Regulating Crypto Assets in Australia

Response to Treasury Consultation Paper – "Crypto asset secondary service providers: Licensing and custody requirements"

Scott Robert Chamberlain
ENTREPRENEURIAL FELLOW, ANU COLLEGE OF LAW

Regulating Crypto Assets in Australia

Response to Treasury Consultation Paper

1. Summary

1.1 This paper is in response to The Treasury's consultation paper "Crypto asset secondary service providers: Licensing and custody requirements". It makes the following ten recommendations.

(a) **Define Crypto Networks:** Crypto assets cannot be defined without first defining the networks on which they exist. Only representations of value or use rights on proper crypto networks should be considered crypto assets.

(b) **Adopt Five Crypto Asset Classifications:** Crypto assets should be divided into five categories: Network Tokens, E-money Tokens, Investment Product Tokens, Proprietary Rights Tokens, and Utility Rights Tokens.

(c) **Define Ownership Rules:** Crypto assets are a new form of property that need greater clarity around when they are controlled and owned.

(d) **Adopt Four CASSPr Classifications:** CASSPrs should be grouped according to their function and differentially regulated according to both the functions they perform and the nature of the assets in which they deal.

(e) **Adjust Traditional Rules Where Warranted:** The problem of regulatory overlap is unavoidable because of the risk of regulatory arbitrage. Instead, traditional regulations should be adjusted or waived where the nature of crypto assets makes compliance unnecessary or impossible.

(f) **Account for Smart Contracts:** Some smart contracts still controlled by their development teams should be considered CASSPrs.

(g) **Consider Regulating Oracles:** Oracles should be regulated because crypto networks depend on them to learn the truth about real world events that might trigger on-chain transactions.

(h) **Lighter Regulation for Inter-operators:** Lighter regulation should be considered CASSPrs that are technically exchanges but are focussed on providing cross-chain interoperability solutions.

(i) **Fix Negotiability:** Consider specific rules for exchanges to ensure consumers get good title to the assets they purchase while protecting the victims of scammers.

(j) **Custodians of Crypto Assets:** The idea of custodians as trustees is strongly supported and should be extended to specific regulations around crypto asset rewards.

1.2 The reasons for these recommendations, and suggested legislative definitions, are set out below.

2. Recommendation 1: Define Crypto Networks

2.1 In answer to Question 3 of the Consultation Paper, ASIC's definition of "crypto asset" is inappropriate because a crypto asset is not just a digital representation of value involving cryptography. This could describe Qantas frequent flyer points in an encrypted database.

2.2 Crypto assets are data entries in a special type of database hosted by a particular type of distributed network such that the entry is sufficiently certain, identifiable, alienable, and transferrable as to be property under common law.

2.3 To properly define crypto assets, we need to properly define the special nature of these distributed networks on which crypto assets exist.

Proposed Definitions

2.4 These are the prosed definitions:

(a) **Crypto asset** means a representation of economic, proprietary, or access rights stored in the canonical shared state of a decentralised public network which is self-contained, uniquely identifiable, and has a value or use.

(b) **Decentralised public network** means a publicly accessible network of multiple independently owned computers that exhibits all the following attributes:

(i) Each computer runs compatible code that uses a byzantine fault tolerant consensus protocol to agree on and maintain a canonical shared state across multiple computers.

(ii) The code each computer runs to be part of the network is open-source code.

(iii) The network's canonical shared state is public.

(iv) The network uses a public key pair cryptography scheme to authenticate messages submitted on the network.

(v) Anyone can create a key-pair to become a user of the network, even if not all users have the same use rights.

(c) **Key pair** means the mathematically or algorithmically paired public key and its corresponding private key (or combination of private keys through a multi-signature arrangement), or substantially similar analogue, such that a message signed with the private key can be authenticated using the public key.

(d) **Multi-signature arrangement** means a system of access control in which two (2) or more private keys are required to sign and submit a message, or any substantially similar analogue, to a decentralised public network.

(e) **Open-source code** means, in respect of a network, software source code that is publicly available to use and modify without charge for purposes associated with that network, even if it is not publicly available free of charge for other uses or purposes.

