Treasury TOKEN Mapping Consultation Response

Dr Adrian McCullagh

All the consultation questions, posed in the Mapping paper, are listed below together with my responses. Before, I detail my responses, I wish to thank the department for this opportunity to respond to the detailed questions set out in the consultation paper. From a policy perspective, parliament does have a difficult task in ensuring that any regulatory framework that is implemented does not overly impede the possible economic benefits that are expected to arise for the Australian economy.

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

RESPONSE:

The role of the Government should be to facilitate an appropriate regulatory environment that assists in the safe growth of any economically beneficial new technology but also attempting to reduce any potentially adverse impact that the same technology could have upon the general populace of Australia. In addition to this facilitated environment, the government should not overreach its regulatory solution as it could stifle the economic and social benefits that the technology could deliver. Finally, the crypto environment is not isolated to Australia. The effect of this technology is impacting most jurisdictions and as such there also needs to be international compatibility resulting in some form of legal harmonisations with Australia's international economic partners.

This role can be very difficult at times to balance. There is a potential public relations nightmare from a press that does not sufficiently understand the new technology and which could generate a general populist backlash against such technology, or possibly worse, an over exuberance in the uptake of the technology resulting in great concerns from an economic perspective.

The press in many instances has misinterpreted this new technology known as blockchain and substantially confused it with cryptocurrencies. Further, even though there has been in 2022, as noted in the consultation paper, a number of high profile failures, a clear investigation into such failures will substantially support the proposition that these failures have been due to a lack of appropriate governance structures. For example, the FTX collapse was not due to a failure in the blockchain technology nor a failure in the crypto currencies, but was directly due to a lack of governance structures being implemented and managed appropriately by the senior management of FTX.

Of course, there have also been some technology failures such as the Terra LUNA stable coin disaster. This disaster concerned the deployment of an algorithmic stablecoin. The algorithm was flawed causing a global loss of US$40 billion. It is suggested that algorithmic stable coins be outlawed and that all stablecoins available to Australian

residents must be fully backed by highly liquid stable assets such as fiat currency, stable precious metal like gold, or government bonds or AAA rated securities.[1]

The advancement of cryptocurrencies over the last 11 years has proceeded notwithstanding a lack of regulatory understanding by government agencies and the stakeholders who participate in the crypto-economy. This position is not just directed at Australian regulators but can also be applied to the SEC in the United States, the FCA in the United Kingdom as well as many other western jurisdictions. The principal regulatory authorities in Australia that should be involved, in my opinion, are as follows:

- Australian Securities Investment Commission,
- Australian Consumer and Competition Commission,
- Australian Prudential Regulatory Authority,
- ACMA, and
- AUSTRAC.

The suggested involvement of APRA is because of the advancement of DeFi, which if not regulated now will become a major economic headache for the Australian economy. Further, most publications of crypto tokens offerings occur via the internet/email and the ACMA has authority over spam and as such greater involvement of ACMA from a techno-legal perspective would assist.

But the involvement of these regulators must not create a turf war between the agencies. Each agency must know the scope and extent of their power and responsibilities, whilst simultaneously avoiding silos of enforcement. They must be directed to work cooperatively, be transparent and share information openly. Such a failure presently exists in the USA, especially when it comes to the role of the SEC and the CFTC. Both these US regulatory authorities are claiming control over the crypto environment causing commercial uncertainty in the US marketplace.

In allocating responsibility to the above regulatory authorities, it is essential that such authorities have sufficient skill sets to understand the intricacies involved, not only from a commercial perspective, but also from a technical perspective. In my opinion, the current regulatory authorities do not have the appropriate skill sets to adequately manage the current regulatory position involving the holistic management of cryptocurrencies in Australia.

[1] Though it has been shown that due to various mis-calculations (even nefarious activity), “AAA” rating for a security does not guarantee stability, as was identified in the cause of the GFC of 2008.

