, sometime soon (see here).

III. Ongoing Blockchain Operations: AML

- Anti-money laundering and anti-terrorist financing laws are covered by the following legislation in Canada:
  - *Criminal Code* at ss.462.31(1) and 462.3(1);
  - *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* ("PCMLTFA"); and
  - PCMLTFA Regulations ("PCMLTFR").
- The relevant Canadian regulator in this space is the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC").
- Draft Canadian federal regulations with respect to "virtual currencies" have been anticipated since 2014, and were released earlier this year.
- Anyone "dealing in virtual currencies" will be required to register with FINTRAC as a "money services business" (see *PCMLTFA*, ss.11.1, 261).

III. Ongoing Blockchain Operations: AML

- The definition of a “virtual currency”:

virtual currency means

(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).

III. Ongoing Blockchain Operations: AML

- What does “dealing in virtual currencies” mean?

- In the course of legislating, regulating, and rendering decisions, Parliament FINTRAC, and the Canadian courts are expected to consider similar virtual currency legislation in other jurisdictions:
  - FinCEN guidelines on regulating virtual currencies (2013).
  - Quebec Autorité des marchés financiers, policy statement at Part 1(5) (2015).
  - New York State’s BitLicense regulations (2015).
  - U.S. model code, “*Uniform Regulation of Virtual Currency Business Act*” (2017).
  - European Parliament’s Virtual Currencies Monetary Dialogue (2018).

III. Ongoing Blockchain Operations: AML

- The Canadian regulations are anticipated “to cover entities such as virtual currency exchanges, not individuals or businesses that use virtual currencies for buying and selling goods and services.” (See: FINTRAC statement dated July 30, 2014.)

- This is consistent with the virtual currency rules enacted in New York State (s.200.3(c)(2)), and the ULC model code (s.103).

- However, what about private individuals who are regularly transacting in cryptocurrencies with a business purpose?

- Private individuals can be caught by companion regulatory regimes if transacting for a business purpose. Examples:
  - tax classification as commercial property with subjective intent to profit (see *Stewart v. The Queen*, 2002 SCC 46);
  - securities registration required for engaging the “business trigger”;
  - Etc.

III. Ongoing Blockchain Operations: AML

- For now, it is fairly certain that the Canadian regulations on "dealing in virtual currencies" will apply to the following types of businesses:
  - cryptocurrency developers;
  - cryptocurrency miners;
  - cryptocurrency exchanges;
  - cryptocurrency brokerages;
  - cryptocurrency clearing houses;
  - cryptocurrency investment firms;
  - cryptocurrency ATMs;
  - cryptocurrency wallets or other bank-like businesses;
  - cryptocurrency bailment companies;
  - businesses offering rewards, points, or coupons through a blockchain mechanism;
  - cryptocurrency trust companies;
  - gambling establishments which accept bets in cryptocurrency; and
  - any blockchain business that holds tokens and facilitates their use as a cryptocurrency (for example, through smart contract micropayment operations).

III. Ongoing Blockchain Operations: AML

- If a business is "dealing in virtual currencies", it must register with FINTRAC as a money services business ("MSB").
- In the new regulations, even foreign MSBs must now register with FINTRAC.
- MSBs have various reporting and KYC obligations.
- The new regulations require:
  - "virtual currency transaction tickets", including extra record keeping obligations for virtual currency transactions over $1,000 CAD; and
  - "large virtual currency transaction records" for transactions over $10,000 CAD.
- KYC obligations in the new regulations can be outsourced to third parties including foreign third parties.

III. Ongoing Blockchain Operations: Taxation

- The Canada Revenue Agency ("CRA") administers tax laws for the federal government and most provinces.

- The CRA has recognized cryptocurrency to be:
  - a form of money;
  - a commodity; and
  - a payments system.

- The CRA has specifically stated that digital currency is not legal tender, and must be treated as commodities that invoke the rules for barter transactions.

III. Ongoing Blockchain Operations: Taxation

- Income tax and other tax classification of digital assets:
  - income;
  - capital;
  - **Inventory (particularly relevant for crypto miners);**
  - foreign specified property;
  - gift;
  - commodity;
  - etc.

- HST/VAT tax on digital tokens as goods or services.

