Token Mapping Consultation Paper - Piper Alderman Submission

Q1) What do you think the role of the Government should be in the regulation of the crypto ecosystem?

Government plays an important role in ensuring appropriate safeguards are in place for the protection of consumers and financial stability. At the same time, the stance that the Government takes to crypto regulation will have a significant impact on whether Australia is perceived as an attractive place for web3 innovation and investment, leading to opportunities, jobs and growth, or the opposite.

Australia has created and can continue to foster blockchain-based businesses that are global leaders and responsible innovators in their field, and so we urge the Government to establish a clear regulatory landscape which ensures consumer protection and fosters homegrown innovation.

With the help of industry, Government can educate itself and the public service around the vast spectrum of valuable crypto use cases, so that regulation is fit-for-purpose, proportionate and sensible.

A number of jurisdictions, such as the EU, UK, Singapore and Hong Kong, are already positioning themselves as leaders in web3 technologies, and there is still a strategic opportunity for Australia to foster web3 innovation and attract and retain global talent which will benefit the Australian economy. Supporting innovation and consumer protection are not mutually exclusive paths. By establishing a clear regulatory framework, the Government can help establish standards to protect consumers and a pathway for innovation that serves Australia over the long term.

The Government could adopt a diverse range of approaches to regulate crypto businesses:

1) Regulate within the existing framework of laws, including the Australian Consumer Law and Corporations Act. This approach requires the least immediate work by the Government and Treasury but would leave all of the gaps and uncertainties present in the important intersections between technology and current laws unaddressed, and would likely result in an undesirable 'regulation by enforcement' model if ASIC was to continue their current approach to crypto businesses.

2) Regulate crypto within the existing financial services regime under the *Corporations Act* with only minor changes to the existing regime and accepting that compliance costs will be substantially more burdensome in Australia than elsewhere. This approach involves a significant risk that unregulated activity will continue to flourish offshore.

[1] With thanks to Tim Masters, Sally Fetouh, Luke Misthos, Lola Hickey and Kelly Kim all of Piper Alderman for their valuable contributions to this paper.

3) Regulate crypto within the existing financial services regime, with substantial modifications and exemptions to address the unique aspects of crypto and create a light-touch model, but understanding that this approach has a significantly higher risk of more burdensome compliance costs creeping in over time.

4) Regulate crypto by creating a light-touch system to create an attractive environment for investment and businesses to move/remain in and be based out of Australia, and secure consumer / investment protections within that environment, using a new regulator or legislation which can be updated and amended as needed.

We submit that if the Government wishes to have a fit-for-purpose approach when regulating cryptocurrency and incorporate the principle of 'same risk same regulation', the substantial ambiguity as to the application of existing financial services legal frameworks means the third and forth options above are likely to be the most attractive.

The approach proposed in the United Kingdom (**UK**) would be a path closer to the third option. The EU and Dubai approaches are closer to the fourth option. Treasury is already well educated as to the approach of overseas regulators and we do not propose to traverse those approaches in detail here.

Some options the Government could implement could include:

1. **Token sales** - The Government could require initial token sales to be registered with a regulator such as a special regulator or the Australian Securities and Investments Commission (**ASIC**). Disclosure relating to the nature of the project would need to be mandated as well as ensuring compliance with anti-fraud regulations such as the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth). It is expected that the European Union will adopt a proposal not dissimilar to this approach under the Market in Crypto-Assets Regulation (**MiCA**) which is expected to receive final approval in the near future.

2. **Exchange Regulation** - Digital Currency Exchange Providers (**DCEs**) already have an obligation to register with AUSTRAC and practices such as know-your-customer (**KYC**) and anti-money laundering (**AML**) policies are well embedded for DCEs. A formal licensing regime which imposes minimum compliance requirements, including in relation to custody of assets, would establish minimum industry standards and help consumers distinguish between licensed and unlicensed offerings, including scam platforms which are often based offshore.

3. **Taxation** - Urgent and considered taxation guidance for taxation of crypto-assets with due consideration given to tax reforms which recognise and equalise tax treatment for businesses which transact using stablecoins and other cryptocurrencies is needed.

4. **Consumer Protection** - Regulation of DCEs and implementing custody requirements should protect consumers from the majority of losses which have been suffered in recent years. We submit a light-touch licensing and registration regime,

imposing minimum compliance standards, product disclosure, terms and conditions and risk disclosure is a high value option to pursue.

