DOMINION BITCOIN MINING COMPANY LTD.
250 Yonge Street, Suite 2201, Toronto, ON M5B 2L7
Tel (CAN) 647-477-7767
Fax (CAN) 647-477-7888
Info@DomBit.ca

Submission to the House of Commons Standing Committee on Finance

Regarding the Review of Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime

Dominion Bitcoin Mining Company Ltd.
250 Yonge Street, Suite 2201, Toronto, ON M5B 2L7 Tel (CAN) 647-477-7767 // Fax (CAN) 647-477-7888
info@dombit.ca

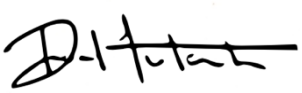
Message from DBMC President, David Luterbach

Dominion Bitcoin Mining Company Ltd. (DBMC) is at the forefront of Canada's movement to embrace cryptocurrencies and blockchain technology. Founded in 2013, DBMC is one of Canada's first Bitcoin companies. We provide bitcoin private key bailment and storage solutions for institutions and individuals. We also provide Continuing Professional Development (CPD) Blockchain Law Workshops that educate Canadians on this transformational industry.

Canada has a long history of innovation in the banking industry, common sense financial regulations, and strong diversified financial markets. As a Canadian business, we are a strong believer that by proactively embracing this new cryptocurrency platform Canada will be able to leverage the financial and technology industry expertise to remain a world leader in this new economy.

We thank you for the opportunity to present this document to the Standing Committee on Finance. As subject matter experts, we are available to answer any questions that may arise from this dialogue.

Sincerely,



David Luterbach
President
DBMC Ltd.

Dominion Bitcoin Mining Company Ltd.
250 Yonge Street, Suite 2201, Toronto, ON M5B 2L7 Tel (CAN) 647-477-7767 // Fax (CAN) 647-477-7888
info@dombit.ca

Modernizing the AML Framework and its Supervision - Addressing the Issue of Money Services Business (and crypto) De-risking

As you know, money services businesses (MSBs), including companies that work in the cryptocurrency space, have had a very difficult time establishing banking relationships due to the perceived risk of money laundering.

The current risk-based approach to anti money laundering paints entire industries with a broad brush as "high risk" despite most business owners doing everything in their power to operate with the highest degree of due diligence.

The FINTRAC examination of banks also automatically flags MSBs as "high risk", triggering more intrusive inquiry, motivating banks to refuse to do business with MSBs because of the added administrative burden. This removes the opportunity for the financial institution to monitor and report suspicious transactions, undermining one of the main pillars of the AML regime.

While assessing clients based on risk of money laundering makes sense, it is self-defeating when those same clients are denied services and are forced to operate without banking. It also creates security issues for those businesses because they have large amounts of cash on their premises.

As a result of de-risking, "good guys" in an industry with a reputation (deserved or not) of being "high risk", have to resort to one of two approaches:

1. being less than forthcoming with banks about the nature of our business in order to have access to bank accounts, or
2. taking their banking offshore.

These policies and practices are hurting innovation and economic development. Companies such as ours have banks unilaterally close accounts, with the statement that it is their policy not to deal with cryptocurrency companies.

We must ask the question: is it possible for the anti-money laundering regime to continue to be both risk-based and yet avoid the inevitable de-risking of money services businesses that serve the unbanked? Are there better approaches to process examinations that do not penalize financial institutions for their relationships with certain industries? Wouldn't the AML regime be more robust and effective if ALL industries had banking relationships where transactions could be easily monitored?

If MSBs are considered risky, the FINTRAC examinations should focus on the MSBs themselves, not hold the banks accountable for their clients' clients. We ask that the examination process not generalize with respect to MSBs and encourage financial institutions to conduct enhanced due diligence instead of denying banking services. This will result in a more

secure economy by bringing more companies under the watchful eye of FINTRAC. It will also encourage innovation and economic growth by allowing entrepreneurs better manage their business risk by having access to bank accounts.

Modernizing the AML Framework and its Supervision - Exemptive Relief and Administrative Forbearance

Rather than attempting to ban or criminalize the use of decentralized, convertible cryptocurrencies such as bitcoin, which arguably cannot be done, FINTRAC should consider a sandbox initiative with the industry to determine how it can effectively cooperate with the industry and create an effective regulatory framework that achieves its objectives.

It is in the interest of the Canadian government to proceed with bringing companies such as ours that deal in cryptocurrencies under the AML regime. In fact, legitimate cryptocurrency companies such as ourselves want to be regulated and are conducting our own KYC voluntarily. We believe there is credibility in meeting and exceeding regulatory standards and want to be a part of the effort to counter money laundering and terrorist financing.

