Dr. Adrian McCullagh & Professor John Flood

Response to the "Crypto Asset Secondary Service Providers: Licensing and Custody Requirements Consultation Paper (The Treasury, Australian Government)

Dear Director—Crypto Policy Unit

We refer to the "Crypto Asset Secondary Service Providers: Licensing and Custody Requirements" consultation paper dated 21 March 2022 to which our response is outlined below.[1]

We thank the Treasury for this opportunity to submit a response to the consultation paper.

Executive summary:

There are four main conclusions to be drawn from our response to the Consultation Paper:

- The distinction between private keys and crypto assets should not be lost. They are not identical even though there may be occasions when they should be combined.
- Present arrangements for the security of private keys is inadequate and we suggest the use of split key arrangements.
- Not all crypto assets are the same and so may require different treatments. And present legal rules are inadequate in addressing crypto assets as financial products.
- Any move towards new regulation should be carried out with a serious commitment to international harmonisation because by its very nature the crypto asset market is global.

Structure of Response

Our response is structured as follows:

1. Preliminary note—the distinction between crypto asset and private key
2. Access to the private key
3. Current Corporations Law custodial obligations
4. Response to Consultation Paper questions
5. Naming of CASSPRs
6. Naming of crypto asset
7. Financial products
8. CASSPr regulation
9. NFTs
10. CASSPr proposed obligations
11. Further issues for consideration not raised in the Consultation Paper

1. Preliminary note—the distinction between crypto asset and private key

We preface our response by providing what we believe should be understood as a crucial ontological distinction between crypto assets and private keys. They are not as we argue below identical and their conflation will lead to confusion and potentially inappropriate regulation, which could lead to unintended consequences. They can be used in distinctively different

[1] See https://treasury.gov.au/sites/default/files/2022-03/c2022-259046.pdf.

ways. We do, however, accept there may be occasions when their usages can overlap and so they may be considered isomorphic.

The underlying technology supporting of crypto assets is a relatively nascent technology which if inappropriately regulated could have a substantial adverse impact upon Australia's future economic well-being as alluded to in the Consultation Paper (p 3).

Actual crypto assets are distributed across the blockchain infrastructure which comprises many hundreds, if not thousands, of nodes. In Australia, many Digital Currency Exchanges, as that term is defined under the Australian Anti Money Laundering and Counter Terrorism Financing Act (AML Act), also act as Crypto Asset Secondary Service Providers (CASSPr). CASSPrs possess private keys required to transact any business concerning a specific crypto asset. In essence, the CASSPr through their business model are providing a custodial service for the private key. The CASSPrs *do not*, however, hold any crypto assets themselves unless they also act as a node/validator depending on whether the consensus protocol is a proof of work or a proof of stake solution.

When a CASSPr registers a person (end user) as a client, the CASSPr must follow their KYC obligations as required under the AML Act. It is not unusual for the CASSPr to generate the private/public key pair necessary for the end user to transact in crypto assets.

According to ISDA (International Swaps and Derivatives Association), crypto assets can be divided into two generally acceptable categories:

- Native Crypto assets, and
- Asset Referencing Crypto assets.[2]

Native Crypto assets are assets that exist solely as a digital asset and do not represent any legal or proprietary interest in other assets. They exist solely as a digital record.

Asset Referencing Crypto assets are assets that reference an underlying asset or right, through a legal or operational mechanism.

Despite the distinctiveness of the crypto asset category, all crypto asset transactions rely on the use of private keys corresponding to public key addresses. But private keys can be used for purposes separate from crypto assets such as generating digital signatures.

Even though we submit private keys are not a financial product per se, the issue is whether private keys inextricably connected to financial products could or should be classified as financial products as a composite arrangement. This appears to us to be a step too far as it is technologically possible for private keys through certain applications (multi-party computations) to access and further process other private keys connect to a digital asset and the question arises therefore where does certainty lie? It is possible for split key arrangements or multi-party computation arrangements to get around this view of private keys purely as a crypto asset. However, we see the logic of regulators desiring simplicity and there may be occasions when it is appropriate to categorise private keys and crypto assets together for regulatory purposes in order to facilitate a holistic policy (page 6). To this end we discuss the

[2] See Categorizing Digital Assets, *Contractual Standards for Digital Asset Derivatives,* at p 7 (ISDA, 2021), https://www.isda.org/a/QVtgE/Contractual-Standards-for-Digital-Asset-Derivatives.pdf.