An important policy consideration will be the desire to foster an attractive domestic DCE and cryptocurrency industry in Australia. This will involve a balancing of different policy objectives but these are not necessarily opposed. The imposition of existing financial services laws to crypto-assets without regard to the specific features of those assets will lead to regulation not being fit for purpose and will drive innovation offshore, which in turn risks undercutting consumer protection as users move to offshore platforms.

Q2) What are your views on potential safeguards for consumers and investors?

It is of paramount importance that when safeguards are introduced, a balance is struck whereby consumers are provided adequate protection (such as via DCE custody and light-touch licensing) and new projects are attracted to locate in and remain in Australia. The application of existing financial services laws or unduly burdensome regulation risks stifling local industry, sending businesses offshore and as a result undermining consumer protection.

An approach similar to the approach taken by the UK's Treasury (**HM Treasury**) in its consultation paper: 'Future financial services regulatory regime for crypto assets' (**UK Crytpoasset Consulation**) appears sound. There, the principle of "same risk, same regulatory outcome" has been proposed, but importantly the regulatory framework to be deployed recognises the unique features of crypto-assets.

HM Treasury is seeking to use legislative and regulatory mechanisms to put in place equivalent or similar safeguards where crypto-assets present similar risks to financial instruments, for example, market manipulation practices.[2] Additionally, when the objective of 'same risk, same regulatory' outcome is not achievable, HM Treasury acknowledges that it may take some time to harmonise international standards between the major jurisdictions but their focus in the meantime is:[3]

- That market prices reflect genuine forces of supply and demand, and should not be manipulated;
- That market participants should be able to trade in a fair and orderly environment; and
- That market participants should have the same opportunities to access information.

Due to the cross-border nature of crypto assets, **the Government cannot regulate the domestic crypto-asset industry in a vacuum**. Some projects may choose to operate in a different jurisdiction that does not impose the same regulatory protections as in Australia while consumers can continue to access that project via peer-to-peer systems, through decentralised platforms or offshore offerings. It is important therefore that Australia is broadly

[2] HM Treasury, *Future financial services regulatory regime for cryptoassets: Consultation and Call for Evidence*, page 15.
[3] HM Treasury, *Future financial services regulatory regime for cryptoassets: Consultation and Call for Evidence*, page 57.

aligned with emerging international standards[4] and provides an attractive regulatory environment to retain and attract jobs to Australia. An inconsistent approach risks stifling the domestic industry while failing to protect consumers.

Q3) Scams can be difficult for some consumers to identify.

a) Are there solutions (e.g. disclosure, code auditing or other requirements) that could be applied to safeguard consumers that choose to use crypto assets?

The greatest risk in the last few years to users of crypto assets has been from counterparty risk from centralised actors. Straightforward custody requirements provide the greatest cost-benefit safeguard for consumers using DCEs to hold digital assets.

There are several practical solutions that could be applied swiftly to assist consumers:

1. **Regulatory framework** - The Government should implement a regulatory framework for initial token sales as well as a light-touch licensing regime for DCEs and custodians modeled on MiCA or the UK. A licensing regime could give consumers greater ability to distinguish between legitimate businesses and unlicensed or offshore operators. Currently, crypto scams are frequently associated with entities that purport to operate a genuine business, but are typically based offshore, are unlicensed and list fake or limited information regarding their activities. These platforms often leave consumers with limited or no practical recourse.

2. **Require bank transfers to match account names** - A simple change the government could make, which would combat almost all scams occurring in the financial sector, would be to require that banks only process fund transfers where the sending party enters an account name matching the destination bank account. At present a scammer may provide bank details for a DCE (for example) but use the name of the party they are impersonating to describe the account name to the victim. The victim of the scam may well believe that their bank would have some check in place, noting banks disclose openly that they do not verify account names.

3. **Listing Standards and Disclosure** - DCEs could be required to implement listing standards before admitting tokens to trading and provide basic token and risk disclosures which might help consumers identify scams.

4. **Education and Social Media Companies** - The Government could become better involved in educating consumers about scams and financial literacy[5]. Further, the advertising of many scams is principally via major social media networks which appear best placed to intercept and delist those advertisements.

b) What policy or regulatory levers could be used to ensure crypto token exchanges do not offer scam tokens or more broadly, prevent consumers from being exposed to scams involving crypto assets?