Treasury TOKEN Mapping Consultation Response

Dr Adrian McCullagh

Consequently, the Government should embark upon upskilling the human resources involved in managing any regulatory framework dealing with cryptocurrencies and the various stakeholders who participate in the crypto economic environment.

A difficult perspective is that new business structures are being deployed daily by crypto stakeholders and in many cases in a regulatory vacuum or in an uncertain regulatory environment. For example, in the last 5 years DEXs (decentralised exchanges) have been created. Basically, a DEX is crypto swapping technology in the form of a smart contract. It is different to a Centralised Digital Currency Exchange (DCE) noted above, as there is no central organisational structure operating the DEX technology. DEXs do not comply with the KYC requirements imposed upon DCEs. This potentially allows the criminal element to take advantage of anonymity and perpetrate money laundering with little legal consequences.

The recent UK Court of Appeal case of *Tulip Trading v Bitcoin Association and others* [2023] EWCA Civ 83 (decided on 3 February 2023) held that software developers may owe a fiduciary relationship to users of a blockchain platform (which in the case was the Bitcoin platform). The involves £3 billion in lost digital due to a hack. The UK Court of Appeal regarded the case as "one of considerable importance and is rightly characterized as a matter of some complexity and difficulty", noting that "the issues raised are of fundamental importance to TTL itself, as its owns substantial assets that it can no longer access, as well as to the financial world generally." The Court of Appeal remitted the case back to trial, so that it will be the first ocassion a court has considered in detail whether blockchain developers owe legal duties to their users.

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

RESPONSE:

Australia has a very robust financial sector. Whilst there have been issues, as identified in the recent Hayne Report, it is still safe to say that Australia has a very secure financial sector. For example, APRA has for many years published pertinent guidance notes and reports that require financial sector participants to implement robust IT security structures. A similar approach should be considered for many participants in the crypto sector. This is especially so for digital currency exchanges as they are a central component in the decentralised finance environment. In suggesting this, the Government needs to determine what legal status should be applied to DEXs. Maybe, a new liability regime could be applied to the coders of DEXs so that some responsibility can be applied. This proposition was recently raised in the Tulip case which is discussed below.

Treasury TOKEN Mapping Consultation Response

Dr Adrian McCullagh

DCEs operating in Australia are required to register with AUSTRAC. But it is a rudimentary task to register with AUSTRAC, by simply filling in a form and submitting it. AUSTRAC has limited capacity to vet every application. As such, new penalties should be considered including deeming the application to be the equivalent of a statutory declaration and drawing to the applicants' attention that any falsehood will amount to perjury and possible criminal liability.

AUSTRAC presently does not have the authority to create a public register listing all DCEs registered in Australia. It is possible to ask AUSTRAC if a particular organisation offering DCE services is registered but there is no open register for inspection. There has been at least one court case in the UK where an organisation was operating in the UK without being registered with the relevant regulatory authority. In fact, the relevant DCE in the UK was a pure scam and all funds deposited with the fake DCE were lost.

If AUSTRAC was authorised to create a public register listing all DCEs operating in Australia, then consumers can at least inspect the register to know if the DCE is registered. The register should also note the public officer and corporate contact information for the relevant DCE.

There needs to be some clarity dealing with custodial wallets. In many cases, regulators and the press misunderstand the nature of a custodial wallet. A DCE does not hold a client's digital assets unless the DCE is also a node, operating in the blockchain, and as such assets are actually recorded on the distributive ledger which are controlled by the various nodes that validate all transactions carried out on the relevant blockchain. A DCE may hold a client's private key necessary to carry out transactions on the blockchain. A better regulatory structure would be to define a custodial wallet as being a record including a client's "private key" held by a DCE that permits the DCE to control the private key required for transactions concerning the client's digital assets. It is this "control" characteristic that a client is submitting to when they engage a DCE for custodial services. There needs to be clarity as to whether a DCE that is holding a client's private key is holding that key as trustee for the relevant client.[2] If a trust relationship is established at law, then this would better protect DCE clients should the DCE become financially stressed requiring the appointment of either an administrator or a liquidator.

