Brane Inc.
Info@Brane.Capital
(416) 500-2477
Ottawa / Toronto

The Secretary
Ontario Securities Commission
20 Queen Street West
22nd Floor, Box 55
Toronto, Ontario M5H 3S8 Fax: 416-593-2318
comments@osc.gov.on.ca

Me Anne-Marie Beaudoin
Corporate Secretary
Autorité des marchés financiers
800, square Victoria, 22e étage
C.P. 246, tour de la Bourse
Montréal (Québec) H4Z 1G3
Fax : 514-864-6381
Consultation-en-cours@lautorite.qc.ca

IIROC
Victoria Pinnington
Senior Vice President, Market Regulation
Investment Industry Regulatory Organization of Canada Suite 2000,
121 King Street West
Toronto, Ontario M5H 3T9
vpinnington@iiroc.ca

May 14, 2019

To Whom It May Concern:

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

We would like to thank the Joint Canadian Securities Administrators (CSA) and the Investment Industry Regulatory Organization of Canada (IIROC) for preparing the Proposed Framework for Crypto-Asset Trading Platforms and for inviting industry stakeholders to participate in this process.

Brane Inc. is a Canadian-based fintech company focused on blockchain technology and digital asset custody. We are developing products and solutions that will make this technology accessible, secure and useful for the global investment community.

We have two business divisions: (1) digital asset custody services, and (2) staking and validation activities on blockchain networks that rely on proof-of-stake consensus protocol, commonly referred to as PoS mining. Founded almost two years ago, through our experience with our PoS mining division, we have come to understand custodianship and its related issues. Accordingly, we have developed highly effective, operating custody solutions appropriate for institutional investors. Custodianship has grown to become our primary business focus, and our answers are from the perspective of this line of business. However, we also believe that our answers are equally applicable from the perspective of our PoS mining division.

We cannot provide comments on ALL the questions as we are not necessarily positioned to provide insight in certain areas, such as those relating to trading activities, self-dealing, market making and clearing. In these cases, we cannot give meaningful answers, however, we will have some overarching comments to make. Our answers are from the perspective of our custody services business – that of the custodianship of digital assets (including crypto assets).

General comments:

We appreciate the extent to which the CSA and IIROC have provided guidance and the consideration they have given to crafting Consultation Paper 21-402 (the 'Paper'), particularly with respect the questions being asked, and we very much appreciate the opportunity to respond.

There is a common theme throughout the Consultation Paper that the risks associated with Crypto-asset Trading Platforms ('Platforms') "... are not entirely different than those applicable to other types of regulated entities such as marketplaces and dealers". This would tend to support the overall position of the paper that existing regulatory requirements may be tailored for Platforms. This is a position with which we strongly agree. We believe that, in most cases, the existing regulatory framework can be extended and applied to Platforms and other industry participants in most jurisdictions.

We do, however, wish to point out that there are additional risks, not addressed within the paper, that are applicable to crypto assets and related blockchain technology. These risks are not specific to Platforms but are applicable to the safeguarding of all crypto assets. We refer to these risks as follows:

- *Centralization Risk* – private keys ensure absolute security on the blockchain, but they *also centralize the risk of a security failure.*
- *Rapid/Binary Outcomes* – if a private key is compromised, related crypto assets can be transferred immediately and can never be recovered.

- *Failure persistence* – unlike networks, for which security can be restored after a hack, security of compromised private keys can never be reinstituted. Mistakes and breaches will haunt users forever.

This risk landscape is less forgiving than anything that is currently regulated or that regulatory bodies have ever seen. In the context of digital asset custody, they combine to form what we refer to as "operator risk". Blockchain technology can provide high levels of cybersecurity, however the centralized nature of private key security results in the potential for a single point of failure. Platforms, and almost all other industry-related entities, ultimately ensure that private keys can be reconstituted by entrusting one individual or functional area (such as the IT department) or systems component (such as a designated HSM) with access to all private keys. Should the operator fail, as with Quadriga CX, or the security infrastructure be breached, as has happened a number of times over the past decade, assets will suffer total loss and be rendered irretrievable. The manner in which Platforms presently operate amplifies operator risk and it is our opinion that regulators should take steps to ensure that Platforms minimize or eliminate operator risk, to protect the interests of investors.