[4]See IMF Policy Paper, *Elements of Effective Policies for Crypto Assets*, page 30.
[5] See Hong Kong Monetary Authority, Conclusion of Discussion Paper on Crypto-assets and Stablecoins, page 25 [4.69].

There does not appear to be any meaningful problem with DCEs offering 'scam tokens', however there are several policy and regulatory levers that could be used to ensure DCEs do not offer such tokens and protect consumers from being exposed to scams involving crypto assets. Some of these include:

1. **Licensing and registration requirements:** A light-touch licensing regime should be implemented requiring crypto token exchanges to register with authorities beyond only AUSTRAC before they can operate. Any licensing regime implemented should be created with regard to the breadth of crypto token offerings and the potential for additional growth in the future.

2. **Listing standards and disclosure requirements:** Regulators could require minimum standards for the listing of crypto tokens on DCEs and require disclosure of information about the tokens offered, such as their underlying technology and risks associated with holding them. This could be part of a holistic approach to help consumers make informed decisions and avoid scams, but leave consumers free to purchase digital assets and goods which they wish to access.

3. **Enforcement actions and penalties:** Government can take enforcement action against scams, including criminal and civil actions, and seek to prevent advertisements of scam projects on major social media outlets. It appears social media and web-advertising is a significant vector for scams impacting consumers.

4. **Education and awareness campaigns:** Government has a role to play in launching education and awareness campaigns to educate consumers on how to identify scams as part of broader financial education. This would help consumers make informed decisions, and be better equipped to detect scams.

Q4) The concept of 'exclusive use or control' of public data is a key distinguishing feature between crypto tokens/crypto networks and other data records.

a) How do you think the concepts could be used in a general definition of crypto token and crypto for the purposes of future legislation?

In the interests of adopting globally consistent standards and avoiding regulatory arbitrage, we would recommend that key definitions have due regard to those adopted in other comparable jurisdictions, such as the UK, EU, Hong Kong or Singapore, or adopted by standard setting bodies such as the Financial Action Task Force.

The UK Financial Services & Markets Bill adopts the following definition of crypto-assets:

> *""cryptoasset" means any cryptographically secured digital representation of value or contractual rights that— (a) can be transferred, stored or traded electronically, and (b) that uses technology supporting the recording or storage of data (which may include distributed ledger technology)."*

The draft Markets in Crypto-Assets regulation adopts the following definition:

> *"'crypto-asset' means a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology;"*

The aspect of 'exclusive use or control' is not sufficient to distinguish crypto tokens from mere data files. The fact that a token's exclusive use and control is recorded and transferable using distributed ledger technology are also essential features.

Paragraph 42 of the Paper states that *"'crypto asset' is effectively an umbrella term for a crypto token and each of the benefits provided by its token system".* This definition and usage of the term should **not** be adopted, as it could lead to grouping of a "token system" which is a financial service/product (for example a yield product) together with a token which is linked to that system but which can be owned or transferred without being used for that service or product.

b) What are the benefits and disadvantages of adopting this approach to define crypto tokens and crypto networks?

See our response above.

Q5) This paper sets out some reasons for why a bespoke 'crypto asset' taxonomy may have minimal regulatory value.

a) What are additional supporting reasons or alternative views on the value of a bespoke taxonomy?

There are a wide variety of crypto-assets types which are used for different purposes. Due to the nature of the crypto asset industry, new blockchain advancements and uses for the technology, the variety of crypto-assets are likely to increase over time. As such, it is likely that a bespoke taxonomy different to the emerging international language could quickly become outdated and require further amendment soon after it is introduced.

Given that blockchain technology remains in its infancy, the introduction of a rigid and Australia specific bespoke taxonomy risks stifling innovation and diverging from new developments in the market. While an analysis of the bundle of rights attaching to a token will remain an important consideration in determining whether a token should be treated as falling within the existing categories of financial products, a regulatory framework which focuses on the activities being provided, rather than the tokens being traded, and aims to provide flexible pathways to compliance for innovative projects will lead to better outcomes than a bespoke taxonomy which results in projects or tokens being found to be financial products, but without any pathway to compliance.

