May 31, 2019

Via Email

Alberta Securities Commission
British Columbia 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
Investment Industry Regulatory Organization of Canada

Re: Bitvo Global Inc. Comments on Consultation Paper 21-402

In response to the joint Canadian Securities Administrators ("CSA") and Investment Industry Regulatory Organization of Canada ("IIROC") Consultation Paper 21-402 – *Proposed Framework for Crypto-Asset Trading Platforms* ("CP 21-402"), please find the commentary of Bitvo Global Inc. ("Bitvo") below.

Background

Thank you for providing us the opportunity to comment on CP 21-402 and the proposed regulatory framework for the regulation of cryptocurrencies by the CSA and IIROC (the "Framework").

Bitvo operates a cryptocurrency exchange platform to facilitate the purchase, sale and trading of cryptocurrencies for fiat currencies and cryptocurrencies for other cryptocurrencies. Bitvo is committed to ensuring that its exchange platform operates in a fair and orderly manner and the security of its customers and their funds are a top priority.

We are in favour of regulation that thoughtfully addresses the unique risks and characteristics of cryptocurrencies, including security and custody. There is considerable uncertainty under securities laws in Canada as to when or whether a certain cryptocurrency may or may not be considered a "security" under such laws. Traditional securities law analysis was not developed with consideration of the unique characteristics of various types of cryptocurrencies, which has lead to uncertainty in Canada, in the United States and internationally as it relates to the application of securities laws to a given cryptocurrency. Without a clear analytical framework to determine whether a cryptocurrency is a security under applicable securities laws in Canada, the Framework seeks to solve the question "how should certain cryptocurrencies be regulated?" without first defining which cryptocurrencies ought to be the subject of the regulation.

The nature of cryptocurrency is diverse. A crypto-asset could be a digitized traditional security, a cryptocurrency used for payment purposes, a utility token, a stablecoin, or another novel use of a digital asset utilizing cryptography protocols to solve a particular problem. There may be different risks inherent in a crypto-asset, or the dealing with a crypto-asset, depending on the nature of the cryptocurrency itself.

The risks inherent in a crypto-asset that is a digitized traditional security will be substantially similar if not the same as those surrounding traditional securities. The application of securities laws to such cryptocurrencies is consistent with the purpose of, and intent behind, such laws. The application of securities laws to a cryptocurrency used for payment purposes may quickly render such payment method unusable. Regulation that does not appropriately contemplate the unique and varied nature of cryptocurrencies may restrict Canadian individuals and companies from participating in global innovation as it relates to the prolific utility, in payments and otherwise, that can be made available through cryptocurrency technology.

As a result, while Bitvo is in favour of a regulatory framework that is implemented with a view to mitigate risk and promote innovation, the Framework as proposed in CP 21-402 does not appropriately achieve that balance for cryptocurrencies that are not digitized traditional securities. The government should consider a standalone regulatory regime developed specifically for platforms dealing exclusively with cryptocurrencies that fall outside of the spectrum of traditional securities (including those that would not be considered securities under the current securities law analysis, which may not be governed under the Framework as proposed). It may be appropriate for this regulatory regime to be administered and overseen by a separate federal regulatory body with a cryptocurrency specific mandate.

Please find our view on certain of the consultation questions posed in CP 21-402 below. For cryptocurrencies that operate as digitized traditional securities, which by their nature and characteristics reflect a traditional security except in the sense that they have been digitized through the use of blockchain and cryptography, the current securities laws in place are appropriate and currently apply, as they have been developed to address the risks associated with such securities. The responses below relate to cryptocurrencies that would not properly be considered digitized traditional securities.

Consultation Paper Questions

1.	**Are there factors in addition to those noted in Part 2 that we should consider?**

A key factor that is missing from Part 2 is the consideration of the cryptocurrencies offered by the platform or broker. The nature of such cryptocurrencies will vary the risk profile of such assets, which, in turn, might require that regulation applies differently to cryptocurrencies with different risk profiles. As discussed above, cryptocurrency that is a digitized traditional security, for example, would be unlikely to require significant (if any) changes from the current securities law regime. The current securities law regime may be unworkable to apply to a cryptocurrency that is a utility token or cryptocurrency used for payments and the application of such laws would render the utility token or payment-based cryptocurrency unusable by Canadians and Canadian businesses.

