

Contact:  
Email:  
Phone:  
Our Ref:

3 March 2023

Director – Crypto Policy Unit  
Financial System Division  
The Treasury  
Langton Crescent  
PARKES ACT 2600

By email: [crypto@treasury.gov.au](mailto:crypto@treasury.gov.au)

Dear Sir / Madam,

#### **SUBMISSION BY CREO LEGAL TO TOKEN MAPPING CONSULTATION PAPER, FEBRUARY 2023**

### About Creo Legal

Creo Legal is a boutique commercial law firm with considerable experience in the web3, crypto, and digital assets space, having serviced crypto-related businesses since 2017. On average, 75% of our clients are startups or early-stage ventures, and half of those have a connection with web3, crypto, or digital assets (**Crypto**). We act for digital currency exchanges, Crypto project founders, investors, and service providers operating in the Crypto space.

In the absence of Crypto-specific legislation (other than in relation to anti-money laundering and counter-terrorism financing) and a historical body of case law, the advice we have given on the application of the *Corporations Act 2001* (Cth) (**Corporations Act**) and other relevant legislation has been reasoned from first principles, typically using the intention of Parliament as a starting point.

We consider ourselves to be a Crypto-native law firm. In our approach to advising Crypto-related clients, we give due consideration to, but are ultimately unrestrained by, the unwritten customs or norms of established industries such as financial and professional services, real estate, retail goods and services, gaming and wagering, and others. This touches on the essence of the Crypto industry which breaks boundaries in all directions, legally, socially, politically, and technologically.

### Submission

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

It cannot be denied that Crypto regulation is necessary. In our opinion, the fundamental driver of regulation ought to be consumer protection. However, as parts of the Crypto arena clearly extend beyond financial products and services, the Government must be clear and unambiguous in its

**Creo Legal** [creolegal.com.au](https://creolegal.com.au)

**E** [hello@creolegal.com.au](mailto:hello@creolegal.com.au) **O** +61 7 3184 9125

**A** Level 34, Waterfront Place, 1 Eagle Street, Brisbane QLD 4000

**P** GPO Box 307, Brisbane QLD 4001

Liability limited by a scheme approved under professional standards legislation.

approach. A failure to be so will stifle innovation, reduce domestic and foreign investment, push skilled Australian workers offshore, and deter overseas skilled workers from migrating to Australia.

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

As described in the consultation paper, the existing regulatory framework for financial products and services focuses on function (or substance) over form. While we generally agree with adopting a functional approach, this presents clear challenges for the Crypto industry, as functions (and forms) are fluid and modifiable due to the ubiquitous use of open-source software, and the inherent interoperability and composability of Crypto products and services (whether financial in nature or otherwise).

Consistent with the existing regulatory framework, in our view mandating some form of pre-contract or pre-investment disclosure would be the most practical, sensible and flexible safeguard for consumers and investors. In that regard, we consider it appropriate to maintain an exception for sophisticated investors using the existing eligibility criteria.

**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?**

As above, pre-contract or pre-investment disclosure ought to be the primary method of protecting consumers. In our opinion, mandating code auditing by law would be highly problematic for the following reasons:

- (i) Assuming that code auditing will be undertaken exclusively by the private sector, this would necessitate government oversight or licensing for code auditors, similar to private certifiers in the construction industry;
- (ii) The code auditing process would be difficult to standardise due to the fluid nature of the underlying software used in Crypto-related products and services. Continuing the analogy with private certifiers in construction, there are considerably more ways to code a piece of software for a specific function than there are ways to build a wall to hold up a roof.
- (iii) Aside from the process itself, the results of a code audit, due to its highly technical nature, would be difficult for consumers to compare against other code audits. Adopting a standardised rating system would necessarily import considerable subjectivity. This has been seen with the various initial coin offering ratings sites which are, in our estimation, entirely useless to the consumer.

**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?**

Maintaining a private sector of competing Crypto exchanges is critical in order for Australia to compete on the global stage. This means adopting a commercially sensible approach to

regulating such businesses. In our opinion, requiring Crypto exchanges to be legally responsible for vetting Crypto tokens and protecting consumers from scams will considerably raise the cost of compliance such that the vast majority of market players would be forced to cease operations.

Crypto exchanges cannot be regulated in the same manner as Tier 1 financial market operators. Establishing a highly-regulated walled garden for Australian Crypto exchanges will make it practically and economically impossible, if not highly undesirable, for domestic and foreign Crypto exchanges and token creators to make their products and services available to Australians.

In our view, it would be sensible to require Crypto exchanges to receive compliant pre-contractor and pre-investment disclosure information from token creators as a condition of being listed. Crypto exchanges could then act as intermediaries for the dissemination of such information to consumers seeking to acquire such tokens.

**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 network for the purposes of future legislation?**

For Crypto tokens, the concept of control is far more relevant and appropriate than the concept of possession given that distributed ledgers are stored on decentralised networks of hardware typically spread across the globe.

