THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: BLC:CBlb030323

3 March 2023

Crypto Policy Unit
Financial System Division
The Treasury
Langton Crescent
Parkes ACT 2600

By email: crypto@treasury.gov.au

Dear Sir/Madam,

Token mapping

The Law Society of NSW appreciates the opportunity to comment on the issues raised in the consultation paper 'Token mapping'. We note that the token mapping exercise in the consultation paper seeks to identify the key activities and functions of products in the crypto ecosystem and to map them against the existing 'functional' definition of financial product. The paper also seeks to identify any practical issues which complicate compliance with the existing Australian regulatory regime.

The Law Society's Business Law Committee contributed to this submission.

Our comments in response to some of the consultation questions are set out in Annexure A to this letter.

We look forward to the opportunity to participate in the later planned consultation, building on the findings of this consultation, particularly in the areas of licensing and custody reforms.

If you have any questions about this submission, please contact Liza Booth, Head of Commercial and Advisory Law Reform, at liza.booth@lawsociety.com.au or on (02) 9926 0202.

Yours faithfully,

Cassandra Banks
President

THE LAW SOCIETY OF NEW SOUTH WALES
170 Phillip Street, Sydney NSW 2000, DX 362 Sydney
ACN 000 000 699 ABN 98 696 304 966
lawsociety.com.au

T +61 2 9926 0333 F +61 2 9231 5809
E lawsociety@lawsociety.com.au

Law Council
OF AUSTRALIA
CONSTITUENT BODY

ANNEXURE A

Question 1: What do you think the role of government should be in the regulation of the crypto ecosystem?

Australia should adopt regulation that is fit-for-purpose and based on the principle of "same activity, same risk, same regulation", as recommended by the Financial Stability Board.[1] We agree that an effective regulatory framework must ensure that crypto asset activities are subject to comprehensive regulation, commensurate to the risks they pose, while supporting innovation.[2] Regulation should also take account of the novel features and the specific risks associated with crypto assets. The role of government should be to encourage innovation and free market competition, while establishing a regulatory framework with the necessary checks and balances to protect investors and discourage fraud. We consider that a regulatory framework that is in line with the framework proposed by the United Kingdom (UK) HM Treasury is appropriate.[3]

We submit that four key elements in a proposed crypto asset regulatory framework are:

1. **Initial Coin Offerings (ICOs) -** The Government may require ICOs to be registered with the Australian Securities and Investments Commission (ASIC) and follow similar prospectus disclosures as required with other initial public offerings (IPOs), if the intended capital equity to be raised meets a certain threshold.

2. **DCE Licensing**– Digital Currency Exchanges (DCE) are presently required to register with AUSTRAC and comply with anti-money laundering and counter-terrorist financing (AML/CTF) regulations; the Government has proposed a further Crypto Asset Secondary Service Providers licensing requirement, so that DCEs will be required to obtain a license to operate. Licensing is an appropriate step to ensure DCEs are monitored, however the greatest issue facing DCEs concerns the custody of customer assets and the ability to return those assets during an insolvency event, which is not expressly dealt with under a licensing regime.

3. **Taxation** – Taxation of crypto assets needs to be approached carefully. Retail consumers face difficulties in identifying what constitutes a capital gain for taxation purposes when trading crypto assets on exchanges.

4. **Custody and Consumer Protection** – A custody framework addressing crypto assets as the legal property of consumers should be adopted in line with the Markets in Crypto-Assets (MiCA) proposal for the European Parliament.[4]

Question 2: What are your views on potential safeguards for consumers and investors?

Safeguards that are too onerous could stifle smaller crypto projects and create a gap in the market favouring projects with higher capital. We endorse 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 Consultation). The principle of "same risk, same regulatory outcome" is suggested as a grounding principle[5]

[1] Financial Stability Board, 'Regulation, Supervision and Oversight of Crypto-asset Activities and Markets',11 October 2022, 1.
[2] Ibid.
[3] See: https://www.gov.uk/government/consultations/cryptoasset-promotions
[4] https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739221
[5] HM Treasury, 'Future financial services regulatory regime for crypto assets', February 2023,57.

with the following outcomes specified in paragraph 9.13 (as paraphrased):

- 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.
- That market participants should have the same opportunities to access information.

Question 3: 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?

Code auditing would cause practical difficulties for many small DCEs and would involve an additional expense that could hamper the development of small start-ups. Simple practical consumer safeguards could include:

- **Legislated Security Requirements** - Crypto exchanges and wallets should implement security measures such as two-factor authentication, encryption, and cold storage to prevent hacking attempts and cyber theft. These practices are commonly adopted by users and exchanges; however, a custody framework could build in some legislative requirements to increase consumer confidence.

