MANUS FERRUM
CONSULTING

Guided Digital Evolution

A response to the Treasury's "Token Mapping Consultation Paper"

PREPARED BY MANUS FERRUM CONSULTING PTY. LTD.

ADMIN@MANUSFERRUM.COM

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

To provide a basic level of protection for investors and consumers of crypto products while providing a regulatory environment that encourages innovation and the free flow of information across crypto networks. In order to provide this environment the government will need to be open to frameworks outside of those that manage traditional financial products and services.

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

Safeguards should be in place to protect consumers and investors. However due to the open-source nature of the crypto ecosystem, regulators should adopt a 'less is more' approach. This will ensure appropriate safeguards do not hinder the development and maturation of the space. Regulators should focus more on providing objective information crypto services/products, rather than outright restricting or prohibiting activities (although this may be necessary in some cases).

By enforcing a detailed list of safeguards, the government would likely create unnecessary hurdles that would dissuade people who actively participate in the ecosystem and leave Australia at a competitive disadvantage.

The open-source and decentralised nature of many crypto assets make it practically impossible to implement the same level of "safety-nets" enjoyed in most traditional financial markets as a preventative measure.

However the permanent and unalterable nature of blockchains and cryptocurrency tokens allow for a method of accountability currently not associated with the space but proven by the U.S. Department of Justice.[1]

Therefore establishing a registry or body that crypto projects can voluntarily register information with will provide a more reliable safety net for consumers and investors. Government-managed portals such as NSW's *Energy Made Easy* or Commonwealth *Smart Traveller* websites will provide a portal for such information. This information could include links to the crypto project website, any related government analysis, etc.

---

[1] Examples: *Colonial Pipeline Extortionists caught* and *Bitfinex Hack*

Q3a) 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 discussed in response to Question 2, a database consisting of basic information regarding each distinct crypto network and token would potentially be beneficial. For example, if the founding development team of a crypto token are publicly known this information could be verified by a government database similar to Smart Traveller or Energy Made Easy. There could also be an option for crypto token projects to submit information to this database for verification.

This database should not form any kind of mandatory reporting regime as this would stifle innovation and would be difficult to meaningfully enforce in the crypto ecosystem. As part of the database, government may also want to consider reviews of a project's GitHub repository to provide further validation of code integrity noting this is a specialised skillset.

The constant evolution and global decentralised nature of many cryptocurrency projects presents a unique challenge to regulators. For example, the relative lack of available knowledge & expertise mean it is very difficult to conduct meaningful code auditing and whitepaper reviews, especially as crypto assets and products continually change function/use case. Therefore the focus should be on verifying the development/founding teams behind crypto projects.

The team is likely to be the most enduring element of a project, and also comprises individuals and sometimes legal entities to which enforcement can be applied. Noting this, there will still be an onus on consumers to understand and stay updated with tokens/projects. To qualify for registration on this database, developers would also need to adhere to a minimum level of communication and published updates, e.g. annual roadmap reports which the project should submit to the database.

Note: the above requirements would not apply to certain crypto network tokens such as Bitcoin, as in our opinion they do not constitute financial products.

Q3b) 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?

As discussed in response to Question 3a, a database consisting of basic information regarding each distinct crypto network and token would potentially be beneficial. In addition, the government could establish a policy specifically for crypto exchanges that manages and in turn audits an established risk matrix/framework (or scorecard) for offering crypto tokens.

This framework would categorise crypto assets on a sliding scale of risk in relation potential scam/fraud. This information could then be used to produce a scorecard result which would provide more information and protection to consumers.

This requires exchanges to demonstrate due diligence and provides an avenue for regulators such as ASIC & AFCA to more clearly identify lack of compliance and mitigate or obviate any potential penalties enforced against an exchange.

This 'scorecard' information could include:

- Project team details registered on a government database
- Potential/free-floating market cap
- Duration of project to date
- Team size
- Number of exchanges listing the token
- Historical papers/published information detailing updates of the project (demonstrating active development)

Q4a) 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?

he concept of 'exclusive use or control' should be a characteristic of any general definition of crypto token and network. It may be that exclusive use or control is a necessary but perhaps not sufficient characteristic of a crypto token/network under future legislation.