III. Ongoing Blockchain Operations: Taxation

- Cross-border definitional problems in Canadian tax law:
  - if crypto holdings have an adjusted cost base of $100k CAD or more, it is considered "foreign specified property". Definitional problems are discussed in our article, "Crypto as Specified Foreign Property"
  - HST is potentially chargeable on crypto transaction "in Canada". But blockchain transactions occur wherever the nodes are, including outside Canada.

III. Ongoing Blockchain Operations: Taxation

- Exchanges could have potential liability to charge and remit taxes.

- Even without an expressly stated intention to form a trust, a resulting trust is presumed to exist in certain cases when one person buys property in the name of another.

    - See: *Nishi v. Rascal Trucking Ltd.*, 2013 SCC 33 at paras. 1, 21; *Belokon v. Krygyz Republic*, 2016 ONCA 981 at paras. 55-56.

III. Ongoing Blockchain Operations: Taxation

- Crypto businesses could have potential liability to charge and remit taxes on the basis of a resulting trust.

- The existence of a trust could trigger a platform’s obligation to remit GST-HST in most transactions involving the supply of cryptocurrency to a third party.

- The platform as trustee could also bear the obligation to disclose all on-platform trades to the CRA, pursuant to the rules applicable to the income taxation of trusts, if the trust is audited by the CRA.

III. Ongoing Blockchain Operations: Crypto Contracts

- The problem:

1. We all want to treat crypto as money.

2. A growing body of cases in the U.S. appears to equate crypto with “money” (or “funds”)—see our article, “Cryptocurrency Can’t Be ‘Money’ in Canadian Commercial Law”.

3. At least in Canada, the use of crypto as non-fiat money is illegal.

III. Ongoing Blockchain Operations: Crypto Contracts

- There is a definitional problem in the federal legislation of Canada and the U.S. regarding “money”.

- Canada’s *Currency Act* at s.13(1):

  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

  (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.

III. Ongoing Blockchain Operations: Crypto Contracts

- United States Commercial Code, § 1-201(24):

> “Money” means a medium of exchange currently authorized or adopted by a domestic or foreign government. The term includes a monetary unit of account established by an intergovernmental organization or by agreement between two or more countries.

III. Ongoing Blockchain Operations: Crypto Contracts

- There may be a fix, but the existing rules do not provide a clear solution.
- Transact with crypto as a commodity (consistent with how the CRA treats crypto).
- Crypto as a commodity in commerce may trigger HST at 13%.
- This is clearly an unintuitive result.
- The only way to remedy the problem is to look at the definition of HST as being charged on the supply of goods "in Canada".
- Presumably, a crypto transfer is not a supply within Canada, because the blockchain exists <u>OUTSIDE</u> of Canada.
- Is this consistent with arguing that $100k of crypto should not be considered "foreign specified property", because the blockchain exists <u>IN</u> Canada?

III. Ongoing Blockchain Operations: Crypto Contracts

What about stablecoins?

- See “Is Tether Constitutional?”, by Christopher Satti (July 9, 2018):

  > "No one other than the Secretary of the Treasury was allowed to print ... money; anything else was counterfeit.
  >
  > ...
  >
  > "By creating Tether, the developers essentially created a USD cryptocurrency. ... [T]hat is the exclusive job of Congress.
  >
  > ...
  >
  > "Tether violates the U.S. Constitution. Congress has the exclusive rights to control and print monies and securities of the U.S."

- However: note that there are presently no widely known indicators that governments intend to enforce against stablecoins.

III. Ongoing Blockchain Operations: Division of Powers

- Different levels of government in Canada have exclusive jurisdiction in respect of currency, banking, bills of exchange, municipal institutions, and other related areas. They all need to work together.

- Old example of alternative medium of exchange: *Alberta References*, [1938] SCR 100, 1938 CanLII 1 (SCC).

- Recent example of alternative medium of exchange: See our article, "Toronto May Soon Drive Virtual Currency Laws Across Canada"

III. Ongoing Blockchain Operations: Payment Systems

- The *Canadian Payments Act* ("CPA") governs the "regulation of systems and arrangements for the making of payments".

- Under the *CPA*, the designation of a payment system in the public interest is at the option of the Minister of Finance.

- The Association's objects include, "to facilitate the development of new payment methods and technologies" (*CPA*, s.5(1)(c)).

