



Blockchain Technology

COALITION OF CANADA

Blockchain Technology Coalition of Canada

Canada Not-for-profit Corporation

1081587-0

**Response to Joint Canadian Securities Administrators/Investment Industry Regulatory
Organization of Canada: Consultation Paper 21-402: Proposed Framework for Crypto-
Asset Trading Platforms**



To the Investment Industry Regulatory Organization of Canada, and the members of the Canadian Securities Association:

British Columbia Securities Commission;
Alberta Securities Commission;
Financial and Consumer Affairs Authority of Saskatchewan;
Manitoba Securities Commission;
Ontario Securities Commission;
Autorité des marchés financiers;
Financial and Consumer Services Commission (New Brunswick);
Superintendent of Securities, Department of Justice and Public Safety, Prince Edward Island;
Nova Scotia Securities Commission;
Securities Commission of Newfoundland and Labrador;
Superintendent of Securities, Northwest Territories;
Superintendent of Securities, Yukon;
Superintendent of Securities, Nunavut;

We are the Blockchain Technology Coalition of Canada. We're a coalition of Canadian blockchain companies working for smart standards and public policy that protects consumers, supports innovation and keeps jobs in Canada.

We would like to thank you for taking the initiative on this consultation. Please find our answers below to the questions posed in your joint statement.

Our recommendations can be summarized as follows: all suggestions and consultations for regulation requirements should be made only after there is consensus, standardization, and clarification of the terms and concepts surrounding in crypto assets.

Let us be specific. The CSA Staff Notice 46-307 lists the following characteristics of the ICO/ITO market as evidence that they are securities:

- Soliciting a broad base of investors, including retail investors;
- Using the internet, including public websites and discussion boards, to reach a large number of potential investors;
- Attending public events, including conferences and meetups, to actively advertise the sale of the coins/tokens; and
- Raising a significant amount of capital from a large number of investors.

It is our view that these standards can apply to consumer packaged goods just as much as they do to ICOs/ITOs, if “investor” is replaced with the word “customer”.



For example, consider the marketing campaign of Red Bull energy drinks, which involves not only internet (and TV and radio) advertising, but also driving around to different public events and private functions, to actively advertise their product, and to reach a large number of potential consumers. And they've raised a significant amount of capital from a large number of customers.

Obviously Red Bull is not a security. Advertising activities and "significant" fundraising are neither necessary nor sufficient conditions of a securities. Thus, these cannot be standards to judge whether a crypto asset is a security.

There are already legal standards for identifying securities. As per the Ontario Securities Act, there are 16 separate *sufficient conditions* for something to be considered a security. Not one of them is in regards to fundraising or advertising. The other 9 provinces have extremely similar language on the definition of securities as well.

It is our estimation that *none* of the 16 separate sufficient conditions for identifying a security, as outlined in any of the Securities Acts of any province in Canada, apply to crypto assets.

To make an example of one particular case: consider definition (c) from section 1 of the Ontario Securities Act: "title to or interest in the capital, assets, property, profits, earnings, or royalties of any person or company."

However, while it may be possible to design a crypto asset to be consistent with that definition, crypto assets per se do not *necessarily* entitle their holders to the capital, assets, property, profits, earnings, or royalties of any person or company.

Moving on, we do not believe crypto assets are *commodities*, either. The government of Ontario defines a commodity under the *Commodities Futures Act*, as "any agricultural product, forest product, product of the sea, mineral, metal, hydrocarbon fuel, currency or precious stone or other gem, and any goods, article, service, right or interest, or class thereof, designated as a commodity under the regulations." Crypto assets are not any of the listed things.

A *currency* is a *medium of exchange* that is *current*. A *medium of exchange* is any object or service that is bought or sold not because of its value as an object or service (also known as its *use value* or *intrinsic value*), but because other people will exchange objects or services for it. Common media of exchange include metallic coins, bullion or bars of gold, or legal tender paper notes. But any good or service could be a medium of exchange. *Money* is the most commonly accepted medium of exchange.