Parliament should consider appropriate regulation to deal with custodial wallets. For example, in 2014, there was a major incident dealing with the Mt GOX DCE. It was possible for personnel working for Mt GOX to illegally

[2] See In Re Celsius Networks LLC et al, Debtors. Case No. 22-10964 (MG) (Jointly Administered)
IN RE: CELSIUS NETWORK LLC (2023) | FindLaw

transfer Mt GOX client bitcoins.[3] Further, as recently as 2022, with the failure of the FTX DCE again, an inside job occurred where FTX client digital assets were surreptitiously illegally used to prop up the research company Alameda Research ,which was closely connected to FTX. There is technology that can track and prevent insiders from illegally carrying out unauthorised activities. It is possible to structure a regulatory framework that identifies the characteristics of such technology and still utilise technology neutral language. Incidentally, the technology I am alluding to involves the deployment of split key framework that utilises Shamir's secret sharing of keys. The obligation imposed upon a DCE could be simply an obligation that they deploy technology that prevents illegal insider activity from occurring.

If the department would like to know more about this technology, I can provide details as the US Silicon Valley company is a client of mine, and I can attain appropriate authority.[4]

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?

RESPONSE:

Gough Whitlam is famously attributed to the following quote: "You cannot legislate against stupidity"[5]. Assuming that to be a rational statement, it does not means the Government should stand idle. Both ASIC and the ACCC have worked tirelessly in trying to educate consumers against scams. Despite efforts undertaken by Parliament and regulators there will always unfortunately be a small (hopefully) sector of consumers who will be scammed. However there are certain strategies that could reduce the risk of successful scams taking hold across the consumer market.

As suggested above, a public register dealing with registered DCEs in Australia could reduce some scams but the task of eliminating successful scam activity is an unrelenting task. Further, as expanded below, DCEs should only register digital assets for any organisation that has registered with the apprpriate regulatory authority. This suggestion is expanded below. Further, the vast majority of crypto-scams are publicised via the Internet. It is noteworthy, as far as the author is aware, that the ACMA has not undertaken enforcement procedures against

[3] MT GOX which stood for Magic: The Gathering Online eXchange. This exchange was based in Japan and at one stage accounted for more than 70% of the global trades in Bitcoin. (2014)

[4] See www.lokblok.co.

[5] Though the quote is also attributed to Jessie Venture when he was the Governor of Minnesota.

any parties who have perpetrated crypto scams to date. It is suggested that ACMA should become more active in monitoring crypto-scams and better coordinate with both the ACCC and ASIC. As an outsider it appears that there is insufficient coordination between ACMA, ACCC and ASIC in dealing with crypto-scams that are carried out via the Internet and in particular SPAM emails. Even though most scams originate internationally there should be a united front in dealing with them especially from a public awareness perspective.

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

RESPONSE:

DCEs should have the knowledge and expertise to better vet any digital assets that they desire to list. Most if not all DCEs registered in Australia require at the time of listing a digital asset requiring a solicitor's opinion letter stating that the relevant digital asset is not a security. Obviously, this is too little when it comes to scams. The rational for this letter is that no DCE wants to list a security as they do not hold the relevant market licence necessary to offer trades for securities. The requirement is simply a risk management mechanism in favour of the DCE but is really does not assist the consumer.

The UK Government on 3 February 2023, through the FCA, announced that any entity that wishes to offer digital assets to UK residents must first register with the FCA. Further, if an entity fails to so register then a criminal offence will occur. In fact, the FCA has announced that instead of acriminal penalty regime a criminal custodial regime will apply. This should have a follow on effect in that all DCEs will only be permitted to list digital assets that relate to entities that are registered with the FCA. This will mean that if a digital asset is offered by an entity that has not registered with the FCA, then it will need to be offered by an off shore entity and not through a registered DCE. By stipulating criminal activity, the FCA can obtain a conviction in absentia and could register the conviction with either or both of Interpol and Europol.

