Public Comment on IOSCO's Consultation Report on Policy Recommendations for Decentralized Finance (DeFi)

19th October 2023

Re: CR/04/2023, submitted to the Board of the International Organization of Securities Commissions (IOSCO) via deficonsultation@iosco.org

Blockchain Australia welcomes the opportunity to respond to IOSCO's consultation on policy recommendations for Decentralised Finance (DeFi). As the peak industry body representing blockchain and digital asset businesses in Australia, we are committed to fostering a regulatory environment that supports innovation while ensuring consumer protection and market integrity. Our members include blockchain developers, DeFi service providers, investors, and other participants involved in the Digital Assets ecosystem.

We commend IOSCO for its proactive approach in seeking industry input on the complex and rapidly evolving DeFi landscape. We believe that a collaborative dialogue between regulators and industry stakeholders is crucial to developing a balanced and effective regulatory framework. In our response, we aim to provide a nuanced perspective that reflects the importance and complexity of DeFi.

We believe that a one-size-fits-all approach will not be an appropriate policy response given the unique characteristics and risks associated with different DeFi protocols and services. Instead, we advocate for an approach that is flexible enough to accommodate the rapid pace of technological change while ensuring adequate consumer protections. We provide our insights on the proposed policy recommendations, their potential implications for the DeFi ecosystem, and specific suggestions for alternative approaches where appropriate.

We look forward to engaging further with IOSCO and other regulatory bodies to promote a better understanding of DeFi and to contribute to the development of a framework for DeFi that is effective, proportionate, and adaptable to the fast-paced evolution of this field. We would welcome the opportunity to further discuss the matters raised in our submission.

Please direct all queries to:

Simon Callaghan

Chief Executive Officer

Blockchain Australia

c/o Hall & Wilcox
L 11 South Tower, Rialto
525 Collins Street
Melbourne VIC 3000

Blockchain Australia

RESPONSE TO CONSULTATION QUESTIONS

Q1 - Do you agree with the Recommendations and guidance in this Report? Are there others that should be included?

The report lacks a sufficiently clear definition of DeFi or decentralisation, which could lead to ambiguity in the implementation of the recommendations. It is crucial to address the general lack of understanding of DeFi among policy makers and regulators globally. DeFi presents unique risks and benefits, and any proposed regulatory framework should adopt a principles-based approach to supervision.

We recommend the following checklist as a starting point for balanced consideration of the risks and benefits of DeFi, and a proportionate regulatory response.

Technology neutrality: How do new measures discriminate against technology, directly or indirectly, including specific protocols or algorithms? If an activity is not illicit, how can policy be sufficiently nuanced to regulate it into safe bounds without banning it entirely? Does the regime require the Government to decide which innovations are subjectively valuable or not, or do market forces decide? What evidence exists to support assumptions about 'regulatory arbitrage' in conversations about technology neutrality, and how can neutrality be maintained at a sub-sectoral level? Does the regulatory regime enable interoperability between entities, including on-chain, off-chain and traditional finance, as it evolves?

Balancing regulation with innovation: What are the opportunity costs generated as a result of excessive or overly restrictive policies? How can policymakers engage in inclusive dialogue with stakeholders, and partner with industry and academia to support education at consumer and executive levels? How can policymakers best communicate about the principles and assumptions underlying the regulatory framework?

Regulatory resilience, efficiency and proportionality: Is the regime likely to become quickly outdated given the fast-paced nature of the industry? Is the regime achieving the policy intent in the least burdensome way possible for both regulators and businesses, or could it be more efficient? Is the burden imposed on businesses by a particular measure justified, relative to the potential harm that is being mitigated?

Consumer protection: Is the code transparent and audited independently? Are market participants free to engage with risk, so long as they give "informed consent" about their investments, and service providers have given all information necessary for such consent? Do market participants have access to customer support or effective complaint resolution mechanisms?

Given the proposed considerations highlighted above, we also make the following recommendations:

Technical Understanding of DeFi

Regulators should have a strong technical understanding of DeFi before attempting to bring it within an existing or new regulatory framework. They should ensure they have sufficient technical resources to properly evaluate the nature of DeFi and engage in broad consultation with the community. The proposed application of existing frameworks or the development of

new frameworks should be technologically neutral in *outcome*. We note that, in order to achieve technology neutral *outcomes*, differing regulatory approaches between DeFi and traditional finance are likely to be necessary.

