Digital Asset Risk for Institutions

Thomas Murray Digital

Re: Australia Securities & Investments Commission Consultation Paper 343, *Crypto-assets as underlying assets for ETPs and other investment products*

July 2021

THOMAS MURRAY | Digital

[redacted]

https://thomasmurraydigital.com

[redacted]

Australia Securities & Investments Commission

Submitted by email to [redacted]

27 July 2021

Sirs,

Re: Consultation Paper 343, *Crypto-assets as underlying assets for ETPs and other investment products*

Thomas Murray Digital (TMD) is pleased to submit its comments to the Australia Securities & Investments Commission (ASIC) in response to Consultation Paper 343, *Crypto-assets as underlying assets for ETPs and other investment products*.

By way of background, TMD is a subsidiary of Thomas Murray, founded in 1994 and now a leading provider of market intelligence, third-party risk monitoring, compliance and technology solutions to the financial services industry. Banks, funds and financial institutions of all sizes leverage Thomas Murray's suite of services on a daily basis, and clients include some of the world's largest banks and asset owners. Thomas Murray's offering has evolved according to the industry's needs, recently introducing a third-party cyber risk assessment tool, regulatory solutions for fund management companies in Luxembourg, and cash correspondent bank monitoring. The company actively monitors and assesses over 100 investable markets and 2,000 financial counterparties, including Global Custodian Banks, Sub-custodian Banks, Cash Correspondent Banks, Transfer Agents, Prime Brokers, Central Securities Depositories, and Clearing Houses, among others, while the company's clients use its technology platforms to analyse their extensive supplier and counterparty networks. Thomas Murray has advised several central banks, regulators and governments on how optimally to structure post-trade capital market infrastructure.

Given the advent of blockchain technology and the birth of digital assets, TMD has been established as a new business line focused on extending Thomas Murray's market information and operational risk assessments from the traditional post-trade securities and cash asset classes into the emerging institutional digital asset sector. TMD assists institutional asset owners, asset managers and service providers, including exchanges and custodians, to understand the capabilities and associated risks of trading and holding digital assets, which will have an increasing presence in institutional portfolios. TMD is also cognisant of the great latent interest in digital asset-backed ETPs and the market's willingness to assume the resulting investment risk, while supporting ASIC's mission to protect retail and institutional investors alike by minimising the operational risks associated with managing such investments.

TMD has devised a comprehensive methodology for the assessment of the capabilities and associated risks of digital asset service providers, initially custodians and exchanges, and expanding to encompass additional services such as technology, fund administration, tokenisation, and clearing houses in due course. This methodology has been devised on the back of Thomas Murray's longstanding and extensive expertise in third-party risk management in the post-trade securities services industry, developed in partnership with ratings agencies, regulators and industry. Thomas Murray's classification of operational risks in the securities services and post-trade capital market infrastructure sectors has become an industry standard for due diligence and monitoring.

We would be pleased to share further details of our methodology with ASIC, particularly the areas where the firm's risk classifications have been extended to cover the novel aspects of digital asset services, should this be of interest. As may be expected, there is a particular focus on asset safety and operational risk as revealed

through examination of wallet and account holding structures, key management, secure architecture, risk management, and cyber security.

Given the firm's core competence, we have focused our response selectively on the proposals and questions set out in Section C, Responsible Entity Obligations, and specifically proposal C1 relating to good practices for the custody of crypto-assets.

We are grateful for the opportunity to submit our comments and hope that they may be helpful in supporting ASIC's efforts to set standards appropriate for the protection of investors and the development of institutional engagement with the digital asset class.

Yours faithfully,

Andrew Wright
Director

Hugo Jack
Manager

Thomas Murray Digital

C – Responsible entity obligations

Custody – proposal C1

TMD is supportive of the good practices proposed for REs in relation to the custody of crypto-assets. Accordingly, our response is most detailed in its discussion of the proposals in response to question C1Q1 and therefore, unless otherwise noted, reference may be made to this answer when considering the remaining questions in section C1.