In contrast to the new UK position, Australia has a criminal penalty regime which is practically useless. Firstly, most scam entities reside external to Australia and thus even if there is a successful prosecution it is problematic for regulators to enforce. Secondly, even if the scam entity does originate in Australia a criminal penalty could become a pyric victory as the scam entity is unlikely to be in a position to make payment to satisfy the penalty. A custodial penalty should substantially reduce the incidents of scams by creating a deterrence penalty against the persons behind the scam.

Treasury TOKEN Mapping Consultation Response

Dr Adrian McCullagh

The FCA acknowledges that many of the crypto-scammers will reside offshore and thus difficulty could arise in directly enforcing the UK policy concerning custodial penalties. Hence, there is no silver bullet to irradicate the activities of scammers, but the policy should create a reduction in the success of scam crypto products being available to UK residents. Further, though this has not been researched, it may be possible to create an international list of those people who have been successfully prosecuted for digital asset scams. IOSCO may be a suitable organisation to coordinate such a list for the benefit of all jurisdictions.

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?

RESPONSE:

As noted above, most Australians do not store their private key on a hardware wallet but instead rely upon a DCE to generate and retain the relevant private key for and on behalf of their respective clients. Hence, most consumers who hold crypto/digital assets do not have exclusive control of the private key needed to transact with their crypto/digital assets. But there is a substantial misconception when dealing with custodial wallets. A DCE does not hold any client's digital assets as the records of such assets will be distributed across the many thousands of nodes that participate. It is only when a DCE is also acting as a node will it hold a record of such digital assets, though some DCEs do hold a summary record off chain of a client's digital assets. In most cases, a DCE will hold on behalf of their clients the relevant private key that is needed to carry out a transaction.

It is the access to the client's private key information by a DCE that results in the ability to control the client's digital assets. This is also a major flaw in the entire business operations of DCEs not only in Australia but globally. Illegal insider activity, as has been identified in the FTX case, needs to be overcome. There are technologies that can deal with restricting insider activities to prevent insider illegal activity, noted above.

I appreciate that a technology neutral regime is desired. Hence, instead of specifying a specific technology it should be possible to detail functional characteristics which can achieve the desired result of better regulating against illegal insider DCE activity.

Hence, when a discussing a custodial wallet, the regulatory focus should be directed at who controls or has the opportunity to control the use of the private key and how this may be achieved.

Consequently, control over the private key is essential. There are technologies whereby no single party has full control over a client's private key and this would, if properly implemented, prevent a single person from committing a crypto-asset crime.

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

RESPONSE:

The concept of ensuring that everyone is on the same page when it comes to definitions is a proper procedure. The difficulty in the implementation of the concept is ensuring that the definitions are correct technically and that there is no confusion as to their meaning. As is discussed below, the definitions currently provided are vague and it is submitted technically incorrect. They are as Lord Atkins stated in *Liversidge v Anderson* [1942] AC 206 the terminology is a "Humpty Dumptyism". That is instead of the words being interpreted in the natural though technical meaning the definitions provided a contorted meaning which do not correspond to reality.

> *The words have only one meaning ... I know of only one authority which might justify the suggested method of construction: 'When I use a word,' Humpty Dumpty said in rather a scornful tone, 'it means just what I choose it to mean, neither more nor less.' 'The question is,' said Alice, 'whether you can make words mean so many different things.' 'The question is,' said Humpty Dumpty, 'which is to be master – that's all*.'
>
> Lord Atkin, *Liversidge v Anderson* [1942] AC 206 at 244-245

Consequently, definitions are an admirable approach, but they must mean what they say and say what they mean. The definitions provided in the consultation paper, it is submitted, fail on this point.

