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

31st July 2023

Re: CR01/2023, Policy Recommendations for Crypto and Digital Asset Markets,
Submitted to the Board of the International Organization of Securities Commissions (IOSCO)
via cryptoassetsconsultation@iosco.org

Blockchain Australia welcomes the opportunity to respond to IOSCO's consultation paper, *Policy Recommendations for Crypto and Digital Asset Markets*. We encourage IOSCO's continued efforts to address market integrity and investor protection issues in the crypto-asset sector globally. This submission has been prepared in close consultation with Blockchain Australia's members. We thank our members for their inputs.

In responding to this consultation, Blockchain Australia on behalf of its members seeks to ensure that the finalised policy recommendations, to be published by IOSCO in early-Q4 2023, will support the following objectives:

- Regulatory clarity
- Risk-based policy
- International consistency
- Business-friendly environment
- Education and awareness

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

High-level policy development objectives

Blockchain Australia encourages and advocates for the adoption of blockchain technology by industry and governments across Australia as a means to drive innovation in service delivery across all sectors of the economy. While our member base is diverse, all broadly support initiatives that can enhance investor protection and market integrity.

Our overarching reflection on IOSCO's consultation paper is that the proposals would be greatly enhanced by further clarity (sectors identified or defined) for crypto-assets. This is due to the vastness in the types of crypto-assets that exist in the sector. We note that the Australian Treasury is currently conducting a 'Token Mapping' exercise, a foundational step in the Australian Government's multi-stage reform agenda that commits to developing appropriate regulatory settings for the crypto sector. Token mapping seeks to build a shared understanding of the types of crypto-assets in the Australian regulatory context.

Recent global and local experiences point to the need for better investor protection and market integrity, where the rising number of scams and company failures have been driven by the bad actors involved, rather than the technology itself.

In general, Blockchain Australia desires the following outcomes from crypto-asset policy development processes:

- **Regulatory clarity**: The virtual asset industry would benefit from clear and consistent regulations that provide guidance on compliance requirements, licensing, and consumer protection. This would help foster trust and confidence among users and businesses.
- **Risk-based policy**: Regulators should adopt a risk-based approach when developing policy for the virtual asset industry. This means assessing the potential risks associated with different types of tokens and implementing proportionate measures to mitigate those risks.
- **International consistency**: Given the global nature of the virtual asset industry, international cooperation among regulators is crucial. Collaboration and information sharing can help address cross-border challenges and reduce friction for entrepreneurs. Eventually, mutual recognition of licences across jurisdictions is desirable.
- **Business-friendly environment**: Regulators should strive to create an environment that encourages growth and productivity in the crypto sector. This can be achieved by providing a path to licensing that is designed with crypto-asset business models in mind.
- **Education and awareness**: Promoting education and awareness about crypto-assets can help government, executives and consumers make informed decisions and protect themselves from potential risks. Governments can collaborate with industry stakeholders to develop educational resources and campaigns.

Proposed checklist for crypto-asset regulators

Consistent with the desired outcomes stated above, we propose that policymakers and regulators should ask the following questions about their policy frameworks, regulatory gaps and compliance systems, throughout the policy cycle.

Market integrity and interoperability: Is the market fair, orderly and transparent, and do new regulatory measures successfully prevent fraud and other criminal activity from increasing? Is the market systemically safe with consideration given to prudential risks? Does the regime enable interoperability between entities, including on-chain, off-chain and traditional finance, as it evolves?

Consumer protection: Is there an effective regime in place that seeks to prevent harms arising from misinformation, abuse and/or poor operational practices? 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 effective complaint resolution mechanisms?

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?

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?