To be *current* is an accounting term that means capable of being sold (or, synonymously, exchanged) within a short period of time, typically one year. An effective currency, however, is typically saleable much faster than that.



The *Currency Act* of Canada uses the words “currency” and “monetary unit” interchangeably. The Act defines the currency of Canada as a dollar, further specifying that a dollar can be offered for payment only if it is a coin minted by the Royal Canadian Mint or a note printed by the Bank of Canada. The only other legal tender of payment, according to the Currency Act, is using the currencies of other countries.

Neither decentralized ledger technologies, nor crypto assets, are countries. It is also not a currency.

So while crypto assets share many functional similarities with ordinary securities, they differ in a crucial way: they do not *necessarily* represent any claim, or title, or interest, or agreement, or indebtedness, or a subscription to any capital, assets, property, profits, earnings, or royalties; nor are they any commodity or derivative thereof.

Thus, crypto assets are not necessarily securities. And as such, we find the use of the word “investors” in the questions below to be inappropriate and confusing, as opposed to clarifying.

So again, we repeat our request: we ask that you adopt a unified, clear, precise definitional framework for crypto assets. Without clear definitions, we risk not only talking past each other, but also misregulating an entire industry.

We would like to thank you for taking the issue seriously, and for seeking comments from the public. We are available for any further discussions if you so require.

Sincerely,

Ash Navabi
Senior Economist and Director of Policy

Blockchain Technologies Coalition of Canada
129 Spadina Avenue
Suite 200
M5V 2L3
<http://joinbtcc.org>



Blockchain Technology

COALITION OF CANADA



1. Are there factors in addition to those noted above that we should consider?

The most important factor to consider is whether the crypto assets in question are, pursuant to the definition of a security in section 1 (1) of the Securities Act, indeed “*titles to or interest in the capital, assets, property, profits, earnings or royalties of any person or company.*”

There are potentially several tests for this. First, is the proposed “Howey Test” as suggested by the United States Securities and Exchange Commission. The Howey Test has three components: (i) that an investment have been made (ii) in a common enterprise (iii) with the expectation of profit *solely* from the work of a promoter or other third-party. No case involving crypto assets has yet been tried under this standard.

A second, potentially much simpler, test could be whether simply if, under any circumstances, the owner of the crypto asset is entitled to any of the *capital, assets, property, profits, earnings or royalties* in an enterprise. Under this standard, we believe very few ICOs would classify. But it is possible that some would indeed classify as securities even under this standard.

This is why we are proposing a comprehensive nomenclature and taxonomy for all things crypto, in order to better understand what needs oversight and what does not.



2. What best practices exist for Platforms to mitigate these risks? Are there any other substantial risks which we have not identified?

In terms of best practices against insolvency, the [recent situation](#) with Binance is a useful case study. It was revealed that Binance has an emergency fund in case of such situations, which it used to recoup the losses from the hack. In world where crypto assets are not under a shroud of regulatory regime uncertainty, we can expect the existence of insurance companies to provide these services for such platforms.



3. Are there any global approaches to regulating Platforms that would be appropriate to be considered in Canada?

Globally, crypto asset regulations continue to be a quagmire of confusion. Companies operate in a perceived gray area of the law, and so attracting funding, as well as talent, is a challenge. Canada has an opportunity to lead in this regard. And it must begin by being explicitly clear about the terms surrounding crypto assets.

The [United State Library of Congress](#) has a collection of nearly 110 countries that have taken public positions on distributed ledger technologies. However, a cursory analysis reveals that most countries have simply sent a press release warning consumers to be cautious. Many others have confused, inconsistent legislation.

In terms of examples of good legislation, we like this hodgepodge mix:

1. From Latvia, crypto assets are explicitly recognized as not being currency: “The position of the Bank of Latvia and the State Revenue Service is that cryptocurrency is a contractual, not statutory, means of payment that can be used in transactions of exchange. Cryptocurrency cannot be considered as official currency or legal tender because the issuance and use of these instruments remains unregulated and they are not linked to any national currency”;
2. Barbados has promised to not regulate utility tokens (or protocol tokens) as securities;
3. The United States has adopted the “Howey Test” to distinguish between securities and non-securities.