A legislative framework based on broad principles rather than individual product features is more likely to remain fit for purpose for the long term. Regulators and Courts are well placed to make individual assessments as to whether the specific features of a token or token network render the token or a particular crypto asset service to involve a regulated offering.

A key role of Government is to ensure there is a pathway which is not unduly burdensome in order to encourage compliance and establish consumer protections.

b) What are your views on the creation of a standalone regulatory framework that relies on a bespoke taxonomy?

As discussed above, a bespoke taxonomy outside of the emerging international taxonomy presents problems. There are strong arguments in favour of a standalone regulatory framework and bespoke regulator including:

1) The highly technical nature of the underlying technology requires specialist knowledge and training which would be best concentrated in an agency staffed and skilled to understand the technology;

2) Such an agency would be well placed to advise the Government and build an ongoing relationship with industry to provide for agile adjustments to the regulatory perimeter impacting crypto-assets;

3) Crypto-assets touch on a variety of regulated areas and relying on existing frameworks may continue to leave gaps;

4) The existing financial services regime was designed for a centralised financial system and, while principles based, addresses specific risks which do not easily map to a decentralised world; and

5) In the event that crypto-assets continue to evolve to automate existing financial systems, a separate regime could provide a bridge to this potential future development, helping Australia be a true leader in financial services.

Importantly, when it comes to financial product regulation, the Government should not permit the addition of “blockchain” to an existing financial product to move that product outside of the regulatory perimeter, but similarly the addition of “blockchain” should not automatically make a product or service within the regulatory perimeter.

c) In the absence of a bespoke taxonomy, what are your views on how to provide regulatory certainty to individuals and businesses using crypto networks and crypto assets in a non-financial manner?

The distinction between what is and what is not “non-financial” is sometimes difficult to distinguish in relation to crypto-assets. In a traditional context, a wide variety of assets exist to which society ascribes value to as an investment, but which are not themselves regulated as financial products (e.g. diamonds, art, gold, stamps, etc.). The commentary of the regulator and public statements of the Government is key to provide guidance and certainty when the financial services laws are framed broadly, as the Paper’s description of the ‘functional perimeter’ demonstrates.

We submit that an activity based approach to assessing crypto networks (particularly as technology will continue to evolve beyond any laws) is preferred to a pure “functional

perimeter" approach given the breadth of the definition of "facility" and the inherent networks supporting tokens. The application of broadly defined laws in current financial services licensing regime breeds uncertainty. Clarity and guidance upfront as to the application of the functional perimeter, but of even greater importance, pathways to functional compliance, is key.

While we understand the 'token, token system, function' taxonomy is not necessarily intended to define the legislative framework, the practical application of these concepts to a given set of facts is likely to capture most tokens and crypto networks. The proposed taxonomy is unlikely to provide "bright-line" guidance to businesses in applying the regulatory framework. It is also unclear how this framework would align with regulatory approaches in other jurisdictions.

We support an approach to defining the functional perimeter which adopts globally recognised terminology and is consistent with the emerging international regulatory consensus and focuses on activities, rather than technology.

An approach which seeks to regulate certain activities with respect to crypto-assets and potentially deems certain types of crypto-assets outside scope is most likely to be workable. For example, MiCA identifies types of services in relation to crypto-assets:

(a) the custody and administration of crypto-assets on behalf of third parties;

(b) the operation of a trading platform for crypto-assets;

(c) the exchange of crypto-assets for fiat currency that is legal tender;

(d) the exchange of crypto-assets for other crypto-assets;

(e) the execution of orders for crypto-assets on behalf of third parties;

(f) placing of crypto-assets;

(g) the reception and transmission of orders for crypto-assets on behalf of third parties

(h) providing advice on crypto-assets;

The UK Government proposes to take a similar approach by identifying types of activities which it proposes to bring within the regulatory perimeter.[6] We submit there is great merit in approaching the regulation of *activities* instead of the regulation of technology.

Many non-fungible tokens (**NFTs**) have non-financial functions (e.g. collectibles, NFTs for gameplay, digital representations of art, etc.). It is intended that the MiCA regime will exclude unique and non-fungible tokens, such as digital art and collectibles. It is also intended to exclude tokens which represent real world assets, such as real estate or product guarantees. The recitals to MiCA state, relevantly:

[6] See HM Treasury, *Future financial services regulatory regime for cryptoassets: Consultation and Call for Evidence*, Table 4.A.