C1Q1. Do you agree with our proposed good practices in relation to the custody of crypto-assets? If not, why not? Please provide any suggestions for good practice in the custody of crypto-assets:

The approach outlined in the consultation paper is well considered and proportionate to the operational risks associated with the safekeeping of crypto-assets that exist today, given the current state of development of the asset class and investors' understanding of the associated investment risks. While the market infrastructure and service provider landscape is still immature compared to the traditional securities industry, it is our view that rapid progress is being made on technological, legal and regulatory, and service provider/infrastructure fronts to serve this asset class.

The eventual future of financial instruments of all kinds will be digital, and so – perhaps counter-intuitively for a new asset class – once the novel requirements of digital assets have been assimilated, the financial services sector will find itself in increasingly familiar territory and able to provide the full range of services and protections afforded to investors in traditional securities, albeit in some cases through new forms of provider and infrastructure. This movement will be aided in time by the gradual tightening of good practice regarding digital assets in order to align it with that of pre-existing types of financial instruments. We would therefore encourage the timely progression of standards from recommendations of good practice – including many of the proposals in Consultation Paper 343 – to regulation, in due course.

We provide commentary and further considerations for good practice against elements (a) to (i) below. While the primary custody function in relation to digital assets is the safekeeping of those assets through securing private keys, there are other aspects of asset servicing that are also important when assessing the suitability of a custodian, and a discussion of this point may be found below in our response to question C1Q3.

(a) The chosen custodian has specialist expertise and infrastructure relating to crypto-asset custody.

It is TMD's observation that institutional investors and market participants currently value experience and expertise in the custodying and servicing specifically of digital assets over general traditional securities custody credentials. This is borne out anecdotally by conversations with Thomas Murray's clients and partners, and evidentially by the market share won to date by 'fintech' providers over traditional players such as bank custodians due to their longer experience and greater focus on digital assets.

This tendency is also echoed in a report on a recent industry survey conducted by Citibank and Global Custodian magazine titled *Is the securities services industry ready for digital assets?* (Citi and Global Custodian, June 2021, https://www.globalcustodian.com/wp-content/uploads/2021/06/Citi-Engaging-with-Digital-Assets-Report.pdf). Over 220 validated institutional respondents, including broker dealers, investment banks, asset managers, commercial banks/custodians, market infrastructural entities, and insurers, were asked to opine on important factors when considering the appointment of a custodian to safekeep digital assets. 47 per cent of respondents stated that experience in working with digital assets and their infrastructures is the most

important factor in choosing a third-party custodian, compared to just 23 per cent of respondents who believe that traditional custody expertise is pre-eminent (ref. Fig. 8 in the report).

While service capabilities and longer history with the management of operational risks relating to digital assets are valued most highly by investors today, and they are currently willing to maintain separate arrangements for the support of those investments, it is important to note that the playing field will be levelled once traditional providers gain sufficient experience. Many have long familiarity with the operation of Hardware Security Modules (HSMs) and the servicing of other, non-cryptographic forms of electronic financial instrument, and in time investors will be sufficiently satisfied with custodians' crypto-asset experience and will begin to place greater value on offerings that are fully integrated with the holding and servicing of their other assets. We note that even institutions that have established, or are establishing, standalone services today to ring-fence their main entities from risk are also developing fully in-house services for the future that will leverage the learnings from these early crypto-asset units.

(b) The crypto-assets are segregated on the blockchain. This means that unique public and private key(s) are maintained on behalf of the RE so that the scheme assets are not intermingled with other crypto-asset holdings.

We believe that ASIC's stance in favour of segregated assets on the blockchain confers several important advantages arising from preventing the commingling of a scheme's assets with those of others. As a matter of principle, and relying on the advantages afforded by modern software (particularly crypto wallet infrastructure), there should be segregation between any proprietary holdings of an RE and those held in a scheme on behalf of underlying clients, in addition to segregation of holdings by custodians at the same level.

Thomas Murray has paid great attention to the trade-offs between omnibus and segregated accounting models in the post trade space, and believes that maximum segregation of client assets is of paramount importance due to the overriding prerogative to protect against difficulties in recovering or porting assets in the event of the default of an intermediary such as a crypto-asset custodian.

Some crypto-asset custodians are arguing for use of omnibus accounts due to claimed operational efficiencies around key management, liquidity, reduced transaction fees, and privacy, but these benefits – particularly reduced transaction fees due to netting – accrue primarily to institutions such as broker-dealers, hedge funds, and other high-volume clients rather than to the buy-and-hold model more commonly of interest to retail investors.