Barbados also has a comprehensive legislation that aims at regulating the security of crypto asset exchanges.

It should be noted that although Canada is a small market from a global perspective, Toronto is quickly becoming an important hub for innovation and investment in DLTs. This is why having the correct approach to regulation in this space is crucial—if regulation is too heavy handed, too burdensome, too anti-business and anti-innovation, firms will simply pack up and leave.

Hence, Canadian regulators need to be writing policy with the utmost attention to detail, specifically having precise and accurate terms. To achieve this requires close collaboration between policy makers and technologists.

Canada’s opportunity to lead can come from a laissez-faire approach to crypto assets, by recognizing that they are nothing new under the sun: insofar as a crypto asset is tied to a title to or interest in another person or entity, it is already a security. This opportunity comes from the fact that currently no other country or jurisdiction has the correct approach to DLTs. No is taking



Blockchain Technology

COALITION OF CANADA

the lead to recognize that DLTs are here to stay, and that they should be a welcome experiment in the financial services industry.

Only this kind of attitude towards policy will engender the climate of entrepreneurship and innovation that can enable many different businesses to succeed at meeting market demand. Hence, Canada must take advantage of this opportunity now.



4. What standards should a Platform adopt to mitigate the risks related to safeguarding investors' assets? Please explain and provide examples both for Platforms that have their own custody systems and for Platforms that use third-party custodians to safeguard their participants' assets.

The first step would be to clarify who is an investor. Is a person who cannot profit *directly* from the earnings of another entity an “investor”? Can a direct analogy be made to persons who give money to online “crowdfunding” campaigns (like for new toys, comic books, music albums, etc.), even though they are not gaining title to the entity they are contributing funds to?

Following clarification on that, security standards for protecting the relationship between Platforms and their partners should not be a matter of centralized regulation. There must be freedom to experiment with different security practices and procedures. Especially in these early days of the technology, forcing a standardization—however broad it may *appear* to be at first—may be a death knell for innovation at best, and (given the infant-like nature of industry in terms of experiences, in the likely event that the adopted standard is later found to be seriously flawed) may invite widespread security vulnerabilities at worst.



5. Other than the issuance of Type I and Type II SOC 2 Reports, are there alternative ways in which auditors or other parties can provide assurance to regulators that a Platform has controls in place to ensure that investors' crypto-assets exist and are appropriately segregated and protected, and that transactions with respect to those assets are verifiable?

The industry is still too new and too experimental to be subjected to a uniform standard of auditing. Experimentation must continue to take place, even in auditing standards. Platform customers will then have incentive to assess the safety features of each Platform. As this is a costly and difficult assessment to make for any retail customer, we anticipate the emergence of a variety of auditing methods and auditors vying and competing for the trust of the retail public, including even a “Yelp”-style user-submitted audit based on ethical hacking principles—*if* regulators clarify that experimentation in auditing standards are allowed.

This experimentation process would, over time, lead to an emergent standard as customer preferences are revealed after trial and error. But this result is still years away. However, while it took centuries for modern accounting practices to become general for ordinary securities, we expect that with the globalization of information, auditing standards for crypto assets will standardize within five to seven years.

It is also worth noting that there are already *voluntary* disclosure programs being created within the industry. As just one example, messari.io is one such instance of an independent research and information registry.



6. Are there challenges associated with a Platform being structured so as to make actual delivery of crypto assets to a participant's wallet? What are the benefits to participants, if any, of Platforms holding or storing crypto assets on their behalf?

There are many challenges for Platforms in this regard, but the number one reason that a participant would want to keep their crypto assets with the Platform is ease of trading with other crypto assets.



7. What factors should be considered in determining a fair price for crypto assets?

Because it is possible to exchange crypto assets in multiple Platforms, using a variety of methods; and because markets for many crypto assets are very thin (meaning that they have low transaction volumes, enabling high price volatility) by traditional standards, fair prices are more nebulous to determine for crypto assets. The only objective “fair price” standard is the price which a seller agrees to accept from a buyer, and vice versa.