Global Nature of DeFi

Given the global nature of DeFi and the ease of shifting innovation from one jurisdiction to another, the regulatory approach should identify and enhance the benefits of DeFi, rather than solely focusing on potential risks. A balanced focus can reduce certain risks while appearing more inviting to stakeholders. For example, utilising Zero Knowledge Proofs allows for better compliance and reconciliation with law enforcement while not compromising on core DeFi values.

Adopting the 'Similar Activity, Similar Risk, Same Outcome' Approach

Further, we note IOSCO's proposal to take the approach of "same activity, same risk, same regulatory outcome", as described in Recommendation 1 of its Consultation Report. In our view, it is critical that a modified approach of 'similar activity, similar risk, specialised regulation, same outcome' is adopted by policymakers, as endorsed by Joni Pirovich, Principal at "Blockchain & Digital Assets – Services + Law (BADAS*L)" who has made a separate submission to your consultation process. We further wish to draw your attention to the Australian Treasury's concise approach, expressed as 'similar activity, similar risk, same regulatory outcome' in its latest consultation paper. (See: Australian Government, The Treasury, 'Regulating digital asset platforms', 16 October 2023, available at: https://treasury.gov.au/consultation/c2023-427004).

Responsible Persons Concept

We also note IOSCO'S proposal to introduce the concept of Responsible Persons. We can see the benefit of introducing regulation of Responsible Persons, but, but note that implementing such a proposal in its present, proposed form comes with several limitations.

Firstly, the concept of identifying Responsible Persons does not address the need for legal recognition of DAOs. We note IOSCO's commentary regarding various DeFi protocols potentially qualifying as collective investment schemes, derivatives or other financial products. However, depending on the relevant jurisdiction, such financial products typically require at least one legal entity to be involved in issuing financial products under any such arrangement before they will qualify as a financial product in a TradFi sense. It is therefore not accurate to conclude that such arrangements involve the "same activity" and in our view, a far more nuanced approach is required.

Further, in our view, the concept of Responsible Persons has a number of limitations, including the following:

- Certain persons who may have initially qualified as Responsible Persons may, depending on the lifecycle of the relevant offering, no longer have any involvement with the relevant DeFi protocol at later stages of its development and operation (see our further discussion of this point under the heading, Identify Responsible Persons;
- The concept of regulating persons who are holders and/or voters of governance/voting tokens as Responsible Persons, would, in a TradFi sense, involve the equivalent of treating shareholders of securities issued by a body corporate as

Responsible Persons. In our view, it would be more appropriate for such persons to have the rights that are typically attributed to shareholders, rather than regulating them as responsible persons;

- IOSCO proposes treating those "with custody" of the relevant assets as Regulated Persons, but such persons are already likely to be regulated as crypto-asset service providers;

- The concept of Responsible Persons will only apply to Responsible Persons who reside in, or who are otherwise subject to a jurisdiction that establishes its regulatory framework based on IOSCO's principles. This is likely to result in regulatory arbitrage, where such obligations cannot be imposed on a person in a non-member jurisdiction.

We again endorse the submission made by BADAS*L on the topic of Responsible Persons and encourage consideration of the concept of "Responsible Roles" as they are likely to change at different stages of development of the product, service or protocol.

Q2 - Do you agree with the description of DeFi products, services, arrangements, and activities described in this Report? If not, please provide details. Are there others that have not been described? If so, please provide details.

We respectfully disagree with several definitions presented in the report. The fundamental issue lies in the portrayal of DeFi products, services, arrangements, and activities as solely a 'replacement' for the traditional financial (TradFi) ecosystem and its arrangements and products. This perspective encourages the push for more regulation and increased human intervention, which contradicts the decentralised nature of DeFi and brings us back to the centralised structure of TradFi.

Agreement with Categorisation of certain DeFi Products and Services

However, we do find the categorisation of DeFi's common products and services to be reasonable. The report defines each DeFi arrangement and its role, contrasting it with a traditional market intermediary and highlighting the technological innovation it brings. We concur that different DeFi offerings will fall under various types of laws and regulatory regimes, depending on the jurisdiction. For example, some DeFi activities may be equivalent to traditional market intermediaries, which could lead to them being treated as such and classified under securities laws.

DeFi's Broader Scope

It is crucial to acknowledge that DeFi encompasses more than just financial services. It also includes contracts, the facilitation of specific obligations, data management, and identity management. These aspects necessitate a different approach to regulatory development compared to TradFi, which may or may not include any of these characteristics.

