



MILLER THOMSON  
AVOCATS | LAWYERS

# **PROOF OF STAKE**

## **Financial Services & Banking**

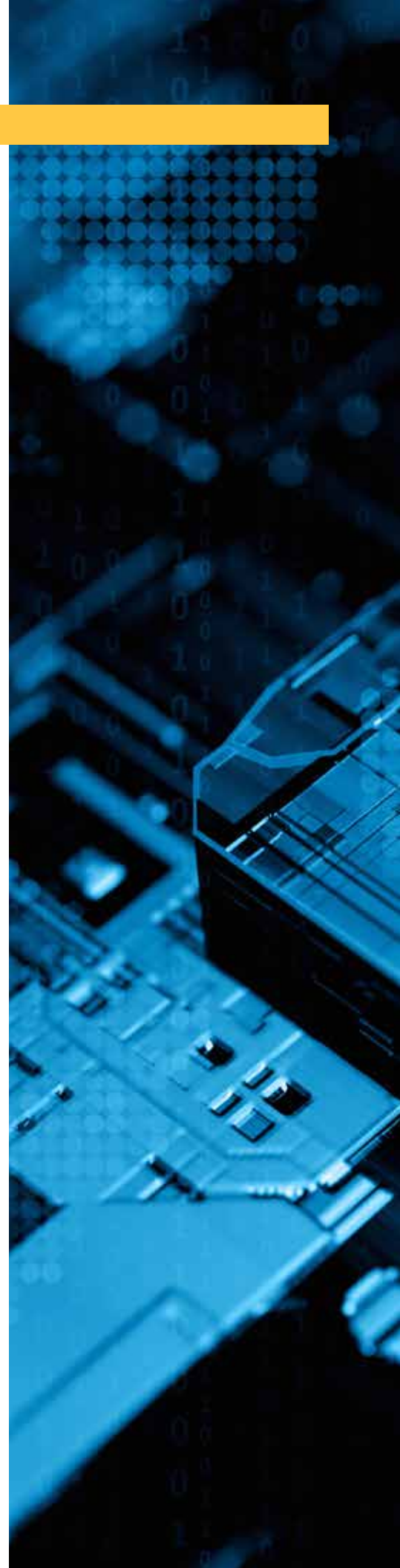
At Miller Thomson, lawyers in our Business Practice are not only proactively alert and informed with respect to the rapidly evolving area of blockchain, cryptocurrency and smart contracts, they are also actively engaged with clients on these matters and gaining real world knowledge and experience. It's from this vantage that we have compiled relative editorial to share with our clients and various stakeholders including government, their agencies, regulatory groups, business owners, entrepreneurs and academics.

We are confident that clients of Miller Thomson will benefit from our multi-disciplinary strategic focus on Distributed Ledger Technology (DLT). Blockchain-based transactions can and will transform every industry sector. It's evident that a blockchain, artificial intelligence, cryptocurrency, and IoT patents arms race is certainly occurring. Our tech-savvy team of lawyers are prepared to help market leaders navigate both legal and regulatory issues as they strategize and build a commercial advantage and address a range of specific concerns such as business risk, privacy and security.

The fabric of Miller Thomson clients spreads nation-wide and includes financial institutions with an economic interest in DLT and related technologies. While enthusiasm in the banking sector is growing with regards to DLT, for financial institutions there are unpredictable implications. Our lawyers can assist no matter where business is transacted – whether in Canada or abroad.

**Bernard Blouin**, Chair  
Business Practice  
bblouin@millerthomson.com  
514 871 5351

**Wayne Logan**, Leader  
Area of Focus: Blockchain,  
Cryptocurrency and Smart Contracts  
wlogan@millerthomson.com  
403 298 2407





# CONTENTS

---

Pg 2

What are the banks doing with Blockchain?

Pg 6

ATB & the value [Block]chain

Pg 10

“Pay Me Back in Crypto”  
Surveying Enforcement Issues  
for Cryptocurrency Litigation  
in Canada

Pg 14

Blockchains, Banks and  
Virtual Vaults

Pg 17

How Smart is Your Contract?  
Legal Considerations Around  
Smart Contracts

Pg 20

Bitcoin and Examples of the  
Global Regulatory Environment:  
It is Anyone’s Guess

```
WINBUTTON  
PUBLIC CLASS OSXFACTORY  
@OVERRIDE  
PUBLIC IBUTTON CREATERBUTTON  
RETURN NEW BUTTON
```

```
PUBLIC CLASS WINBUTTON  
@OVERRIDE  
PUBLIC VOID PAINT()  
SYSTEM.OUT.PRINTLN
```

```
PUBLIC CLASS OSXBUTTON  
@OVERRIDE  
PUBLIC VOID PAINT()  
SYSTEM.OUT.PRINTLN
```

```
PUBLIC CLASS MAIN {
```

```
PUBLIC STATIC VOID MAIN()  
{GUIFACTORY FACTORY = new
```

```
FINAL STRING APPEARANCE
```

```
IF (APPEARANCE EQUALS  
FACTORY = NEW OSXFACTORY  
} ELSE IF (APPEARANCE EQUALS  
FACTORY = NEW WINFACTORY  
} ELSE {  
THROW NEW EXCEPTION
```

```
FINAL IBUTTON BUTTON =
```

```
BUTTON.PAINT();
```

```
THIS IS JUST FOR THE  
WITH ABSTRACT FACTORY  
@RETURN
```

```
PUBLIC STATIC STRING  
FINAL STRING[] APPEARANCE
```

```
APPEARANCEARRAY
```

# What are the banks doing with Blockchain?

By Jeffrey Roode, Partner

Last year, J.P. Morgan Chase CEO Jamie Dimon famously called blockchain's first use-case – Bitcoin – a “fraud”. He later said that he regretted that remark and said “the blockchain is real”.



To take one example, cross-border bank-to-bank transfers are currently generally completed using the Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT is a centralized system which allows information about transactions to be exchanged among its members but it does not actually clear or settle the transactions – members must maintain accounts with one another directly or using correspondent banks to do so and each member must maintain its own ledger. SWIFT transfers can take several days and may require human intervention to correct errors. In addition to being faster and less error prone, a decentralized ledger system to effect bank to bank transfers would also avoid the need for banks to maintain separate ledgers and correspondent banking relationships.