(f) **Private key** means a unique element of cryptographic data, or any substantially similar analogue, which is:

(i) Held by a person.

(ii) Mathematically paired (alone or in combination with other private keys through a multi-signature arrangement) with a public key.

(iii) Associated with an algorithm that is necessary to cryptographically sign and submit messages on a decentralised public network.

(g) **Public address** means a payment endpoint for crypto assets on the network typically, but not always, derived from or associated with a user's public key.

(h) **Public key** means the unique, publicly available element of cryptographic data, or substantially similar analogue, of a key pair.

(i) **User** of a decentralised public network means any person who

(i) holds a private key used to interact with that network (alone or as part of a multi-signature arrangement):

(ii) controls a computer or device that holds a private key used to interact with that network (alone or as part of a multi-signature arrangement).

Use Definitions Consistently Across All Areas of Regulation

2.5 These definitions should be used across all Australian regulatory frameworks. The term "crypto asset" should refer only to a representation of economic, proprietary, or access rights stored in the canonical shared state of a network considered a decentralised public network.

2.6 The definition of decentralised public network is designed to cover those blockchain projects that are "genuinely" decentralised. There will be many blockchain projects that do not, or cannot, fit this definition, and that is its whole point. Data entries should not be considered property unless they exist on a decentralised public network.

3. Recommendation 2: Five Crypto Asset Classifications

3.1 In answer to Questions 29-31 of the Consultation Paper, the following (exhaustive) five classifications of crypto assets are proposed.

(a) **Network token** means a crypto asset that is an unbacked medium of exchange or unit of account on a network with no identifiable counterparty other than the network itself.

(b) **E-Money token** means a crypto asset that is not a network token and satisfies at least one of the following:

(i) It represents a deposit of an equivalent value of sovereign fiat currency.

(ii) It represents a promise or understanding to redeem the token for a fixed value of a sovereign fiat currency, or goods or services of equivalent value.

(c) **Securities Token** means a crypto asset that:

(i) Is not an E-money token or a Network Token.

(ii) Embodies rights to financial returns from, or participation interests in, investment vehicles of the kind emblematic of securities.

(d) **Proprietary Rights Token** means a crypto asset that:

(i) Is not a Network Token, E-Money Token, or a Securities Token.

(ii) Embodies rights or claims to tangible or intangible property.

(e) **Utility Rights Token** means a crypto asset that is not any other kind of crypto asset, typically those embodying on use or access rights to networks, services, or memberships.

3.2 There are no types of crypto asset that should be banned.

4. Recommendation 3: Define Ownership Rules

4.1 In further answer to questions 29-31, it is not enough to simply define or classify crypto assets. Crypto assets are a new form of property. They are intangible but capable of possession through control of the private key.

4.2 To properly regulate CASSPrs in relation to their dealings with crypto assets, it will be necessary to also clarify the nature and rules governing their ownership.

Nature of Crypto assets

4.3 The government should clarify that on creation, a crypto asset is:

(a) A digital chose in possession.

(b) Possessed by the user that controls it.

(c) Capable of assignment at will.

(d) Capable of being the subject of a security interest or trust.

(e) A chose in possession even if it was intended on creation to embody rights or claims otherwise indicative of a chose in action.

4.4 Something like paragraph 3.4(e) is necessary because choses in action often have legal restrictions on assignment and cannot be stolen (since they cannot be possessed). But crypto assets can trade at will on decentralised public networks. If a counterparty wants to restrict who can own or trade an asset that embodies rights against them, they need to use the network's rules, not legal authority to enforce such restrictions.

Control vs Ownership

4.5 Crypto enthusiasts often insist "Not your keys, not your coins" by which they mean if you do not control the private keys, you do not own the assets. But if crypto assets are truly a form of property, there must be a distinction between ownership and control, one that becomes relevant when considering the rules for custodians.

Control of Crypto assets

4.6 A user controls a crypto asset if the user holds a private key that can (alone or as part of a multi-signature arrangement, but independent of any other user) cryptographically sign and submit a message to a decentralised public network that:

(a) Exercises any type of access right or function because the network exclusively associates that crypto asset with the user.