CRYPTO-NETWORK

Paragraph 26 of the consultation paper sets out the definition of a crypto network. This definition relates to a singular entity in the first sentence whereas in the second sentence of paragraph 26 it sets out a definition of plurality. First sentence defines a crypto network as "*a distributed computer system capable of hosting crypto tokens*". This definition in relating to a distributive computer system appears to cover multiple computers that

are somehow connected to one another. In other words, the definition could easily cover the definition of "Internet". In 1997 the US Supreme Court in the case of *Reno v ACLU*, defined the Internet as being "*an international network of interconnected computers".* It is submitted that the definition of a crypto-network as set out in the consultation paper will not achieve its desired result as there is a failure in the validation definition to recognise that a crypto network comprises a group of computers that operate under a peer to peer consensus relationship in the validation of crypto transactions.

The second sentence concerns the plurality of crypto networks. The second sentence states that crypto networks are platforms on which crypto tokens and smart contracts are recorded. The introduction of "platforms" appears to be out of place. It is difficult from my technical perspective to understand what crypto-networks are based on the definitions provided within the consultation paper. It is further submitted that paragraph 27 builds on this confusion by introducing the term data structures.

Paragraph 29 then attempts to define what a public crypto network is as:

> *A **public crypto network** aims to provide certain information security guarantees in a way that does not require a trusted third party to store and process data.*

It is suggested that there are a number of errors in this statement. A public crypto network does rely upon trusted third parties. These trusted third parties are commonly referred to as nodes and it is expected that every node has implemented the peer-to-peer consensus algorithm as generally understood by all other nodes who form part of the crypto network. The reference to trusted third party in this context should really state as follows:

> *"that does not require a central/sole trusted third party to store and process data".*

CRYPTO-TOKEN

From a conceptual perspective paragraph 33 is correct but most consumers who hold a crypto token rely upon a digital currency exchange to generate and retain the relevant private key needed to carry out any future transactions. This is generally referred to as a custodial wallet. In contrast to a custodial wallet, it is possible for the consumer to implement a non-custodial wallet which can either be a software wallet stored on the consumer's computer or a hardware wallet.

According to the SwiftX report, which was published in September 2022, it is expected that approximately 1,000,000 Australian residents will for the first time acquire a crypto asset. It is also expected that the vast majority of these new owners of cryptoassets will rely upon a custodial wallet. It is also expected that as these new

consumers become comfortable and better understand the importance of their private key that they will eventually migrate to a hardware wallet.

It is gratifying that Treasury has identified that the central issue revolves around the control of the private key and not necessarily the possession of the private key. The Law Reform Commission [England and Wales] in their consultation report, it is submitted, got hung up on the term "possession", when the real issue is "control" of the private key. There is a general saying in relation to crypto assets that "not my key not my crypto". It is this lack of control, however, the private key in relation to a custodial wallet that has caused substantial commercial harm to the entire crypto token market.

For example, as noted above, the Mt Gox and FTX incidents resulted from insiders at both those respective digital currency exchanges having access to the relevant clients' private keys.

SMART CONTRACTS

Paragraph 35 defines a smart contract as "computer code that has been published to a crypto network's database". This definition suddenly introduces the term " database" and does not fit with the above definition of a " crypto network" (singular).

It is suggested that more thought needs to be undertaken as regards to the above definitions as they are fundamental to the entire consultation paper. This point is emphasised in paragraph 36.

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?

RESPONSE:

in August 2000, the Taskforce on Industry Self-regulation published its Report titled "Industry Self-Regulation in Consumer Markets". A central theme of the self-regulation report was that in regulating markets and future proofing the regulation such regulation should be written in technology neutral language.[6] This approach to drafting regulation has substantially benefited the Australian economy.

[6] See also Federal Attorney General (Mr Daryl Williams QC) 1998 report by the Electronic Commerce Expert Group "Electronic Commerce : building the legal framework / report of the Electronic Commerce Expert Group to the Attorney General"

Treasury TOKEN Mapping Consultation Response

Dr Adrian McCullagh

The difficulty in dealing with a crypto market and the regulating the various stakeholders and products utilised in such a market is that the entire market is dependent upon new technologies and these technologies together with new business models are rapidly evolving which generally outpaces the regulatory framework and the capability and capacity of regulators to adequately monitor and police such business environments.