The inclusion of exclusivity may be limiting. We anticipate that non-exclusive, shared use and control mechanisms may arise in the future, particularly in relation to decentralised autonomous organisations and ‘public good’ Crypto assets and smart contracts. Today, it is possible to create a smart contract which gives the smart contract operator the right to redeem, destroy, or otherwise deal with a token held in a private user’s wallet. This possibility may already be inconsistent with the concept of exclusive use and control.

We prefer the concept of rivalrousness as this is sufficiently flexible to cover exclusive and non-exclusive use or control mechanisms.

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

Referencing the concept of ‘use and control’ in a general definition of a Crypto token would likely result in a broad legal definition which captures various types of tokens, such as non-fungible tokens (NFTs), which are not inherently financial or risky in nature. Tokens themselves do not necessarily require regulation. It is the token systems and Crypto assets which bear a much higher inherent risk to consumers.

**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?**

Creating an exhaustive, bespoke crypto asset taxonomy is a futile endeavour, given the pace of advancement and innovation in the Crypto space. While today many Crypto tokens, systems and assets relate to financial products, future tokens, systems and assets will relate to other aspects of society which will bear little to no risk to consumers. For these reasons, we generally agree with the approach of developing a high-level taxonomy which focuses on product function in order to more easily distinguish between risky and benign tokens, systems and assets.

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

We are not in favour of reinventing the wheel. The existing regulatory frameworks for financial products, commodities, personal property, privacy and data security, need only be augmented to ensure appropriate application to the Crypto space.

**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?**

Regulatory certainty can be easily achieved by specifically excluding certain types of Crypto tokens, systems, networks, activities, or assets, from the ambit of statutes such as the Corporations Act.

**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?**

The wrapping or tokenisation of a real world asset creates a financial derivative. If the wrapped asset is tradeable on a market, then any real world asset (whether traditionally an investment vehicle or not) can become financialised. Adopting the same regulatory treatment as the underlying asset may be problematic in certain circumstances. For example, a token representing a bail of hay is considerably more risky to the consumer than a bail of hay. However, consistent with our comments above, it is the Crypto asset issuer (such as the person who creates the market for the tokenised bails of hay to be traded) which is introducing risk and ought to be the focus of the regulation.

**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?**

Mandating a right of redemption may only be appropriate for certain types of real world assets, such as real estate and other assets which are traditionally used as investment vehicles. Redemption of underlying assets becomes decidedly less appropriate or

beneficial when considering the possibility of wrapping non-financial goods or assets, such as other Crypto tokens or assets, creative works and collectible items, and social, cultural, or political rights (e.g. votes).

**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?**

Yes. However, this must be balanced with the promotion of competition amongst crypto asset service providers. Due to the transparent nature of the Crypto space, competitive advantages commonly arise from efficient and innovative internal business structures and practices, collaborations and partnerships with third parties, and other aspects of businesses which are not publicly disclosed on the blockchain. Requiring such businesses to completely reveal their inner workings will inhibit their ability to compete in the market.

However, there are certain activities or arrangements which may require regulatory intervention and/or require public disclosure, such as:

- (i) asset custody arrangements for Crypto tokens, other assets, and fiat currency (for example, digital currency exchanges disclosing how they hold customer funds, including proof-of-reserves); and
- (ii) collaborations or partnerships giving rise to conflicts of interest, for example, paid referral arrangements, paid sponsorships, promotions, and endorsements, non-arm's length dealings which might otherwise appear to be arm's length (e.g. a code auditor being a related entity). These issues are already largely dealt with by the Australian Consumer Law.

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

Some initiatives may include:

- (i) pre-contract or pre-investment disclosure;
- (ii) segregation of customer funds from business working capital;
- (iii) minimum capital reserves, such as for digital currency exchanges and asset-backed tokens (e.g. stablecoins);
- (iv) maximum debt-to-asset ratios, such as for tokenised managed investment schemes and funds.

**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?**

We do not consider it necessary to specifically include certain types of intermediated Crypto assets which might otherwise not be captured by the existing definition of ‘financial product’ in the Corporations Act. The existing definition is sufficiently broad to capture products from which consumers might require protection.

Referencing the intermediation would be problematic given that intermediation of itself does not introduce risk to consumers, except where there are conflicts of interest or non-arm’s length arrangements (which can be addressed through pre-contract or pre-investment disclosure). Relying on the existing functional perimeter would be more appropriate across a broad and expanding set of possible circumstances.

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

For the above reasons, we prefer to rely on the existing functional perimeter.

**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?**

Creating a regulatory barrier-to-entry for new public Crypto networks is anti-competitive, discourages innovation, and is unlikely to be technology agnostic given that existing public Crypto networks compete against each other based on feature-set and technological or practical advantages. Introducing regulatory favouritism in a nascent industry will make Australia an unattractive jurisdiction for domestic and foreign Crypto businesses. Australian consumers will simply access or acquire wrapped assets issues overseas, rather than those issued domestically.

