27 July 2023

The Fintech Task Force
of the Board of the International Organization of Securities Commissions

Submitted via email: cryptoassetconsultation@iosco.org

Dear Board and Fintech Task Force,

Public Comment on IOSCO's Consultation Report on Policy Recommendations for Crypto and Digital Asset Markets

Thank you for the opportunity to provide comments on the Consultation Report published in May 2023 titled 'Policy Recommendations for Crypto and Digital Asset Markets', available here: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf (**Report**). This submission responds to Questions 1 and 2.

We invite the Board to refer to related and previous policy submissions made by BADAS*L at www.badasl.com/policy.

The efforts of IOSCO are to be applauded. Much helpful guidance can be absorbed by the global web3 sector from the Report, particularly around conflicts of interest and market manipulation.

Disappointingly, the Report lacks balance. For example, the Report does not convey how the technology is being used to reduce the human risks of fraud with deterministic smart contracts and increase resiliency of and affordability to access digital infrastructure with decentralised blockchain networks. Each of which go towards IOSCO Principles around fraud, custody protections, and operational and technological risk.

As a result, the Reports misses the opportunity to provide useful and beneficial guidance on the application of existing IOSCO Principles where retail market participants have direct access to crypto-token activities facilitated by smart contracts, and does not identify the gaps or further IOSCO Principles that are necessary for 'securities markets' facilitated by global and decentralised blockchain networks. For example, there is no specific IOSCO Principle regarding obligations or expectations upon decentralised network participants. For further information that supports a more balanced representation of the technology's capabilities as a premise to identify the further IOSCO Principles necessary, please refer to TheValueProp database of positive use cases of the technology at https://thevalueprop.io/.

The Report unfortunately (but unsurprisingly) picks up the 'same activity, same risk, same regulation' (**same-same-same**) phrase as a guiding principle. However, in multiple places in the Report the word 'similar' is used which is not the same as 'same' and causes confusion. We would encourage the Fintech Task Force and Board to reflect carefully where the Report has used the word 'similar' because that is not in keeping with same-same-same. Instead, we have been and continue to advocate for a more appropriate guiding principle of 'similar activity, similar risk, specialised regulation, same regulatory outcome' (**similar-similar-specialised-same**).

To illustrate the lack of utility of same-same-same and the soundness of similar-similar-specialised-same, Example 1 is provided below.

> ***Example 1: Crypto-token custody services provided by a human-managed legal entity versus crypto-token custody activities facilitated by a smart contract***
>
> To mitigate against the risk of theft or loss of crypto-tokens, numerous policies and procedures around human activities may be implemented at significant time and cost in a

centralised and human-managed entity providing custody *services*. However, despite these policies and procedures the 'ability' for a human or humans to make mistakes or to steal crypto-tokens remains.

In contrast, the risks in relation to interactions with a deterministic smart contract that performs a crypto-token custody *activity* are different (particularly where there are no persons holding admin keys). By engaging one or multiple independent audits of the smart contract, as well as a bug bounty program, the risk of a smart contract vulnerability that can result in theft or loss is substantially reduced. Furthermore, if crypto-tokens are moved from the smart contract without permission, the public ledger avails the public of the ability to trace and apply public pressure around the return of crypto-tokens which is not apparent in traditional finance.

If retail market participants access a smart contract directly, then they bear the risk of key management which they do not bear when using crypto-token custody services. If accessing crypto-token custody services, the participants bear the risk of human fraud or mistake regarding key management. The risks are different.

The same-same-same approach does not distinguish between *services provided* versus *activities facilitated* by a smart contract, whereas the similar-similar-specialised-same approach does. The means by which retail market participants access the *service* or the *activity* are different, and thus the risks are different.

Whilst the Report provides helpful guidance in respect of centralised and human-managed crypto-token custody *services*, it does not go far enough in respect of crypto-token custody *activities* facilitated by a smart contract. It would be most helpful if, for example, the Fintech Task Force provided a Recommendation linked to existing IOSCO Principles regarding a minimum level of education and security services that should be required of developers of smart contracts that facilitate crypto-token *activities* and that can be directly accessed by retail market participants. Such a Recommendation would protect retail market participants in a specialised way that the same-same-same approach currently fails to achieve.

If a regulator were to apply an outcomes-focussed approach, the same-same-same approach would likely lead the regulator to require re-intermediation to achieve the 'same' outcome for the 'same' risk. This is an appalling result in circumstances when the technology has capacity to reduce risk including the risk of the intermediary, and cost. Reduced risk and reduced cost is the desired result to improve the experience and affordability of the crypto-token activity for the retail market participant.

The tokenisation paradigm extends to non-financial things and increasingly decentralised blockchain infrastructure will be used for trusted non-financial online transactions (such as digital identity and reputation credentials, social media posts, online advertisements, emails, messaging). Where these non-financial things are represented as transferable crypto-tokens, an inevitable financial and speculative element creeps in. However, the existing IOSCO Principles and existing securities and financial services laws and frameworks are simply insufficient such that same-same-same simply cannot hold merit in these growth areas. However, similar-similar-specialised-same would be more fit and agile to deal with the particular and specific risks arising from a 'securities-like' crypto-token activities arising from crypto-tokens primarily created for non-financial purposes but subsequently used for financial purposes by retail or non-retail actors.

Further to the recently published Digital Assets report by the UK Law Commission,[1] the appropriate terminology is crypto-tokens and crypto-token activities. As such, it would be more appropriate for the Report to use language such as "The IOSCO Standards apply generally to all crypto-token activities." As the Ripple case in the US has recently established,[2] a crypto-token in and of itself is not

[1] See, UK Law Commission, Digital assets at https://www.lawcom.gov.uk/project/digital-assets/.
[2] See US District Court Order dated 13 July 2023 at https://www.nysd.uscourts.gov/sites/default/files/2023-07/SEC%20vs%20Ripple%207-13-23.pdf.

necessarily a security for US securities law purposes – it is the facts and circumstances of the transaction or scheme that, for US securities law purposes, determines whether there is a security.

We welcome the opportunity to discuss this submission and assist the Fintech Task Force and Board with the consultation.

Yours sincerely,

Signed by:
Joni Pirovich
260D7EA1A8EBD030

Joni Pirovich
Principal
Blockchain & Digital Assets – Services + Law (BADAS*L)

A web3 focussed firm providing legal, strategic and policy services.