- On this basis, it is entirely foreseeable that cryptocurrency payment mechanisms will eventually be subject to regulation under the CPA, further complicating the division of powers problem.

III. Ongoing Blockchain Operations: Financial Institutions

- Various financial institutions in Canada are federally regulated, “so as to contribute to the public confidence in the Canadian financial system” (“OSFI Act”, ss.3.1, 4(4)).

- Any business engaged in “the business of banking” must be incorporated or continued under the *Bank Act*, and is subject to the *Bank Act.* (See our article, “Financial Institution Regulations”).

- The question of whether a business is in fact engaged in “the business of banking” is important. In Canada, such classification carries various duties and regulatory requirements under the *Bank Act*.

III. Ongoing Blockchain Operations: Financial Institutions

- Whether a given business is a bank, or engages in banking, requires fact-specific consideration. Consider that:

> Banking is both so complex and dynamic that there may well be no essential core for a court to identify…. Notwithstanding the complex and comprehensive legislation in relation to banking, Parliament has left room for the courts to operate when specific issues of jurisdiction and definition arise…. [M.H. Ogilvie, *Bank and Customer Law in Canada*, 2d ed. (Markham, Ontario: Irwin Law, 2013) at 10.]

- The difficulty in determining whether a business is operating as a bank is compounded by the different rights of banks between jurisdictions and at different times in history.

III. Ongoing Blockchain Operations: Financial Institutions

- Many cryptocurrency businesses—particularly those that issue cryptocurrency—may be subject to the *Bank Act*. Consider the following.

- It has been held that "banking" includes:

  - the act of obtaining "information which formerly ... clients had in their own ledgers where the entry had manually been made by employees and servants" (*Central Computer* at para. 7).

  - "activity which aids in providing funds 'at the lowest cost to borrowers and the highest return to savers'" (*Canadian Commercial Bank (Re)*, 1986 CanLII 1644 (AB QB)at para. 10).

- Also, the attempted creation of a new medium of exchange in Canada in the 1930s was considered to be "banking" (*Reference Re Alberta Statutes*, [1938] S.C.R. 100).

III. Ongoing Blockchain Operations: Financial Institutions

- Any business engaged in "the business of banking" must be incorporated or continued under the *Bank Act*, and is subject to the *Bank Act.* (See our article, "Financial Institution Regulations").

- The question of whether a business is in fact engaged in "the business of banking" is important.

- In Canada, such classification carries various duties and regulatory requirements under the *Bank Act*.

III. Ongoing Blockchain Operations: Financial Institutions

- Even if a crypto business is not a bank, it may still owe fiduciary duties to third parties.

- Consider whether the crypto business also operates as an exchange.

- Consider whether relationships with third parties involves an expectation of duties owed by the crypto business.

- Consider whether any disclaimer in the crypto business’ Terms of Use can contract out of certain fiduciary duties.

III. Ongoing Blockchain Operations: Financial Institutions

The ongoing case of QuadrigaCX

III. Ongoing Blockchain Operations: Financial Institutions

- See the November 2018 Standing Committee recommendations respecting virtual currency activities (pages 64-65):
  - #26: require identification for individuals to own a wallet;
  - #27: mandatory license for crypto #exchanges;
  - #32: update financial institution reporting regulations.
- At the very least, I foresee crypto exchanges coming under the jurisdiction of the Office of the Superintendent of Financial Institutions ("OSFI").
- QuadrigaCX has given more reason for this to happen.

III. Ongoing Blockchain Operations: Financial Instruments

- Three monetary instruments are defined in the *Bills of Exchange Act*, which are instruments inherited from English law.

- The defined monetary instruments are bills of exchange, cheques, and promissory notes.

> 16 (1) A bill of exchange is an unconditional order in writing, addressed by one person to another, signed by the person giving it, requiring the person to whom it is addressed to pay, on demand or at a fixed or determinable future time, a sum certain in money to or to the order of a specified person or to bearer.
>
> 165 (1) A cheque is a bill drawn on a bank, payable on demand.
>
> 176 (1) A promissory note is an unconditional promise in writing made by one person to another person, signed by the maker, engaging to pay, on demand or at a fixed or determinable future time, a sum certain in money to, or to the order of, a specified person or to bearer.