Hence, any bespoke taxonomy must clearly identify the various components comprising the market and define each component in plain non-confusing language that corresponds to what the market understands them to mean.

For example, the definition of "function" and "crypto asset" are each, in my opinion confusing. The term "function" is basically the resultant output from a token system. Yet, the examples provided appear to identify a function as a procedure. For example, receiving money is different to the actual money that has been received. Receiving money is a process whereas money received is the resultant of the process.

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

RESPONSE:

A regime for all seasons (like the man for all seasons) will only confuse both the existing financial market stakeholders and emerging crypto market stakeholders. Hence, a bespoke standalone regulatory framework is suggested. In suggesting this, a standalone framework can be designed as a complimentary framework to the existing regulatory framework and be drafted as a result driven framework. What is important is that digital asset design and business models are rapidly developing in the crypto/DeFi marketplace and as such by having a result driven regime it should be possible to cover future anticipations.

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?

RESPONSE:

This is interesting as the question concerns "non-financial" aspects. An example of a direct non-financial aspect would be the privacy concerns of the various consumers who participate in the crypto environment. Due to the immutability characteristic embedded in all blockchain deployments and the requirement of the GDPR for the right to be forgotten, there are technical issues that remain to be addressed. IBM has proposed a GDPR solution

but there remain questions as to its efficacy (see : What does GDPR mean for blockchain technologies? - Servers & Storage (ibm.com)).

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?

RESPONSE:

Stablecoins certainly have great potential from a commercial perspective. Ronald Coase's 1937 seminal paper "The Nature of the Firm" identified the benefits of firms/corporations and the transaction costs involved. It is not uncommon for an international transaction concerning payment to take a number of days from a cleared funds perspective.

Presently, a share transfers in Australia for ASX listed entities is set at T plus 2 days. Due to various intermediaries (the ASX itself, various Brokers and financiers) who are involved in friction costs for these transaction a delay occurs in settlement.

It should be possible in utilising a stablecoin to reduce this time frame to less that 20 minutes. From a macroeconomic perspective the reduction in time frame will give to the recipient the opportunity to circulate the funds received immediately after receipt. That is, instead of waiting for say 2 days for receipt of cleared funds, due to transaction delays, the recipient can immediately upon receipt use the funds for further commercial opportunities. From an economic perspective this could increase circulation of funds 30 times (average 10-hour day multiplied by 3 [3 X 20 minutes =1 hour]).

According to Gary Gensler (Chairman of SEC) all stablecoins are securities. But it is difficult to follow the rationale of this pronouncement at law. A stable coin is meant to be stable and thus should not substantially fluctuate in value. For example, the USDC is backed by a number of stable assets and as such the value of the USDC should remain stable to the value of the US$. Note that not all stable coins are 1 to 1 backed by a stable asset. This was evident with the collapse of the TerraUSDC stable coin which was an algorithmic stable coin. There obviously needs to be some specific regime dealing with stablecoins and there it is suggested some consideration to either regulating algorithmic stablecoins or outlawing them entirely.

Treasury TOKEN Mapping Consultation Response

Dr Adrian McCullagh

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?

RESPONSE:

The liquidity of the backed assets is entirely important. Circle, the issuer of USDC, has indicated in writing that USDC is backed as follows:

- 61% – by cash and cash equivalents,
- 13% - by Certificates of Deposit – meaning CDs issued by foreign (non-U.S.) banks,
- 12% - by U.S. Treasuries bonds,
- 9% - by commercial paper accounts, and
- 5% - by municipal and corporate bonds.

It is clear that if there was a run on the USDC, that Circle could fairly promptly meet the cash drawings upon the USDC. These above noted assets are highly liquid and as such should be a commercially safe structure for holders of USDC. But this does not mean that there would be sufficient USDC being available for other crypto currency holders to acquire USDC as a default safe harbour for crypto investments. As of 27 February 2023, the aggregate total value of the 3 major stablecoins (USDT, USDC and BUSD) amounts to approximately US$124,635,506,000.00) which far less than the total market value of crypto/digital assets presently available US$1.08 Trillion (see coinmarketcap).