- **Education** – Government sponsored consumer scam education, as provided for other subsets of scams prevalent in other industries, would assist consumers to identify scams.

- **Insurance** – An insurance product designed specifically to protect consumers from losses due to hacking and theft of their crypto-assets, similar to existing financial products over tangible assets, would be of practical assistance; such policies could include higher premiums for low-risk events like quantum hacks and 51% attacks.

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?

The appropriate regulatory lever is through the establishment of a licensing regime, with a disclosure requirement for what assets are permitted to be traded on the exchange.

The Government could implement a "Token Watch" style public website as part of wider public crypto asset education which monitors suspicious activities likely to lead to "pump and dumps" or other scams with a 'traffic' light system, similar to www.scamwatch.gov.au. The technology is available to monitor trends in all crypto assets (such as that utilised by Eventus, alongside other forensic tools offered by third parties such as Ciphertrace or Chainalysis) which could be used to provide the data to this public monitoring tool.

Question 4: 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

A crypto token is a unit of digital information that can be 'exclusively used or controlled' by a person - despite that person not controlling the host hardware where that token is recorded.

This exclusive use or control differs from other record keeping systems which rely on records maintained by a third party.

We note the useful discussion of the nature of crypto assets and how they are distinguished from other assets and data by the UK Jurisdiction Taskforce of the LawTech Delivery Panel in the *Legal Statement on the Status of Cryptoassets and Smart Contracts*:

> that data should be seen not as constituting the cryptoasset but rather as being, respectively, the record of it and the key to dealing in it. Thus, the commercial value of a cryptoasset is not in the recorded data itself but in the fact that the person possessing that data is able to effect and authenticate dealings in the cryptoasset in accordance with the rules of the system. Putting it another way, it is not what the data tells you but what it allows you to do.[6]

Question 5: 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?

In the UK, HM Treasury does not intend to expand the definition of "financial instrument" to include crypto assets for the purposes of UK legislation. The Consultation Paper notes the difficulties of retrofitting an existing regime to a new asset class. However, in line with the principle of "same risk, same regulatory outcome", HM Treasury will:

> Seek to use other legislative and regulatory mechanisms to put in place equivalent or similar safeguards where cryptoassets present similar risks to financial instruments (e.g. market manipulation practices which arise from the fact that cryptoassets are traded in a way which resembles financial instruments).[7]

This is a sensible approach and presents a middle ground between creating a new bespoke taxonomy and retrofitting into previously established definitions. A bespoke regime is also more likely to create overlapping regulatory regimes and confusion for market participants.[8]

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

See the response to question 5 (a) above.

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?

We reiterate our view that the four elements of a regulatory framework should address the items set out above in question 1: Registration of ICOs at a certain capital threshold, DCE licensing, development of taxation legislation and, most significantly in relation to consumer protection, development of a custody and licensing framework. Government also has an important role to play in educating consumers as to the potential for scams and the importance of securing personal crypto assets.

---

[6] UK Jurisdiction Taskforce, LawTech Delivery Panel, "*Legal Statement on the Status of Cryptoassets and Smart Contracts",*16. See: https://lawtechuk.io/insights/cryptoasset-and-smart-contract-statement.
[7] HM Treasury (n 5) 15.
[8] Ibid.

Question 6: 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?

We consider this issue in relation to three potential categories:

i. In situations where stablecoins are backed by a common value, such as fiat currencies (AUD, USD, GBP) or commodities (such as gold or silver), it is not certain that existing currency/commodity laws can effectively apply to a stablecoin, due to, for example, the cross-border 24-hour trading nature of crypto assets.

ii. Situations will also arise where there are stablecoins, like algorithmic or hybrid stablecoins, which maintain the 1:1 value of their currency in the market without being pegged to anything. While these are considered stablecoins, they do not base their value on something else, and instead rely on complex algorithms and smart contracts to buy and sell assets to maintain the peg price.

iii. Non-fungible tokens (NFTs) which are representative of separate intellectual property or real-world assets.

The rights conveyed by the wrapped assets are limited to the crypto asset, they do not convey property rights in the wrapped real-world asset. Any reform in this area should be limited to addressing legislated custody requirements as set out in our response to question 1.

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 consider that reforms are not required, as the issuers of such assets, that are "swapped" for real-world assets like a 1:1 exchange of stablecoin to fiat, or an NFT that conveys a right to be awarded a real world good or attend an event that is exchanged, have obligations under the existing Australian Consumer Law.

Question 7: 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?

We note that this would appear to be an onerous requirement to place on all DCEs (or Crypto Asset Secondary Service Providers). Any such obligation needs of course need to be balanced against issues for individual holders, such as how to exercise rights and issues in insolvency. As previously stated, it is our view that crypto asset service providers are subject to the obligations imposed under the existing Australian Consumer Law.