- Consider our article "Cryptocurrency and Monetary Instruments".

III. Ongoing Blockchain Operations: IT Contracts

- IT contracts including:
  - third party vendor agreements (e.g. third party KYC verifiers);
  - node agreements;
  - mining coalition agreements;
  - “browsewrap” agreements (i.e. Terms of Use) attempting to indemnify the platform for its non-compliance.

III. Ongoing Blockchain Operations: Data Privacy

- Public/permissionless blockchains may present a problem with GDPR compliance.

- However, "GDPR compliance is not about the technology, it is about how the technology is used."(See EU Blockchain Observatory and Forum, "Blockchain and the GDPR".)

- Can blockchain data be anonymized, or subsequently varied?

III. Ongoing Blockchain Operations: Data Privacy

- **Blockchain Use Case: storage of sensitive data.**

- Aside from privacy concerns, storing data containers on the blockchain itself would potentially make blockchain processes sluggish.

- Potential fix to privacy issue and throughput problem: use a distributed ledger to keep records of hashes that point to encrypted data on centrally managed cloud storage.

- Owner of the data in this case potentially has the capability to delete the data container, rendering the hash stored on the blockchain useless.

- However, does use of a central data site defeat the purpose of sblockchain?

III. Ongoing Blockchain Operations: Data Breaches & Cybersecurity

- In Canada, there is mandatory breach notification and reporting requirements since November 2018.

- Failure to sufficiently notify/report may invoke a fine upwards of $100,000.

- Cybersecurity standards have also been provided by OPC in various decisions.

- See also guidance by other provincial privacy commissioners, other regulators, industry best practices.

III. Ongoing Blockchain Operations: Data Breaches & Cybersecurity

Work with a lawyer to draft a breach plan to:

- minimize delay to react to breaches;
- maximize effectiveness of the reaction to breaches;
- minimize liability for breaches; and
- minimize damage caused by breaches.

III. Ongoing Blockchain Operations: Smart Contracts

- AI & algorithmic governance in smart contracts.
- Every smart contract should have an underlying legal contract to deal with issues like:
  - choice of forum;
  - choice of law;
  - neutralize effect of *contra proferentum* (i.e. presumptions against contract drafter);
  - Etc.

III. Ongoing Blockchain Operations: Insurance

- Blockchain and cryptocurrency is a risky business space at present, albeit with the potential for great reward.

- Consider whether your insurer will insure crypto/tokens.

- If not, plan for appropriate coverages of an amount in fiat currency to cover the loss of digital assets – note the broad value fluctuations.

IV. Enforcement/Litigation

- Much of the existing blockchain litigation arises specifically from litigation over cryptocurrency.
- How does a party enforce a cryptocurrency-denominated contract, or defend against such enforcement?

IV. Enforcement/Litigation

- As previously indicated, in Canada, cryptocurrency should be considered a commodity rather than “money”, to avoid the risk of voiding contracts denominated in cryptocurrency.

- Likewise, a judgment or arbitral award for cryptocurrency is presently only possible in Canada if cryptocurrency is not considered “money”, and is not tied to “monetary value” (*Currency Act*, s.12).

- Therefore, a legal proceeding in Canada for cryptocurrency should proceed on the basis that cryptocurrency is a commodity (i.e., a type of good).

IV. Enforcement/Litigation

- This approach is consistent with the law's treatment of foreign currency as a commodity, in the context of obligations payable in foreign currency:

> In English as well as American law, the courts adhered for many years to the "commodity theory" with respect to obligations payable in foreign currency. According to this theory, foreign currency was not treated as money in the sense of a medium of exchange, but as a commodity in the sense of an object of a commercial transaction. In this respect, foreign currency transactions were on more than one occasion likened to transactions involving chattels such as cows. [Guy David in "Money in Canadian Law", (1986) 65 Can. Bar Rev. 192 at 215.]

- On the commodity view of cryptocurrency, the aggrieved party should seek the remedy of specific performance or a mandatory injunction, instead of damages.

IV. Enforcement/Litigation

- Specific performance is the remedy of compelling a person to perform a contractual obligation.

- It is distinguishable from money awarded through the more common form of compensatory relief, known as "consequential damages".