In Australia, ANZ has successfully issued an Aus. $ Stablecoin. It may be worth considering whether only an Australian registered bank should be permitted to issue an Aus. $ backed stablecoin. No further comment is made on this issue as it is outside the expertise of the submitter. But it will be difficult to regulate/police foreign organisations that issue foreign currency backed stablecoins.

The issue then involves the liquidity rate of the backed assets, and it may be useful to only permit highly liquid assets to be accepted for the Australian market.

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?

RESPONSE:

Treasury TOKEN Mapping Consultation Response

Dr Adrian McCullagh

Intermediated token system providers such as DCEs are best placed to determine the validity or transparency of any digital asset that they list on their exchange. Currently, to list a digital asset on an Australian DCE, the DCE requires a solicitor's letter from the issuer stating that the relevant digital asset is not a security. This is not, it is suggested, sufficent transparency. It could be that a DCE, if it does rely upon this process, be required at law to publish the issuer's solitor's letter. Of course, if this is a requirement at law then the law firm providing the opinion will certainly be conservative in its advice; much like a legal and financial statement embodied in an IPO under the corporations law.

Another issue is the current listing system focuses upon DCE but Decentralised DCEs (DEX) are becoming popular principally due to the failures involving various DCEs such as Mt GOX in 2014, FTX in 2022, Celcius in 2022 as well as others. Theoretically, since a DEX involves smart contract deployment with no centralised involvement then illegal internal human activity should be impossible. But very few if any DEXs have implemented KYC procedures as required under the Anti-money Laundering and Counter Terrorism Financing laws. DEXs can be exploited for money laundering and terrorism financing arrangement especially if combined with certain stablecoins available in the market.

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

RESPONSE:

This issue has been discussed above under question 2.

Continuous disclosure requirements as required under the ASX rules might be considered for digital asset issuers to remain listed on an exchange. The difficulty of this approach is that the cost burden imposed upon an issuer could drive the crypto market offshore which only creates a problem for Australian consumers and crypto-entrepreneurs. There is a fine balancing act with what ever solution is settled upon.

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?

RESPONSE:

Treasury TOKEN Mapping Consultation Response

Dr Adrian McCullagh

Section 763A (Financial Product) which references section 763B, section 763C and Section 763D is fairly wide in its impact. The principal gap is that for these sections, there is no clarification as to what the term "benefit" means. SECT 200AB of the *Corporation Act 2001* does provide a meaning of the term "benefit" but it has no relevance to a financial product. Consequently, what does "or other benefit" mean. As noted above, should a stable coin be classified as a financial product and if so why? Does the accelerated settlement time constitute a sufficient benefit to warrant a determination of a stablecoin being classified as a financial product. If it was so classified then how does the holder of the stablecoin transact with the stablecoin. Does the holder need an AFSL, which seems to be an unnecessary regulatory imposition. Finally, such a determination would require every DCE that provides a market for a stablecoin would also be required to have an Australian Market Licence which again would be an unnecessary financial and regulatory burden.

Further analysis needs to be undertaken to deal with Stablecoins as a simple determination that a stablecoin is a financial product will have a substantial impact and many unintended consequences.

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

RESPONSE:

Parliament may want to look at DeFi structures more closely. One area that warrants further investigation is Liquidity Pools and Staking arrangements. For example, in order to stake the digital asset "ether", the holder needs to possess at a minimum of 32 ether which as of 27 February amounts to US $1642 X 32 = US$52,544 (Aus $ 2345 X 32 = Aus$75,000). Most Australian holders of ether will not own Aus $75,000 worth of ether. Hence some Australian CDEs actually pool their client's holdings of ether so as to stake the minimum of 32 ether. This is obviously a MIS as defined under section 10 of the *Corporations Act 2001*.