(b) Removes the crypto asset from its exclusive association with the user.

(c) Moves or returns that crypto asset to its exclusive association with the user.

or any substantially similar analogue for the user having exclusive, independent control of the crypto asset or of the access rights associated with control of the crypto asset.

Ownership of Crypto assets

4.7 A person who controls a crypto asset should be treated as the owner that asset unless they acquired control of the crypto asset in bad faith or with actual or constructive knowledge of another person's prior claims to the crypto asset.

4.8 A person should always be regarded as having actual or constructive knowledge of another person's prior claims to a crypto asset if they hold the private key that controls the crypto asset:

(a) Through illicit or dishonest means.

(b) On the express or implied condition or understanding that it would only be used with the consent of the crypto asset's legal owner.

(c) As part of a multi-signature arrangement established by the crypto asset's legal owner.

4.9 The customers of a crypto asset custodians should always be treated as the legal owners of the crypto assets the operator holds on their behalf. The custodian should not be able to apply those assets to capitalise its own operations or meet its own debts.

4.10 These proposed rules give crypto assets negotiability. It is important that other users be able to assume that, barring bad faith or prior knowledge, they acquire good title to the asset from the person who possesses it. Otherwise, the common law rule that you can only give what you have would lead to endless (and probably fruitless) litigation between users.

Airdrops, Forks, and Staking Rewards

4.11 There are many ways networks and smart contracts give users control of crypto assets without the user necessarily doing anything to acquire that control. These things are generally a type of reward – a new asset that arises from a network or a smart contract as an airdrop, staking reward, or the consequence of a network fork.

4.12 We define these crypto asset rewards follows:

(a) **Crypto asset reward** means a crypto asset that comes into a user's control because of:

(i) Their control of other crypto assets.

(ii) Their usership of the network.

(iii) Their network conduct.

(iv) A change to the decentralised public network's rules.

(v) A fork of any part of the decentralised public network's rules.

4.13 Users need clarity around when they are deemed to control and own these assets. It is important because of the tax consequences. Users need to be able to *not claim* ownership and control to avoid holding assets they don't desire or attracting unwanted tax liabilities.

4.14 A user of a decentralised public network should be deemed to have acquired a crypto asset reward at the earliest of the following times:

(a) If:

(i) they were required to do anything within the rules of the decentralised public network for them to control the crypto asset; and

(ii) they did those things in expectation or understanding they would receive the crypto asset reward,

then the moment the crypto asset came into their control.

(b) In any other case – the first moment they initiate any valid transaction within the rules of the decentralised public network in respect of any of the crypto asset rewards.

Security Interests in Crypto Assets

4.15 Since crypto assets are a form of personal property, the ability to create and enforce security interests in that property in favour of third parties needs to be considered.

4.16 A user who controls a crypto asset subject to a security interest:

(a) Should be required, so far as is possible, given the rules of the decentralised public network:

(i) To use their private keys to give effect to the security interest.

(ii) To refrain from using their private keys contrary to the security interest.

(b) Should not be held liable for any breach of the security interest except to the extent that breach arises from their non-compliance with section 4.18 above (for example, if the asset is destroyed because the network fails, or its users vote to implement code changes).

Disposal of Crypto assets

4.17 A user should be considered to no longer own a crypto asset the moment all the following are true:

(a) They cease to control the asset.

(b) They either have no legal rights, or have abandoned any legal rights they might have, to compel another user (for example, as a custodian) to sign and submit a message with that other user's private key that would constitute control.

5. Recommendation 4: Regulate Four Different Types of CASSPr

5.1 In answer to question 1 of the Consultation Paper, the proposed definition of CASSPr is inappropriate because it is too broad.

5.2 While the name and the text of the Consultation Paper indicate that it is supposed to capture only "secondary service providers", the actual text of the definition is so broad as to capture miners/validators of the chains themselves because they are arguably involved in holding and transferring crypto assets on behalf of users, often in return for fees.

5.3 So, regardless of the acronym, the content of the definition needs to match the label on the tin and focus on "secondary service providers" who are users of the network on behalf of customers (they have their own key pair for interacting with the network). This means three things:

(a) The definition should exclude miners and validators. You cannot provide secondary services if you are the chain itself. This prevents miners/validators from being considered custodians or exchangers of the crypto assets manifested on the chain they underpin.

