australia@aima.org

aima.org

Director - Crypto Policy Unit
Financial System Division
Treasury
Langton Cres
Parkes ACT 2600

Submitted via email: crypto@treasury.gov.au

3 March 2023

Dear Sir / Madam,

Token Mapping Consultation Paper

The Alternative Investment Management Association[1] (AIMA) welcomes the opportunity to provide comments on the Australian Treasury's Token Mapping consultation paper[2] (the Consultation Paper).

As the global representative of the alternative investment industry, AIMA's involvement with crypto assets reflects the growing interest of our fund manager members in this evolving asset class. An increasing number of our member firms are considering, or already active in, various crypto asset markets or making use of products using distributed ledger technology (DLT).

These AIMA member firms include:

(i) crypto hedge funds employing alternative active strategies in crypto assets;

(ii) established alternative investment fund managers looking to diversify their existing portfolios through either active or passive investments in crypto assets; and

1 The Alternative Investment Management Association (AIMA) is the global representative of the alternative investment industry, with around 2,100 corporate members in over 60 countries. AIMA's fund manager members collectively manage more than US$2.5 trillion in hedge fund and private credit assets. AIMA draws upon the expertise and diversity of its membership to provide leadership in industry initiatives such as advocacy, policy and regulatory engagement, educational programmes and sound practice guides. AIMA works to raise media and public awareness of the value of the industry. AIMA is committed to developing skills and education standards and is a co-founder of the Chartered Alternative Investment Analyst designation (CAIA) – the first and only specialised educational standard for alternative investment specialists. AIMA is governed by its Council (Board of Directors). For more information, please visit www.aima.org.

2 Australian Treasury, Token Mapping Consultation Paper (February 2023).

(iii) various other fund managers, fund service providers and platforms using technology to offer innovative services to investors, leveraging upon the potential benefits of DLT.[3]

AIMA is very supportive of developing appropriate regulatory settings for the crypto ecosystem in Australia. AIMA supports the Australian Government's commitment to a fact-based, consumer conscious and innovation friendly approach to policy development, particularly in a market disruption of leading-edge technological innovation.

Crypto assets, by operation, invoke both rights for and actions from the interacting parties. Regulating activities relating to crypto assets requires careful consideration and planning. AIMA members believe a licensing regime for the market activities in crypto assets needs to be balanced between:

(a) consumer (and businesses) protection using statutory frameworks and excessive "red-tape" that stifles innovation; and

(b) flexibility in administering the legislation and clear rules to foster regulatory clarity.

[3] The AIMA Digital Assets Working Group (AIMA DAWG) is a cross section of senior industry experts including investment managers, allocators, custodians, exchanges and other service providers. The group is tasked with driving AIMA's regulatory engagement, thought-leadership initiatives, and operational guidance in the area of digital assets.

ANNEX

Token Mapping Consultation Questions

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

Governments should ensure that crypto assets are subject to appropriate statutory frameworks, while not stifling digital innovation with excessive "red-tape" in financial services. It is crucial to devise appropriate and proportionate crypto asset regulation and security safeguards for a robust digital economy that is accessible to both existing participants and new entrants.

The Government should prioritise providing greater regulatory certainty for crypto assets with increasing institutional investment interest, such as exchange/network tokens, in order to support greater investment activity. Additionally, the Government should prioritise clarifying how existing legislation applies to existing regulated activities using DLT; developing clear, risk-based and proportionate regulations for new DLT-based activities; and achieving alignment with international standards to support cross-border activity and provide legal clarity. We believe that the Government and regulators should take caution not to apply disproportionate or overly burdensome requirements to firms seeking to enter the crypto ecosystem, particularly where the activities do not pose a risk to financial stability, and seize the opportunity to position Australia at the forefront of the global crypto assets industry.

One way to achieve this is for the Government to act as the knowledgeable gatekeeper and trusted verifier of prudent practices, consumer protection measures and overall mechanism of how such 'promises' are ensured. For example, a licensing regime that mandates sufficient information disclosure or professional audits of the technology that claims to provide such protection without the conventional intermediaries. It is, therefore, important for the Government to be equipped with relevant tools and resources to perform this role in a meaningful way.