Staking of ADA under the Cardano blockchain is entirely different. Staking in Cardano platform is the process where ADA token holders delegate their ADA voting power to a stake pool, which does not require the movement of the ADA. Hence, there is no direct contribution in staking in Cardano. This way, ADA holders do not risk losing custody of their hard-earned tokens. Consequently, there is no contribution to a pooled project or structure. All that is staked is the voting power and not a contribution of money or money's worth which is an essential element for an interest in a MIS to arise.

Treasury TOKEN Mapping Consultation Response

Dr Adrian McCullagh

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?

RESPONSE:

This point has already been discussed above.

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?

RESPONSE:

One area that should be considered is the regulation of a DAO (decentralised autonomous organisation). According to the Bragg Report, DAOs should be recognised under the *Corporations Act*. It has been reported that in 2021, the total value of crypto funds held in DAO treasuries reportedly surged from $400 million to $16 billion, and the number of US holders of interests in DAOs rose from just 13,000 to 1.6 million.[7]

It is likely, that this accelerated increase in DAO participation will not abate in the near future. Consequently, urgent attention, it is suggested, should become a priority. As identified in the Harvard paper, the potential disadvantages of DAOs include:

- ***Potential fraud.*** The more freewheeling nature of DAOs lends itself to investors being defrauded or misled when funds are raised.
- ***Crypto-related risks.*** DAOs face the risk of (i) significant fluctuation in the value of the funds held in their treasuries, given the instability in pricing that has been associated with cryptocurrencies; (ii) hacking and cybersecurity breaches (which have led to several high-profile debacles involving the theft of substantial amounts of funds from DAO treasuries and member accounts see DAO attack 2016)
- ***Lack of legal status—and potential for unlimited liability. See CFTC v Ooki DAO.*** https://www.cftc.gov/PressRoom/PressReleases/8590-22ses

A DAO[8] is basically a special type of smart contract that regulates its members participation in the decision-making process. BUT, anyone can establish a DAO and there are currently NO quality control standards dealing with the

[7] A Primer on DAOs (harvard.edu) Harvard Law School Forum on Corporate Governance. Sept 17, 2022.
[8] The author is presently finalising an academic paper dealing with possible regulatory framework for the introduction of DAOs in Australia.

code that regulates the operations of the DAO. This is a major risk as there is no minimum coding standard needed to create a DAO. This is a major flaw in DAOs.

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?

RESPONSE:

This has been discussed above. The ACMA has been designated as the regulatory authority to monitor and police spam activity and online advertising. Greater involvement of the ACMA is suggested.

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?

RESPONSE:

DeFi is structured around the deployment of smart contracts. But as noted in question 10 there is no regulatory control over the development and deployment of smart contract code. Proper software verification activity such as that possibly provided by NATA (National Association of Testing Authorities) maybe a useful model to adopt.

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

RESPONSE:

As noted above, the UK case of Tulip Trading may provide assistance by sheeting liability to the coders of smart contracts and thus the coding sector may take more appropriate steps in testing their smart contract code prior to deployment.

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?

RESPONSE:

Treasury TOKEN Mapping Consultation Response

Dr Adrian McCullagh

This has been discussed in question 10.

b) 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?

RESPONSE:

None that has been published so far.

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?

RESPONSE:

This is a very complex question that cannot be easily answered. I recommend to the department the following texts which may answer this question:

- *DeFi and the Future of Finance* by Campbell R. Harvey, Ashwin Ramachandran, Joey Santoro (available on Kindle)
- *How to Maximise a Return in DeFi* by Dr Liew Voon Kiong (available on Kindle)
- *The Real Business of Blockchain* by David Furlonger and Christophe Uzureau

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

RESPONSE:

None of which the author is aware.

Final Note: If the department would like to discuss any aspects on this response, then the author will try to make time to discuss. This is especially so if any explanation concerning DeFi and DAOs is desired. One point not discussed above is the role of hardware wallets and the ability to transact digital assets without using a DCE. That is, if 2 entities simply exchange their relevant public key addresses then a transaction can be implemented without the involvement of a DCE. It is possible to overcome this flaw if the department is interested.

3 March 2023