We suggest that, because of these risk considerations, existing best practice processes and regulations that govern capital markets today need to be applied in the context of cryptoasset trading Platforms. This would include segregation of assets and duties, regular audits, obtaining appropriate and sufficient insurance coverage, transparent reporting and compliance with applicable regulations. While it is important for regulators and industry participants to comprehend what is new about this technology, consideration should initially be given to understanding what existing rules and best practices can be applied, and how, to entities working with this new asset class.

We expect that the trend towards decentralization initiated by the adoption of blockchain technology and crypto assets certainly will result in an amplification of risk (financial and otherwise) layered on top of a diffusion of accountability. Tracking all of the risks and accountability will become more and more difficult unless rules and guidelines are well developed now. Without such guidelines, identifying clear delineation of responsibilities will become very difficult – making the mitigation of related risks nearly impossible over time.

Specific Answers and Comments to Questions Posed in the Consultation Paper:

PART 2 – Nature of crypto assets and application of securities legislation

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

   We believe that it will be in the in best interests of investors to prohibit pooled crypto assets or 'floats'. Most Platforms pool assets, citing reasons of practicality and expense. The recent hack of the world's largest Platform – Binance – demonstrates the vulnerability of participants' assets when such concessions are made. In this instance, the Platform's entire hot wallet of Bitcoins, worth over $40 million, was stolen, facilitated in part by the pooling of client crypto assets.

More generally, we recommend that control and custody of crypto assets be clearly defined. For example, what the custodian does with those funds must be tightly controlled and clearly delineated.

At present, most Platforms provide, or plan to provide, a number of services related to the trading of crypto assets, including acting as an ATS, clearing and settlement, price determination and custodian. Given the risks we have highlighted above, particularly with respect to that of operator risk, we suggest that the combination of all of these functions present conflicts of interest. In order to clearly delineate fiduciary responsibility, we recommend that the provision of all crypto asset trading market related activities in a single entity, or group of related entities, be prohibited and, in particular, we recommend that Platforms should not be permitted to conduct custody services of crypto assets.

Investors in the crypto asset space should be concerned with the concentration of risk over time in entities that, perhaps, could be classified as "too big to fail". As traditional assets become "tokenized" and crypto assets become more commonplace as mediums of exchange, the failure of any one entity that is permitted to operate as "all things to all people" could be catastrophic to a broad spectrum of the investing public and could impact those who have no interest in, nor any direct exposure, to this asset class. Restricting potential fiduciary conflicts of interest should mitigate this exposure.

We highlight the special nature of separate custody as it clarifies to whom the custodian has fiduciary responsibility. Traditionally, custodianship of client assets invested with registrants and/or investment funds has been provided by qualified and, in the case of investment funds, independent custodians (as defined in NI 31-103 and NI 81-102). Crypto assets should likewise require involvement of a qualified and independent custodian in the provision of that service (either as a qualified custodian itself, or through partnership with one).

PART 3 – Risks related to Platforms

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

Of the ten risks noted in the Paper (pp 4-5), we highlight the first three and the last (addressing safeguarding of assets, inadequate policies and procedures, investors' risk of loss due to insolvency, and inadequate system resiliency and security controls) in our response. We believe that there are a number of ERMs and ISMSs that are respected currently that provide models for application in the space today.

Mature processes and procedures exist today for traditional markets that are equally applicable to Platforms – such as ERM frameworks, ISMSs, control frameworks (COSO and COBIT), etc. – and should be mandatory for such Platforms.

For example, the standards promulgated by the International Organization for Standardization ('ISO') and National Institute of Standards and Technology ('NIST') with respect to cybersecurity frameworks and ISMSs are well developed and are applicable to systems and processes used by Platforms. We suggest that any participant in the crypto asset space be independently certified under one or more of these standards.