Recommendation: DeFi Ecosystem Mapping by jurisdictions

We recommend that IOSCO guides local jurisdiction regulators in undertaking a DeFi Ecosystem Mapping exercise, in consultation with industry and the developer community. This would provide a more comprehensive understanding of the diversity and benefits of DeFi products and services. Such an exercise would ensure that any regulatory development is informed, nuanced, and beneficial for all stakeholders involved in the DeFi ecosystem.

Q3 - Do you agree with the Report's assessment of governance mechanisms and how they operate in DeFi? If not, please provide details.

The report provides a framework for understanding governance in DeFi, categorising participants into groups based on their responsibilities. Each group plays a key role in the DeFi ecosystem, contributing to various aspects such as funding, development, deployment, usage, operations, and infrastructure support. ANNEX D of the report offers analytical tools to evaluate DeFi at multiple levels, including organisation decentralisation, transparency, legal compliance, and fairness.

However, we believe a blanket approach to this analytical framework is not suitable. It should be refined to consider governance mechanisms that promote oversight and separation of concerns without stifling innovation.

Some examples of such initiatives and arrangements include (non-exhaustive):

1. Governance-less protocols: These protocols operate without human intervention once the initial contracts are deployed. Analysis involving DAO decentralisation tests and market participant relationships may not fully apply here.

2. Separation between protocol and operation activities: Some architectures separate entities involved in smart contract deployment from those facilitating issuance offerings and ongoing operations. Given the operational activities the latter entity is required to be licensed and comply with all regulations, while the former may not. Examples include Project Orchid and PBM smart contracts facilitated by DBS.

3. Permissioned DeFi: This type of DeFi arrangement is designed for institutional investors and regulated financial institutions. It requires participants to undergo regulation-compliant processes before accessing the protocols and services.

Q4 - Do you agree with the risks and issues around DeFi protocols identified in this Report? If not, please provide details. Are there others that have not been described? If so, please provide details. How can market participants help address these risks and/or issues, including through the use of technology? How would you suggest IOSCO members address these risks and/or issues?

The report outlines numerous risks associated with DeFi protocols, but not all risks should apply equally to every protocol service. These risks depend on the protocol's arrangements, products, market participants, governance structures, and technological setups. A blanket approach to assessing risk levels and market participant exposures would not be an appropriate policy outcome.

The following is a non-exhaustive list of tools and technology enhancements that could further promote a healthy, resilient, transparent market infrastructure for both participants and investors:

1. Use of ZKPs for decentralised identities: Zero-knowledge proofs (ZKPs) can be used to verify the identity of participants in DeFi activities without revealing their actual identities. This can help mitigate the risks associated with pseudonymity/anonymity and lack of visibility into actual control. This could equally encourage market participants to be verified and accountable, while still maintaining their privacy. (See: supporting Link 1, Link 2).

2. Multi-oracle infrastructure: A multi-oracle infrastructure can provide more reliable and accurate data for DeFi activities, reducing the risks associated with lack of comprehensive market data and challenges in monitoring and assessing off-chain to on-chain pricing. It would also mitigate risks related to single points of failure in offchain data infrastructure.

3. Promotion of programmatic prudential constraints: Smart contracts are uniquely built to execute pre-defined logic and constraints. By embedding prudential constraints and limitations into DeFi protocols codebases, it is possible to programmatically limit the amount of financial risks (market, liquidity, credit, interest) associated with strategies in DeFi. By extent, such constraints would also promote a resilient and stable market infrastructure. As a consequence, supervisors could gain access to prudential metrics on a near real-time basis, which is unparalleled in traditional financial markets.

4. Promotion of leaderboards of protocol disclosures: By promoting market participants to creating and assigning independent labels to protocols that provide proper disclosures, supervisors could incentivize transparency and accountability. This would reduce the risks associated with lack of visibility into actual control and accountability issues amongst participants. On the same note, labelled protocols and associated participants would be incentivised to use such “disclosure ratings” as a market-driven trust mechanism to become integrated into the tech stack of compliant, authorised and licensed market operators.

5. Off-chain attestations: Off-chain attestations and signatures by market participants (custodians, broker-dealers, third party providers, auditors) can be used to verify the compliance of certain DeFi arrangements, activities with regulatory requirements, reducing the risks associated with legal compliance. This could also assist in reconciling the data gap between on-chain and off-chain activities as well as the roles of associated market participants involved in DeFi operations.

These are only some of the techniques that could help enhance market trust and resiliency.

Not every DeFi service would be subject to all enhancements in equal measure.