Response to specific IOSCO Recommendations

IOSCO Key Area	IOSCO Recommendations & Blockchain Australia Response
1. Conflicts of interest arising from vertical integration of activities and functions	RECOMMENDATIONS ON GOVERNANCE AND DISCLOSURE OF CONFLICTS **Recommendation 1 –** **Regulators should use existing frameworks or New Frameworks to regulate and oversee crypto-asset trading, other crypto-asset services, and the issuing, marketing and selling of crypto-assets (including as investments), in a manner consistent with IOSCO Objectives and Principles for Securities Regulation and relevant supporting IOSCO standards, Recommendations, and good practices (hereafter "IOSCO Standards"). The regulatory approach should seek to achieve regulatory outcomes for investor protection and market integrity that are the same as, or consistent with, those that are required in traditional financial markets.** **BA Response** – In our view, policymakers should take into account and accommodate the unique nature of CASP-related offers, including the fact that the lifecycle of transactions can be quite different for such offers (eg. where such operators provide atomic settlement) and including where a traditional clearing and settlement facility may not serve its usual purpose. This principles-compatible framework should then allow for the differentiated treatment of a crypto-asset according to its token classification and ris+k-profile (e.g., if a global stablecoin is marketed to consumers, if it could impact financial stability). In this way, both stablecoins and other crypto-assets would be treated appropriately for the potential risks they pose but within a single overarching framework. This would encourage certainty among market participants as to their regulatory treatment, as well as enhance coordination globally. But it is not the case that certain crypto-activities demand additional requirements so much as all crypto-activities require tailored requirements for the potential risks they pose and based on a token's inherent characteristics, within a comprehensive principles-based framework. We firmly believe that the best guarantee against potential risks to financial stability arising from crypto-asset activity is the implementation of comprehensive and coordinated risk-sensitive regulatory frameworks in all jurisdictions. This will ensure mitigation of potential risk domestically while

reducing the likelihood of regulatory arbitrage internationally. The IOSCO recommendations are a welcome step to reaching this outcome.

However, we also encourage consideration of the policy principles and checklist that we have proposed in this submission. As a tangible step forward, IOSCO could consider adopting a globally consistent taxonomy for crypto-assets to provide clarity as to the legal character of such assets.

Question 2 –
Do respondents agree that regulators should take an outcomes-focused approach (which may include economic outcomes and structures) when they consider applying existing regulatory frameworks to, or adopting new frameworks for, crypto-asset markets?

BA Response –
Yes, please refer to our response to Recommendation 1 and our overarching comments set out at the beginning of this submission.

Recommendation 2 –
Organizational Governance - Regulators should require a CASP to have effective governance and organisational arrangements, commensurate to its activities, including systems, policies and procedures that would, amongst other things, address conflicts of interest, including those arising from different activities conducted, and services provided by a CASP or its affiliated entities. These conflicts should be effectively identified, managed and mitigated.

A regulator should consider whether certain conflicts are sufficiently acute that they cannot be effectively mitigated, including through effective systems and controls, disclosure, or prohibited actions, and may require more robust measures such as legal disaggregation and separate registration and regulation of certain activities and functions to address this Recommendation.

BA Response –
We agree with IOSCO's recommendations on governance and disclosure of conflicts. We note that CASPs can and do in fact engage in various functions at the same time, including providing exchange services, brokerage, market-making, staking and performing other functions. We note that to an extent this may be compared to the role of a prime broker in a TradFi context, which will perform various regulated services for its clients simultaneously, offering custody, trading and execution services.

Recommendation 3 –
Disclosure of Role, Capacity and Trading conflicts - Regulators should require a CASP to have accurately disclosed each role and capacity in which it is acting at all times. These disclosures should be made, in plain, concise, non- technical language, as relevant to the CASP's clients, prospective clients, the general public, and regulators in all jurisdictions where the CASP operates, and into which it provides services. Relevant disclosures should take place prior to entering into an agreement with a prospective client to provide services, and at any point thereafter when such position changes (e.g., if and when the CASP takes on a new, or different, role or capacity).

BA Response –
We agree with this Recommendation.

Question 3 –
Does Chapter 2 adequately identify the potential conflicts of interest that may arise through a CASP's activities? What are other potential conflicts of interest which should be covered?

BA Response –
Yes. Key risks appear to be covered.

Question 4 –
Do respondents agree that conflicts of interest should be addressed, whether through mitigation, separation of activities in separate entities, or prohibition of conflicts? If not, please explain. Are there other ways to address conflicts of interest of CASPs that are not identified?

BA Response –
We do agree, however in accordance with the policy principles set out in our overarching comments, we consider that prohibition may not be necessary where other policy and regulatory solutions exist, including strong disclosure frameworks that are communicated in a clear and concise way to consumers.

Question 5 –
Does Recommendation 3 sufficiently address the manner in which conflicts should be disclosed? If not, please explain.