As already noted, above, we agree with the statement on page 4 that, for Platforms, "... the risks are not entirely different than those applicable to other types of regulated entities such as marketplaces and dealers". We also highlight the additional risks that we previously described. In addition, we believe that these unique technology-related risks significantly amplify the risks the risks noted in the Paper in the context of Platforms.

We also draw attention to the additional risk of "operator risk" with respect to Platforms. Even if Platforms take reasonable steps to address system resiliency, integrity and security controls, most process and system-based solutions will retain an element of centralizing operator risk, in that some individual, or small group of individuals, within the Platform's organization will retain the ability to reconstitute private keys that would permit access to client funds or accounts. This is particularly true of HSM-based solutions, which are primarily used by Platforms in their operations. Although this can expose crypto assets to loss through fraudulent or criminal actions, it also exposes participants to the risk of loss in other ways, such as the recent failure of Quadriga CX, in which private keys were lost altogether.

We believe that, in order to properly safeguard participants' crypto assets, Platforms should not be permitted to provide custody services to participants if they also provide a platform of exchange of such crypto assets.

PART 4 – Regulatory approaches in other jurisdictions

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

We agree with the statement (pg 6) that "... the existing regulatory requirements will apply to regulate Platforms within those jurisdictions." Having said that, it is our opinion that the critical consideration when applying these regulations is the intent of both the Platform and its participants. Accordingly, sweeping regulations – such as Order 2019 in Malaysia which specifies that all digital currencies, tokens and crypto assets be classified as securities – are too broad to be considered in this fashion in Canadian (and other North American) markets. For example – Starbucks accepting crypto payments – should not be a regulated transaction.

Clearly Canadian regulations will be influenced, in part, by actions taken in the United States, particularly by the SEC. While not perfect, the recently re-tabled Token Taxonomy Act of 2019 is an example. We do not, however, recommend that Canadian regulators adopt a "wait and see" approach as that could very well result in unnecessary delays in the development of a domestic regulatory approach with

respect to Platforms. We encourage the CSA, IIROC and other Canadian regulatory bodies to continue to lead the development of a regulatory and oversight framework.

PART 5 – The Proposed Platform Framework

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.**

   We encourage the development of verified ERMs, ISMSs, and financial and systems controls – including audit oversight and reporting (such as SOC 1 and SOC 2 Type I and Type II reports) – regardless of the use of self-custody or 3rd party custodians. In either case, the custodian at a minimum should be ISO 27001 - and ISO 27017 certified if cloud-based technology is being applied. Additional certifications should also be considered, such as NIST (minimum Level 3).

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?**

   We believe that it is appropriate for regulatory authorities to require SOC 1 and SOC 2 (Type I and II) reports of Platforms and custodians. With respect to the scope of SOC 2 reports – regulators will need to be aware of the scope of the SOC 2 reports being prepared and ensure that such scope is appropriate in all cases. As such, it would be prudent for regulators to either establish minimum scope requirements or review the scope proposed by a Platform on a case by case basis.

   We anticipate and encourage the development of industry best practices. This would address full documentation and stringent testing of systems and processes. At Brane Inc., our entire design approach to systems engineering is rooted in risk mitigation and regulatory compliance, and the application of industry-leading solutions for processes and systems. However, simply developing processes and systems is insufficient from the perspective of stakeholder requirements; the safety and security of these systems must be demonstrable. Independent certifications and SOC 2 reports are two means by which assurance can be provided, but additional approaches should also be used. A potential example of an additional approach, which we use, is the application of "formal verification" which is used for software and software in certain industries (such as aerospace and military). In this context, formal verification proves (or disproves) the correctness of intended algorithms underlying a system or automated process using formal mathematical methods and it is helpful in proving the correctness of systems such as cryptographical protocols. We encourage the adoption of formal verification

methods by the industry to provably demonstrate the effectiveness of internally developed systems and processes.

Any industry oversight and self-regulation will take time to mature. It may therefore be necessary for regulators to establish minimum scope standards – to minimize the risk of industry-led establishment of best practices becoming insufficient. A potential example is the pervasive use of HSMs (hardware security modules) across the industry. HSMs are very secure and have been used for years in traditional banking services, but they cannot be used to manage risk nor distribute it in any way, leading to the operator risk we have described above. The previously mentioned hack of Binance involved the theft of API keys, underscoring the weakness of HSMs as a custody tool. HSMs may be appropriate for lower value, high volume-high speed transactions on which the storage of information is ephemeral but they are not appropriate for the long-term storage of high value crypto assets.