While these crypto-assets might be traded in market places and be accumulated speculatively, they are not readily interchangeable and the relative value of one crypto-asset in relation to another, each being unique, cannot be ascertained by means of comparison to an existing market or equivalent asset. Such features limit the extent to which these crypto-assets can have a financial use, thus limiting risks to users and the system, and justifying the exemption.

It is noteworthy that emphasis is put both on the unique and non-fungible nature of the relevant assets. We agree that the law should generally adopt a substance over form approach to the extent that technology such as NFTs and/or fractionalisation is used to circumvent the regulatory framework for products which are plainly financial products.

Australia could adopt such an approach to exclude from the functional perimeter certain types of assets, such as digital art or in-game assets such as trading cards, skins or collectibles. Where the primary function of an NFT or token is non-financial but may have incidental financial elements, it would be appropriate to apply the incidental exemption, with appropriate regulatory guidance around its application to NFTs or tokens. The fact that a NFT has value in the secondary market (like basketball cards or event tickets), does not mean that it should be classed as a financial product or regulated as such.

It may be appropriate to allow regulatory discretion to bring certain types of crypto-assets within or exclude them from the functional perimeter in future subject to appropriate public and industry consultation, with appropriate changes and clarity for those crypto-assets which are within the functional perimeter.

Q6) Some intermediated crypto assets are 'backed' by existing items, goods, or assets. These crypto assets can be broadly described as 'wrapped' real world assets.

a) Are reforms necessary to ensure a wrapped real-world asset gets the same regulatory treatment as that of the asset backing it? Why? What reforms are needed?

At this time, widespread trading of tokenised real-world assets (for example, property or commodities) has not grown significantly, we suggest, for the reason that it is not possible to do so under current laws. For example ASIC has never, to our knowledge, granted permission for an alternative approach to the unavailability of insurance in respect of a crypto-asset or service which is a financial product.

Existing laws, such as the Australian Consumer Law, already provide strong consumer protections, such as protections against misleading and deceptive and unconscionable conduct, which will apply to persons who tokenise and sell real-world assets. In some cases, existing financial services and other licensing regimes may also apply.

The main source of risk in relation to wrapped or backed assets in crypto-asset markets at this time is in relation to stablecoins, which represent a growing percentage of the total value of crypto-assets. Stablecoins have evolved as an important component of the crypto-ecosystems for payment and mitigating volatility. However, there have been a number of incidents of stablecoins which did not maintain full asset backing and un-backed or

algorithmic stablecoins. Stablecoin legislation which sets basic requirements for licensing and proof of reserves[7] will help to address these issues and encourage the adoption of stablecoins as an efficient means of payments[8].

To the extent that markets in tokenised real-estate assets begin to emerge in future (e.g. tokenised real estate), it may be appropriate to bring these assets within the regulatory frameworks to ensure adequate consumer protections (e.g. in relation to trading or custody of tokenised property interests and to ensure the underlying assets are safe).

Currently there appears no possible way for a registered managed investment scheme to issue tokenised interests representing the assets held by the scheme, and ASIC has not provided guidance or indicated it would support a retainer MIS being used in this way.

b) Are reforms necessary to ensure issuers of wrapped real-world assets can meet their obligations to redeem the relevant crypto tokens for the underlying good, product, or asset?

We do not consider that reforms are necessary at this stage to ensure that issuers of wrapped real-world assets can meet their obligations to redeem the relevant crypto tokens for the underlying goods because existing laws such as the Australian Consumer Law, financial services laws (to the extent this can be used at all) and criminal laws already provide protection for consumers.

In many cases, the dealing in the underlying assets may already be regulated (e.g. operating a real estate business).

To the extent that markets in tokenised real-world assets begin to emerge, it may be appropriate to bring certain categories of tokenised real-world or wrapped assets or services provided in relation to those assets within the regulatory perimeter by providing for custody requirements for the goods.

As noted above, it is clear that no tokenised retail managed investment scheme can be issued in the current environment.

Q7) It can be difficult to identify the arrangements that constitute an intermediated token system.

a) Should crypto asset service providers be required to ensure their users are able to access information that allows them to identify arrangements underpinning crypto tokens? How might this be achieved?