**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?**

No. The functional perimeter of the Corporations Act is sufficiently broad to capture intermediated Crypto assets which might be of concern from a public policy perspective. Once caught, the existing requirements for disclosure, target market determinations, etc., are more than sufficient to protect consumers.

**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?**

Disclosure of paid referral arrangements, paid sponsorships, promotions, and endorsements, non-arm's length dealings are important for consumer protection. These issues are already largely dealt with by the Australian Consumer Law.

For Crypto tokens, systems, or assets which are financial products, the existing provisions of the Corporations Act are more than sufficient to protect consumers.

**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?**

It would be virtually impossible to regulate free open source software. Introducing regulatory red tape would unnecessarily increase compliance costs for technology providers, thereby discouraging innovation.

There are currently no laws which require traditional (web2) software developers to be licensed, have their code audited, or undertake any form of regulatory compliance (aside from compliance with the Australian consumer law). The fact that software is open source does not increase the risk to the public.

If the original authors voluntarily release their code to the public on open source terms, anyone should be able to use it. Open source software has existed since the dawn of computing in the 1950's and we see no reasons at all (existing or new) to regulate its dissemination.

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

As above, the existing laws which encourage software developers not to engage in criminal, anti-competitive, anti-consumer behaviour, are sufficient to address any similar risks relating to smart contract applications. The fact that software is open source has no impact on this issue whatsoever.

**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 contracts involve no intermediary. In traditional finance, intermediaries such as brokers must be licensed and have appropriate insurance.

Smart contracts have a predictable and consistent function and behaviour, whereas conventional brokers are human beings with diverse interests and motives and who make mistakes, or perhaps break the law.

Smart contracts are transparent. All of the code and activities (transactions) of a smart contract are publicly accessible and reviewable by any person at any time. Conventional brokers operate private businesses and have no obligation or desire to disclose their activities to the public.

In our opinion, the predictability, consistency, and transparency of smart contract applications overcome the lack of regulatory oversight and insurance protection.

**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?**

As above, conventional pawn broker lending is markedly opaque compared to smart contract applications. The code and activities of smart contracts are public information and can be analysed by anyone at any time.

However, the anonymous or pseudonymous nature of smart contract interactions can make it difficult to analyse consumer outcomes if identities cannot be verified. For example, one person with two Crypto wallets can be executing a valid strategy for profit, even though analysing each wallet's activities may not indicate that any profit was generated.

Due to the poor availability of data in conventional financial services and the nascent nature of the Crypto industry, it does not appear presently possible to undertake a rigorous quantitative analysis on consumer outcomes.

The recent Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry showed that, despite the comprehensive regulatory regime in Australia, misconduct was pervasive even in traditional finance, resulting in poor consumer outcomes.

**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?**

The key differences in risk may be summarised as follows:

- (i) **Liquidity risk:** AMMs typically rely on liquidity pools to enable trading, which means that there may be less liquidity available for some assets compared to crypto asset exchanges. Due to the pricing mechanisms of existing AMMs, users may face a higher risk of slippage and price volatility.
- (ii) **Price discovery:** The price discovery mechanism is different for AMMs and crypto asset exchanges. AMMs use an algorithm to determine the price of assets, while crypto asset exchanges use traditional bid-ask order books to facilitate trades between buyers and sellers. There may be more price volatility on AMMs.



- (iii) **Transparency:** AMMs are completely transparent as the code and activities of their smart contracts are publicly accessible. However, Crypto asset exchanges facilitate trading using proprietary technologies and systems. Many Crypto asset exchanges use third party market making services and liquidity provider services which distort the natural forces of supply and demand in the market.
  - (iv) **Smart contract risk:** Since AMMs operate using smart contracts, this presents a security risk where there are vulnerabilities, bugs and other exploits which could be used by malicious parties to steal funds or otherwise cause loss to consumers.
  - (v) **Regulation:** Currently, Crypto asset exchanges in Australian and abroad are subject to some government and regulatory oversight (even if only from the perspective of anti-money laundering and counter-terrorism financing), which can provide some protection for consumers. AMMs, on the other hand, currently operate in a completely unregulated manner which means that users may be more exposed to fraud, scams and other criminal activity.
- b) Is there quantifiable data on consumer outcomes in trading on conventional crypto asset exchanges compared with user outcomes in trading on AMMs?**

Some Crypto asset exchanges voluntarily disclose their trading data, although the accuracy of such data may be questionable in the absence of mandatory disclosure by law. Undertaking a quantitative analysis would only be possible with the cooperation of major Crypto asset exchanges.

All trading data for AMMs are publicly accessible and may be analysed by any person at any time. However, the anonymous or pseudonymous nature of smart contract interactions can make it difficult to analyse consumer outcomes if identities cannot be verified.

We are open to engaging in further discussions with government and industry participants on a public or private basis.

Yours faithfully  
**Creo Legal**