As previously stated, some information could be made available to users through a government sponsored "Token Watch" website as set out in the response to question 3(b).

Question 8: 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?

Not in our view. As set out in our response to Question 5 (a), it is our view that the Government should follow the HM Treasury proposals, which is to not expand the definition of "financial instrument" (or in the case of the *Corporations Act 2001*, to not expand the definition of "financial product" or "financial service").

Question 9: 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?

A stablecoin like AUS, or the Government backed Perth mint token-like PMGT, are commonly used for stores of value for assets on exchanges which are executed as back-to-back trades. The growing prevalence of central bank digital currency (CBDC) could be an important part of the development of the nascent crypto asset market as these assets contribute to consumer confidence in the value of the assets. In our view it is premature to impose any restrictions over the issue of these assets.

Question 11: 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?

Yes. As set out in our response to question 1, ICOs should be required to be registered with ASIC if they meet a certain capital threshold with similar prospectus requirements as other regulated IPOs. There is some merit in adopting the anti-hawking provisions of the *Corporations Act 2001* to apply to crypto assets (notwithstanding such assets should not be deemed a financial product for the purposes of that Act).

We suggest that the key focus of the Government should be on public education and the application of the existing Australian Consumer Law to the crypto asset economy, rather than looking for a bespoke legislative solution.

Question 12: 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?

Smart contracts are self-executing code. There does not seem any need to look at smart contracts on a legislative level, provided the rights granted by any associated crypto asset are properly dealt with under a legislative framework.

Question 13: Some smart contract applications assist users to connect to smart contracts that implement a pawn-broker style of collateralised lending (i.e. the 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 and conventional pawnbroker lending differ in several key ways, including the following risk differences:

- **Technology risk**: Smart contract lending relies on blockchain technology and smart contracts to automate and enforce loan agreements. As a result, there is a risk of technology failure, such as a software bug or a hack, which could result in the loss of borrower funds or the failure of the loan agreement. On the other hand, conventional pawnbrokers rely on traditional legal agreements and physical collateral, which are less susceptible to technology failures.
- **Collateral risk**: Smart contract lending often requires borrowers to provide cryptocurrency or other digital assets as collateral for the loan. The value of these assets can be volatile and subject to rapid fluctuations, leading to a risk of collateral value fluctuations. In contrast, conventional pawnbrokers typically accept physical assets such as jewellery or electronics which are generally more stable in value.
- **Regulatory Risk**: Smart contract lending is a relatively new and unregulated industry, which can result in regulatory uncertainty and potential legal risks. Conventional pawnbrokers, on the other hand, are subject to more established regulatory frameworks and may have less legal risk.
- **Counterparty risk**: In smart contract lending, borrowers and lenders may be anonymous and may not have a direct relationship with each other, which can lead to a risk of fraud or default. In conventional pawnbroker lending, the lender and borrower have a direct relationship, and the lender has physical custody of the collateral, reducing the risk of fraud or default.

Question 14: 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?

AMMs being decentralised and crypto asset exchanges being centralised is key to understanding the differences in risk between the two services. Both allow consumers to buy, sell and trade crypto currency, although one is governed by a central entity that oversees and controls its operation, while the other operates on blockchain networks using smart contracts.

AMMs do not have a centralised entity and traditional channels that are usually available for consumers, such as a team to handle complaints, or an IT team to resolve faults in the system are not made available for consumers using AMMs.

AMMs use a pricing algorithm to determine the value of each asset in the pool, while exchanges rely on order books to match buyers and sellers. This means that the price of assets on an AMM can be more volatile and subject to sudden fluctuations, which can lead to impermanent losses for liquidity providers. Exchanges, on the other hand, provide more stable pricing and may offer tools such as limit orders and stop-loss orders to help users manage risk.

In terms of risk, using an AMM carries the risk of impermanent loss, which is the difference in the value of the assets in the pool compared to the value of those assets if they were held individually. Impermanent loss can occur when the price of one asset in the pool changes relative to the other assets, which can lead to a reduction in the overall value of the pool.

Additionally, AMMs may also be subject to technical risks, such as vulnerabilities in the smart contract code or network congestion.

Using a crypto asset exchange carries different types of risk, such as security risks associated with centralised custody of assets and the risk of price manipulation. Additionally, exchanges may be subject to regulatory risks, such as changes in laws or regulations that could impact their ability to operate.

Overall, the key differences in risk between using an AMM and using the services of a crypto asset exchange stem from the decentralised nature of AMMs and the use of a pricing algorithm to determine asset values.