In our business, we want to uphold the highest standards of integrity, and do not wish to facilitate the movement or conversion of illicit funds. This is why we source what we call "Genesis coins" - coins that have been freshly mined and have not been part of transactions with criminals.

A sandbox initiative is a useful concept, but it must be a truly collaborative effort, unlike the Ontario Securities Commission sandbox, which appears to operate less like a collaborative effort, and more like temporary injunctive relief – they promise not to prosecute… yet. There needs to be more trust. Companies who willingly to collaborate with regulators before being compelled to do so should get the benefit of the doubt.

There are many positive aspects to the underlying technology of cryptocurrencies - the blockchain and cryptography - that, among other uses, can also be used to combat crime. We are in the early days of this technology and the potential is only just beginning to be explored.

It is undeniable that criminals have tried to use cryptocurrency to hide their transactions from government agencies; they use cash for the same nefarious purpose. Nevertheless, with every technological innovation, opportunists enter the space to misuse that innovation for profit and malfeasance. That is not a reason to oppose or undermine these innovations.

Counter to the commonly-held belief that bitcoin is anonymous, its more accurate to call it pseudonymous; there are ways to track the flow of bitcoin between wallets. The IRS recently partnered with a private company called Chainalysis that can track bitcoin wallet transactions and link them to bad actors.[1] A similar company called Elliptic also tracks bitcoin wallet transactions for criminal activity.[2] We think these services provide immense value and should be commonly-used tools by financial institutions and government agencies.

[1] https://www.ethnews.com/extensive-irs-chainalysis-partnership-further-revealed
[2] https://www.elliptic.co/

There are now subscription-based and free web-accessible portals to track wallet activity as well, such as BitRank, which can trace the transactions of Bitcoin wallets and assess the level of risk associated with them[3]. A sandbox initiative could explore ways to incorporate these applications into risk assessment.

The current system of identity verification that relies on government-issued ID is inefficient and vulnerable to massive privacy breaches. The centralization of personal data in, for example, Equifax's database, creates an irresistible temptation for identity theft. It's not a matter of if, but when the next hack will occur.

Companies in this space are, in fact, exploring new ways to implement new technology such as blockchain to make the KYC process smoother, less burdensome and more resistant to identity theft.

We think there is a real opportunity here to both bring responsible crypto companies under the FINTRAC purview and test new applications to help all regulated entities meet their regulatory record-keeping and KYC obligations, while protecting customers' privacy.

Incorporating technology such as machine learning, biometrics and social media for identity verification can reduce the regulatory burden on regulated entities, and assuage privacy concerns by removing the central repository of personal data, such as those on Equifax's servers.

Social media is an amazing tool to verify identity. People volunteer an incredible amount of their personal information online, and have little to no argument for protecting their privacy when identity verification can be achieved using publicly available data.

In fact, we believe that Distributed Ledger Technology can help solve problems on both sides of the customer identification coin - that of identity theft and identity verification. For example, company called Civic has developed a platform to empower people to control and protect their identities, obviating the need for a centralized repository of personal data, such as credit bureaus, and providing cryptographically secure data protection that is hack-resistant[4]. Similarly, another startup called Shyft is attempting to solve the same problem by collecting available data on people to develop useful personal profiles that include credit, reputation and regulatory due diligence[5]. Government entities should be exploring ways to incorporate these approaches into their operations, if at all possible.

It's important that Canada not close the door too early on technologies based on over-hyped negative media, only to play catch-up as other countries embrace new ways of conducting financial transactions driven by consumer demand. These are very early days for

[3] https://bitrankverified.com/home
[4] https://www.civic.com/
[5] https://www.shyft.network/solution

Dominion Bitcoin Mining Company Ltd.
250 Yonge Street, Suite 2201, Toronto, ON M5B 2L7 Tel (CAN) 647-477-7767 // Fax (CAN) 647-477-7888
info@dombit.ca

blockchain technology and the industry is populated by talented, driven, innovative professionals.

We propose a multi-year initiative where the regulated entities can operate how they feel is expedient, sharing information at regular intervals with the regulator; a meaningful partnership with willing industry members to collaborate to design a modern, effective AML framework that is both effective and efficient, using best-in-class technologies. We believe Canada is well poised to be a leader in fintech, including using new technology to combat money-laundering and update identification verification processes, while protecting privacy.

Thank you for your time and consideration.

Sincerely,

Lara Wojahn

Lara Wojahn
Chief Compliance Officer
DBMC Ltd.