US Department of Commerce paper on "Developing a Framework on Competitiveness of Digital Asset Technologies" below in section 11.[3]

2. Access to the private key

As noted above, the private key is an essential component in carrying out a crypto-asset transaction. Consequently, every crypto asset end user must have access to their relevant private key.

There are three ways for an end user to gain access to a private key:

1. A software wallet that resides on an end user's untrusted computer or mobile device.
2. A hardware wallet like a Ledger Nano x or Trezor hardware device that has enhanced security features.
3. A custodial service whereby the CASSPr will generate the private/public key pair and will publish/provide the public key whilst keeping the corresponding private key securely stored for the sole access of the rightful end user.

In our view the Consultation Paper focusses on position three and does not address either of the first two even though position two is the most dangerous from a criminal/counter terrorism financing policy perspective. For example, it is easy for holders of hardware wallets to exchange their public keys and then transact a transfer of any crypto asset without involving a CASSPr. As a consequence, it is possible to avoid the FATF Travel rules which every CASSPr is required to implement, monitor and report.

The rationale behind a CASSPr providing a custodial service is that most end users do not possess the background knowledge and expertise to properly prevent their private key(s) from being compromised. Interestingly, most CASSPrs recommend that end users acquire a hardware wallet and move their private key to the wallet. They reason that if the CASSPr no longer has possession of the private key there is a subsequent risk reduction as the CASSPr can no longer be held accountable for a compromised private key.

It is also possible through technology to require all hardware wallet manufacturers to implement private key split key structures whereby one part of the private key that has been split is held by a CASSPr thus requiring all crypto asset transactions to involve a CASSPr and thus the Travel Rule can be enforced. Since the CASSPr will not hold the entire private key their risk profile is reduced because they will be in the same position as if the private key in its entirety were held only by the end user in their hardware wallet. The only corporation that has developed such technology as far as we are aware is Lokblok Inc, in California, with their patented solution.

3. Current Corporations Law custodial obligations

The present state of the law fails to encompass all the issues thrown up by the digital universe. The Corporation Act 2001 [Cth] (Corps Act), however, does include provisions dealing with custody arrangements but the Corps Act is restricted to custody of Financial Products. Section 766E provides as follows:

[3] See "Developing a Framework on Competitiveness of Digital Asset Technologies", https://www.federalregister.gov/documents/2022/05/19/2022-10731/developing-a-framework-on-competitiveness-of-digital-asset-technologies.

Meaning of provide a custodial or depository service

*(1) A person (the **provider**) provides a **custodial or depository service** to another person (the **client**) if, under an arrangement between the provider and the client, or between the provider and another person with whom the client has an arrangement, (whether or not there are also other parties to any such arrangement), a **financial product,** or a beneficial interest in a **financial product,** is held by the provider in trust for, or on behalf of, the client or another person nominated by the client.*

It is highly doubtful, that a private key would amount to a financial product. The term Financial Product is defined under section 763A of the Corps Act as follows:

Section 763A General definition of financial product

(1) For the purposes of this Chapter, a financial product is a facility through which, or through the acquisition of which, a person does one or more of the following:

(a) makes a financial investment (see section 763B);

(b) manages financial risk (see section 763C);

(c) makes non-cash payments (see section 763D).

As stated above, a private key does not fit within this definition as a private key is not really a financial investment, nor a financial risk nor a non-cash payment.