BA Response –
Yes.

2. Market manipulation, insider trading and fraud	RECOMMENDATIONS ON ORDER HANDLING AND TRADE DISCLOSURES (TRADING INTERMEDIARIES VS MARKET OPERATORS) **Recommendation 4** – **Order Handling - Regulators should require a CASP, when acting as an agent, to handle all client orders fairly and equitably. Regulators should require a CASP to have systems, policies and procedures to provide for fair and expeditious execution of client orders, and restrictions on front running client orders. Regulators should require that a CASP discloses these systems, policies and procedures to clients and prospective clients, as relevant. Orders should be handled promptly and accurately recorded.** **BA Response** – Blockchain Australia agrees with IOSCO's recommendations on order handling and trade disclosures. We note that CASPs can and do in fact engage in various functions at the same time, including providing exchange services, brokerage, market-making, staking and performing other functions. We agree that rules that address CASPs providing multiple functions are required. However, we suggest that such rules specifically take into account the unique nature of CASP-related services and any local modifications to existing laws. For example, whether an operator of any particular kind of digital currency exchange is considered to be operating an exchange in the form of a financial market will need to be considered, based on the development of local laws. Those local laws need to reflect the unique nature of the services that CASPs provide. We note that rules in relation to order handling are required, but that such rules should be customised to reflect the unique nature of digital currency exchanges and other trading venues. For example, the unique nature of DEXs, and the extent to which they differ from CEXs or even traditional markets (in that they are decentralised) must be taken into account. Further, any rules related to settlement must take into account the nature of atomic (instantaneous) settlement, where this is a feature of the exchange. **Recommendation 5** – **Trade Disclosures - Regulators should require a CASP that operates a market or acts as an intermediary (directly or indirectly on behalf of a**

client) to provide pre- and post-trade disclosures in a form and manner that are the same as, or that achieve similar regulatory outcomes consistent with, those that are required in traditional financial markets.

BA Response –
We agree with this Recommendation.

Question 6 –
What effect would Recommendations 4 and 5 have on CASPs operating as trading intermediaries? Are there other alternatives that would address the issue of assuring that market participants and clients are treated fairly?

BA Response –
Disclosure of whether a market intermediary (broker/dealer) is executioner on a principal or agency basis will clarify the current ambiguity in the operating model between CASPs.

From the perspective of an *intermediary acting as principal* – we agree, to the extent of providing information on the bid and/or ask price as well as depth information.

From the perspective of an *intermediary acting as an agent* – agents by definition should be taking reasonable steps to deliver best execution for clients and thus are not in control of the bid-ask spread as principal. Therefore, pre-trade information would not be available beyond non-binding estimates. Warning disclosures of illiquidity should allow for customers to be made sufficiently aware of risks in the long tail of illiquid assets where execution may be aggregated across less mature markets.

Question 7 –
Do respondents believe that CASPs should be able to engage in both roles (i.e. as a market operator and trading intermediary) without limitation? If yes, please explain how the conflicts can be effectively mitigated.

BA Response –
From the perspective of an *intermediary* – if a market operator should choose to also be an intermediary on their own market, policies and procedures should be in place to ensure:

1. The individuals, algorithms (or related entity) that are part of the intermediary operations does not receive (or have access to) asymmetric information from the market operations that potentially

leads to abuse (eg. identity, balance, trading behaviour, transaction history of other participants and insider trading).

2. The sequencing of orders does not give preference to their own intermediary operations.
3. Disclosures that the market operator (or their related entity) is also a principal on their own market along with associated risks introduced to other customers.

Question 8 –

Given many crypto-asset transactions occur "off-chain" how would respondents propose that CASPs identify and disclose all pre- and post-trade "off-chain" transactions?

BA Response –

CASPs should only need to disclose in respect of trades on their own exchange. We do not anticipate that a CASP should be required to identify third party "off-chain" transactions.

Recommendation 6 –

Admission to Trading - Regulators should require a CASP to establish, maintain and appropriately disclose to the public their standards— including systems, policies and procedures— for listing / admitting crypto assets to trading on its market, as well as those for removing crypto-assets from trading. These standards should include the substantive and procedural standards for making such determinations.