The variety of crypto assets means that it is difficult to create a perpetual bright line for regulatory purposes. Technology in the crypto assets space has and will continue to develop extremely quickly, thus AIMA believes that regulation which attempts to exhaustively categorise current crypto assets and technology could become outdated and outmoded extremely quickly – potentially before the new rules are even published in the relevant statute or regulatory guidance.

AIMA recommends that the application of any existing or new regulation to crypto assets must be sufficiently flexible to be able to develop alongside the underlying technology, whilst pursuing its key objectives including consumer protection, anti-fraud and financial stability. Each crypto asset should be considered according to its characteristics. The goal for regulation of crypto assets should be to aim for the same regulatory objectives leading to regulation of similar risks and activities to achieve comparable outcomes.

In addition to being able to deal with future developments in new crypto assets, AIMA recommends flexibility in the regulation of individual assets over time.

AIMA suggests that the future function of a token is a valid consideration for any regulatory regime and that immediate classification as a security may be a disproportionate result – especially if objectively the issuer did not intend for the token to function as a security or to be traded as such by investors. This is also the case for sufficiently decentralised organisations for which the regulatory objectives and framework of full securities laws are less relevant. A hybrid regulatory regime could be applied to this end. In such scenarios, we suggest that the application of regulatory obligations should occur proportionately, taking a holistic view of the abovementioned fundamentals of assets to ensure that particular investor protection, financial stability and other regulatory goals are achieved without placing unnecessary costs or restrictions on the issuer, financial institutions and investors, including the principle of "same risk, same regulatory outcome".

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

Institutional investors and allocators must have confidence in market structures and infrastructures in order for the crypto assets industry to truly institutionalise. We believe that all institutions that operate as gatekeepers to the crypto ecosystem should be subject to an appropriate standard of regulation.

AIMA believes that regulated financial institutional involvement in the crypto ecosystem would benefit consumers/investors and the regulatory community because regulated financial institutions constantly conduct risk identification/monitoring and risk management from both a prudential and conduct perspective. Furthermore, the existing regulatory frameworks have put in place safeguards such as market integrity rules that aim to guard against financial stability risks.

We support regulations designed to maintain and enhance sound legislative and regulatory structures which protect and enforce investors' property, shareholder and creditor rights in a fair, equitable and proportionate manner. We also encourage development of sound regulation dealing with the safe-keeping of assets and we support the implementation of robust and proportionate corporate governance structures. We also support efforts to establish common global definitions and templates for regulatory reporting and clearly defined and internationally harmonised market abuse definitions for sustaining the integrity of markets. These examples of regulatory principles and outcomes that we support should be applicable to the crypto ecosystem in order to take account of the fact that the activities and risks appear to be the same, but it many instances a different regulatory approach or framework might be required given the specificities and risk of different technologies.

We strongly believe that regulation should accommodate the diversity of actors across the crypto asset industry. As such, we support a more proportionate application of rules for firms that is based on the nature, size and complexity of their operations. Furthermore, in the context of

investment management, we believe that rules should reflect the significant differences in the business models, products and distribution channels of investment managers servicing retail investors and those of investment managers servicing professional and institutional investors. Regulatory principles, including any activity-specific principles, must be drafted in a way that recognises this diversity and does not encourage regulators to adopt a "one-size-fits-all" approach to the regulation of different subsectors, each with their own specificities, within an overall category.

(3) 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?

In 2022, the FTC reported that most crypto scams are investment scams – since 2021, US$575 million of all crypto fraud losses reported to the FTC were in relation to bogus investment opportunities.[4] The second most common, with US$185 million in reported losses in 2021, was 'romance scams' in which scammers strike up a relationship to build up trust and then ask for money. The third most common scam, with US$133 million in reported losses, was due to business or government impersonations.