Q5 - Do you agree with the description of data gaps and challenges in the Report? If not, please provide details. Are there others that have not been described? If so, please provide details. How can market participants address these data gaps and challenges, including through the use of technology? How would you suggest IOSCO members address data gaps and challenges?

The report provides a comprehensive overview of the numerous challenges and gaps in sourcing, decoding, interpreting, and monitoring data related to DeFi markets, participants, infrastructure, and transactions. These gaps exist at various levels in the stack, including settlement, asset, smart contracts, and application front-ends, with varying degrees of availability, completeness, accuracy, and standardisation. The report also considers the significant costs and specialised resources required for data extraction and analysis.

While we generally agree with the report's depiction of these challenges and gaps, we do not necessarily believe that a top-down enforcement of data provision and completeness on DeFi participants would yield the most effective policy outcome. Instead, we propose a market-driven approach that could incentivise the adoption of data standards and improve aggregation methods by data providers and protocols.

DeFi protocols rely on the trust sourced from their transparency and accountability to their user and market participant communities. If providing complete and accurate data bolsters this trust, or conversely undermines it, protocols and participants would be motivated to promptly address these gaps.

We have already suggested some improvements to address these gaps in response to Question 4. Furthermore, here are examples of initiatives that could meet these data needs:

1. Encourage the establishment of data marketplaces: Data brokers are motivated to invest resources (capital, skills, infrastructure) to mine, decode, aggregate, and standardise data when there is a demand for their data from sophisticated consumers. Conversely, they indirectly support or promote platforms (protocols) and participants that provide the highest quality, most accurate data.

2. Incentivise financial intermediaries and sophisticated data consumption entities: Licensed and sophisticated market participants who integrate DeFi platforms into their stack have more demanding data needs, both for compliance and auditing purposes. They exert both indirect and direct pressure on protocol platforms to improve their data provision standards. They often also contribute to the creation of independent data standards organisations.

3. Promote best practice standards and frameworks through independent fora: Several ERC standards have been developed in response to industry participants' needs (e.g., ERC-3643 on permissioned tokens) for compliance. Similarly, the pressure and incentives from both data brokers and intermediaries/participants are the most effective tools for encouraging protocols and participants to adopt data provision methods.

These are just some non-exhaustive examples of ways to overcome existing challenges in data accessibility and accuracy.

Q6 - Do you agree with the application of IOSCO Standards to DeFi activities contained in this Report? Are there other examples of how IOSCO Standards can apply?

We would like to express our belief that the IOSCO Standards should not be uniformly applied to all DeFi activities as outlined in the Report. As we have previously highlighted in our response to Question 1, we believe that the majority of the Recommendations, in their current form, fail to consider the unique structure of DeFi markets. Instead, they seem to apply principles that are more suited to centralised, traditional financial markets primarily.

Given the above statement, we recommend that IOSCO:

Recognise the Diversity of DeFi Arrangements and Activities

While we acknowledge that the IOSCO Principles may be applicable to some DeFi arrangements and activities that offer products and services similar to those provided by traditional market intermediaries, we would like to emphasise that not all DeFi arrangements and activities are equivalent.

Calibrate Regulations According to the Unique Nature of DeFi

We believe it is essential that any regulations are calibrated in accordance with the unique characteristics of DeFi. This will ensure that the regulatory framework is both relevant and effective, promoting the growth and development of the DeFi sector while ensuring the protection of all stakeholders.

Q7 - Is there any additional guidance that you would find relevant to help IOSCO members comply with these Recommendations? If so, please provide details.

IOSCO is understood to regularly survey its members to identify their capacity-building needs and to shape its programs accordingly. Additionally, we recommend the following initiatives to further assist IOSCO members:

Revise the Global Certificate for the Regulation of Securities Markets

IOSCO's *Global Certificate for the Regulation of Securities Markets*[1], delivered in partnership with Harvard Law School, is a promising initiative. We suggest that IOSCO review the curriculum of this course to strengthen the components related to digital assets and crypto regulation. This would provide a structured way for IOSCO members to enhance their workforce's blockchain regulation credentials and capacity. This certificate program also involves completion of the online IOSCO Capacity Building Toolkit[2]

Develop a Global Certificate for the Regulation of Crypto and Digital Assets Markets

In addition to revising the existing certificate program, IOSCO could consider developing, alongside a training partner, a new Global Certificate for the Regulation of Crypto and Digital Assets Markets. This would provide a structured way for IOSCO members to increase the blockchain regulation credentials and capacity of their workforce.