Banks have recognized that for the full benefits of distributed ledger technology to be realized, there is a need to work together to develop common standards. In 2015, a group of nine international banks founded a consortium known as R3 to work on distributed ledger technology. R3, which now has over 70 members (including some Canadian banks), has developed an open-source distributed ledger platform known as Corda upon which distributed ledger and smart contract solutions can be built. Corda's technology differs from the version of blockchain that supports Bitcoin in a number of ways, including the ability to ensure privacy of transactions (transactions are not available on all network nodes) and the fact that mining is not required for new transactions.

This change of heart is not surprising given the enormous potential for distributed ledger technologies such as blockchain to transform the banking industry. By allowing multiple parties to have access to the same information in real time, distributed ledger technology has the potential to deliver enormous cost savings to banks as well as the potential to reduce errors and delays in settlement.

A 2016 report by Accenture<sup>1</sup> identified a number of potentially significant use-cases for blockchain in banking including intra- and inter-bank cross border payments, cross-border remittances, corporate payments, person-to-person payments and cash pooling.

<sup>1</sup> Accenture Mobility, "Blockchain Technology: How Banks are Building a Real-Time Global Payment Network", 2016.

<sup>2</sup> Payments Canada Press Release, "Payments Canada, Bank of Canada and R3 release detailed findings of blockchain experiment" (Sept. 29, 2017) Online: <https://www.payments.ca/industry-info/our-research/payments-canada-bank-canada-and-r3-release-detailed-findings-blockchain>

Several Canadian banks are also investors in SecureKey, a Toronto-based company which announced in March 2017 that it was working with IBM to develop a new digital identity sharing network using blockchain technology. Once complete, this network will allow consumers to verify their identities for new banking services as well as for utilities and government services such as the issuance of driver's licenses.



In Canada, a consortium comprised of R3 together with its Canadian member banks, Payments Canada and the Bank of Canada undertook “Project Jasper” in an attempt to determine whether distributed ledger technology could be used in the wholesale payment system which is used by the Canadian banks to pay one another. According to Payments Canada, this marked the first time that a central bank and a payment system operator had worked together with the private sector in a blockchain experiment.<sup>2</sup> While the initial phases of the project ultimately concluded that distributed ledger technology was not yet ready to support the domestic inter-bank payments system, further work continues.

Canadian banks are also investigating the potential of distributed ledger technology on their own. For example, in September 2017, RBC revealed that it was testing a blockchain-based system to transfer funds between its U.S. and Canadian banks by integrating the system as a “shadow ledger” to the current ledger it uses to track these activities.

Banks in both Canada and the U.S. have also filed patents covering blockchain or distributed ledger technologies in a wide variety of use cases. Set out below are just a few examples of Canadian and U.S. patent applications by banks found in a recent patent search. ◆

Bank	Jurisdiction	Description
TD	Canada	A System and Method for Implementing Hybrid Public-Private Block-Chain Ledgers
TD	Canada	Systems and Methods for Tracking and Transferring Ownership of Connected Devices Using Blockchain Ledgers
RBC	U.S.	Distributed Ledger Platform for Vehicle Records
Bank of America	U.S.	System for Transforming Large Scale Electronic Processing Using Application Block Chain and Multi-Structured Data Stores
J.P. Morgan Chase	U.S.	Systems and Methods for Providing Data Privacy in a Private Distributed Ledger
Bank of America	U.S.	Transparent Self-Managing Rewards Program Using Blockchain and Smart Contracts
Bank of America	U.S.	Block Chain Alias for Person-To-Person Payments
TD	U.S.	Systems and Methods for Establishing and Enforcing Transaction-Based Restrictions Using Hybrid Public-Private Blockchain Ledgers

## ABOUT THE AUTHOR



**Jeffrey Roode** is a Partner in Miller Thomson LLP's Financial Services Specialty Group. His practice encompasses corporate/commercial and information technology law with a focus on retail financial services including payments and Fintech.

**[jroode@millerthomson.com](mailto:jroode@millerthomson.com)**  
**416 597 4387**

# ATB & the value [Block]chain

Engaging in Inspired Solutions



ATB's Chief Transformation Officer, Wellington Holbrook once described Blockchain as a "solution looking for a problem". Nowhere is that more evident than in the financial sector, where players big and small are collaborating across many facets of operations to leverage the capabilities of the 'chain'.



As a mid-sized financial institution, where does ATB land? Certainly our level of investment is a few standard deviations away from the larger banks, so we have to be selective with where we invest efforts. We've made a conscious effort to explore applications of the technology that, at core use, benefits Albertans. Our size allows for rapid deployment and execution of a proof of concept (POC), adding velocity to the iterative loop that's necessary to take us from exploration to scale and contribute to the global Blockchain conversation. Part of this exploration will also lead us to 'inspired by Blockchain' POC's versus outright locked up distributed ledger Blockchains. Textbook Blockchains are very infrastructure intensive, so using current technology to attain benefits comparable to Blockchain are certainly areas that many organizations will explore.

## What's up with ATB & Blockchain?

### *Sovrin stewardship*

The Sovrin Foundation was established to govern the global self-sovereign identity (SSI) network, providing an enduring solution for global identity that places control of an identity back in the hands of the individual. Our stewardship with Sovrin allows us to provide the human governance and trust frameworks to collaborate across industry to further the work, with the opportunity to have Albertans and Alberta-based businesses be amongst the first to access the capabilities developed here. With giants like IBM announcing stewardship and more in the pipeline to join, this is one entity to watch.

The ecosystem around Sovrin is actively growing by the day and with it the number of potential use cases. Use cases around employment records for onboarding and digital education credentials are being explored with ATB to provide Blockchain expertise and guidance as needed. The challenges we

see with our work here is that the technology is new with components still undergoing evolution, providing a natural latency to the process. We anticipate the technology to mature in the next year or so, leading to a conversation with key stakeholders on scaling out across Alberta on the horizon.