2.	**What best practices exist for Platforms to mitigate the risks outlined in Part 3? Are there any other significant risks which we have not identified?**

In order to effectively safeguard customers' funds, Platforms should operate on a full reserve basis with segregated accounts, meaning that customers' funds are held separately from the Platform's funds and must at all times be equal to the sum total of the aggregate amount in all customers' accounts. This

should be true for the total value of all funds as well as the value of each asset class (i.e. Canadian dollars, Bitcoin, etc.).

To further safeguard crypto assets held on customers' behalf, Platforms should hold the majority of these assets in "Cold Storage" (offline, not connected to the Internet). Only amounts required to facilitate daily trading liquidity on the Platform and withdrawal requests made by customers should be held in "Hot Storage" (online, connected to the Internet). Access to both Hot and Cold Storage should be restricted to a small group of trusted individuals.

Best practice Cold Storage procedures include locating Cold Storage offsite at a secure third-party location, requiring multiple signatures of a group of trusted individuals to access and implementing secure backup and disaster recovery protocols.

Appropriate information disclosure can also help mitigate risks facing participants when they are looking for a Platform on which to trade. Platforms should publicly disclose information about the Platform that allows participants to educate themselves and effectively choose Platforms they would like to transact with. Platforms should also provide information about the crypto-assets they list, including reference to the assets' websites, whitepapers, etc. as applicable. All fees charged by a Platform should be transparent, easy to understand and easy to locate on a Platform's website.

Prior to launching to the public, a third-party security and threat assessment should be conducted on the Platform's website and associated infrastructure. Any identified deficiencies should be addressed prior to offering services to the public and the Platform should be vigilant in ensuring the ongoing safety of its infrastructure and of crypto-assets in its storage.

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

Bermuda implemented a *Digital Asset Business Act* (the "DABA") to govern a digital asset business. The definition of a "digital asset business" under the DABA includes a business that issues, sells or redeems cryptocurrencies, a business that operates a payment service provider business that utilizes cryptocurrencies, a business that operates an exchange platform, a business that provides custodial wallet services and a business that operates as a cryptocurrency service vendor.

The DABA is a standalone, comprehensive regulatory regime drafted with the particularities of cryptocurrencies in mind, which includes provisions pertaining to anti-money laundering, custody and security, information disclosure, crisis management and regulatory oversight. This approach creates certainty for businesses looking to provide digital asset services, as such services are clearly defined and the regulatory requirements applicable to such businesses are clearly defined and have been drafted with regard to specific risks to which the different types of cryptocurrency related business models are exposed. This approach provides the sought-after benefits of regulatory certainty and consumer protection without sacrificing innovation and the ability of businesses to succeed on a global scale.

If Canada's approach is inconsistent with regulatory approaches in other countries, it may result in decreased ability for Canadian companies to innovate or succeed internationally, it may drive Canadian users of cryptocurrencies to non-Canadian companies over which Canadian regulators have no oversight and it may limit Canada's access and contribution to a new technology that is making waves on a global scale.

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 standards that should be adopted by a Platform to mitigate the risks related to safeguarding investors' assets are, for the most part, outlined in our response to question 2.

Key considerations include segregating customer assets and operating on a full reserve basis to ensure funds are always available.

With respect to storing customer assets, fiat assets should be stored in a regulated financial institution that is located in a trusted jurisdiction. Digital assets held in Hot Storage should be minimized to only the amount required to facilitate trading on the Platform and allow for customer withdrawals. The majority of customer assets should be held in Cold Storage.