Just like with exchanges for ordinary securities or currencies, a DLT Platform could act as a market maker. That is, a Platform could be an intermediary for transactions. (Note well that it is not necessary for a Platform to be involved in a transaction.) This is consistent with how fair prices are determined in ordinary exchanges.

Regulators should refrain from legislating fair price requirements for Platforms. Platforms face economic incentives to report truthfully the bid and ask spreads, especially if Platforms are subject to competition. If Platform X, acting as a market maker, is misrepresenting bid and ask spreads in a predatory manner, then Platform Y can attract buyers and/or sellers from Platform X by offering more truthful information about spreads.

There is also the possibility that a Platform that exercises unfair market making practices will be exposed by its own participants. As it's currently possible for the same individual to have multiple anonymous stores of crypto assets, the same person can participate as both buyer and seller of the same crypto asset within the Platform, and judge the posted bids and asks with their own bids and asks.

Indeed, as crypto asset markets mature, specialized auditing firms can arise that grade the honesty of Platforms in this very manner. In the meantime, however, the dedication of decentralized yet vigilant crypto asset market participants has been working to keep Platforms fair and honest.

Notwithstanding these and related effects, regulatory fair price requirements could potentially amount to implicit price controls—which could cause a market shortage (in the case of a price maximum), or a market surplus (in the case of a price minimum). In both cases, this creates an incentive for Platform participants to seek to make exchanges elsewhere, in perhaps riskier environments offering less liquidity than a Platform.

To be precise, all 3 of the following factors must be considered for determining a fair price:

1. Did the rightful owner of crypto asset make the decision to sell (to any party) on their own free will and accord;



2. Did the rightful buyer of the crypto asset make the decision to buy (from any party) on their own free will and accord; and
3. If the Platform was acting as market maker, did it truthfully represent the bid and ask to the participants?



8. Are there reliable pricing sources that could be used by Platforms to determine a fair price, and for regulators to assess whether Platforms have complied with fair pricing requirements? What factors should be used to determine whether a pricing source is reliable?

The only reliable pricing sources for a Platform are the bids and asks posted by the buyers and sellers on the Platform in question. Given the thin markets that currently dominate crypto asset exchanges, reliable pricing sources for many crypto assets may be sparse. As well, the anonymous nature of the ownership and distribution of crypto assets makes conventional regulation difficult.

As such, at the current time, we cannot recommend a prima facie rule to determine fair pricing— notwithstanding evidence of coercion against the buyers and sellers, or willful misrepresentation on behalf of the market making Platform.



9. Is it appropriate for Platforms to set rules and monitor trading activities on their own marketplace? If so, under which circumstances should this be permitted?

It is appropriate for Platforms to set rules and monitor trading activities on their own marketplace. Exchanges have already started doing this themselves. Indeed, [Nasdaq reports](#) that seven crypto exchanges are currently using their proprietary monitoring software.



10. Which market integrity requirements should apply to trading on Platforms? Please provide specific examples.



11. Are there best practices or effective surveillance tools for conducting crypto asset market surveillance? Specifically, are there any skills, tools or special regulatory powers needed to effectively conduct surveillance of crypto asset trading?



12. Are there other risks specific to trading of crypto assets that require different forms of surveillance than those used for marketplaces trading traditional securities?



13. Under which circumstances should an exemption from the requirement to provide an ISR by the Platform be considered? What services should be included/excluded from the scope of an ISR? Please explain.

Section 12.2 (1) of the [National Instrument 21-101](#) requires an independent systems review to report “report in accordance with established audit standards”. However, audit standards are still being established for crypto asset Platforms. Determining optimal organization for custody of crypto assets for Platforms, and determining best practices for cyber security and other efficient technologies is still very much a work in progress.

As a result, we recommend a very broad approach to regulating this area. There are various competing standards and protocols in place to prevent and identify cyber security threats; many technologies are possible for organizing and constructing a marketplace; and disaster recovery can be approached from multiple angles, and is also open to experimentation.