Care must be taken here over terminology. Some of these arguments are based on a potentially misleading interpretation of the term 'omnibus' rather than on any true need to sacrifice segregation, but they may be used as a 'straw man' by custodians to put forward arguments that favour the custodian's convenience over client interests. The term may be applied in the context of using the hierarchical deterministic (HD) protocol defined in Bitcoin Improvement Protocol 32 to generate any number of private-public key pairs in a tree-like structure. The master private key must always be kept strictly secure with an HD structure as, if compromised, all assets held in any wallet in the tree may be stolen. Wallet addresses generated in this way, although derived from a single master key pair, enable segregation and sub-division of assets across multiple wallets in ways that enable custodians to move assets between hot and cold storage, or to limit the value held in any single wallet address, while preserving the allocation of a node in the tree structure to a named underlying client (since the custodian acts in this scenario as the ultimate record of ownership, in the absence of a Central Securities Depository or the blockchain itself underlying the asset storing ownership information). However, to permit this, the client (e.g. an RE) may need to give up control over the movement of assets.

Another argument held up in favour of omnibus accounts is privacy. The theory is that wallet addresses may be tied back to an underlying beneficial owner and threaten security. This is unlikely to be of concern to REs. In any case, use of segregated on-chain wallets, which would be identified in the first instance as being associated with a custodian, and not any underlying beneficial owner, can be accompanied by periodic rotation of wallet addresses. Any additional resulting on-chain transaction fees would be minor in comparison to the security afforded, and may in any case be mitigated as so-called 'Level 2' blockchain transaction scaling solutions are rolled out.

Since crypto-assets exist 'live' on the Internet and are unlocked by private keys that bear some of the characteristics of bearer instruments, particular care would need to be taken over the question of actual legal ownership in an omnibus account. In some cases, ownership rights are limited to a share in the interests of the account or wallet, which in turn holds a fungible pool of assets. This model is common in bearer markets such as Germany, Switzerland, Austria and Benelux. In case of a shortfall, a loss is born *pro rata* with other stakeholders in the omnibus account, irrespective of how the shortfall arose. Although this is often explicitly spelled out in the custody agreement between a custodian and client, the reality remains that clients with differing risk profiles (e.g. pension funds and hedge funds) may have their assets bundled together.

Use of segregated on-chain wallet addresses gives custody clients such as REs the crucial ability to validate beneficial ownership of assets through the value chain and to verify that any transaction instructions are carried out accurately, and that assets are not moved unless authorised by the client. This is unfortunately not yet prevalent among digital asset custodians: many clients will not put assets into omnibus accounts by choice, but at present that choice is lacking. We therefore support ASIC's proposal to set the standard by defining segregation of assets as good practice, as is common in the traditional securities space where balances reported by custodians are reconciled to Central Securities Depository account records.

(c) The private keys used to access the scheme's crypto-assets are generated and stored in a way that minimises the risk of unauthorised access. For example:

(i) solutions that hold private keys in hardware devices that are physically isolated with no connection to the internet (cold storage) are preferred. Private keys should not be held on internet-connected systems or networked hardware (hot storage) beyond what is strictly necessary for the operation of the product; and

This is sensible, although care should be taken with the processes surrounding transfer to/retrieval from HSMs of private keys – particularly any manual procedures – to ensure that undue human factor risk is not introduced. Some custody offerings treat private keys in a similar way to physical security for bearer instruments. Good practice would be to design a custody solution such that digital assets can be migrated from the cold/offline environment to a hot/online wallet environment with as much automation as possible.

Reliance on manual processes introduces 'key person' risk and/or the need to give trusted access to a pool of people, who in turn require vetting and monitoring, in order to provide sufficient coverage. At times of high asset price volatility, manual processes may also lead to increased investment risk due to an inability to access funds and transact quickly. If these processes are inadequate, malicious internal actors (acting alone or together) could potentially make unauthorised use of private keys, leading to theft of assets. While rare, inside exploitation of cold storage access is suspected in some cases such as Swiss exchange Trade.io's 2018 loss of up to US$7.8 million in value represented by its proprietary TIO tokens.