Based on that, AIMA submits that raising greater awareness is crucial for safeguarding consumers. While technological vulnerabilities increase the potential for scams, a large number of crypto consumers are being led into scams out of naivety or lack of visibility. As set out in our response to paragraph (b) below, AIMA recommends that as a first step, all gatekeepers to crypto assets markets should be subject to appropriate regulation. As part of that, the Government may be able to develop rules specific to institutions such as crypto exchanges. Those platforms could be required to provide hacking and fraud risk ratings for investments, and real-time alerts of fraud and hacking attacks. Just as the ACCC is continuing to advocate with the finance sector and financial firms to increase efforts to combat scams and cyber threats, these efforts could also extend to crypto exchanges.[5]

(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?

AIMA believes that all institutions that operate as gatekeepers to crypto assets markets should be subject to an appropriate standard of regulation. We recommend that all institutions holding themselves out as "exchanges" or market makers should be subject

[4] Federal Trade Commission, "Reports show scammers cashing in on crypto craze" (3 June 2022), <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze>.

[5] Australian Competition & Consumer Commission, "Targeting scams: Report of the ACCC on scams activity 2021" (July 2022), <https://www.accc.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scams%20activity%202021.pdf>, 45.

to authorisation and minimum regulatory requirements, including robust systems and controls requirements in relation to cybersecurity risk management, as well as all relevant AML checks, market manipulation prohibitions and frontrunning protections.

AIMA recommends that market abuse and specific and general anti-fraud prohibitions are applied to crypto assets exchanges and market makers. This should include market manipulation prohibitions for crypto assets that are traded on what are open secondary markets. To this end, we also suggest that crypto assets exchange operators be subject to market abuse detection and reporting obligations in the same manner as securities exchanges. Some crypto assets may already be covered by traditional market abuse rules, for example, where a public issuer has issued a token or a particular crypto asset is influenced by the price of a public security. Nonetheless, AIMA believes the direct application of market abuse rules to crypto assets is an important step towards institutionalisation – in particular anti-market abuse rules.

(4) 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?

The purpose of exploring the concept of 'exclusive use or control' of data is to establish that, despite being unable to be possessed, data objects can still be the subject of property rights. Information, not just public data, cannot generally be treated as the subject of property rights because it cannot be exclusively controlled. Crypto tokens and crypto networks exist via computer code – they are, in substance, bits of information. However, due to the particular technological features in combination with cryptography, they are able to be exclusively controlled. Accordingly, AIMA submits that 'exclusive use or control' is an important pre-condition to be able to treat crypto tokens on crypto networks as property and subject to property rights. This makes it necessary but insufficient on its own for an adequate definition of crypto tokens or crypto networks.

The Consultation Paper notes that 'exclusive use or control' is used in Article 12 of the American Uniform Commercial Code (UCC) (2022 Amendments), which regulates "controllable electronic records". The prefatory note to Article 12 states that this concept is meant to apply more broadly than to existing technologies, and aims to apply to electronic assets that have yet to be developed or even imagined. Article 12 of the UCC uses the concept of 'exclusive use or control' to outline electronic records that can be subject to property rights and attract rights of protection for purchasers. AIMA recommends that, while the concept is important, a general definition should make more specific reference to the technological features of crypto tokens and crypto networks to more accurately capture the DLT-specific technologies to which existing regulatory frameworks should extend.

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

Adopting 'exclusive use or control' as the only distinguishing feature in a definition for crypto tokens and crypto networks may introduce flexibility and technological neutrality, but will fail to address the specific issues with crypto assets and DLT arising today. As noted above, the decision to focus on "controllable electronic records" under Article 12 of the UCC was to keep the concept deliberately vague to serve the purposes of consumer protection within that particular context. Accordingly, AIMA submits that participants in the crypto ecosystem in Australia would benefit from legislation and definitions that are specific to crypto assets and DLT. To create a definition that is specific to this context requires reference to DLT and the defining technological features of crypto assets.