Best practice Cold Storage procedures are outlined in our response to question 2. Platforms utilizing their own custody solution should abide by these best practices and Platforms utilizing a third-party custody solution need to ensure they are working with a trusted entity that abides by these best practices. Bitvo would be pleased to discuss with the CSA and IIROC specific practices for the safeguarding of crypto-assets.

5. Other than 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?

We would encourage the CSA and IIROC to consider input from accounting firms and accounting industry groups to determine what type of regulatory approach would enable such firms to be comfortable providing audit and similar services to cryptocurrency businesses, including audit of internal controls and verifiability of cryptocurrency transactions.

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 the Platforms holding or storing crypto assets on their behalf?

From an operational perspective, each Platform should have a mechanism in place allowing a participant to instruct actual delivery of cryptocurrencies to such participant's wallet outside of the Platform, most often through a withdrawal procedure. By requiring actual delivery of crypto assets on completion of each trade without the off-chain option, this would create logistical challenges, timing delays and increased costs as it relates to cryptocurrency-to-cryptocurrency trades as there may be discrepancies in timing of verification on the respective distributed ledger protocol underlying such transfer and the settlement of such transaction.

There are significant benefits to a participant when a Platform holds or stores cryptocurrencies for the participant due to greater ease of use and likely increased security and peace of mind.

Many participants find the current process of handling and managing their own external wallet to be cumbersome or confusing and may take a less intensive approach to the security of their cryptocurrencies than the Platform would. Such participants appreciate a third party, such as the trusted

Platform through which they acquired the cryptocurrency, taking care of that element of their cryptocurrency ownership. If a participant loses his or her private key to an external wallet, the cryptocurrencies may be lost forever. If such participant loses his or her password to the Platform, he or she would be able to recover the cryptocurrencies held on such Platform. Furthermore, by not settling every transaction on the applicable blockchain, the Platform and the participants are able to avoid mining verification costs and timing delays associated with the verification of such transactions on-chain. The transaction can occur in real-time and the participant can have the peace of mind that the trade occurred immediately exactly on the terms contemplated.

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

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 fair price of a crypto asset should be determined in the same manner as traditional financial assets, as set by the supply and demand of traders at a point in time. It is essentially the market clearing price of the most recent trade on a Platform as set by willing buyers and/or sellers. As the cryptocurrency market is a global market, there is stronger price discovery for cryptocurrencies than for most other asset classes.

Reliable pricing sources include large Platforms with significant trading liquidity as well as trusted websites such as coinmarketcap.com, which aggregate real-time pricing information of hundreds of Platforms globally. In determining whether a pricing source is reliable, the quoted price can be compared to other Platforms as well as trusted websites such as coinmarketcap.com. A pricing source can be determined to be reliable if the price is established based on the most recent legitimate transaction completed.

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?

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

For an efficient marketplace to exist, the integrity of trading activity on the marketplace is critical. Every Platform ought to set rules and monitor trading activities on their own marketplace. Platforms should not be engaging in deceptive practices, such as false trading, front running and preferred trading.

Certain negative impacts of such deceptive practices may be inherently limited in the case of cryptocurrencies due to the 24/7 availability and global nature of cryptocurrency trading activities. For instance, as cryptocurrency platforms are typically open for trading 24/7, there is a reduced risk of certain market manipulation activities developed to take advantage of market open and/or close. In addition, the global nature of cryptocurrency trading transactions with global price information available in real-time creates barriers to market manipulation activity and tends to limit the impact of such activities.

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?

The industry employs a wide variety of approaches and products to conduct market surveillance on trading activities. Given the unique nature of cryptocurrencies, to determine best practices for market surveillance, it is important to consider the risks that are intended to be mitigated. These risks may include market manipulation, false trading, fraud or other improper activities. To ensure a fair and efficient market, Platforms monitor market activity to identify and investigate anomalies in trading activity or unusual or suspicious transactions.