An emerging model is the use of a so-called 'warm' solution that aims to combine the security advantages of physically isolated offline storage with the speed advantages of internet-connected systems. These rely on automation to cross the 'air gap' to the cold storage through narrow specialist communications protocols such as optical QR code readers or laser communications rather than harder to secure TCP/IP connections.

They are supported by robust, secure architecture of the processes, software and hardware comprising the entitlement system that unlocks access to the HSM. This model will become best practice for clients who do not need or want the ultimate security offered by cold storage. Increased automation also facilitates transactions and client service potentially on a 24x5 or 24x7 basis, outside traditional banking hours, removing the need for client instruction cut-off times, to the extent that no manual intervention is required.

(ii) the hardware devices used to hold private keys should be subject to robust physical security practices.

Agreed. Additionally, wider security reviews of HSMs should be conducted, to the extent not covered by proposal (f), covering the custodian's vendor management programme, the Secure Software Development Lifecycle for the software running on the HSM, and the maintenance and deployment of that software.

Various standards and assurance options are available to verify physical security and it may be left to the market at this stage to determine which are considered appropriate.

(d) Multi-signature or sharding-based signing approaches are used, rather than 'single private key' approaches.

Use of multi-signature or sharding approaches provides important additional layers of security and flexibility. A single private key approach perpetuates single point of failure risk, whereby unauthorised access/theft or loss of the key can cause permanent loss of assets. Options for speed of transactions, disaster recovery, and recovery and resolution are also reduced with use of a single private key. As the consultation paper outlines, both multi-signature and sharding approaches more effectively mitigate the risk of the theft or hacking of private keys, since multiple keys/shards would need to be compromised. Of these, a multi-signature approach is superior not just because it obviates the need to reconstitute a private key on a single device in order to sign a transaction but importantly due to increased transparency and auditability. Multi-signature transactions show which signature-holders have signed the transaction, supporting accountability. This also affords additional operational security options such as enforcement of signature requirements across multiple levels of seniority, teams/geographies and organisations.

For blockchains that do not (yet) support multi-signature transactions, multi-party computation (MPC) offers a superior alternative to Shamir's Secret Sharing (SSS) since it removes the need to reconstitute pieces of a key on a single device. Instead, partial signatures are created on their respective host devices and these then combine (once enough parts have been processed) to sign the transaction without that single point of failure/risk. As the result is blockchain-agnostic, MPC may be used in place of SSS. MPC may also be layered on top of multi-signature solutions for increased security, but does not act as a substitute for them as MPC does not provide the same accountability and auditability advantages. Not all HSMs yet support the relatively new MPC approach, but we recommend that MPC is added to the proposals for good practice where it may be used.

Given that sharding constitutes a minimum level of additional security for the most basic blockchains, that multi-signature and MPC approaches may also be used and are now sufficiently mature and simple to deploy, and that the digital asset industry is adept at evolving rapidly and benefits from having little or no legacy infrastructure, there can be no serious argument for not encouraging their use.

(e) Custodians have robust systems and practices for the receipt, validation, review, reporting and execution of instructions from the RE.

As a critical part of the activity that custodians of traditional assets undertake today, this should clearly be in the scope of good practice for digital asset custodians. There is little value to securing HSMs but leaving weak links elsewhere in the chain. This depends on a broad view of the secure architecture of the whole system, encompassing its design and processes as well as software and hardware. A key requirement is the enforcement of segregation of duties, ensuring that no one individual is able to process all parts of any given activity (as addressed by good practice (f)). In combination with use of segregated on-chain wallets (as addressed by good practice (b)), clients may reconcile independently the custodian's activity against the underlying blockchain wallet, ensuring that no transactions have taken place without authorisation and that authorised transactions have been executed correctly.

(f) REs and custodians have robust cyber and physical security practices with respect to their operations, including appropriate internal governance and controls, risk management and business continuity practices.