(b) The definition should include only those service providers that are users of the network, in that the nature of the service requires it to have its own public/private key pair on one or more underlying chain. This excludes those entities, like non-custodial wallets, that give people the tools they need to interact with the chain, rather than being the service that interacts with the chain on the user's behalf.

(c) The definition should also exclude someone who participates in the provision of financial services related to an offer or sale or a crypto asset. Unless they are interacting with the chain via a key pair on a client's behalf, they are not a CASSPr.

Four Different CASSPrs According to Function

5.4 In answer to Question 2 of the Consultation Paper, CASSPrs should be separately defined and regulated according to the function they perform on behalf of users of the chain. Four discreet functions are suggested as follows:

(a) **Crypto Asset Exchanges:** the principle activity is providing a marketplace for people to buy and sell crypto assets for fiat or other crypto assets. They should be licensed and regulated in a way consistent with their market-making function and any custody function they perform.

(b) **Crypto Asset Custodians:** the principle activity is storing or holding crypto assets on another's behalf. They should be licensed and regulated in a way consistent with their custodial function.

(c) **Crypto Asset Oracles:** the principle activity is informing the network about the state of the outside world. These entities have received insufficient scrutiny. Oracles can be both software agents and actual people or professionals. Chains need oracles to be reliably informed about the state of the world outside the chain. The trusted nature of this function means oracles should be regulated.

(d) **Crypto Asset Interoperability:** the principle activity is to allow networks to interoperate so that crypto assets on one chain are instantly swapped for assets on another chain.

Different Regulations for Each Function

5.5 In answer to Questions 5-10 of the Consultation Paper, the policy objectives are all suitable, but there should not be a one-size-fits all licence regime for CASSPrs.

5.6 Licence requirements and conditions for CASSPrs should be tailored to their function. Exchanges that custody assets while providing a market require different regulation from pure custodians that have no marketplace services.

5.7 Further, each CASSPr should be separately accredited depending on the types of assets with which they wish to deal. Digital currencies are different from tokenised shares or real estate, which are different again from Bored Ape NFTs. CASSPrs should not be lumbered with the relatively expensive and useless KYC/AML/CTF regulations if they are only dealing in assets that are not money or money-like.

6. Recommendation 5: Adjust Traditional Rules

6.1 In answer to Question 10 specifically, differentiated regulation by function and type minimises, but does not eliminate, regulatory duplication. Elimination is impossible without regulatory arbitrage as everyone will simply wrap a blockchain token around their traditional financial product and call it "crypto".

6.2 Instead, special rights and exemptions will be needed where traditional rules are irrelevant, or even harmful, given the purpose of the protections, the nature of the crypto asset, and the nature of the chain on which it exists.

6.3 For example, a crypto asset controlled by a series of smart contracts might be a managed investment but meeting the requirements for anyone to be an independent trustee or manager might be irrelevant or even impossible. The answer isn't to give CASSPrs a one-stop-discount-shop for selling securities to the public without a prospectus. The answer is to adjust the managed investment registration rules so that licensed CASSPrs can register managed investments schemes involving crypto assets without needing a trustee or manager.

7. Recommendation 6: Account for Smart Contracts

7.1 In response to questions 5-10, the government should consider that people are not the only potential service providers in crypto asset ecosystems, so regulation may also need to account for some smart contracts.

7.2 Smart contracts can be defined as follows:

(a) **Smart contract** means a collection of code and data deployed to multiple (but not necessarily all) computers on a decentralised public network that users interact with via messages cryptographically signed with their private key.

7.3 Smart contracts can be divided into three categories:

(a) **Network smart contract** means a smart contract where all the following is true:

(i) Any user of the network can interact with it.

(ii) All its code is open-source code.

(iii) Its code cannot be changed or disabled, except through a governance process open to all users by virtue of being users of the network.

(b) **Community smart contract** means a smart contract where all the following is true:

(i) All its code is open-source code.