BA Response –

We agree, however, we are unsure as to the precise application of some of the examples of proposed requirements set out within Recommendation 6. For example, we note the expectation that information, including audited financial statements may be available, but that for certain offers, there may be no clearly identifiable entity issuing the crypto-asset.

Recommendation 7 –

Management of Primary Markets Conflicts - Regulators should require a CASP to manage and mitigate conflicts of interest surrounding the issuance, trading and listing of crypto-assets.

This should include appropriate disclosure requirements and may necessitate a prohibition on a CASP listing and/or facilitating trading in its own proprietary crypto- assets, or any crypto-assets in which the CASP, or an affiliated entity, may have a material interest.

BA Response –
Blockchain Australia agrees that a CASP should be required to disclose certain information, where it lists or facilitates trading in its own crypto-assets (or crypto-assets in which they may have or own material interest), however, we do not propose a prohibition on CASPs listing their own tokens (or their affiliates' tokens), noting that such conflicts could be managed through disclosure.

Question 9 –
Will the proposed listing/delisting recommendations in Chapter 4 enable robust public disclosure about traded crypto-assets? Are there other mechanisms that respondents would suggest to assure sufficient public disclosure and avoid information asymmetry among market participants?

BA Response –
Yes, and in addition, a prohibition on transacting with clients, or allowing clients to transact where there is information asymmetry.

Question 10 –
Do respondents agree that there should be limitations, including prohibitions on CASPs listing and/or trading any crypto-assets in which they or their affiliates have a material interest? If not, please explain.

BA Response –
Please see our response to Recommendation 7 above, in relation to proposed listings of the CASP's (or its affiliates') own tokens.

RECOMMENDATIONS TO ADDRESS ABUSIVE BEHAVIOURS

Recommendation 8 –
Fraud and Market Abuse - Regulators should bring enforcement actions against offences involving fraud and market abuse in crypto-asset markets, taking into consideration the extent to which they are not already covered by existing regulatory frameworks. These offences should cover all relevant fraudulent and abusive practices such as market manipulation, insider dealing and unlawful disclosure of inside information; money laundering / terrorist financing; issuing false and misleading statements; and misappropriation of funds.

BA Response –
We agree with this Recommendation.

	Recommendation 9 – **Market Surveillance - Regulators should have market surveillance requirements applying to each CASP, so that market abuse risks are effectively mitigated.** **BA Response** – Agree; although query analogy given unlike traditional financial markets there would be multiple trading venues and trading in other jurisdictions. **Recommendation 10** – **Management of Material Non-Public Information - Regulators should require a CASP to put in place systems, policies and procedures around the management of material non-public information, including, where relevant, information related to whether a crypto-asset will be admitted or listed for trading on its platform and information related to client orders, trade execution, and personally identifying information.** **BA Response** – We agree with this Recommendation.
3. Cross-border risks and regulatory cooperation	OVERARCHING RECOMMENDATION ADDRESSED TO ALL REGULATORS **Question 13** – **Which measures, or combination of measures, would be the most effective in supporting cross-border cooperation amongst authorities? What other measures should be considered that can strengthen cross-border co-operation?** **BA Response** – We agree with many of the measures outlined in Chapter 6 and provide additional commentary and suggestions below. - Agree with the recommendation to strengthen and broaden MMOU/EMMOU arrangements. We endorse setting up specific protocols for CASPs. - Agree with the recommendation for supervisory colleges/networks. These could provide a platform for real time information sharing, - joint decision making and more collaborative supervision of multinational CASPs. - Regulatory sandboxes may be worth consideration. - Promote standardisation of regulatory frameworks.

- Promote more technology driven solutions including chain analysis tools, enable DID/SSI solutions, and zero-knowledge proofs.
- A crypto-SWIFT network to enable worldwide travel rule compliance.
- Encourage stronger cooperative arrangements (like MLATs) that can help take action against cross-border crypto crimes.
- Training and workshops around the implemented capacities so CASPs remain well-informed.
- Consider 'ancillary' guidance to facilitate a supportive business environment for CASPs e.g. guidance to banks, insurance companies, payment providers and audit firms on devising reasonable risk appetites for providing services to CASPs,
- Require the publishing of a list of key contact persons for services to CASPs.