Agreed, and even more essential for digital assets than for traditional securities due to the increased cyber risks. The operations should be covered by comprehensive programmes that look at secure architecture by covering the design of processes in addition to software and hardware. Physical security must encompass the whole organisation, beyond HSMs and servers down to any devices used in the external validation or signing of transactions as part of an entitlement system, including Multi Factor Authentication devices. Risk management must cover vendor management (assessment of the practices of vendors for third party risk, particularly where they supply core systems, for all the governance and controls exercised by the RE or custodian) and Secure Software Development Lifecycles. Business Continuity/Disaster Recovery processes will also become increasingly important as custodians must demonstrate that they have escrow or 'living will' arrangements that allow independent recreation of wallet structures and client access to assets in case of compromise or inability to operate of the RE/custodian or any key vendor.

Thomas Murray's operational risk assessments look for effective implementation of a 'three lines of defence' risk control model. This should comprise firstly procedures and controls at the level of the business unit executing a process, and that include risk and control self-assessments e.g. on an annual basis to ensure understanding and compliance with the procedures and controls as designed by management. The second line is an independent risk management and/or compliance department that has input into the design of procedures and controls and that checks for deficiencies in their execution and in their scope in case of negative events. The third line comprises the internal audit function.

(g) The systems and organisational controls of the custodian are independently verified to an appropriate standard—for example, through a SOC 2 Type II or equivalent report.

Asset owners and REs would of course benefit from external assurance reports on a custodian's controls environment. However, for a young crypto-asset industry, certifying compliance over a substantial period of time with mature policies that meet the requirements of complex standards may be practically difficult at first. That said, TMD observes that several institutional-grade custodians believe this to be a requirement of many investors and a point of potential differentiation, and are undergoing SOC 2 Type I and even Type II assessments. However, we not that while it is good practice, a significant number of custodians within the legacy securities industry do not have such reports due to a combination of factors, primarily a purported lack of client demand.

It may be that a subsidiary of a bank set up to custody digital assets effectively inherits a comprehensive controls environment from its parent, but auditors are insisting that it must undergo a review as if it were a

blank slate such as a startup fintech company, and obtain its own report. However, in such cases most of the work will already have been done and so it is more a matter of time than additional effort.

Where reports are unavailable, ASIC and the market may look more closely themselves at the custodian's controls environment and the levels of independence of the higher tiers of the 'three lines of defence'. Even where reports are available, it should be borne in mind that there is no independently defined scope for the controls that are audited, and an organisation may therefore to an extent define its own boundaries, particularly for a more free-form review such as an ISAE 3000 report compared to a somewhat more standardised ISAE 3402/SOC 2 report that has a greater chance of capturing all significant financial processes.

One other observation is that custodians will sometimes cite SOC reports but on closer examination it transpires that they have in-sourced a custody solution from a third party provider, and it is that system provider who has undergone assessment and not the provider of the overall custody service.

In some cases, organisations are undergoing separate assessments of their Key Ceremony (generation of private and public key pairs) and key management as a discrete and critical set of processes, in addition to more general organisation-wide reviews.

Good practice in this area will emerge as more reviews are carried out. It is possible to review publicly available confirmations of engagements of auditors that set out the scope of reviewed control objectives to build up a picture.

(h) REs and custodians have an appropriate compensation system in place in the event a crypto-asset held in custody for REs is lost.

We agree with ASIC's proposal that there should be an appropriate compensation system in place in the event of a loss of crypto-assets. The components of such a compensation system would typically be set out in the commercial agreement between the custodian and the RE. It should address the custodian's ability to meet requirements set out in the compensation policy by explaining the scope of support provided through a compensation scheme and defining the liabilities and indemnities afforded to both parties in case of a loss event.

While insurance is an important part of an appropriate compensation system, there is as yet no standardised approach to insurance among digital asset custodians. Some only insure the value of assets held in hot storage; others insure a proportion (and often a small one) of the value of assets held in cold storage; and yet others cover a proportion of assets held across both storage mechanisms. Much insurance cover stops at the point that assets are moved, so transactions – the riskiest part of the lifecycle – are not covered by it.