(ii) Its code can be changed or disabled by a sub-set of the network's users, such as those that interacted with the contract or who own governance tokens or some other right not available to other users by virtue of being a user of the network.

(c) **Developer smart contract** means any smart contract that is not a network or community smart contract, and includes a smart contract where any of the following is true:

(i) Any part of the code is closed source.

(ii) Its developers and promoters (alone or through a multi-signature arrangement) retain preferential rights to unilaterally edit or disable the contract, including through mechanisms such as a kill switch, a master set of private keys, or manufactured dominance of governance rights.

7.4 In the context of regulating CASSPrs:

(a) A network smart contract is part of the network and so should not be considered a secondary service provider.

(b) A community smart contract is a user of the network, but one that lacks legal personality. Neither the contract nor its developers or users should be considered Secondary Service Providers.

(c) However, a developer smart contract is an agent of the developer such that anything done by the developer smart contract is deemed done by the developer as a user of the network.

7.5 Developer smart contracts should be defined, treated as a secondary service provider, and required to hold whatever licences or accreditations that a non-smart contract-based service has. This will better protect users while incentivising projects to become genuinely decentralised.

8. Recommendation 7: Consider Regulating Oracles

8.1 In response to questions 5-10, the government should also consider regulating oracles.

8.2 Crypto networks do not know any truth outside the network. For any information on the state of the outside world – prices, identity, verifications, certifications – they rely upon oracles.

8.3 We would define oracles as follows:

(a) **Oracle** is a person, computer, or decentralised public network that feeds off-chain data to a decentralised public network with the purpose or potential to influence transactions on the network.

(b) **Warrants the accuracy of the data** means:

(i) If the oracle is feeding data from a third party, it accurately reports the third party's data, not that the third party's data is accurate.

(ii) If the oracle is feeding data it owns, controls, or represents it has verified, it warrants the data is true, not just that it is truthfully reported.

Oracle Warranties

8.4 Oracles are thus a form of secondary service provider unique to crypto networks. Because information from oracles can automatically trigger on-chain transactions, their reliability is crucial. Their trusted role makes it worth considering oracle-specific regulations.

8.5 If the oracle is a person, that person should warrant the accuracy of the data to all users of the network, subject to any lawful terms and conditions of service communicated publicly to the entire network.

8.6 If the oracle is a computer, the person operating the computer should warrant the accuracy to all users of the network, subject to any lawful terms and conditions of service communicated publicly to the network.

8.7 If the oracle is multiple computers that comprise a decentralised public network, then no liability should arise.

No Liability for Third Party Data Providers

8.8 Since oracles often feed their data from third party data sources, those third parties need to be protected. Absent fraud, any third party from whom an oracle sources data should not be liable in law or equity to anyone for any kind of loss, damage, or suit arising in any way from any network's use of that data, even if the third party was in any way aware of, or agreed to, the oracle's use of their data.

9. Recommendation 8: Lighter Regulation of Interoperability

9.1 In response to questions 5-10, the government should consider tailored (lighter) regulations for exchanges that are really interoperability solutions.

Interoperability Prevents Silos

9.2 One major problem for crypto networks is interoperability. It is hard for networks to talk to each other, meaning assets and the value they represent become siloed. It's like if you could not send email between Hotmail addresses.

9.3 To solve this problem requires interoperability service providers. These entities function like exchanges, straddling chains while providing a common interface for users. But they are conceptually distinct because they involve automated swapping of tokens like swapping packets of information. They will grow in importance as the need for interoperability between chains increases.

Interoperability Should Be Regulated Lightly

9.4 The phrase "Internet of Value" and "moving value like information" are dreams that necessitate interoperability is same way we can send and receive emails without using the same email client. The main barrier to this innovation are money transmission laws which turn a simple exchange of information into a regulated friction point.

9.5 To facilitate interoperability, the government should consider tailored (lighter) regulation of interoperability solutions, like Interledger Protocol (https://interledger.org/) in the same way routers have been given exemptions from privacy and IP laws to facilitate information flows across the internet.

10. Recommendation 9: Negotiability and Consumer Protection

10.1 In response to questions 5-10, the government should consider rules to ensure consumers receive good title to crypto assets they purchase through exchanges while also protecting consumers against scammers.