Functionality inherent in blockchain technology may be of assistance to regulators. All transactions utilizing Platforms are completed "on chain" – that it the transaction, including the wallets involved, are recorded on the blockchain. This permits regulators to monitor directly all transactions "real time" as they occur, rather than relying on compliance with any reporting regulations. Certain blockchain networks that support the use of smart contracts could permit the active participation of regulators to enforce compliance with regulatory requirements as transactions occur (rather than monitoring the actions of exchanges and traders after the fact via compulsory reporting). The technology required to support this is not yet fully mature, but it is an approach the regulators should be considering as the framework is developed.

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?**

We are not in a position to comment on the first part of this question, although we support delivery of crypto assets to participants' wallets. Although it is possible that trading of cryptocurrency could occur on chain only on a P2P basis, this approach is not presently practical and lacks any degree of oversight. Regulatory oversight of Platforms would provide necessary governance, oversight and protection for investors.

With respect to the second part of this question, we believe that self-custody on the part of Platforms is potentially dangerous on an institutional scale, due to operator risk and the unique technology risks noted previously. As a minimum, Platforms that wish to store crypto assets on behalf of participants should be required to comply with custodian requirements that ensure custodianship is undertaken by qualified custodians, utilizing acceptable controls and processes, and which do not allow for pooling of assets.

We reiterate our previous comment that permitting Platforms to be all things to all participants provides them with too much power today and sets up the creation of a

high degree of systemic risk in the future as crypto assets become more prevalent as a medium of exchange.

We have no specific comments with respect to Questions 7 through 12 inclusive.

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.**

    We do not foresee a circumstance in which an exemption from an ISR would be appropriate or should be permitted. As we commented previously, the establishment of the scope of the ISR requires careful consideration on the part of regulators but should – at the minimum – consider and include normal industry best practices and the unique risks we have discussed throughout our response, particularly operator risk.

We have no specific comments with respect to Question 14.

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?**

    As we have noted throughout this response, we believe that there are several potential conflicts of interest with which Platforms will have difficulty managing given current business models. This difficulty derives from operator risk and is a primary reason for our recommendation that Platforms be denied self-custody of participants' crypto assets. We have further discussed these conflicts of interest in the "General comments" section, above and in our response to Question 1.

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.**

    We recommend that full crime insurance coverage that addresses all fiat funds and crypto assets, regardless of the method of storage, be required. Platforms and custodians that operate in a transparent manner and with good oversight should be capable of obtaining full crime coverage.

    We, as a custodian, have not had particular difficulty obtaining crime coverage however we can comment that the market for underwriting the risks associated with crypto assets is limited and some underwriters' understanding of the technology and the industry remains limited.

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

    While it should not be considered equivalent to insurance coverage, the maintenance of participants (and Platform) crypto assets across multiple wallets distributes the related risk and responsibility of security – reducing the amount of insurance coverage required and making insurance coverage more readily obtainable.

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?**

    Similar to the key points discussed throughout our response, all models of clearing and settling crypto assets presently utilized by Platforms introduce a centralized point of failure – covering ownership, settlement, price discovery, and safekeeping. Permitting Platforms to continue to conduct all the services they presently provide could result in future systemic risk.

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.**

    While Platforms are better able to comment on the significant risk differences, we believe that, over time, settlement will most likely trend towards on-chain settlement only as crypto assets become more readily accessible and assets regularly used, resulting in a natural mitigation of clearing and settlement.

We have no specific comments with respect to Questions 21 and 22.

We encourage the CSA and IIROC to continue to engage with members of the industry as it develops regulatory and legislative guidance.

We would be happy to provide additional information or answer any questions that you might have in relation to our submission.

Yours truly,

T. Paul Rowland, CPA, CA,
CPA (Illinois), CGMA

Chief Financial Officer & Corporate Secretary