In sum, we believe that authorities should rely on existing cooperation and information sharing arrangements where such arrangements exist, and new arrangements should be considered where they do not.

The goal of such arrangements should be to share information on adverse situations and enforcement actions against non-compliance in a timely manner. However, we also believe that the best guarantor of international financial stability in the crypto-asset sector is aligned regulatory frameworks between jurisdictions, forming the basis for an increased level of mutual recognition between supervisors. Such a mutual recognition framework would ensure single-supervision that can also reduce the risk of supervisory lapse and avoid a "race to the bottom."

Additionally, while not directly addressed in Chapter 6, we also believe that improved coordination between domestic supervisors in many jurisdictions would also benefit the sector.

4. Custody and client asset protection	RECOMMENDATIONS ON CUSTODY OF CLIENT MONIES AND ASSETS **Recommendation 12 –** **Overarching Custody - Regulators should apply the IOSCO Recommendations Regarding the Protection of Client Assets when considering the application of existing frameworks, or New Frameworks, covering CASPs that hold or safeguard Client Assets.** **BA Response –** We agree with this Recommendation. **Recommendation 13 –** **Segregation and Handling of Client Monies and Assets - Regulators should require a CASP to place Client Assets in trust, or to otherwise segregate them from the CASP's proprietary assets.** **BA Response –** We endorse the recommendation that regulators require CASPs to segregate Client Assets from Proprietary Assets, except in instances where: - Client assets are supplemented with additional operating capital belonging to the CASP for execution speed, and liquidity (therefore in surplus, not deficit) - Incidental omnibus venues for settlement between trading venues - Immaterial values. (From time to time there may be immaterial shortfalls from onchain network fees, or other offchain fees paid in kind) - Any other incidental venues required for the safekeeping of client assets (e.g. Incidental venues or services used in network upgrades or migrations) Blockchain Australia notes that in Australia, crypto-asset trust services are not yet readily available, and thus CASPs should be required to provide bankruptcy remote account equivalents through legal or accounting means. Blockchain Australia agrees where CASPs take legal and beneficial title to Client Assets for re-use or rehypothecation (e.g. lending or staking on a principal and not agency basis) CASPs should be required to: - Disclose associated risks

- Receive consent

Recommendation 14 –
Disclosure of Custody and Safekeeping Arrangements - Regulators should require a CASP to disclose, as relevant, in clear, concise and non-technical language to clients:

i. How Client Assets are held, and the arrangements for safeguarding these assets and/or their private keys.

BA Response –
We agree with this aspect of the Recommendation.

ii. the use (if any) of an independent custodian, sub-custodian or related party Custodian;

BA Response –
We agree with this aspect of the Recommendation.

iii. the extent to which Client Assets are aggregated or pooled within omnibus client accounts, the rights of individual clients with respect to the aggregated or pooled assets, and the risks of loss arising from any pooling or aggregating activities;

BA Response –
We agree in relation to disclosure, and note that pooled client accounts in relation to on-chain location are currently industry norms; primarily due to prohibitively expensive on-chain network fees required for unaggregated onchain addresses.

iv. Risks arising from the CASP's handling or moving of Client Assets, whether directly or indirectly, such as through a cross-chain bridge; and

BA Response –
We agree with this aspect of the Recommendation.

v. Full and accurate information on the obligations and responsibilities of a CASP with respect to the use of Client Assets, as well as private keys, including the terms for their restitution, and on the risks involved.

BA Response –

We agree with this aspect of the Recommendation.

Recommendation 15 –
Client Asset Reconciliation and Independent Assurance - Regulators should require a CASP to have systems, policies, and procedures to conduct regular and frequent reconciliations of Client Assets subject to appropriate independent assurance.

BA Response –
We agree with this Recommendation. We make note of the recommendation that regulators have the resources and capability to evaluate audits and independent reviews where necessary. We suggest including independent review assurance over security arrangements and controls. Further commentary is below.

Q15a - We note the risks of prescribing the manner in which custody is held from a technology perspective, as that may become prone to obsolescence, and may be better suited to industry self-regulation.

Q15b - Regulators may require that CASPs, as part of their policies and procedures, conduct an annual assessment of whether their custody procedures are up to date with industry developments.

Q15c - In addition to safeguards listed in Recommendation 15, additional safeguards may include regular backup of records.