Clarifying Regulations And Reducing Regulatory Overlap

The use of terms "virtual currency" and "digital currency" cause confusion - most people cannot discern the important differences between them. As the blockchain industry expands to various sectors, it requires more specific terms to denote different types of digital tokens. We recommend the PCAMLTF use definitions based on three readily identifiable functions: “cryptocurrency”, “utility tokens” and “security tokens”, defined as follows:

- Cryptocurrency (blockchain based decentralized payment and settlement systems), for example Bitcoin, Bitcoin Cash, and others;

- Utility Tokens, (blockchain based digital tokens designed to represent future access to a company’s product or service and includes coupons.) for example: Ethereum, Airmiles, etc.;

- Security tokens (blockchain based digital assets that derive their value from an external, tradable assets or equity, and by function are subject to provincial securities regulations. Commonly referred to as ICOs or Tokenized assets.

In Canada, prosecuting money laundering cases is complex; it is difficult for prosecutors to explain the facts of the case to judges and juries such that they can follow their narrative. This hurdle grows even higher when blockchain-backed digital tokens are the subject matter. Canadian legislation needs to have easily recognizable, clear, and defensible legal definitions of blockchain backed digital tokens: the terms “digital currency” and “virtual currency” are opaque, inaccurate, and confusing. Japan, Switzerland, the USA, and other countries are moving towards more narrowly-defined function-based definitions and we recommend Canada does so as well.

A further clarification can be made with respect to the category of cryptocurrencies, with an amendment of the *Currency Act* to include cryptocurrencies such as Bitcoin as “money”. AML legislation relies on specific dollar amount valuations as triggers for reporting requirements, however, there is no prescribed method of valuing cryptocurrency. If cryptocurrency was defined as non-fiat money, like gold, then the *Currency Act*[6] empowers the Governor in Council to dictate a matrix for valuation. We recommend using the average daily price from multiple Canadian cryptocurrency exchanges and are happy to assist further in this regard.

---

[6] **Valuation of gold, etc.**
15 Notwithstanding any other law, where any law of Canada or any treaty, convention, contract or agreement to which Canada is a party makes reference to
(a) a currency of a country other than Canada,
(b) a unit of account that is defined in terms of currencies of two or more countries,
(c) gold, or
(d) a combination of any of the things mentioned in paragraphs (a) to (c),
the Governor in Council may make regulations specifying, or specifying the means or method of ascertaining, determining or calculating, the equivalent dollar value of that currency, unit of account, gold or combination thereof.

Dominion Bitcoin Mining Company Ltd.
250 Yonge Street, Suite 2201, Toronto, ON M5B 2L7 Tel (CAN) 647-477-7767 // Fax (CAN) 647-477-7888
info@dombit.ca

Cryptocurrency is already on the edge of satisfying the common law definition of money, as it is defined by the Supreme Court of Canada (SCC) in the case of *Re. Alberta Statues* and in the precedent-setting case of *Moss v Hancock*. According to the SCC, money is:

1 "...that which passes freely from hand to hand throughout the community in final discharge of debts and full payment for commodities...
2. "...being accepted equally without reference to the character or credit of the person who offers it" and
3. "...without the intention of the person who receives it to consume it or apply it to any other use than in turn to tender it to others in discharge of debts or payment of commodities."
4. "...not necessarily legal tender. Any medium which by practice fulfills the function of money."

In the context of AML prosecutions, the lack of a clear definition of cryptocurrencies has repeatedly prompted challenges with mixed results. In the US case of Ross Ulbrict,[7] after a jurisdictional challenge over the legal definition of Bitcoin, Justice Forrest found "Bitcoin is clearly money" and was therefore captured by AML laws. However in the more recent case of Mitchell Espinoza[8] the court reached the opposite conclusion and dismissed AML charges on the basis that Bitcoin was not money nor was the transaction caught by AML laws. "The Espinoza decision underscores the uncertainty that still surrounds the legal treatment of virtual currency and the hesitation courts may have toward applying money transmitting laws and AML laws to this novel context."[9] In the dozen or so AML prosecutions that have taken place in the United States, the legal definition of cryptocurrency was argued.

Including cryptocurrencies as a form of money would have far-reaching consequences for the entire cryptocurrency industry and participants' AML programs. As such, we suggest studying this approach along with industry leaders to determine the impact it would have on their business models and effectiveness of their AML programs as part of the aforementioned sandbox initiative.

Thank you.

Sincerely,

Cloudesley Hobbs
Chief Legal Officer
DBMC Ltd.

[7] *United States of America v. Ross William Ulbricht*, 14th Cir. Ct. 68, (KBF), (2014)
[8] *State of Florida vs. Espinoza*, Order Granting Defendant's Motion to Dismiss the Information (Fla. 11th Cir. Ct. Jul. 22, 2016)
[9] Virtual Currencies: Court Rules that Selling Bitcoin Is Not Money Transmitting and Selling Bitcoin to Criminals Is Not a Crime https://identitymindglobal.com/blog/virtual-currencies-court-rules-that-selling-bitcoin-is-not-money-transmitting-and-selling-bitcoin-to-criminals-is-not-a-crime/