Establish an IOSCO Seminar Training Program in Crypto (STP) and Digital Assets Regulation

IOSCO's Seminar Training Programs (STP) are valuable resources for junior to mid-level securities regulators. We propose that IOSCO consider establishing a Seminar Training Program specifically focused on Crypto and Digital Assets Regulation. This would increase blockchain regulation knowledge and awareness among mid-level IOSCO member staff.

Develop an IOSCO-Endorsed Resource of Crypto and Digital Asset Definitions

Many IOSCO members are currently developing crypto regulations. To support this process and promote consistency, we suggest that IOSCO develop an endorsed resource of crypto and digital asset definitions. This resource should support member digital asset legislation and regulation activity, and would also provide a foundation for an IOSCO digital assets knowledgebase and training activities.

---

1 https://www.iosco.org/training/pdf/Save%20The%20Date%20-%202023%20Global%20Certificate%20Program.pdf

2 https://www.iosco.org/members_area/capacity_building_online_toolkit/

Q8 - Given the importance of the application of IOSCO Standards to DeFi activities, are there technological innovations that allow regulators to support innovation in DeFi/blockchain technologies while at the same time addressing investor protection and market integrity risks? If so, please provide details.

The below recommendations are examples of features or functions that could be applied to DeFi or blockchain projects that could improve the transparency and auditability of these projects while mitigating risks. While these recommendations provide a foundation of areas to explore this list is, by no means, exhaustive.

1. **Proof of Reserve**

Proof of Reserve is a feature of blockchain technologies that allows participants to audit or verify the amount of cryptocurrency or tokens that a blockchain or protocol may be operating with. Implementing Proof of Reserve for DeFi protocols can significantly improve transparency and auditability. This feature can be implemented at varying levels of any protocol for example in peer to peer transactions or at the exchange level. Proof of Reserve audits can also be conducted in myriad ways dependent on the mechanics of the protocol and the needs of the audit and or users.

2. **Automation of Trading Halts**

Given that inter-chain operability and automated trading are key features of DeFi protocols it is crucial that rigour is placed around the criteria by which trading halts might also be automated. Automated trading halts could be an effective method to improve market stability, protect users, prevent flash crashes, and bake in compliance and regulatory alignment into protocol operations. However, it is crucial that these automated functions, when defined, are considerate of the specific context of the protocol and the target users of that protocol.

3. **Blockchain Explorers**

Exposing the transactions, functions, and history of the blockchain is crucial to maintain the transparent and decentralised nature of DeFi projects. Moreover, the implementation of blockchain explorers (or provision of open-API data) is a common feature of many blockchain projects. This provides all stakeholders (including regulators) with real-time feedback and troubleshooting capabilities while ensuring that the protocol maintains a commitment to transparency and auditability without compromising the protocol performance.

4. **Cyber Regulations**

Similar to other technologies, DeFi projects should not be exempted from cybersecurity obligations that technology companies or projects are subject to in their respective jurisdictions. In addition to this, any specific obligations required of fintech companies should similarly be applicable to the DeFi project.

5. **Technology Audits**

Similar to cyber regulations, DeFi projects should be required to conduct, at regular intervals, independent technology audits to ensure the security, privacy, and stability of the

technology.

Q9 - Are there particular methods or mechanisms that regulators can use in evaluating DeFi products, services, arrangements, and activities, and other persons and entities involved with DeFi? If yes, please explain.

We have recommended a number of extra tools and practices in our answer to question 5. Additionally, we recommend the following enhancements to further assist in the evaluation of DeFi products, services, arrangement and activities. While these recommendations provide a foundation of areas to explore this list is, by no means, exhaustive:

Third-Party Audits and Community Engagement

One of the key methods that regulators can employ in evaluating DeFi products, services, arrangements, and activities, involves taking into consideration the self-initiated audits, bug bounties, and community suggestions/proposals that most DeFi projects undertake. These initiatives provide valuable insights into the functionality, security, and overall performance of the DeFi products and services.

Collaboration with Industry Experts

In addition to this, regulators could also collaborate with auditors who possess expert knowledge of the product, as well as the surrounding industry, common practices, and risks. This collaboration would not only enhance the regulators' understanding of the DeFi landscape but also provide them with informed advice on recommended positions.

Chain Analytics

Chain analytics is another effective mechanism that regulators can use in their evaluation process. This method involves the analysis of blockchain data to gain insights into the transactions and activities within the DeFi space. A number of providers exist in the marketplace already.