It is important that users of crypto products and services are provided access to information about products and services. Information on the products offered by a service provider should be made available to consumers, such as product and risk disclosures. The MiCA

[7] See Hong Kong Monetary Authority, Conclusion of Discussion Paper on Crypto-assets and Stablecoins, page 4.
[8] See IMF Policy Paper, *Elements of Effective Policies for Crypto Assets*, page 26.

regime, for example, would impose minimum content requirements for crypto-assets whitepapers, which include:

> *(0a) information about the offeror or the person seeking admission to trading;*
> *(0b) information about the issuer, if different from the offeror or person seeking admission to trading;*
> *(0c) information about the operator of the trading platform when it prepares the white paper; (ca) if different from the persons referred to under 0a-0c, the identity of the person which prepared the crypto-asset white paper and the reason why that person prepared the crypto-asset white paper;*
> *(a) information about the crypto-asset project,*
> *(c) information about the offer to the public of crypto-assets or their admission to trading on a trading platform for crypto-assets;*
> *(d) information on the rights and obligations attached to the crypto-assets;*
> *(b) information about the crypto-assets;*
> *(e) information on the underlying technology;*
> *(f) information on risks;*
> *(g) information on principal adverse environmental and climate related impact of the consensus mechanism used to issue the crypto-asset.*

It would be appropriate to require a crypto-asset service provider to put in place and publish details of relevant procedures, such as terms and conditions of use and, for crypto-asset exchanges, applicable policies on the admission of crypto-assets to trading and market integrity.

Although detailed information should be provided by service providers, regulation should not impose unnecessarily burdensome requirements to provide information on the technical arrangement of the asset being provided. Detailed technical information may not provide any useful information or protection to consumers. However, it may be appropriate to require operators of intermediated token systems to undertake code or cyber-security audits, details of which should be published in relevant disclosure.

b) What are some other initiatives that crypto asset service providers could take to promote good consumer outcomes?

Crypto asset service providers can take several initiatives to promote good consumer outcomes. While consumers should also be supported by a robust legal framework, it would also be sensible for service providers to promote good consumer outcomes through:

1. **Education and transparency:** Service providers can provide resources that educate consumers about the risks and benefits of using their platforms and provide transparency in their operations. Such practices are already common among large established exchanges. Services providers can explain the terms and conditions of their services, fee structures, the risks associated with investing in crypto assets as well as providing information about the technical aspects relating to cryptocurrency.

2. **Security measures:** Crypto asset service providers should be required to maintain robust security measures in place to safeguard consumer funds and data. They

should regularly audit and update security protocols to ensure they are up-to-date with the latest threats.

3. **Customer support:** Customer support provides a level of transparency and legitimacy to entities which works to encourage growth, investment and development. Service providers should have responsive and knowledgeable support teams that can help consumer understanding.

4. **Dispute resolution:** Service providers should have a clear and efficient process for resolving disputes. This can include having a dedicated team to handle consumer complaints, providing mediation services, or having an independent arbitrator to settle disputes.

Q8) In addition to the functional perimeter, the Corporations Act lists specific products that are financial products. The inclusion of specific financial products is intended to both: (i) provide guidance on the functional perimeter; (ii) add products that do not fall within the general financial functions.

a) Are there any kinds of intermediated crypto assets that ought to be specifically defined as financial products? Why?

Crypto-assets or services which are in reality financial products should be caught under the existing financial services framework but only with a clear pathway to compliance or acknowledgement that they cannot presently comply with the existing framework.

We submit that the Government should focus attention on types of crypto-assets which should be excluded from the financial services and future crypto-assets regime at this time, such as digital art and collectibles or tokenised real-world assets (excepting tokenised financial products), and considering what changes could be made to ensure activities which are, or which wish to be offered as, financial products or services can comply with the existing (or future amended) financial services laws.

Additionally and as noted above, the Paper states at paragraph 42 that ‘crypto asset’ is effectively an umbrella term for a crypto token and each of the benefits provided by its token systems. We submit that this is an unhelpful definition, and that any assessment of whether crypto assets are financial products should be narrowed to the activities which are being sought to be regulated, and in the policy context consideration of whether, if regulated, they could comply with such regulation, is essential.

b) Are there any kinds of crypto asset services that ought to be specifically defined as financial products? Why?

See response above.