This disparity may be understandable given the nature of the risks associated with safekeeping crypto-assets, for which the market has not yet reached consensus on optimal structures. Different environments entail different classes of insurable risk: hot storage insurance more closely resembles cyber insurance, whereas cold storage may be more closely aligned with property insurance. In any case, REs and custodians should consider the level of cover in proportion to the value of assets under custody and compare this to other resources such as self-insurance using the custodian's balance sheet. On that topic, the industry has not met the Basel Committee on Banking Supervision's preliminary proposals to require 100% reserve backing of the value of crypto-assets with favour, and indeed investors likely understand and are willing to accept some of the risk of investing in such currently volatile assets, rather than to pay very high custody service fees.

Apart from compensation for loss, Thomas Murray holds that a custodian should accept full responsibility for the timeliness, completeness and accuracy of information provided to clients (e.g., in the case of crypto-assets, should there be the equivalent of 'corporate actions' such as airdrops or forks), and agree to make

clients whole for any losses incurred as a direct result of the custodian's negligence or misconduct, including through any sub-custody provision or other supply chain within its control.

(i) If an external or sub-custodian is used, REs should have the appropriate competencies to assess the custodian's compliance with RG 133.

There appears to be a trend in favour of sub-custody models in the digital asset class, including in some cases the ability for clients to choose their own sub-custodian from among a panel of approved providers, facilitated by common operating standards and APIs. These arrangements lead to increased counterparty risk and operational risk, as Thomas Murray observed during the early years of global custody, when the industry saw a proliferation of intermediaries to support the ecosystem.

Given the complexities and scale of assessment obligations, and in order to avoid duplicated and fragmented due diligence efforts, REs and custodians may opt to partially outsource these activities to a third party and/or to rely on external specialist input from a firm such as Thomas Murray. Mutualised efforts increase awareness and uptake of best practice in the market and ensure high quality and consistent assessment of relevant risks. The benefits of such an approach to service providers are the ability to maintain standard high-quality responses to due diligence exercises and to focus attention on satisfying new and evolving requirements, rather than on having to expend effort on answering similar questions in many different formats.

C1Q2. Are there any practical problems associated with this approach? If so, please provide details.

We do not anticipate any problems with the proposals set out in the consultation paper. We believe they constitute a light touch in defining good practice, and a solid foundation for ratcheting up standards in the future. Any complexities or costs entailed in their enactment will be relatively minor in proportion to the protections they will give, and – due to the digital nature crypto-assets – will be enabled and minimised in time by evolving technology.

C1Q3. Do you consider there should be any modifications to the set of good practices? Please provide details.

Several additional considerations are discussed in the answer to C1Q1 above and may be brought into the definition of good practice. Principal among them are the consideration of what may be widely varying capabilities among digital asset custodians, particularly if and when custody is expanded beyond Bitcoin and Ether, due to differing risk appetites, operational capacity and regulatory licensing. This would include TMD's definition of Asset Servicing Risk, which in the context of digital assets covers support for events that are perhaps somewhat analogous to corporate actions, such as forks, airdrops, staking and mining, and eventually for the servicing of tokenised and digital-native securities (income, tax, corporate actions, voting). Use of MPC and the so-called 'warm storage' model may also be considered marks of good practice. Finally, custodians should not be exempt from the KYC and AML/CTF practices outlined in proposal C2(a), and should work to ensure compliance with the Financial Action Task Force's Travel Rule.

C1Q4. Do you consider that crypto-assets can be held in custody, safely and securely? Please provide your reasons.

Yes, crypto-assets can certainly be held safely and securely. They are the next stage of evolution of electronic financial instruments. While the use of the Internet and distributed ledgers is novel, and at least partially

replaces the function of a Central Securities Depository as ultimate record of ownership, the infrastructure for digital assets is rapidly maturing, particularly so with regard to custody. Custody solutions benefit from multiple overlapping layers of protection, and with time it seems increasingly unlikely that any truly institutional-grade custodian would oversee a serious and uncompensated loss of assets.

C1Q5. Do you have any suggestions for alternative mechanisms or principles that could replace some or all of the good practices set out in proposal C1? Please provide details.

No, we believe that all of the good practices set out in proposal C1 are sensible and proportionate. They need not be replaced, but may be supplemented with some of the additional considerations described above.

C1Q6. Should similar requirements to proposal C1 also be imposed through a market operator's regulatory framework for ETPs? If so, please provide reasons and how it could work in practice.

We have no comment to make on this question, given Thomas Murray's area of competence.