Crypto Currency Exchanges Warrant Good Title

10.2 Crypto asset exchanges are the main touch point between code-governed communities and the outside world. They are also the main point through which ill-gotten assets are liquidated into other assets or fiat currency. Exchanges are therefore best placed in terms of resources and information to maintain the systems necessary to catch scammers and "make whole" their victims.

Proposed Regime

10.3 The proposed regime would have three elements:

(a) **Exchanges warrant good title:** First, exchanges should be required to warrant good title to all who purchase from their platforms. A person buying from a licenced exchange should be assured of good title.

(b) **Exchanges Compensate Victims:** Secondly, exchanges should be required to compensate any person whose stolen assets were sold through the exchange if the exchange had prior knowledge the assets were tainted. An exchange should be deemed to have knowledge if advised by a reputable block explorer/forensic business that the assets come from a tainted or blacklisted address.

(c) **Exchanges Have Freeze Powers:** If the operator of a crypto asset exchange service receives a crypto asset that it reasonably believes is subject to a prior claim, the operator should be able to:

(i) Refuse to accept the crypto asset.

(ii) Accept the crypto asset but hold it separately on trust until the competing claims are resolved, or otherwise directed by law.

(iii) Transfer the crypto asset within 21 days to the party it reasonably believes is the rightful legal owner.

(iv) Advise both parties of the identity and contact details of the other.

(v) Report the transaction to law enforcement.

10.4 This suite of rights and obligations would incentivise people to use licenced exchanges (they are guaranteed good title) and protect consumers from scams by incentivising exchanges to use their resources and knowledge to avoid dealing in tainted assets.

11. Recommendation 10: Custodians of Crypto Assets

11.1 The Consultation Paper notes that custodians will be required to hold their customers assets on trust. This is such an important obligation, support for it should be emphasised.

Definition of Crypto Custodian

11.2 A crypto custodian can be defined as follows:

(a) **Custodian of a crypto asset** means a person who controls a crypto asset they do not exclusively own, and always includes:

(i) The operator of a crypto asset exchange service in respect of the crypto assets its customers have left in the operator's control.

(ii) The developer of a developer smart contract in respect of the crypto assets they control because of users' interactions with the contract.

Obligations on Custodians

11.3 Custodians of crypto assets are in a powerful position because, like how land title registries don't record beneficial ownership of land, the networks will be unaware of the assets real owners and treat the custodian as the owner when it comes to exercising any benefits attached the assets.

11.4 Unless otherwise agreed in writing, the custodian of a crypto asset (other than a community smart contract) should always hold that crypto asset on trust for the benefit of the legal owner of the crypto asset.

11.5 The fact custodians hold crypto assets on trust should imply further additional obligations to not, without the express consent or direction of the legal owner of the underlying crypto assets:

(a) Deal with the crypto asset.

(b) Create a trust or security interest of any kind over the crypto asset for the benefit of any third party.

(c) Apply the crypto asset for its working capital of to satisfy its creditors.

(d) Lend the crypto asset.

The Problem of Crypto Asset Rewards

11.6 Finally, it should be noted that crypto assets have the problem of crypto asset rewards (previously defined) like forks, staking rewards, airdrops, and voting rights which can accrue to the on-chain controller of an asset. It may require special steps or technical upgrades to avail the owner of these rewards, but they can be exceedingly valuable.

11.7 Given that custodians are to be trustees of their client's assets, regulations should specifically provide for crypto asset rewards as follows:

(a) Custodians must be prohibited from acquiring for themselves any crypto asset rewards that accrue to them by virtue of their control of their client's crypto assets. This is consistent with a fiduciary's duty against self-dealing and conflicts of interest.

(b) Custodians must not unreasonably fail or refuse to pass through all crypto asset rewards to their clients. Clients should be able to expect that custodians will institute reasonable technical upgrades to claim any such rewards.

(c) Custodians must be required to pass through all crypto asset rewards to clients if the custodian has accrued the same crypto asset rewards on crypto assets it owns outright. If the custodian can claim a reward for themselves, they should also claim it for clients.

****End of Response****

Scott Chamberlain

26 May 2022