AIMA notes, however, that the focus of 'exclusive use or control' surfaced a further crucial distinction in Article 12 of the UCC. The prefatory note to Article 12 explains that its concept of "controllable electronic record" distinguishes between (i) the record and (ii) the rights being evidenced by the record. A "controllable electronic record" is one where gaining control of the electronic record gives the controller the right that accompanies the record. The association between right and record is even stronger for crypto assets that are currencies, such as Bitcoin and Ethereum, where the record is itself inherently valuable. Not recognising this distinction can lead to ambiguity. The Australian Securities and Investment Commission (ASIC)'s definition of 'crypto assets' in Consultation Paper 343 – Crypto-assets as underlying assets for ETPs and other investment products is as follows:

> *"a digital representation of value or rights (including rights to property), the ownership of which is evidenced cryptographically and that is held and transferred electronically by a type of distributed ledger technology or another distributed cryptographically verifiable data structure."*

ASIC's definition is sufficiently confined for its purpose of administering the Australian Financial Services (AFS) licensing regime for managed investment schemes. In particular, the definition justifies ASIC's approach in the relevant disclosure requirements and establishes the risk profile of crypto assets. However, AIMA considers that this definition may inadvertently include data structure, that represents value or rights, operated on a private network,[6] whose sole intent and purpose are to on-ramp physical assets onto a digital ledger. An example of this use case is the digitisation of a fund administrator's books and records maintained for the fund using DLT, where each digital certificate represents a share in the fund and such records are cryptographically secure to avoid tampering or error. ASIC's definition does not adequately make use of the distinction

[6] Refers to 'Network of participants' as described in INFO 219 – Evaluating distributed ledger technology.

between right and record, as brought to light through the 'exclusive use or control' concept – if it did, then the definition would not capture data structures that are merely records.

(5) **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?**

AIMA is not in favour of a bespoke taxonomy, see further our responses in (b) below.

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

Existing financial and other regulatory regimes did not envisage the advent of crypto assets, thus regulators and legislators globally are moving to consider how the new instruments are, or should be, covered. However, it is important to highlight that many crypto assets have many similarities to existing categories of assets and could in fact fall within existing regulatory classifications with certain minor modifications.

Some function as a means of payment and are intended to function in a similar way to making electronic payments or transfers with existing currencies – instead using DLT to record transactions rather than centralised ledgers. Other crypto assets function as a means of accessing a particular commercial service, asset or utility, in a similar manner to purchasing retail vouchers or participating in crowdfunding schemes in return for a particular utility – but with the ownership of the asset being recorded using DLT. Some crypto assets confer ownership or other equity-like rights in a particular issuer – simply these are processed and recorded.

AIMA supports the proposal for crypto assets and intermediaries to be subject to regulations in line with the principle of same activity, same risk, same regulation, where they clearly perform an equivalent economic function and application to one performed by instruments and intermediaries in the traditional financial system. However, we strongly believe that regulation should take account of the novel features of crypto assets and fully harness the potential benefits of the associated technology.

AIMA believes that crypto assets should be viewed merely as an extension of existing financial and non-financial assets which require the same overarching regulatory considerations and outcomes, considering their specific purpose, characteristics and degree of fit within existing regulatory rules and requirements.

We acknowledge that when developing rules and regulations for crypto asset activities and markets, there is a need to first understand better what exactly the technological differences are to those in the traditional financial system (e.g., decentralisation,

continuous on-chain settlement, immutability and irrevocability of transactions, no single point of failure, traceability and transparency of information, automation of many of the functions in the value chain). Subsequently, with greater understanding of how crypto asset activities are not the same, despite them presenting similarities, it would be prudent to use basic principles of financial regulation in order to craft appropriate regulatory frameworks that achieve the same objectives being sought when regulating traditional finance.

The key questions include:

- What is the fundamental purpose of the crypto asset?
- What are the characteristics of the crypto asset, its underlying asset/service (if any) and the DLT upon which it has been generated?
- Does the asset fit accordingly into an existing regulatory classification?

Several jurisdictions have moved to clarify that crypto assets fit into the scope of traditional securities, commodities and money classifications. However, pure "cryptocurrencies" are generally less likely to be regulated. AIMA believes that those crypto assets which look and function like a traditional investment contract or security should indeed be regulated as such.