### *R3 Consortium Development*

The R3 network is one of the more established groups which is relying upon Corda, a bespoke distributed ledger designed specifically to facilitate financial transactions for the member organizations. Our membership with the consortium is to collectively further the applications of distributed ledger technology with members focusing on near-future solutions with a clear and measurable value proposition. The collective is rapidly spinning up POCs in a bid to move them to production state and shifting resources towards solutions that will be production ready in short order. The opportunities here leverage the core Corda platform, which is also being scaled in parallel.

### *Oil Settlement with IBM*

ATB has built a POC with IBM using Blockchain to streamline the reconciliation/actualization of energy contracts within the industry, creating efficiency and opportunity to rethink the value ATB can deliver to a process that also carries with it a modicum of tradition. We have validated the model with select energy industry players who are working with us to design the next round of solution development and pilot testing. There is a strong opportunity to shape the pilot (which is expected late 2018) should we be able to onboard specific industry players within the energy transport and buying space. We're excited about this one as it provides significant efficiencies to the energy industry not only in Alberta, but across the country.

## *Supporting Alberta Entrepreneurs – Blockchain payment settlement*

Looking across the value chain, we don't believe it's necessary to always be the lead in execution on Blockchain innovation. ATB is also taking to providing back end payment settlement for up and coming Alberta entrepreneurs in this space. By providing the payment engine that can essentially plug into enterprise Blockchains, we expand the value we can deliver to furthering innovation happening within multiple industries.

## *Supporting Alberta Entrepreneurs – Cryptobusiness banking pilot*

One of ATB's mandates is to serve Albertans and find ways to make banking work for them. With our foray into Blockchain, one opportunity we see is within the cryptocurrency-based business space. There is a significant amount of entrepreneurial activity in this space, with crypto-exchanges and mining companies being spun up at a rapid pace. This activity could lead to growth opportunities for an FI if they can bridge the gap between a



We recently demonstrated our payment settlement capabilities with Calgary-based GuildOne, a company that paired smart contracts with Blockchain to optimize the settlement and payment of royalty contracts within the industry. Our second POC will be with another local Calgary startup, ReWatt Energy, where carbon-offset credits can be aggregated across independent producers and supplied to larger producers – something that does not happen today given the high inefficiencies within the process.

The opportunity to provide this type of service to entrepreneurs that may choose to rapidly scale out this work to a concrete business offering is significant for ATB.

cryptocurrency business and banking services. Due to Anti Money Laundering and KYC regulation, cryptocurrency businesses need a unique approach to be able to acquire bank accounts, which are required for the business to be viable. There is also a reputational risk when it comes to banking these businesses, as banks need to ensure that a customer relationship isn't misconstrued as an endorsement of that exchange or cryptocurrency as a standard investment vehicle.

ATB has a small pilot underway with a handful of cryptocurrency businesses to be able to “de-risk” the businesses so that we can provide them banking services, as we do for any other start-up business. Currently the pilot is in early stages with a bespoke approach to our engagement. Consistent with vendors that work with these types of businesses, the customer relationship we maintain should in no way be misconstrued as an endorsement of the exchange itself or of cryptocurrency as an investment vehicle. ATB’s challenge will be to find a way to scale our services provided in the pilot so that if this becomes a known offering, we will be able to match the pace of incoming requests.

## On the horizon

As we’ve illustrated, the opportunity for ATB (and other FI’s that approximate ATB in size and impact) are inspired solutions rather than a “one-chain to rule them all” type approach. We also see opportunity within the Blockchain ecosystem to insert ourselves into different areas - you don’t need to own the network to provide value to Albertans.

We foresee Blockchain activities starting to be put into operation within the next year, and commercialized shortly thereafter. This is consistent with the market view where we are seeing significant amounts of patent activity by FI’s. It will be intriguing to see what the commercial outcome of those patents are as Blockchain is unique in the requirement for participation from competitors and allies alike within an industry segment. The ownership of a patent itself could spin out into a source of revenue. It may be worth noting that the decentralized nature of Blockchains living within an ecosystem seems at odds with patent ownership, which traditionally creates points of centrality and potential bias. Over time we will learn more about what IP is protected and how those protections are enforced.

For this solution to many problems, the question appears to not be so much of a ‘when’ or even a ‘who’ given that the technology dictates collaboration in arenas where there may not have been any. The question when it comes to Blockchain, appears to be that of ‘how’.

To learn more about ATB Financial’s innovation around Blockchain, visit [www.atbalphabeta.com](http://www.atbalphabeta.com) or follow Chief Transformation Officer Wellington Holbrook (@Wellington\_ATB) and Director of Innovation Mike Brown (@Mike\_Brown\_yyc) on twitter. ♦

## ABOUT THE INTERVIEW

Created by ATB Financial through interview with Wellington Holbrook, Chief Transformation Officer, and Mike Brown, Director of Innovation (Blockchain).

For questions or feedback, please contact Sonu Jaswal ([sjaswal@atb.com](mailto:sjaswal@atb.com)).



**Wellington Holbrook**



**Mike Brown**

# “Pay Me Back in Crypto”

## Surveying Enforcement Issues for Cryptocurrency Litigation in Canada

By Keegan Boyd, Partner and Ivan Mitchell Merrow, Associate

Decentralized digital currencies known as cryptocurrency or “crypto” are increasingly being used for payment across the world. As the adoption of digital currency grows, so too does the potential for disputes and lawsuits. Wars previously waged over funds held in bank accounts will increasingly be fought over digital “money” that exists only on the Internet.



Consider this classic debt repayment scenario with a crypto twist:

***You enter into a binding commercial contract to provide cryptocurrency in exchange for services. You deliver the cryptocurrency on time pursuant to the contract, but you never receive the services as promised. You want to sue for breach of contract and get your cryptocurrency back, but the cryptocurrency is stored in one or more online “wallets” and its valuation is unstable.***



Individuals and companies seeking to recover cryptocurrency have to grapple with a number of novel issues. Where is the cryptocurrency stored and who has jurisdiction over it? Is cryptocurrency considered an “asset” or “money”? Can cryptocurrency be garnished in the same manner as funds in a bank account?