That said, a good marketplace will be proactively conducting ISRs on its own accord. Thus, we recommend that marketplaces voluntarily submit ISRs for the next five years, until which time patterns can be observed and perhaps a generalized approach can better be conceived.



14. Is there disclosure specific to trades between a Platform and its participants that Platforms should make to their participants?

Yes. Platforms should be forthright that the so-called “hot wallets” used for trading on the Platform are significantly less secure than the “cold wallets” outside of the Platforms. This security discrepancy is poorly understood by the general public, and it would be a best practice for Platforms to be proactive about educating customers in this way.

Platforms should also disclose what kinds of insurance they have *and don't have* that will affect customer crypto assets. For example, they should be to what extent customer accounts are protected from theft, technical malfunctions, and other disasters.



15. Are there particular conflicts of interest that Platforms may not be able to manage appropriately given current business models? If so, how can business models be changed to manage such conflicts appropriately?

Insofar as Platforms are acting as market makers or dealer-restricted person, they ought to be liable to complying with the same ethics and protocols for those roles in ordinary securities legislation.

Determining and conceiving of the best business models should be the sole prerogative of the entrepreneur. It is, in fact, the entrepreneur who senses Any directives regarding business models would be a recipe for stultification, homogenization, and stagnation of innovation and value creation.



16. What type of insurance coverage (e.g. theft, hot-wallet, cold-wallet) should a Platform be required to obtain? Please explain.

No Platform should be required, by law, to obtain any insurance. Such a requirement is at best unnecessary (as any legitimate and sophisticated platform will be acting in its own and its customers' best interests by knowing what kind of insurance to get, and it would optimally advertise such insurance as a marketing strategy to attract more customers), and at worst a subsidy to rich incumbents while simultaneously a deterrent against new entrants.

Platforms without insurance not only save operations costs, but they also provide more consumer choice. This can allow an uninsured start-up Platform with to compete with larger yet insured incumbents by offering cheaper services. Consumers can then judge for themselves whether the cost savings from the new Platform are worth the increased security risk.



17. Are there specific difficulties with obtaining insurance coverage? Please explain.

Yes. In our experience, insurance companies of *all* types are wary and hesitant to work with any decentralized ledger technologies business. The most common reason is concerns over compliance with anti-money laundering (AML) regulations. Hence, our recommendation is clarity from regulators on how DLT businesses can be compliant with AML regulations.



18. Are there alternative measures that address investor protection that could be considered equivalent to insurance coverage?

Yes. Following the recent example from Binance, the Platform itself can set aside some of its profits (in either fiat currency or crypto assets) in a different, sequestered or partitioned account. Binance calls it the “[Secure Asset Fund for Users](#)”, or SAFU. This could be its emergency re-capitalization fund, which it could deploy to recoup customer losses in the event of a hack.

It’s worth noting that this innovation was developed independently by Binance, without any government mandate or oversight. [And it worked](#). Our belief is that as long as Platforms are allowed to innovate without permission, we will continue to see innovations like this on behalf of customer-centric Platforms.



19. Are there other models of clearing and settling crypto assets that are traded on Platforms? What risks are introduced as a result of these models?

Like many other functions in this space, clearing houses are a particular business model. As in other sections of this response, we worry that setting a national standard for a business model would be a recipe for stultification, homogenization, and stagnation of innovation and value creation



20. What, if any, significant differences in risks exist between the traditional model of clearing and settlement and the decentralized model? Please explain how these different risks may be mitigated.

If Bank X owes \$10,000 to Bank Y, and Bank Y owes \$10,000 to Bank Z, and Bank Z owes \$10,000 to Bank X, then there are two ways the banks can settle their debts with each other. First, each bank can choose to remain quiet with respect to the debts of the whole system, and that money has to change hands several times. This method has several features. First, it requires that each bank have enough cash to cover all of its debt by the end of the day. Second, it requires limited coordination between the banks.