We respectfully submit that the comment from CSA and IIROC that short selling and/or margin trading should not be permitted does not appreciate the benefits of such activities for the market, including in preventing market manipulation. For example, if a market participant is acting to manipulate prices in an inflationary way on a Platform and the Platform allows other participants to take advantage of this through short selling, the market would be able counteract and limit the potential manipulation naturally. Market participants would be incentivised to do this to profit from the spread that existed between the manipulated Platform and other Platforms, which would result in the manipulated Platform's pricing coming back in line with that of other Platforms, creating a more consistent global price for digital assets.

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?

There are anti-money laundering and anti-terrorist financing considerations that are more specific to the trading of crypto assets than for marketplaces trading traditional securities. These are addressed under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* and the regulations promulgated thereunder, including the proposed amendments thereto. Surveillance of such risks typically falls under the jurisdiction of The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

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

If a Platform is acting as the counterparty to the trade, the Platform ought to disclose that information to the participant. The terms of the trade, including pricing, ought to be consistent with the market at the time of the trade. If there is any discrepancy between the terms of the trade and the terms of the equivalent trade if made on the market, such discrepancy ought to be disclosed to the participant.

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?

Trading by employees of the Platform may create a conflict of interest, for example, where the employee has access to non-public information which might result in a material change in the market price of a cryptocurrency, such as the new listing of a cryptocurrency on a Platform. Bitvo manages these risks through policies and procedures prohibiting trading on the basis of information that gives employees and advantage over non-employee participants.

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

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

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

Only a small number of insurance providers have invested the time, resources and capital required to adequately understand the cryptocurrency industry and provide coverage. As a result, insurance coverage for the crypto industry is thin and prohibitively expensive such that only the largest Platforms can afford to have a small portion of their assets insured.

Insurance coverage is one way of managing the risk associated with the potential loss of participants' assets. Risk of loss can also be managed by adhering to robust practices, policies and procedures with respect to handling customer assets (as discussed in our responses to questions 2 and 4), combined with ensuring a Platform is adequately capitalized such that a loss of assets can be absorbed by the Platform. These factors should ensure that the risk of loss can be appropriately managed while the industry waits for adequate insurance coverage to become available at commercially reasonably rates.

Concluding Remarks

Cryptocurrencies are a global development. A key benefit of many cryptocurrencies is the fact that such assets are not limited to a geographic region and may be transferred internationally without delay and only nominal cost.

The intentions behind the Framework, being increased regulatory certainty and consumer protection, are laudable and regulation that achieves such goals in a meaningful and measured manner will be welcomed by the industry. The Framework looks to apply existing securities laws in a variety of manners, from marketplace rules to dealer and IIROC requirements, to cryptocurrencies that do not bear the characteristics of traditional securities (and which the Framework does not appear to define with clarity). Existing securities laws apply appropriately to digitized traditional securities, however a patchwork approach to regulating a new and diverse asset class, such as cryptocurrencies, may not achieve the desired goals. On the contrary, this approach may encourage Canadian companies to move offshore, provide a regulatory monopoly to Canadian crypto-asset companies that already wish to deal in traditional securities thereby stifling innovation and domestic competition and push Canadian consumers to use cryptocurrency platform services from non-Canadian entities (as Canadian entities would not compete internationally on the same footing).

If Canada follows the approach of other jurisdictions seeking to balance regulatory certainty and consumer protection through a standalone regulatory regime developed specifically for cryptocurrency, Canada would establish an environment that will enable companies in the industry to thrive while protecting the interests of Canadians. In doing so, Canada can position itself as a hub for innovation in this nascent sector. By developing a cryptocurrency specific regulatory regime, including appropriate considerations from applicable securities laws and anti-money laundering laws, this would enable a standalone framework to create regulatory certainty and address risks facing the industry head-on without having to shoehorn solutions from existing laws not developed with these risks in mind. This would enable the framework to protect and promote Canadians and Canadian businesses.

Thank you for the opportunity to comment on the Framework. Bitvo appreciates the approach by the CSA and IIROC to consult with industry to collaborate in establishing a regulatory framework governing cryptocurrency platforms that balances risk controls and consumer protection without stifling innovation or restricting normal course adoption of cryptocurrencies in everyday life.