A financial investment is defined in section 763B as follows:

*For the purposes of this Chapter, a person (the **investor**) **makes a financial investment** if:*

*(a) the investor gives money or money's worth (the **contribution**) to another person and any of the following apply:*

(i) the other person uses the contribution to generate a financial return, or other benefit, for the investor;

(ii) the investor intends that the other person will use the contribution to generate a financial return, or other benefit, for the investor (even if no return or benefit is in fact generated);

(iii) the other person intends that the contribution will be used to generate a financial return, or other benefit, for the investor (even if no return or benefit is in fact generated); and

(b) the investor has no day-to-day control over the use of the contribution to generate the return or benefit.

Even though the so-called investor may provide money or money's worth, a stablecoin will not provide a financial return or other benefit unless the term "benefit" is given such a wide meaning that the simplicity of using a stablecoin is in itself such a benefit. A stablecoin allows its holders to avoid the volatility of other crypto assets like bitcoin and ether. The holder does not have to cash out their holdings into a fiat currency but can wait until they wish to re-enter the market. In essence, a stablecoin is much like the gold is for fluctuating international

currency market when there exists a global financial incident or disruption to the global economic wellbeing. However, the recent US report on stablecoins raises a number of regulatory issues around market integrity and investor protection which are concerning but we do not discuss here.[4]

4. Response to Consultation Paper questions

The Consultation Paper throughout its content refers (for example page 7) to the custody of crypto assets by a third party but that is not what is held by the CASSPr. A CASSPr does not hold the crypto assets per se. The crypto assets are stored on a blockchain which is replicated across many nodes. The CASSPr will at most hold the private key which we argue will not amount to a financial product. Consequently, we disagree with the following:

> *The safekeeping of financial products under the Corporations Act by custodians (as custodial or depository service providers). Crypto assets that are financial products would benefit from these minimum requirements.*

The reference to the Mt Gox incident is a prime example of what is stored by a CASSPr. All evidence supports the position that the incident was an inside activity as the insider was able to gain access to multiple private keys held in custody and thus was able to transfer the crypto assets without authority of the rightful owners.

Consequently, we submit that there needs to be a reconceptualization of what is being held in custody and that all CASSPrs should be subject to "fit and proper person" analysis.[5]

5. Naming of CASSPrs

The nomenclature of "Digital Currency Exchange" or "Crypto Asset Secondary Service Provider" is, in our opinion, not that significant. What is important is that there be a consistent use of a single term so all participants know what is included under the appropriate regulatory framework. Thus, CASSPr is an acceptable name as it appears to fit with regulatory objectives.

6. Naming of crypto asset

The ASIC definition is adequately wide enough to cover the various types of crypto assets whether they be "Native" or "Asset Referencing."

7. Financial products

As has been argued above, a CASSPr does not hold any crypto assets, but instead holds on behalf of end users their respective private keys which are needed to carry out crypto asset transactions.

From a policy perspective, any regulation of crypto assets should begin with the issuing of a crypto asset. Certainly, some currently issued crypto assets are securities as they are really an interest in a managed investment scheme. But we argue that many crypto assets should not be so classified. For example, we do not agree with Gary Gensler's, chair of the US Securities and Exchange Commission, statement that a stablecoin is a security under US legislation (Securities

[4] See Report on Stablecoins, President's Working Group on Financial Markets, November 2021, https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

[5] We note on page 16 of the Consultation Paper a proposal for directors to be fit and proper persons.

Act 1933 – investment contract) which is similar structured as that detailed in section 9 of the Corps Act, is correct.[6]

8. CASSPr regulation

We submit that CASSPrs should be regulated where they hold private keys for their clients (end users). In doing so, the regulations must be clear that a CASSPr does not hold the crypto-assets but instead the CASSPr is holding the private key and as such certain security issues should addressed in the same manner as APRA has designated for Approved Deposit-Taking institutions. For example, CSP 234 aims to ensure that an APRA-regulated entity takes measures to be resilient against information security incidents (including cyber-attacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats. A similar styled requirement should be considered as the custodians of private keys are likely to grow in number.