## Background

Cryptocurrency is digital “money” with special properties that make it impossible to counterfeit. The underlying technology that makes cryptocurrency special is called “blockchain”.

Blockchain ensures that every cryptocurrency transaction gets recorded in the currency’s code. The ledger gets automatically distributed across many different computers and systems. Collectively, the systems verify each transaction. No one computer can copy or counterfeit a blockchain-based cryptocurrency because it would get rejected by the rest of the system. Cryptocurrency can be bought, sold and converted to other currencies.

Cryptocurrency does not depend on any bank or financial intermediary to confirm that funds are available for a given transaction. Nor does cryptocurrency depend on a sovereign country or resource to “back” the currency.

Numerous digital currencies currently exist. The more well-known are Bitcoin, Bitcoin Cash and Ethereum or “Ether”. Other alternative coins or “altcoins” emerge daily as individuals design and market their own forms of cryptocurrency. Individual units of cryptocurrency are often referred to as “tokens”.

In the consumer market, the most well-known cryptocurrency, Bitcoin, can be used to purchase various goods and services, including software from Microsoft’s online Xbox store. Earlier this year, Bitcoin was temporarily accepted as payment by KFC Canada for fried chicken.



Unsurprisingly, businesses are also experimenting with cryptocurrency as a form of payment in commercial transactions. As the use of cryptocurrency gains acceptance, it is increasingly important to consider the unique aspects of enforcing one's rights in the event a cryptocurrency transaction goes awry.

## Cryptocurrency Enforcement Considerations

In the simple example above, you have a binding contract to receive services in exchange for payment in cryptocurrency. You transfer the appropriate number of tokens, but no services are rendered. You now wish to commence a claim to recover the cryptocurrency that you paid. How your claim is framed will likely affect the procedures available to you and the potential for recovery.

The first cryptocurrency issue to consider is whether digital tokens are properly considered "money" or "property". It is a basic question, but the legal consequences may be significant. The jurisdiction of certain courts, such as the Small Claims Courts of Ontario, are limited to claims for "money". Currently, cryptocurrency is not considered legal tender in Canada so it is unclear whether courts would consider a cryptocurrency debt as a liquidated debt. If your claim is framed in terms of lost "money",

expert evidence may be required to enable the court to determine the Canadian dollar value of the cryptocurrency, particularly given the large fluctuations seen in the trading value of many cryptocurrencies, including Bitcoin.

Special enforcement considerations also arise if you plan to ask the court for an order to retrieve cryptocurrency as "property". The following preservation and enforcement procedures serve to highlight some of the unique considerations at play:

- **"Mareva" orders:** Courts can make pre-trial orders to prevent the transfer of assets where there is a real and substantial risk that they will be disposed of prior to trial. Even if one is successful in convincing the court to "freeze" cryptocurrency holdings, practical difficulties may arise from the decentralized nature of cryptocurrency. Are the cryptocurrency assets held in an online "wallet" or on a currency exchange? Have they already been distributed or sold? Who do you serve with the *Mareva* order if there is no bank with established processes to freeze the relevant accounts? While the blockchain provides a historical record of all transfers, it is difficult, if not impossible, to trace cryptocurrency tokens to specific individuals without at least some information to link those individuals to a particular cryptocurrency wallet.

•**Orders for the interim recovery of personal property:** Originally called “replevin”, this common law remedy allows you to go beyond freezing assets and actually retrieve “personal property” prior to trial. Strong proof of ownership and an enforceable claim against the opposing party are typically required. This remedy may be appropriate if you have compelling grounds to retrieve specific cryptocurrency tokens that you transferred to another party. For example, a rare set of “altcoins” that are not in wide circulation may have unique speculative value. An equivalent sum in Canadian dollars may be worth far less than the potential upside of holding the cryptocurrency itself.

•**Execution:** After successful judgment, how do you get your cryptocurrency back? If the court order is for the specific retrieval of personal property, you would presumably enforce the order by identifying the location of the crypto, serving the order, and demanding that your tokens are returned. Again, though, practical difficulties will almost certainly arise in finding, locating, and retrieving the digital currency. It may practically be easier to enforce a monetary award as there are established procedures for enforcement, including the registration of a writ against real property or garnishing the funds held in relevant bank accounts.

The decision on whether to frame your claim for lost cryptocurrency in terms of “property” or “money” needs to be carefully considered to ensure you are not inadvertently creating procedural barriers when it comes to enforcement. After a court action has begun, pivoting may be difficult and costly. Given the volatility and uncertainty associated with certain forms of cryptocurrency, a judgment may be worthless or exponentially more valuable compared to when the legal action was commenced.

The cost of enforcing orders for the repayment of cryptocurrency may also depend on the location of online crypto holdings. If the tokens are held internationally, issues may arise from the fact that Canada and many other jurisdictions have yet to

recognize cryptocurrency as legal tender. While the blockchain provides evidence of the underlying transactions and will identify the relevant cryptocurrency wallets involved, it may be practically impossible to identify the individuals or entities to serve with an order. The enforcement steps necessary to recover cryptocurrency tokens may also be prohibitively expensive.

In sum, it is important to think carefully before you say “pay me back in crypto.” There are many unique considerations that will impact the best litigation strategy, and early strategic planning with legal counsel is essential to increase your odds of recovery. ♦

## ABOUT THE AUTHORS



Keegan Boyd is a Partner in Miller Thomson LLP’s Commercial Litigation Specialty Group. His practice encompasses a wide range of complex commercial litigation, including contractual disputes, shareholder and partnership disputes, and asset recovery.

[kboyd@millerthomson.com](mailto:kboyd@millerthomson.com)  
416 597 6086



Ivan Mitchell Merrow is an Associate in Miller Thomson LLP’s Commercial Litigation Specialty Group. He acts for a broad range of individuals, organizations, and businesses to resolve disputes, prosecute contracts, defend law suits, handle appeals, and enforce judgments.