Of course, if a crypto asset does not logically fit into an existing regulatory classification, we advise against seeking to simply squeeze them in without first thinking about what regulation is actually needed. This view is emphasised throughout our response in this submission, generally speaks to the importance of the role of government in understanding the operation of crypto assets, crypto networks, and how they ensure (or not) the intended promises given to the consumers, before identifying an appropriate way to demonstrate such purposes and qualities.

(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?**

AIMA believes that the general consumer protection framework should apply alongside the financial services regulatory regime. For example, the doctrine of misleading and deceptive conduct as well as the unfair contract terms regime that are currently entrenched in the *Competition and Consumer Act 2010* (Cth) should equally apply in the context of crypto assets with necessary modifications. Meanwhile, regulators should also issue regulatory guidance that sets out the expectations and "guardrails" that industry participants need to work within.

(6) **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?**

It is important that any new regime for crypto assets does not overcome or somehow replace existing relevant legal requirements simply as a result of the underlying asset being tokenised.

The United Kingdom Law Commission is currently considering the same issue.[7] In one of the responses to its Digital Assets: Consultation Paper, the Association of Global Custodians – European Focus Committee states that "it is likely that the relationship between a digital asset token and the underlying tokenised asset will often depend, at least in part, on the terms on which the digital asset token is issued. For example, it may confer all, or only certain, property rights in the tokenised asset on the holder of the digital asset token. This flexibility may, however, create uncertainty for investors and there may be advantages in introducing limited legislative measures, where necessary, to ensure alignment of property rights as between the digital asset token and the underlying tokenised asset".

(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?**

Please see our response to (a) above.

(7) **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?**

Institutional investors and allocators must have confidence in market structures and infrastructures in order for the crypto assets industry to truly institutionalise. This includes confidence in the stability and transparency of the trading environment, and the degree of counterparty risk to which firms may be exposed. It is clear that any underlying counterparty risks must be mitigated sufficiently in order for the crypto assets market to become truly institutionalised. Regulatory protections for crypto assets should be focused upon anti-fraud/market abuse provisions for the trading of the assets, client assets protection for assets custodied by intermediaries and market stability – rather than seeking to restrict investments and/or trading in particular assets. Although the

[7] United Kingdom Law Commission, Digital Assets: Consultation Paper (July 2022).

overarching regulatory questions remain the same as for other assets, crypto assets themselves are highly heterogeneous and will require flexibility of regulatory responses to achieve similar regulatory outcomes. The creation of an aptly regulated environment is particularly important for investment managers as firms must fulfil their fiduciary duties, meet redemptions and maintain the structure of portfolios in the interests of clients.

It is important to distinguish the role of 'service providers' and 'issuers' of crypto tokens, as the latter, in some cases, is in a better position to have mandated access to information that allows users to identify arrangements underpinning the tokens. Such access is currently argued to be sufficient by simply having open-source codes. However, this requires certain hurdles in expertise to interpret and fully understand the 'information' in the codes, which voids the purpose of allowing access in the first place. The Government, in developing a licensing regime, may incorporate a simple checklist that crypto token issuers or service providers must display to the users of the tokens. The item on the check list can be those functional parameters or principles that are used in assessing traditional financial assets service providers.

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

AIMA does not have any specific comments on this question.

(8) **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?**

By way of general comment, we think that the existing financial services regulatory framework in Chapter 7 of the Australian Corporations Act provides an appropriate basis upon which it is possible to characterise a particular crypto token or asset as a financial product (if necessary). We do not see a need to specifically define or prescribe specific intermediated assets as financial products in the law. We say this because; (a) in the first instance, given the potential broad scope of potential categories of intermediated assets it may become very difficult to define or prescribe with precision a comprehensive listing of all types of tokens which may, or may not be financial products; and (b) given the broad definition of a financial product, which includes a facility through which a person does any, or more of, making a financial investment, manages a financial risk or makes non-cash payments (see s763A of the Corporations Act), there is scope for a wide range of arrangements to be characterised as a financial product. Accordingly, we do think there is a potential enhanced role for regulatory guidance which can set out appropriate

frameworks against which to assess particular types or categories of intermediated crypto assets.