Q9) Some regulatory frameworks in other jurisdictions have placed restrictions on the issuance of intermediated crypto assets to specific public crypto networks. What (if any) are appropriate measures for assessing the suitability of a specific public crypto network to host wrapped real world assets?

We submit that only a specialised regulator with deep knowledge of the crypto industry should be taking steps to 'pick the winners' when considering public crypto networks and whether some should be permitted over others. To date, a relatively small number of well known public crypto networks have come to prominence, such as Bitcoin, Ethereum, Solana and Polkadot.

The market is better placed to distinguish between different types of public crypto networks. Under a future licensing regime, crypto asset service providers will provide an important gatekeeper function by only admitting to trading tokens associated with public crypto networks which maintain proper disclosure and can be widely traded.

In establishing a regulatory framework, it is appropriate to distinguish between the different layers of the web3 technology stack. This means distinguishing between public crypto networks, the tokens associated with or which trade on those networks, and intermediaries or software applications which facilitate services on those networks. In web3, public crypto networks operate as a kind of market infrastructure, but there is typically no central authority or controller responsible for that infrastructure and who can be the subject of regulation.

Accordingly, these networks cannot be regulated like traditional market infrastructure. Similarly, it is likely to be difficult to regulate tokens which are linked to the functions for which those tokens are used.

There needs to be a clear understanding of and distinction between the provision of products or services by centralised actors which can usefully be the subject of regulation and the mere provision of technology and infrastructure. The regulatory framework should generally focus on centralised intermediaries who provide products or services using public or private crypto networks. The case for regulation is most pressing in relation to centralised actors who take custody of consumers' crypto-assets.

Q10) Intermediated crypto assets involve crypto tokens linked to intangible property or other arrangements. Should there be limits, restrictions or frictions on the investment by consumers in relation to any arrangements not covered already by the financial services framework? Why?

A number of jurisdictions, such as Hong Kong and Singapore, are considering imposing a requirement on crypto-asset service providers to implement knowledge type quizzes before permitting consumers to trade crypto-assets. Such measures serve an important function of ensuring that consumers are properly knowledgeable of the features of crypto-assets before engaging in trading.[9] It also incentivises crypto-asset exchange to assist in educating their users.

This approach also strikes the right balance of ensuring consumer protection, while not excluding retail access to digital assets by applying finance-based suitability tests. The imposition of finance based tests would likely drive consumers to unregulated providers and

[9] Monetary Authority of Singapore, Proposed Regulatory Measures for Digital Payment Token Services, page 11-12.

would exclude retail consumers from the growth in the digital assets industry and web3 technologies.

There is a natural limit on introducing friction for retail users in the context of a global peer to peer ecosystem. Strict limits or burdensome requirements for centralised services may send consumers to offshore platforms or DeFi systems to bypass those requirements.

Q11) Some jurisdictions have implemented regulatory frameworks that address the marketing and promotion of products within the crypto ecosystem (including network tokens and public smart contracts). Would a similar solution be suitable for Australia? If so, how might this be implemented?

There is no compelling case for introducing specific laws relating to crypto promotions in Australia as may be the case in other jurisdictions when Australia already enjoys very strong consumer protection under the Australian Consumer Law. The creation of a simple and light-touch custody and licensing system, plus registration for token offerings, would provide more than adequate guardrails for the advertising of projects in Australia.

Q12) Smart contracts are commonly developed as 'free open-source software'. They are often published and republished by entities other than their original authors.

a) What are the regulatory and policy levers available to encourage the development of smart contracts that comply with existing regulatory frameworks?

If the Government wishes to encourage the use of smart contracts under existing regulatory frameworks, it need only ensure regulators publicly state this, and those regulators engage proactively grant targeted exemptions where the use of smart contracts will not match the existing regulatory framework.

b) What are the regulatory and policy levers available to ensure smart contract applications comply with existing regulatory frameworks?

By creating a welcoming environment for smart contract development, with targeted exemptions to ensure where a smart contract cannot comply with existing regulatory requirements it will be exempted from doing so, a broader level of compliance could be encouraged, keeping projects and jobs on-shore and providing regulators with projects and people to regulate.

Q13) Some smart contract applications assist users to connect to smart contracts that implement a pawn-broker style of collateralised lending (i.e. only recourse in the event of default is the collateral).

a) What are the key risk differences between smart-contract and conventional pawn-broker Lending?