[imerrow@millerthomson.com](mailto:imerrow@millerthomson.com)  
905 532 6607

# Blockchains, Banks and Virtual Vaults

By James Swanson, Partner

Blockchains, also known as distributed ledger technologies or DLTs, can be thought of as many things in addition to a platform for cryptocurrencies – a type of database, an evolution or revolution in cloud computing, a new means to ensure security and authenticity of identity, transactions and records, and even as a form of operating system or platform or infrastructure as a service. Blockchains can not only provide solutions for any number of current issues in finance, banking and online commerce, but also opportunities to develop new business models or disrupt current ones.

For example, the distributed and the self-evidencing properties of a typical blockchain can help defeat the current pandemic of cybersecurity and privacy breaches, identity theft and fraud.

Distributed means that the distribution of multiple and identical copies of a blockchain across a network or the Internet makes it virtually impossible for hackers to make changes to the blockchain without authority to do so, because, in a typical blockchain, at least a majority of those copies must be altered simultaneously, while at the same time the changes would be clearly apparent to users.

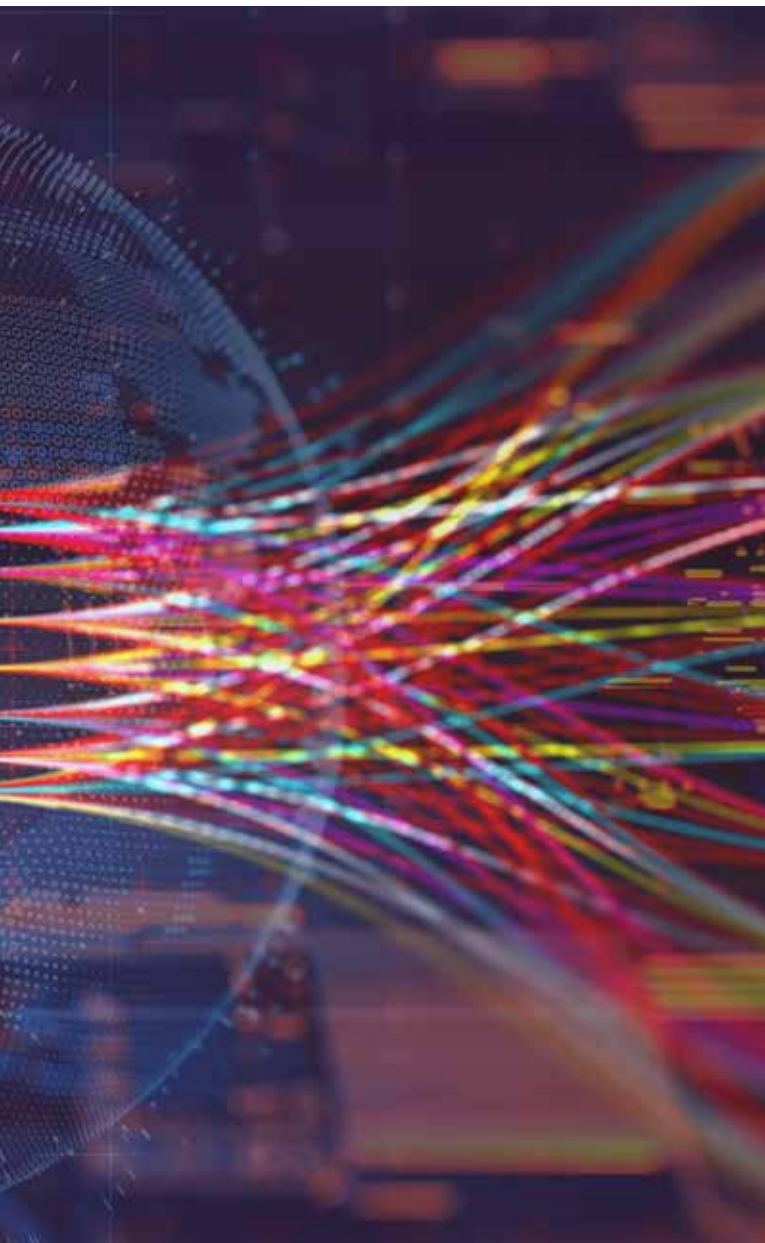




Self-evidencing means that a user can tell if data has been tampered with just by looking at blockchain, making fraud exponentially more difficult and visible.

Although we are only limited by our imaginations, examples of use cases for blockchains in the financial and banking industries include:

- Enabling secure and permanent archiving and verification of identity, credentials and permissions, limiting access to resources, records and money to only those authorized. Identity can be immutably stored on a blockchain and called on by software applications on behalf of other users as required to authenticate identity and associated rights and obligations.
- Providing a secure and permanent means of keeping records of transactions, transfers, account balances, property rights, titles, interests, licenses, debits and credits. As records are properly entered into a blockchain, they can be encrypted, hashed (a means of confirming data remains unchanged when compared with versions known to be valid), linked to each other by mathematical functions to confirm validity in connection with prior transactions or blocks, and distributed across a network or the Internet making alterations without permission virtually impossible.
- Providing opportunities to automate processes and track transactions in new and useful ways. Examples include:
  - o Proxy voting, which was recently tested by NASDAQ on its Estonian exchange.
  - o Automated RFP and tendering processes.
  - o Use of “smart contracts”. These are conceptually like a vending machine – something of value goes into one end (like coins into the machine) and something of value comes back (like a bottle of soda). Of course, smart contracts are virtual and capable of much more complex transactions than a vending machine.





- Eliminating intermediaries and associated costs. Intermediaries (such as government registries, banks or lawyers) have traditionally been required because parties to a transaction or agreement may not know and/or trust each other. With the use of blockchain technologies, the need to know or trust the other party is eliminated, as can be the intermediary, and replaced with trust in the code to the blockchain itself. This presents potential opportunities for financial institutions to stay relevant by providing trusted blockchain platforms while also using automation for increased efficiencies.

With sufficient interactivity and connectivity, and perhaps a dash of automation or artificial intelligence, records of identity, title, account balances, etc. can be immutably recorded, and any type of transaction or transfer of value can be carried out and completed very quickly with minimal, if any, human involvement.