- The invocation of specific performance for cryptocurrency obligations is supported by the following:

  - cryptocurrency as "software" appears to be subject to protections provided in the *Sale of Goods Act* (*Bennett v. Lenovo*, 2017 ONSC 1082 at paras. 13-16; *The Software Incubator v Computer Associates* [2016] EWHC 1587 (QB) at paras. 68-69); and

  - the *Sale of Goods Act* expressly permits the remedy of specific performance (see *Sale of Goods Act*, s.50).

IV. Enforcement/Litigation

- Alternatively, if it is not as obvious that a contract is involved, the broader equitable remedy of a mandatory injunction should be investigated.

- A mandatory injunction should be sought where the relief claimed is restitution (for example, to reverse a mistaken cryptocurrency payment, or to address a cryptocurrency theft).

IV. Enforcement/Litigation

- A court cannot treat cryptocurrency as money, but can award a CAD equivalent of cryptocurrency.

- This is very confusing, for reasons discussed in our article on "Enforcing Cryptocurrency Contracts".

- But even if this is possible, the issue of valuation must be dealt with.

IV. Enforcement/Litigation

- Valuation of cryptocurrency in CAD is a novel issue.

- Expert evidence is needed. However, a court may be motivated to adopt a higher/lower valuation in certain cases. For example:

  (1) is extorted cryptocurrency is covered within an insurance policy's coverage limits? Crypto value may be lower to sympathize with the insured.

  (2) is share value dependent on a company's crypto holdings? Crypto value may be higher in a security for costs context if there is a bull market.

  (3) what valuation makes sense in a contract dispute? More dependent on the facts.

IV. Enforcement/Litigation

- What if the crypto-currency dispute occurs across borders?

- Cross-border commercial disputes between private parties engage private international law, which the Supreme Court of Canada has described as follows:

> Private international law is in essence domestic law, and it is designed to resolve conflicts between different jurisdictions, the legal systems or rules of different jurisdictions and decisions of courts of different jurisdictions. [*Van Breda v. Village Resorts Ltd.*, 2012 SCC 17 at para. 15.]

IV. Enforcement/Litigation

- **First step: serve pleadings.**

- A claim or counterclaim arising out of a contract may be served on an opposing party outside Ontario, if the contract:

  - was made in Ontario;
  - is governed by Ontario law;
  - states that Ontario courts have jurisdiction over disputes arising from the contract; OR
  - was breached in Ontario.

  [See Ontario's *Rules of Civil Procedure*, R.R.O. 1990, Reg. 194, r.17.02(f).]

- Other grounds of service are also available, including with leave (i.e., the court's permission) (r.17.03(1)).

IV. Enforcement/Litigation

- **Second step: does the Ontario Court have jurisdiction?**

- Ask whether the matters at issue have a "real and substantial connection" to Ontario. This test is context- and fact-specific (*Van Breda* at para. 35).

- Presumptive connecting factors—which the defence can rebut—have been identified for tort cases (*Van Breda* at paras. 80-81, 93-94, 100).

- The list of presumptive connecting factors is not closed (*Van Breda* at paras. 91).

- Future cases are expected to clarify which presumptive connecting factors exist for contract law matters, and how they may be rebutted (*Van Breda* at para. 85, 92).

IV. Enforcement/Litigation

- Here are some guiding principles relevant to cryptocurrency businesses:
  - carrying on business in Ontario is a presumptive connecting factor (*Van Breda* at para 122; Rules of Civil Procedure, r.17.02(p));
  - website accessibility from Ontario is not on its own a presumptive connecting factor (*Van Breda* at para. 87);
  - advertising within Ontario is not on its own a presumptive connecting factor (*Van Breda* at paras. 87 and 114); and
  - it remains to be determined whether e-trade within Ontario is a presumptive connecting factor (*Van Breda* at paras. 87 and 114).

IV. Enforcement/Litigation

- The recent case of *Arend v. Boehm*, 2017 ONSC 3424 (CanLII) is instructive for cryptocurrency businesses.

- This case involved BitRush Corp., which was centred in Toronto but had investors, officers and businesses around the world.

- A proceeding was commenced against BitRush's former CEO and others, alleging oppression and breach of fiduciary duties, and seeking the transfer and cancelation of shares of various classes.