Enhanced Regulatory Approach

However, it is important to note that the approach defined on how the regulator is to analyse and understand DeFi and products is currently rather vague. This lack of clarity could potentially cause harm, allowing regulators to potentially bypass seeking support or advice from more experienced players in the industry. It also leaves room for preconceived views to direct the efforts in analysing a product, without increased validation of assumptions.

In conclusion, while the current regulatory mechanisms have their merits, there is a need for more structured and inclusive approaches that leverage industry expertise and community engagement. This will ensure a more comprehensive and accurate evaluation of DeFi products, services and arrangements.

Q10 - Do you find the interoperability between this report and the IOSCO CDA Report to be an effective overall framework? If not, please explain.

The reports provided by the International Organization of Securities Commissions (IOSCO) offer an effective overall framework for its members. Both reports are well-researched, clearly written, and contain complementary structures with useful case studies and annexes. This aids in promoting learning in the complex area of cryptocurrency and digital asset trading. However, we recommend that a number of enhancements be applied:

Need for Collaborative Governance Approaches

IOSCO could further enhance policy effectiveness by allocating more weight to collaborative governance approaches. These approaches would support IOSCO members to work together and bring coordinated enforcement against actors who engage in geographical and regulatory arbitrage, thus harming the overall reputation of the industry.

Importance of Cooperation and Information Sharing

Both reports highlight the importance of cooperation and information sharing. For instance, the DeFi report's Recommendation 8 and 9, and the CDA report's Recommendation 11 stress the need for regulators to share information and cooperate with regulators and relevant authorities in other jurisdictions.

Utilisation of IOSCO MMoU and EMMoU: Enhance EMMoU Adoption

The reports suggest the use of the IOSCO MMoU and the EMMoU as governance mechanisms. The MMoU, which relates to information sharing, has approximately 129 member signatories. The EMMoU, which enacts greater collaborative powers, currently has only 23 IOSCO member signatories.

The EMMoU is a critical governance framework that supports improved coordination of IOSCO members in bringing effective enforcement actions against transnational digital asset crime. However, the low level of IOSCO member signatories is undermining its potential. We recommend that IOSCO should make stronger mention of the EMMoU and further encourage IOSCO members who have not yet become signatories to progress with their evaluation and consideration of it.

Strengthen Regional Collaboration

We also suggest strengthening regional collaboration by inviting IOSCO regions to consider piloting crypto and digital asset governance EMMoU working groups. These groups would promote effective and timely sharing of knowledge, policy, and regulatory action. This would further enhance the effectiveness of the overall framework and contribute to the positive development of the industry.

CLOSING REMARKS

Blockchain Australia appreciates the opportunity to provide feedback on the IOSCO's policy recommendations for Decentralised Finance. We believe that the unique nature of DeFi requires a nuanced and balanced regulatory approach that recognises its diversity and potential for innovation. We urge IOSCO to consider our proposed policy principles and interpretations, which aim to balance the risks and benefits of DeFi, and to adopt a proportionate regulatory response.

We also recommend that IOSCO engage in a broad consultation with the DeFi community, and jurisdiction regulators to develop a globally consistent definition and taxonomy for DeFi, as well as to calibrate regulations according to the unique nature of DeFi. We believe that these steps will ensure a regulatory framework that is both relevant and effective, promoting the growth and development of the DeFi sector while ensuring the protection of all stakeholders. Blockchain Australia stands ready to assist IOSCO in this endeavour and looks forward to further engagement on this important issue.

About Blockchain Australia

Blockchain Australia is the peak industry body representing Australian businesses and business professionals participating in the digital economy through blockchain technology. Blockchain Australia encourages the responsible adoption of blockchain technology by the government and industry sectors across Australia as a means to drive innovation and create jobs in Australia.

The Blockchain Australia membership base consists of 120+ leading cryptocurrency and blockchain-centric businesses and 100+ individuals across multiple verticals, including:

- Accounting and Taxation
- Artificial Intelligence
- Art
- Banking
- Building & Construction
- Cyber Security
- Development
- Digital ID
- Education
- Energy and Resources
- Entertainment
- Gaming
- Health and Wellbeing
- Insurance
- Investment
- Legal
- Professional Services
- Recruitment
- Real Estate
- Risk and Compliance
- Supply Chain
- Venture Capital

This policy submission was coordinated by Blockchain Australia's Digital Assets Working Group in close consultation with our membership base. Blockchain Australia thanks Chloe White (Chair), William Remor (Co-Coordinator) and Michaela Juric (Secretary).

Our other policy submissions are available for viewing at https://blockchainaustralia.org/submissions/