Given the profusion of different types of crypto tokens/networks and the high likelihood of continuing novel variants, exclusive use or control could form a key part of a multiple indicia test when defining crypto tokens/networks. Additional potential indicia could include:

1. *Distributed Ledger Functionality*: sufficiently decentralised consensus mechanism of funds provided by the network via computer networks.
2. *Pseudonymous addresses*: allow for a degree of anonymity in processing transactions (i.e. participants are publicly identifiable only through their public address)

Q4b) What are the benefits and disadvantages of adopting this approach to define crypto tokens and crypto networks?

The approach provides an appropriately flexible framework that captures the essential characteristics which collectively distinguish a crypto token/network from other forms of assets, products and data. By not strictly defining a set of criteria, the definition can adapt to evolving technology and use cases.

A disadvantage of this approach is that the set of indicia is not prescriptive which reduces certainty.

Q5a) What are additional supporting reasons or alternative views on the value of a bespoke taxonomy?

We agree that an exhaustive bespoke taxonomy has minimal regulatory value for the same reasons briefly mentioned in the paper (i.e. possible functions are too broad to meaningfully capture). A high-level taxonomy is preferred.

The crypto space is still new, with numerous products/services being proposed and tested. It would not be appropriate to create a detailed taxonomy at this time since the industry is rapidly changing and new functions/use cases are proliferating. As a result a high level taxonomy based on a set of key functions is the most appropriate at this stage.

Q5b) What are your views on the creation of a standalone regulatory framework that relies on a bespoke taxonomy?

Given the evolving nature of crypto assets a meaningful standalone regulatory framework may be difficult to establish. Therefore for the foreseeable future any framework should be kept high-level and when possible, map to the traditional financial services framework as closely as possible without undermining innovation and consumer freedoms.

Q5c) 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?

Firstly, clear identification of the responsible regulator. Secondly, clear guidance from said regulator as to the relevant carve outs in existing and future financial services legislation for crypto assets used in a non-financial manner

Q6a) 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?

There should be regulatory requirements on any entity offering wrapped real world assets. If a crypto asset purports to wrap a real world asset, the regulations relating to that real world asset should be applied as far as practicable to the corresponding token and its issuer.

Q6b) 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?

Yes, there will be a requirement to impose additional disclosure requirements on issuers of wrapped real-world assets to ensure that rights are assigned to owners of the wrapped real-world assets. This will assist in the ability to enforce those rights if the issuer defaults or the wrapped asset is compromised.

As part of this, issuers should be required to demonstrate proof of sufficient assets to back the value of wrapped real world assets issued on a 1:1 basis. For reference a similar regime has been proposed in Singapore (*MAS Framework*).

Q7a) 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 would be better for crypto asset service providers to have a government sponsored database to refer users to similar to Smart Traveller. That said, short summaries of tokens listed on a crypto asset service provider including links to token whitepapers etc. may be useful.

This practice is already taking place in a limited manner on existing crypto exchanges such as Binance and Swyftx.

Q7b) What are some other initiatives that crypto asset service providers could take to promote good consumer outcomes?

Relevant initiatives include risk management courses and scam/fraud awareness courses tailored to address common issues in the crypto/digital asset environment.

Q8a) What are additional supporting reasons or alternative views on the value of a bespoke taxonomy?

The following intermediated crypto assets ought to be specifically defined as financial products because they are issued with an expectation of return on investment. The issuer will also generally be charging a fee.

1. Wrapped real world assets
2. Crypto token staked for the sole purpose of earning a financial benefit
3. Crypto assets provided as collateral or liquidity for a financial service or dealing such as a loan.

Q8b) What are additional supporting reasons or alternative views on the value of a bespoke taxonomy?

Crypto asset provider staking services where an exchange charges a fee for providing the staking service should specifically defined as financial products. An example of this would be a service that advertises 5% APY but charges a 0.5% fee for service. This is because they are service offerings which charge a fee with an expectation of return.

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?

The following factors may be useful in assessing suitability of a public crypto network to host wrapped real world assets:

1. Sufficient decentralisation (for example, measured by Nakamoto Co-efficient)
2. The manner of launching of the project (e.g. pre-mining, early release of token tranches to private investors)
3. Robust code auditors perhaps measured by developer contributions and independent stress tests

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. If an intermediated crypto asset is not covered by the financial services framework of the kind proposed by the consultation paper then they do not need additional regulation. This is because the proposed framework covers those assets and networks that need to be regulated.

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?