Banks and financial institutions may be reluctant to implement blockchain platforms or solutions for any number of reasons, but let's address two of the most likely:

1. A desire to avoid disruption to current and profitable business models. In most cases disruption is inevitable. An organization can wait to have someone else carry out the disruption, perhaps damaging or destroying their current business, or they

can do it themselves thereby controlling the disruption with the hope that they will live long and prosper.

2. Fear of not complying with legislation and regulations. Legislation and regulators tend to be technology neutral, focusing on processes, protection of the public, and compliance with regulatory requirements, by whatever technical means. Use of blockchain technologies will in most cases be permissible as long as the processes and activities of the organization using a blockchain are compliant, and in fact blockchain technologies may even enhance the organization's legislative and regulatory compliance. ♦

## ABOUT THE AUTHOR



Partner Jim Swanson brings decades of practical experience in legal issues related to technology, intellectual property and new media. He enjoys helping clients to grow their business, deal with complex and leading edge legal issues and resolve disputes in a results oriented manner.

[jswanson@millerthomson.com](mailto:jswanson@millerthomson.com)  
403 298 2447

# How Smart is Your Contract?

## Legal Considerations Around Smart Contracts

By Imran Ahmad, Partner



In a 2016 report<sup>3</sup> by the World Economic Forum, it was suggested that smart contracts based on blockchain technology could potentially codify financial agreements in a shared platform and guarantee execution based on mutually agreed conditions. This would significantly reduce manual efforts required to support the execution of financial agreements and thereby, in theory, accelerate business processes. While the benefits associated with the application of blockchain technology to smart contracts is promising (e.g., operational simplification, counterparty risk reduction, clearing and settlement time reduction and fraud minimization), it brings with it important technical and legal issues.

<sup>3</sup> World Economic Forum, The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services, August 2016.

## Smart Contracts – A Primer

Broadly speaking, smart contracts are self-executing electronic instructions drafted in computer code. This allows a computer to “read” the contract and, in many instances, effectuate an instruction or transaction, should certain conditions be met – hence the “smartness” of the contract. Put differently, a smart contract will self-execute the stipulations of an agreement when predetermined conditions are triggered. The parties to the contract typically “sign” the agreement using a cryptographic security code and deploy it to a distributed ledger, or blockchain. When conditions in the code are met, the program automatically triggers the required action.

The underlying technology to smart contracts, blockchain, is a register (or ledger) of all transactions that have occurred for a given smart contract. Each transaction (or block) is authenticated by a network of computers before it is added to the chain of all prior transactions using cryptographic techniques and a large amount of computing power. The blockchain, or distributed ledger, is open and transparent for all to see. The record is intended to be secure, permanent and immutable.

Blockchain uses encryption and a combination of public and private “keys” for security. The system utilizes mathematical techniques to match a public address with a private security access key for each participant in a transaction. If these two items match, the transaction can then be broadcast to the other participants in the blockchain for verification and entry into the ledger.

## Key Legal Challenges

### *Cybersecurity*

One of the key concerns around smart contracts is whether they can be hacked and manipulated for improper use. The concern is not hypothetical. In July 2016, a hacker exploited code vulnerabilities in the so-called Decentralized Autonomous Organization (“DAO”) to redirect \$50 million into an account controlled by the hacker. DAO was an investment fund where, instead of leaving decisions to a few partners, anyone who invested would have a say in which companies to fund. The more an investor contributed, the more their weight mattered. The distributed structure was meant to ensure that no one could run off with the money – in theory. However, a hacker, who was also a participant in the fund, was able to manipulate the code and transfer \$50 million in cryptocurrencies without proper authorization. While the hacker was apprehended and the funds recovered, the incident demonstrates that the “security” around smart contracts is not absolute.

### *Contract Law*

Another key question that comes up about smart contracts is whether they are really contracts. Broadly speaking, a contract is a legally enforceable promise or promises which must meet a number of conditions imposed by law, such as multiple parties, the capacity of parties, mutual assent, and consideration. Further, there are a number of defenses to the enforcement of contracts, including mistake, misrepresentation, duress, undue influence and unenforceability on public policy grounds.

For a smart contract to be enforceable, it would need to meet all of the traditional requirements of a valid contract under law. Based on Canadian caselaw in the area of electronic commerce, it is unlikely that smart contracts will require any special set

of new law or regulations. Rather, existing legal principles will be adapted and perhaps modified, either by statute or by the courts, to deal explicitly with the requirements of smart contracts or other emerging technologies.

What is unclear at this stage is how smart contracts will take each legal requirement for contract formation and demonstrate that they are met with the proposed smart contract solution the parties are entering into.

### *Financial Crimes Enforcement*

Smart contracts also raise concerns from an anti-money laundering standpoint. Under Canadian law, participants in financial transactions are required to know and verify the identity of counterparties and report any suspicious activity to law enforcement or to block the transfer of fund to specific individuals or organizations. Since smart contracts are designed to self-execute without human intervention, users of these smart contracts will need to build technical contracts that allow them to comply with such legal requirements.

Further, smart contracts often will keep the identity of parties anonymous, which will further complicate the work by financial institutions who are required to report such transactions and law enforcement who will be tasked with investigating them.

### *Other Issues*

In addition to the above, there are a host of other issues that should be taken into consideration when it comes to smart contracts, including how legal disputes between contracting parties will be settled and how evidence will be provided to the courts. For example, given the courts' limited expertise in deciphering code, parties to a smart contract may need to retain a neutral third party to securely maintain and produce the smart contract in natural language for a court to review as part of a potential dispute.

Similarly, if the parties to a smart contract are using a third party platform, they may be required to agree to an established set of overarching basic legal provisions, such as dispute resolution, governing law and venue. These would need to be clearly disclosed and agreed upon by the parties to the smart contract to be enforceable. While simple in theory, demonstrating that this was done in a manner that the parties clearly understood what agreeing to such provisions meant (so as to not vitiate their consent), is not likely to be straightforward.

## Conclusion

Blockchain technology and smart contracts have the potential to positively transform financial markets and the business of banking. Assuming that the technology is further developed and broadly adopted, smart contracts will need to meet the same legal standards as traditional paper agreements.