- Jurisdiction was easy to establish, because this step only required "a good arguable case", which meant no more than a "serious question to be tried", or a "genuine issue", or that the case had "some chance of success."

IV. Enforcement/Litigation

- In *Arend v. Boehm*, jurisdiction was established on the basis of the following factors:
  - Bitrush was domiciled in Ontario;
  - BitRush was traded on a public market in Canada;
  - BitRush was "doing business in Ontario"; and
  - a significant percentage of BitRush shares in issue remained in escrow with its transfer agent located in Toronto.

IV. Enforcement/Litigation

- In an attempt to rebut the presumptive connecting factors, Boehm “stressed that he [had] never been in Ontario and that he carried most of his activities for BitRush in Austria.”

- The Court found that this excuse did not rebut the presumption of jurisdiction because, as an officer of the corporation, Boehm “would have understood and expected that disputes dealing with the affairs of the corporation would be dealt with at the place of incorporation” (i.e. Ontario).

IV. Enforcement/Litigation

- **<u>Third step: should the Ontario Court decline jurisdiction?</u>**

- It can do this if another forum with a real and substantial connection to the matter is demonstrably preferable (*Van Breda* at paras. 103-105), on the basis that the other forum "is in a better position to dispose fairly and efficiently of the litigation" (*Van Breda* at para. 109).

- This analysis is context- and fact-specific.

IV. Enforcement/Litigation

- In the case of *Arend v. Boehm*, the Court accepted jurisdiction because shareholder oppression claims were at issue, and a foreign court does not have jurisdiction to decide oppression claims under Ontario’s corporate law legislation. Moreover, many of the applicable contracts between the parties were governed by the laws of Ontario.

- However, the case of *Mt. Gox Co., Ltd (Re)*, 2014 ONSC 5811 (CanLII) had a different result…

IV. Enforcement/Litigation

- Mt. Gox was a Japanese corporation located and headquartered in Japan, and formerly operating as an online Bitcoin exchange.

- The platform halted Bitcoin withdrawals and suspended all trading in February 2014 due to the theft of approximately 850,000 Bitcoins.

- A Tokyo Court entered the Japan bankruptcy order in April 2014, which formally commenced bankruptcy proceedings.

- At that time, there were approximately 120,000 customers with a Bitcoin or fiat currency balance with Mt. Gox, living in approximately 175 countries around the world.

IV. Enforcement/Litigation

- A class action was subsequently commenced in Ontario.

- The Court recognized that because the corporation’s center of main interests was in Japan, the Japanese bankruptcy proceeding was a foreign proceeding under Canadian bankruptcy legislation. On this basis, the Canadian proceeding was stayed (i.e. halted).

- The Court also noted that two class actions initiated in the U.S. were also stayed by U.S. courts for similar reasons.

V. Final Thoughts

- A difficult balance: racing toward market opportunity, and achieving global regulatory compliance.

- **Practical strategy to work within the rules:** limit initial jurisdictional scope of blockchain operations.

- “Sharding” as a potential partial response to conflicting rules across jurisdictions.

V. Final Thoughts

- Hope for the future: *Wisconsin Central Ltd. v. United States*, 585 U.S. ___ (2018).

- The SCOTUS dissenting opinion states:

> [W]hat we view as money has changed over time. ... [P]erhaps one day employees will be paid in Bitcoin or some other type of cryptocurrency.... Nothing in the statute suggests the meaning of this provision should be trapped in a monetary time warp, forever limited to those forms of money commonly used in the 1930's.

- Although the Bitcoin comment in dissent is *obiter dicta*, the majority opinion also suggests an openness to the idea of cryptocurrency being "money" in future cases:

> While every statute's meaning is fixed at the time of enactment, new applications may arise in light of changes in the world. So "money," as used in this statute, must always mean a "medium of exchange." But what qualifies as a "medium of exchange" may depend on the facts of the day. Take electronic transfers of paychecks. Maybe they weren't common in 1937, but we do not doubt they would qualify today as "money remuneration" under the statute's original public meaning.

FIN

SMARTBLOCK LAW

PROFESSIONAL CORPORATION

https://smartblocklaw.com

info@smartblocklaw.com | 1-833-BIT-LAWS | 250 Yonge Street, Suite 2201 | Toronto, Ontario, M5B 2L7, Canada