9. NFTs

The concept of NFT issuance is still very immature. FATF has indicated that there could be some possible anti-money laundering activity associated with NFTs but it is too early to ascertain. Further, NFTs cover a very wide spectrum of associated underlying assets and as such we submit a separate investigation be undertaken by the government. Basically, NFT technology is in its infancy and as such we recommend that wait and see stage should be adopted.

For example, ISO TC307 has established a small ad hoc group of experts (TC307 AHG3) to investigate the relationship between physical assets and NFTs. The first author of this submission of a member of AHG3.

10. CASSPr proposed obligations

The proposed obligations appear to be appropriate in the circumstance. As for airdrops this is a complex issue. Clearly, recipients of airdrops are receiving the drop due to their ability to influence other possible acquirers of the relevant crypto asset. Airdrops are not usually managed by a CASSPr but the issuer of the crypto asset and as such regulating issuers at the source of the problem may be a better solution.

Liquidity measures could be a solution but if the liquidity requirement is too high and onerous then there could be a concentration of the CASSPr market to only a few raising competition issues. Care will need to be taken as this is a nascent environment and the Government surely does not wish to destroy the market prior to it reaching some maturity.

Although the Consultation Paper is primarily concerned with the regulation of Australian digital institutions, the issues and questions raised by the paper are global in nature. The recent US Department of Commerce paper (see note 3 above) asks how the US will maintain its competitive lead in the global digital asset market. Given the size and scale of the US digital market—fundamentally the largest—it is likely that it will take the lead in development and regulation. No individual country will want to place itself at a competitive disadvantage with the US through over-regulation. In this respect it is essential that any regulation should take

[6] See SEC Chair's statement, https://www.sec.gov/news/statement/gensler-statement-presidents-working-group-report-stablecoins-110121.

into account aspects of international harmonisation. That is not to say a country such as Australia should slavishly follow US regulation but it should be seen advocating mechanisms that could engender consensus on regulation throughout the world. These could include the OECD, the International Bank of Settlements, the World Bank and IMF, the European Investment Bank to suggest a few. It is necessary to prevent and avoid regulatory arbitrage emerging and international harmonisation is the key to achieving this end.

11. Further issues for consideration not raised in the Consultation Paper

We also draw your attention to the recent UK case of *Tulip Trading Limited v. Bitcoin Association for BSV* dealing with crypto assets.[7] This case concerns the stealing of certain private keys that were claimed to be owned by Tulip. Tulip argued that the 16 developers of the Bitcoin blockchain platform owed Tulip a fiduciary duty or a tortious duty of care to assist Tulip in reclaiming the relevant private keys necessary to recover the relevant crypto assets associated with the stolen keys. Without going into the details of this case, the court rejected Tulip's arguments. But a more relevant issue does arise out of this matter.

According to Chainalysis US$10.1 billion was stolen through DeFi applications.[8] DeFi applications operate through the use of smart contracts, which involve complex commercial arrangements operating on a blockchain. If the same value was stolen in the tradition financial sector, there would be multiple government enquiries across multiple jurisdictions. But this has yet not occurred. The most likely reason is that the various jurisdictional regulators do not have the expertise or the capacity to undertake serious investigations as to the causes of loss. Lack of regulatory oversight in dealing with DeFi products is substantially damaging the reputation of the evolving market.

We submit there needs to be a regulatory framework established for DeFi products before they are released for public consumption. For example, security validation testing of DeFi products should be mandatory. The *Tulip* case should not be the dispositive law when it comes to DeFi products even though the rationale for the Bitcoin platform does make sense.

If you would like to discuss any aspects of this response, then we are available to further discuss for clarification.

Kind regards

Dr Adrian McCullagh
[redacted]

Professor John Flood
[redacted]

27 May 2021.

[7] *Tulip Trading Ltd v Bitcoin Association For BSV & Ors* [2022] EWHC 667 (Ch).

[8] See Theft, Money Laundering, and NFT Market Manipulation Underline Importance of Safety and Compliance in Web3, Chainanalysis, May 12, 2022, https://blog.chainalysis.com/reports/chainalysis-web3-report-preview-safety-compliance-defi/.