The alternative method to settle these daily debts is for the banks to communicate with each other, and figure out that, on net, no one owes anyone anything. This also has two interesting features. First, the banks now longer have to carry as much cash as they might possibly need to settle their immediate debts with other banks. And second, this requires quite a lot of coordinated communication.

The economic incentives—particularly that of having to carry less cash—greatly favored the second method. Hence, some enterprising men started specializing in this interbank communication and debt clearing. As more and more banks embraced the second option, the interbank communication institutions became known by a new name: *clearinghouses*.

So these clearinghouses developed step by step, as opposed to all at once. They have their roots in New York and London and Edinburgh. They developed organically and through market mechanisms.¹

But then the clearinghouses started consolidating. And soon enough, they were intertwined with the regulatory state. By the 1890s, there was already the New York City Clearinghouse Association (NYCHA). And these centralized information hubs had a problematic downside: they incentivized individual banks to lend out more than they could cover with their deposits, than if the banks were not able to coordinate their lending decisions in concert.

This issue of credit in excess of reserves has a name. It is called *fiduciary media*. And according to some economists, including Ludwig von Mises and the Nobel laureate Friedrich Hayek, the issue of fiduciary media is what enables the business cycle (that is, the cyclical pattern of economic ups and downs). Here is the theory in brief:²

¹ Selgin, George A. (1988). *The theory of free banking: Money supply under competitive note issue*. Rowman & Littlefield pub Inc, pp. 26-29.

² Ebeling, Richard M. (1983). *The Austrian Theory of the Trade Cycle and Other Essays*. Ludwig von Mises Institute.



First, banks issue new fiduciary media. As these media are given out as loans, they in effect lower interest rates. This has two conflicting effects: one, investors who get this new fiduciary media get to use this money to start (long-term) investment projects. And two, the lower interest rates induce savers and consumers to save less and spend more money in the present. As this state of affairs represents both an increase in consumption *and* production, this is seen as boom times for the economy.

Unfortunately, this activity creates an intertemporal discoordination: the investors are making goods for the long term, but the consumers are spending all their money in the short term. Sooner or later, this mismatch between what investors are making and what producers are spending their income on, makes it difficult for investors to sell their inventory. They must liquidate: halt production, fire employees. The beginning of a bust.

This centralization of credit—aided and abetted by clearing houses—creates an increased risk of systemic failure.

Hence, by decentralizing the clearinghouse settlement model, crypto asset Platforms are limiting the issue of new credit. By limiting the issue of new credit, the booms will be smaller, as will the busts. The risks of systemic failure are reduced.



21. What other risks are associated with clearing and settlement models that are not identified here?

The existence of a powerful regulatory body enables what economists call “regulatory capture”. That is, the rise of a cozy, “revolving door” relationship between the regulator and the regulated. In the case of the New York clearinghouses, despite laws against over-issuing credit, because of the regulator’s cozy relationship with the clearinghouse association that the law was openly flaunted.

By setting strict, yet convoluted standards that *require* industry expertise, the regulator is effectively asking to be “captured” by the special interests.³

The only remedy against this is by strictly limiting the regulatory powers to begin with, by limiting the scope and scale of what can be regulated.

³ McSherry, Bernard and Berry K. Wilson. "Overcertification and the NYCHA's Clamor for a NYSE Clearinghouse." *The Quarterly Journal of Austrian Economics* 16, No. 1 (Spring 2013): 13–26.
<https://mises.org/library/overcertification-and-nychas-clamor-nyse-clearinghouse>



22. What regulatory requirements, both at the CSA and IIROC level, should apply to Platforms or should be modified for Platforms? Please provide specific examples and the rationale.

The only requirements should be ethical: maintaining fiduciary duties, revealing material information, etc., as outlined above.

The CSA and IIROC should avoid any and all regulations of business plans, cybersecurity strategies, and other operational and capital expenditures. These are highly sensitive areas that determine the growth and international competitiveness of Canada's crypto asset Platforms. We recommend as light a touch as possible, in order to allow innovation without permission.

Otherwise, we risk irreversibly damaging our burgeoning high tech industry, and dooming it to the stultification, homogenization, and stagnation of innovation and value creation.