The regulatory guidance mentioned above could go further and also specifically identify those assets which, in the regulator's view, are financial products. Regulatory guidance can also be updated over time as the market evolves and can be a more flexible and "real time" mechanism than a formal approach to including specific intermediated assets as financial products (or for that matter excluding them from the definition) for example by way of regulations. We note also that the regulator has the ability to determine that a facility, interest or thing is not a financial product and this mechanism can also be used to provide certainty for industry participants when dealing in crypto assets as to whether it will give rise to financial product licensing considerations (s765A(3)) of the Corporations Act).

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

In this regard, we refer to our comments in (a) above. We consider that there is sufficient flexibility in the current legal regime, and an enhanced role for the regulator to play, in assisting to clarify the scope and extent of the application of financial services regulation to crypto asset activities.

(9) **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?**

As noted in AIMA's responses to other questions, institutional investors and allocators must have confidence in market structures and infrastructures in order for the crypto assets ecosystem to truly institutionalise. This includes confidence in the stability and transparency of the trading environment, and the degree of counterparty credit and cybersecurity risk to which firms may be exposed.

AIMA believes that all institutions that operate as gatekeepers to crypto assets markets should be subject to an appropriate standard of regulation.

We recommend that all institutions holding themselves out as "exchanges" or market makers should be subject to authorisation and minimum regulatory requirements, including robust systems and controls requirements in relation to cybersecurity risk management, as well as all relevant AML checks, market manipulation prohibitions and front-running protections. At this stage, we do not have any specific measures in mind for assessing the suitability of a specific public crypto network to host wrapped real world assets.

(10) **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?**

AIMA does not have any specific comments in relation to this question.

(11) **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?**

The Government should provide a "best in class" regulatory environment that can properly support the promotion and development of new and existing technologies while ensuring a well-founded, clear and robust legal basis for such developments. AIMA acknowledges that greater regulatory clarity for crypto assets is necessary for consumer protection and would welcome the introduction of clear and consistent regulation of the sector.

In the United Kingdom, the Government is looking at enhancing consumer protection by ensuring that crypto asset promotions can be held to equivalent standards as promotions of financial services products with similar risk profiles.[8] This would mean firms being required to use specific risk warnings and positive frictions in their consumer journeys, in addition to the overarching requirement that their promotions are clear, fair and not misleading. As previously stated, AIMA believes that regulatory and supervisory approaches for crypto assets should be based on a "similar risk, similar regulatory outcome" principle.

(12) **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?**

As noted in AIMA's responses to other questions, providing a "best in class" regulatory environment with a clear legal basis for technological developments will have the positive effect of providing certainty that smart contracts will be subject to existing regulatory frameworks.

AIMA submits that the Government should not try to directly regulate the substance of the code within smart contracts. Regulation is most efficient where there are insufficient market forces to incentivise actors to act well, and where there are central points to which regulation can be applied. Regulations which impose restrictions on the substance of a contract, such as employment law and tenancy law, apply to employers and landlords,

[8] *See*, United Kingdom Government, Policy statement on approach to cryptoasset financial promotions regulation (February 2023).

respectively. The decentralised governance and automation that smart contracts allow create a dependency on the technology itself without clear recourse to a central owner or controller on whom liability can be imposed for detrimental outcomes.[9]

Rather than focus on the substance of the contract, regulation may be more effective in assuring that the technological stack underlying the smart contract meets a particular standard. The Malta Digital Innovation Authority (MDIA) that was established in 2018 focused its regulation of smart contracts, and DLT more broadly, to address the relevant technological arrangements, rather than regulating crypto assets. The resulting law targeted assurance that the technology passed quality tests that would address certain vulnerabilities. Malta's resulting Innovative Technology Arrangements and Services Act (2018) introduced licences for which developers could apply. This allows developers to voluntarily gain certification that can provide a level of trust in the market – given the losses that can arise from technological vulnerabilities in crypto networks, actors are incentivised to seek expertise.[10]

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

Smart contract applications are wide-ranging and can cover a number of industries and sectors. Beyond the technological assurance referred to in AIMA's response in paragraph (a) above, AIMA submits that smart contract applications as a category is too broad and varied to be considered monolithically.