No, the current regulation surrounding the marketing and promotion of financial products/services should be sufficient to use within the crypto ecosystem as current frameworks regulating marketing and promotion of crypto products would be sufficient.

Q12a) What are the regulatory and policy levers available to encourage the development of smart contracts that comply with existing regulatory frameworks?

As discussed in response to Questions 2 and 3a, a database consisting of basic information regarding each distinct crypto network and token would potentially be beneficial.

Q12b) What are the regulatory and policy levers available to ensure smart contract applications comply with existing regulatory frameworks?

At this point in time we are unaware of regulatory/policy levers that would be effective in ensuring smart contract applications comply with existing regulatory frameworks.

Q13a) What are the key risk differences between smart-contract and conventional pawn-broker lending?

Smart-contract lending has the potential to reduce counterparty risk for lenders as collateral is often drawn from a large decentralised pool of assets and recovery of collateral is automated. On the other hand smart contract lending does not have an identifiable party against which collateral claims can be enforced.

Regulating pawn-broker lending smart contracts is significantly harder as theoretically anyone could anonymously create and enter into a smart contract with consumers in Australia under any agreed terms and conditions.

Q13b) Is there quantifiable data on the consumer outcomes in conventional pawn-broker lending compared with user outcomes for analagous services provided through smart contract applications?

As far as we are aware quantifiable data of this kind is not available.

Q14a) What are the key differences in risk between using an AMM and using the services of a crypto asset exchange?

Use of an AMM presents the following risks when compared to crypto asset exchanges:

1. Impermanent loss

Use of AMMs create exposure to impermanent loss. Impermanent loss is the decreased value of your assets within a liquidity pool compared to an equal investment of the same assets held outside of a liquidity pool. This occurs whenever there is a price change of the token/s from when they were initially deposited in the pool.

The larger the price movement that occurs from the initial deposit, the larger the impermanent loss. Impermanent loss can be thought of as an unrealised opportunity cost. The loss is measured by the difference between the value of an investment into a liquidity pool against holding the same investment outside of a liquidity pool. Since liquidity pools are programmed to maintain a certain ratio of tokens (e.g. 1:2), the implicit price of both tokens changes to accommodate this, which may not reflect the actual market price movements.

Impermanent loss occurs in any decentralised exchange that facilitates liquidity pools. The loss suffered is also generally higher for investors that deposit crypto-assets with higher volatility. Liquidity providers receive fees from trades made within the liquidity pool which serves as a way to offset the impermanent loss incurred. Many AMMs also use different pricing functions, in attempts to further reduce impermanent loss.

2. Programmable market depth

The price of tokens within a liquidity pool is determined by the programmable ratio set by the creator of the pool. For this reason, the size of the liquidity pool has to be large enough so that individual trades do not dramatically change the price of the token pair. In traditional exchanges market depth is created by users submitting buy and sell orders at various price points. Usually these orders are heavily weighed near the current market price meaning it would take a large volume of trades to move the price considerably.

In AMMs however, this market depth is not driven by “investor-demand” but by the automatic price function which maintains the ratio. Therefore if the AMM is not large enough to accommodate a period of high trading volume, then significant price slippage would occur since the liquidity pool will automatically adjust the pool to maintain the token ratio. In essence, a traditional exchange would likely avoid the same price slippage since traders will dynamically alter their orders respectively. In AMMs, it is difficult to avoid this price slippage if the liquidity pool lacks sufficient size.

3. Increased susceptibility to frontrunning and other market manipulation tactics

The code-driven nature of AMMs means it is much easier for bad actors to predict the outcome of certain trades since it is programmatically determined. Additionally, the existence of the Mempool which allows people to view unconfirmed transactions further increases this vulnerability.

As a result, AMMs are much more susceptible to illegal trading activity compared to traditional exchanges. Examples of commonly used strategies include frontrunning, backrunning, wash trading and sandwich attacks.

Q14b) Is there quantifiable data on consumer outcomes in trading on conventional crypto asset exchanges compared with user outcomes in trading on AMMs?

Yes. One of our directors has written a research thesis that relates to the topic. This thesis found that AMMs are generally the first to reflect new information into prices (i.e. price discovery) compared to centralised crypto-asset exchanges.

For consumers this means that prices in AMMs can more accurately reflect the asset's market value faster than traditional asset exchanges.

Please find the links to the aforementioned research thesis and related video explainer

ADMIN@MANUSFERRUM.COM