Q15d - Fair and reliable valuation of crypto-assets held in custody should be required for CASPs offering services in which margin, leverage, or collateral is applied.

In addition to the safeguards listed, CASPs should seek to mitigate the following risks in relation to custody:

- Policies to eliminate key-person risk, where custody access may be permanently lost
- Regular review of access controls
- Background checks on fit and proper persons handling custody
- Disaster recovery policy and procedures in relation to private key recovery

Recommendation 16 –
Securing Client Money and Assets - Regulators should require a CASP to

	adopt appropriate systems, policies and procedures to mitigate the risk of loss, theft or inaccessibility of Client Assets. **BA Response** – We agree with this Recommendation. We recommend regulators prescribe tiered amounts of minimum capital required in order to conduct a CASP business.
5. Operational and technological risk	RECOMMENDATION TO ADDRESS OPERATIONAL AND TECHNOLOGICAL RISKS **Recommendation 17** – **Management and disclosure of Operational and Technological Risks - Regulators should require a CASP to comply with requirements pertaining to operational and technology risk and resilience in accordance with IOSCO's Recommendations and Standards.** **Regulators should require a CASP to disclose in a clear, concise and non-technical manner, all material sources of operational and technological risks and have appropriate risk management frameworks (e.g. people, processes, systems and controls) in place to manage and mitigate such risks.** **BA Response** – We have considered a number of relevant factors that could potentially be captured within operational and technological risks, including: - Asset mechanics made freely accessible and explained in simple concise terms for general consumption (e.g. asset management policies if asset-backed, liquidity policy, security policies (e.g. hot / cold / warm, etc.) & blockchain technologies used (e.g. EVM, consensus mechanism, detailed smart contract reliance, etc.) - Risk of bridges for cross-chain transfers is a risk unique to DLT. - Standards around audit of DLT smart contracts. - Onchain transnational smart contract lifecycle management. - CASPs should, where possible, provide extensive consumer-protection technologies (e.g. multifactor authentication (for key actions like: transfer, withdrawal, password change, etc.)

	- This may fall somewhere along the lines of a contractor/third party policy; CASPs should be obligated to disclose second & third party risks to customers, instilling transparency (to a maximum extent) to help bridge information gaps.
	- Transparent policies in relation to treatment of chain forks.
	  - Account abstraction included as both a risk and a solution to DLT operational security.
	  - Lifecycle management of tokens.
	  - External monitoring / surveillance.
	  - Autonomous processing (smart contract) bugs.
	  - Irrevocable errors (e.g. user errors cannot be reversed).

6. Retail access, suitability, and distribution	RECOMMENDATION FOR RETAIL DISTRIBUTION **Recommendation 18 –** **Retail Client Appropriateness and Disclosure - Regulators should require a CASP, to operate in a manner consistent with IOSCO's Standards regarding interactions and dealings with retail clients. Regulators should require a CASP to implement adequate systems, policies and procedures, and disclosure in relation to onboarding new clients, and as part of its ongoing services to existing clients. This should include assessing the appropriateness and/or suitability of particular crypto-asset products and services offered to each retail client.** **BA Response** – We have considered a number of relevant factors that could potentially be captured within retail client appropriateness and disclosure, including: - An AFSL framework should be developed for all crypto assets and service providers, and it should be intuitively structured around the nature of crypto. For more information on financial advice, please refer to our submission to the Australian Senate Inquiry 2021. - On advertising, we note that within Australia, the ACCC has delegated its authority to ASIC in relation to misleading and deceptive conduct for crypto-assets. We advise caution in ensuring that any additional regulations related to marketing are genuinely warranted, are fair, and do not stifle the industry's growth. - We agree that suitability/appropriateness assessments should not give clients the false impression that they understand crypto-assets and associated risks. We suggest that these assessments should be reviewed on a regular basis to keep pace with changes in products

	and consumer knowledge, and to avoid 'gaming' of the assessment by fraudulent actors. - We agree that regulators should require CASPs to have an efficient and effective mechanism to address client complaints. Any independent dispute resolution bodies/services should be independently reviewed on an annual basis to ensure the fair and reasonable consumer outcomes are achieved. - Clear and unambiguous risk warnings could be made a part of all user experiences.

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

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