Given the significant costs associated in building smart contracts and the underlying infrastructure to support them, businesses should also invest resources in developing a legal architecture built on existing statutory and judicial guidance. This will avoid unnecessary issues down the road. ♦

## ABOUT THE AUTHOR



Imran Ahmad is a Partner at Miller Thomson LLP and practices in the areas of cybersecurity, privacy and technology law.

[iahmad@millerthomson.com](mailto:iahmad@millerthomson.com)  
416 597 6031

# Bitcoin and Examples of the Global Regulatory Environment: It is Anyone's Guess

By David W. Chodikoff, Partner

The worldwide cryptocurrency craze has continued with astonishing speed and intensity. It was in 2009 that Bitcoin was created by an unknown person or group of persons, known under the name of Satoshi Nakamoto.<sup>4</sup> Bitcoin was released as an open source software. Basically, Bitcoins are created as a reward for a process more commonly referred to as “mining”. In simple terms, mining is a validation of transactions and, in so doing, the cryptocurrency “miner” is rewarded for solving complex math problems.

In 2017, it was estimated that the number of “unique active users” of cryptocurrency wallets was between 2.9 million and 5.8 million.<sup>5</sup> Because of the decentralized nature of cryptocurrencies, nation-states cannot shut down the network or alter the technical parameters of cryptocurrency mining. However, governments can choose to ban cryptocurrencies, shut down exchanges or use other regulatory tools to limit the growth of the peer-to-peer economy.



<sup>4</sup> Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, online: <[www.bitcoin.org](http://www.bitcoin.org)>.

<sup>5</sup> Dr. Garrick Hileman & Michel Rauchs, Global Cryptocurrency Benchmarkings Study, University of Cambridge, Judge Business School United Kingdom, 2017.

The fact remains that the legal status of Bitcoin and other cryptocurrencies vary greatly from one country to the next. Another reality is that the rollercoaster valuation of Bitcoin and other cryptocurrencies since December 2017 to the present day, has not deterred Millennials, the largest group of believers and investors, from mining and investing in the cryptocurrency market.

What has become clear with the increased global interest in cryptocurrencies and the speculative nature of cryptocurrency trading, is that governments are taking aim to control

the treatment of cryptocurrencies. According to a study conducted by the University of Cambridge, almost 60% of all cryptocurrency mining takes place in China.<sup>6</sup> The reason is simple: mining requires cheap electricity and land. Both of these requirements are fully available in China's provinces. However, China continues to take dramatic steps to discourage cryptocurrency trading. In 2017, the Chinese government banned initial coin offerings, closed local cryptocurrency trading exchanges and limited Bitcoin mining. In January 2018, Chinese authorities indicated that they plan to block domestic access to Chinese and offshore cryptocurrency platforms that permit centralized trading. It is clear that the Chinese government is trying to push cryptocurrency miners out of their country. Often, one reads that the reasons for this Chinese policy towards the cryptocurrency miners is the fact that they do not pay tax, pose a continuing threat to the environment and mining operations tend to be a fire hazard.

Following the crackdown in China, South Korea was thought of as a country of refuge for cryptocurrency miners and investors. There has been a high level of confusion regarding the direction of regulation in South Korea. However, in late January 2018, the government imposed a new rule disallowing anonymous accounts from trading cryptocurrencies. Moreover, those trading in cryptocurrencies face external scrutiny. Specifically, on January 26, 2018, the New York State Department of Financial Services had requested customer information on accounts connected with cryptocurrency trading among six of Korea's commercial banks that maintain branches in New York.<sup>7</sup>



6 Ibid.

7 Yoon Yung Sil, "Business Korea – The U.S. seems to be concerned that virtual currency can be a loophole in financial sanctions on North Korea", (30 January 2018), online: <comcapint.com>.

India was yet another country thought to be a friendly environment for cryptocurrencies. However, this situation appears to be quickly changing. The Indian government's concerns are no different from other governments. Some of the key problem areas include money laundering, tax evasion, the sponsorship of terrorism and the growth of various other types of illegal activities. The Indian national budget was released in early February 2018 and the Finance Minister noted that cryptocurrency is not recognized as legal tender in his country. The government has yet to produce a fully formulated regulatory regime to prevent the threats posted by money laundering and tax evasion. However, India's Tax Department has issued notices to 100,000 cryptocurrency investors after watching the activities of major trading platforms. Even with this recent clampdown, the India cryptocurrency market is healthy and still growing.

In other parts of the world, Bitcoin and other cryptocurrency phenomena continue to take hold. Some nations are making it all the more attractive to create mining operations. Others are facilitating the creation of exchange platforms and encouraging the creation of investment pools. Nation-state regulators are trying to keep pace, but to date, most states are falling behind the continuing technological advancements in the cryptocurrency world.

It is far too early to tell if the cryptocurrency craze will end badly or if it will be a bona fide "asset" class. What is clear is that governments around the world are not working in concert and that there is a global patchwork of laws and regulations. Unless there is a coherent, cohesive international effort to regulate and monitor cryptocurrency activities, lots of people will get hurt, be it investors or speculators. ♦



## ABOUT THE AUTHOR



David W. Chodikoff is Editor-in-Chief of Miller Thomson's newsletter entitled Taxes & Wealth Management published by Thomson Reuters. Leading the Tax Litigation team at Miller Thomson, David is a Tax Partner specializing in Tax Litigation (Civil and Criminal).

**[dchodikoff@millerthomson.com](mailto:dchodikoff@millerthomson.com)**  
**416 595 8626**





## Innovation in the Legal Industry

Miller Thomson is proud to be a founding member of the Global Legal Blockchain Consortium (GLBC). The GLBC's mission is to 'organize and align stakeholders in the global legal industry with regard to the use of blockchain technology...'

[www.legalconsortium.org](http://www.legalconsortium.org)



GLOBAL LEGAL  
**BLOCKCHAIN CONSORTIUM**

## Don't Forget About Taxes

With all the excitement surrounding blockchain technology, smart contracts and cryptocurrency, considering how a transaction will be taxed may be an afterthought.