Smart-contract lending has developed as a solution to enable fully automated lending on-chain by allowing for collateralized loans using on-chain assets. It is inherently and fundamentally different to "pawn-broker lending" and we were surprised to see this

comparison in the Paper. The two are inherently and fundamentally different and pose different risks, including:-

1. **Availability / Cost Risk:** Smart contracts are open, readable, accessible pieces of code which can offer collateralized lending irrespective of a borrower's social status. The code is entirely unbiased in respect of the customer and will perform as it is programmed to do, with very minimal costs and full code-disclosure to the person interacting with the code.

   Pawn-broking lending is far more socially driven, with the pawn-broker in a significantly greater position of power over a, typically, far more disadvantaged and vulnerable borrower. The regulation of pawn-broking is detailed[10] and the costs of that compliance are passed on to the borrowers who use those services.

2. **Technology risk:** Smart-contract lending relies on blockchain technology and smart contracts to automate and enforce loan agreements. As a result, there may be some risk of technology, such as a software bug or a hack, which could result in the loss of borrower assets or the failure of the loan agreement. That risk is mitigated by the code necessarily being open-source.

   Conventional pawn-brokers rely on traditional legal agreements and physical collateral, which may be susceptible to technology failures involving compliance with laws requiring ownership ledgers for goods posted as security. There is no openness to the code or technology risk.

3. **Regulatory Risk:** Smart-contract lending is a relatively new industry, and around which there is regulatory uncertainty given yields are offered to lenders who fund smart contracts which provide borrowing.

   Conventional pawn-brokers, on the other hand, are subject to more established and detailed regulatory frameworks which are unlikely to change. They remain a very expensive way for customers to obtain a loan.

4. **Counterparty risk:** In smart-contract lending, the terms of the loan are programmatically enforced and, absent a technology failure, there is no counterparty risk.

   In conventional pawn-brokers, the significant regulation over the industry assists in reducing the counterparty risk of a pawnbroker breaching their obligations, but a substantial information and dollar cost imposition rests on a borrower via pass-through costs of the pawnbroker.

5. **Crime risk:** Smart-contracts using public blockchain technology permit tracing of transactions, reducing or eliminating their usefulness as a place for crime to be done.

[10] See for example the *Pawnbrokers and Second-hand Dealers Act 1996* in NSW.

Pawnbroking is an area where stolen goods may be more readily sold given the costs of enforcement (locating the goods, obtaining orders for return etc) to victims.

b) Is there quantifiable data on the consumer outcomes in conventional pawn-broker lending compared with user outcomes for analogous services provided through smart contract applications?

We are not aware of any pawn-broker lending which is remotely analogous to smart-contract lending or any data which has considered such an ill-matched comparison. We do not consider that such data, if available, would be helpful in informing policy choices given the tremendous differences and entirely different customers who use smart contract lending and pawn-broker style lending. We submit that the comparison is not helpful.

Q14) Some smart contract applications assist users to connect to automated market makers (AMM).

a) What are the key differences in risk between using an AMM and using the services of a crypto asset exchange?

A centralised crypto asset exchange will have custody, security and regulatory risk in respect of the crypto assets stored at that exchange, creating a counterparty risk. An AMM which is a smart contract will not have the same counterparty risk profile and the security risk profile will be dependent on the coding of the AMM smart contracts.

AMMs may also be subject to technical risks, such as vulnerabilities in the smart contract code (but noting these are readable code and so flaws can be more readily detected and addressed) or network congestion, and the lack of any human based technical support.

b) Is there quantifiable data on consumer outcomes in trading on conventional crypto asset exchanges compared with user outcomes in trading on AMMs?

At this time we are not aware of quantifiable data outside of the assets lost due to the failures of centralised exchanges which did not segregate client assets in separate custody as compared to trading on AMMs. This data would be very useful and we suggest that a business such as Chainalysis or Elliptic may be able to assist in tracking AMM data in particular.

Conclusion

We thank Treasury for the opportunity to make this submission, and hope the matters above are of use to the Government when making policy decisions in this space, which decisions will help decide whether Australia will follow a US ‘regulation by enforcement’ model and leave users at risk to offshore entities, or a UK / EU or Middle Eastern model to support more Web3 development in Australia and encourage Australian’s to use trustworthy Australian businesses.