The Canada Revenue Agency has stated that it will generally treat cryptocurrency as a commodity and not as a fiat currency. It also commented that using cryptocurrency to purchase goods or services would be considered a form of barter transaction and that the income tax and GST/HST rules apply.

Generally, the exchange, lending, borrowing or issuance of a financial instrument is an exempt supply and not subject to GST/HST. It is uncertain whether the Canada Revenue Agency will consider cryptocurrency or tokens to be a financial instrument for GST/HST purposes. The determination may depend on the underlying rights and attributes of the specific cryptocurrency or token.

When building smart contracts or transacting using cryptocurrency, don't forget to turn your mind to income tax and GST/HST matters.



Colleen Ma, Associate  
Miller Thomson Calgary

[cdma@millerthomson.com](mailto:cdma@millerthomson.com)  
403 298 2422

# Focus Area

---

## About Our Blockchain, Cryptocurrency and Smart Contracts Team

With recent developments and applications of Blockchain, cryptocurrency and Smart Contracts, the Internet is becoming a truly revolutionary platform for all sorts of business processes including not only communication and related data management and documentation challenges, but also product and services marketing, payment processing and, most importantly, value attribution and exchange.

Blockchain, cryptocurrency and Smart Contracts are almost certain to impact almost every form of modern business, including those in financial services and banking, the production of digital creative content and online retailing and distribution of virtually everything.

It will also transform how companies interact with their stakeholders and how governments deal not only with their citizens, but also with each other. Huge issues of data security and digital file administration are at play.

Just as the technology is emerging in fits, starts and the occasional false step, the law is struggling to keep up with the proliferation of possibilities that Blockchain, cryptocurrency and Smart Contracts present.

Today, the law and regulation governing securities, telecommunications, currency and consumer protection, to name a few, are all being carefully reviewed, both within national jurisdictions and through global and/or multi-jurisdictional agencies, with a view to reform and revision.

Miller Thomson is prepared for both the turmoil and the opportunity that Blockchain has unleashed, not just in the wild and woolly world of crypto-currencies and ICOs, but also for the wider universe of ledger-enabled business process solutions that are now beginning to appear.

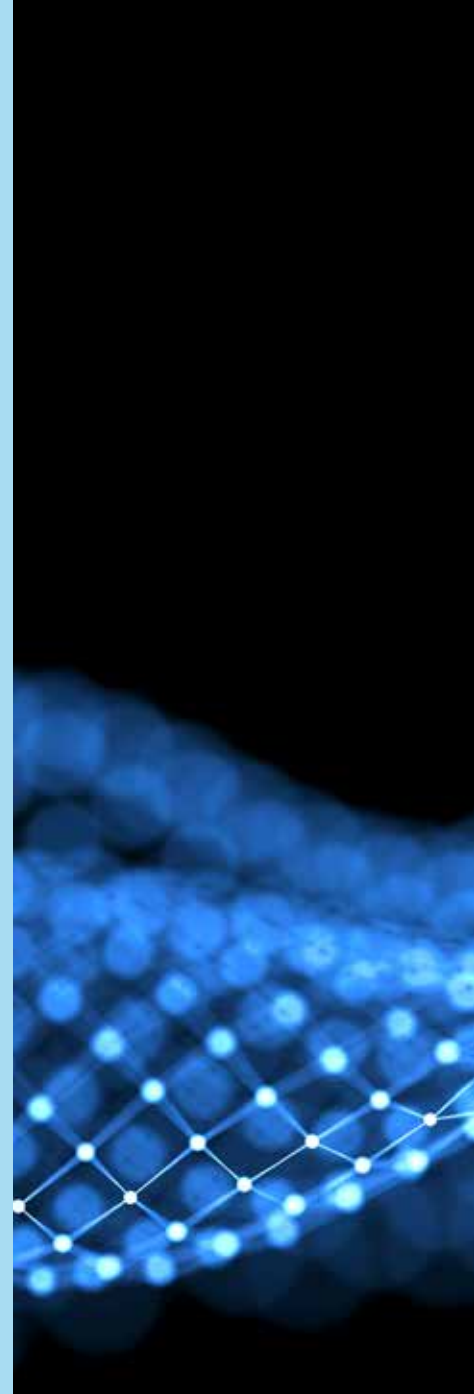
From start-ups and emerging companies to the angel investors and venture capitalists who back them, right through to the established data-dependent and data-exchange driven operations in banking and finance, entertainment, transportation/logistics and large industrial operations, especially those that use the Internet of Things where Blockchain technology solves big problems, Miller Thomson is equipped to advise.

Whether the client is large or small and whether Blockchain, cryptocurrency and Smart Contracts are central or peripheral to its future success, our team at Miller Thomson has acquired the practical expertise and depth to provide valuable insight and real-time guidance about what is happening around the world, what the law currently or potentially permits and prohibits in Canada, how inherent risks of a proposed business idea can be reduced or eliminated and, most importantly, how transactions rooted in Blockchain technology need to be appropriately and accurately documented.

Because Miller Thomson is a national full-service law firm, our Blockchain, cryptocurrency and Smart Contracts team is able to deal with a range of legal issues including:

- Capital markets and securities
- Cybersecurity
- Financial services
- Intellectual property
- Litigation and dispute resolution
- Mergers & Acquisitions
- Private equity
- Tax
- Entertainment

For more information about cryptocurrency, ICOs, or blockchain technology, contact any member of Miller Thomson's Blockchain Group.



# Navigating turmoil



**MILLER THOMSON**

AVOCATS | LAWYERS

With blockchain regulations still in development, exactly where regulations will apply is not always clear. Companies can find themselves subject to different laws in different jurisdictions. Our multi-disciplinary team of lawyers focussed on blockchain, crypto currency and smart contracts bring practical expertise and experience to help business leaders navigate effectively and make informed decisions.

**Equipped to advise with real time guidance**



**MILLER THOMSON**  
AVOCATS | LAWYERS

[MILLERTHOMSON.COM](http://MILLERTHOMSON.COM)



© 2018 Miller Thomson LLP. All Rights Reserved.  
All Intellectual Property Rights including copyright in  
this presentation are owned by Miller Thomson LLP.