As noted above, AIMA recommends that it is most useful for the Government to provide greater regulatory clarity for crypto assets within the patchwork of existing regulatory frameworks. Since smart contracts and smart contract applications are an avenue through which crypto tokens and crypto networks can be accessed, the creators of the particular smart contract applications are more likely to be incentivised to comply with the regulatory frameworks that clearly apply to what they build. For example, the set of regulations applicable to Uniswap as an automated market maker are different from the set of regulations applicable to smart contract applications that facilitate the creation of decentralised autonomous organisations (DAOs). Clarifying the application of the respective financial and corporate laws to the relevant smart contract applications would reduce the friction and uncertainty in compliance.

(13) 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).

[9] Joshua Ellul, Jonathan Galea, Max Ganado, Stephen Mccarthy, and Gordon J. Pace, 'Regulating Blockchain, DLT and Smart Contracts: a technology regulator's perspective' (2020) 21 ERA Forum 209-220 <https://doi.org/10.1007/s12027-020-00617-7>, 216.

[10] Ibid., 217.

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

We understand the Treasury is concerned with "smart contract lending" as described in paragraphs [190]–[191] (Annexure 3) to the Consultation Paper. Under that structure, smart contracts facilitate secured lending in two ways. First, smart contracts pool and match supply-side financiers and demand-side borrowers, with price discovery (e.g. equivalent to traditional interest) being driven by supply and demand. Second, smart contracts allow collateral to be made available to supply-side financiers and automatically liquidated upon agreed triggers being met (such as a loan-to-value ratio), avoiding the need for cumbersome enforcement processes. As noted in paragraph [193], apart from the initial decision to use the protocol, the decision to lend, and to liquidate collateral, is entirely non-discretionary.

There are a number of key risks present in this smart contract structure which are not present in traditional secured lending. The precise detail of these risks will depend both on the smart contract structure and the traditional lending structure used as a counterfactual. However we have set out some headline risks below in general terms (and in no particular order):

- Smart contract protocols may not be legally enforceable, rectifiable or persistent, creating uncertainty and risk for lenders and borrowers.
- Unclear property status of crypto assets may undermine security rights and remedies of lenders, affecting credit availability and cost.
- Automated lending may prevent lenders from controlling who they lend to, exposing lenders to money laundering, know-your-client and credit risk.
- Automated lending may create interface risk between smart contracts and traditional financial institutions or protocols, affecting property rights and performance.

These key risks are expanded on below.

- The smart contract protocols which automatically effect the lending and security are (arguably) not "contracts" in the legal sense (as discussed in paragraph [167]). The first consequence of this is that it is not clear how any dispute as to the content of such smart contracts could be interpreted legally. For example, any dispute as to the content of the smart contract – such as whether there were legally implied terms, how the pricing calculations apply to unforeseen scenarios, whether the financier actually has a legal entitlement to retain proceeds of liquidated collateral, whether an instruction from a smart contract protocol to withdraw/deposit funds is duly authorised – may not be capable of being

determined by a court. A second related issue arises where the smart contract relies on external data which is subsequently varied, interrupted, manipulated or found to be incorrect. In that circumstance it is not clear how, or whether, the financiers or borrowers are entitled to seek that the smart contract be rectified to reflect their actual intention. This becomes particularly problematic in the context of insolvency, where it is necessary to precisely understand what rights and obligations exist – there is no clear regime to compromise, deal with, or set-off obligations in the scenario where relationships are "governed by software rather than law" (see paragraph [171]). All of the aforementioned concerns are exacerbated in the context of a DAO lacking a central clearing counterparty where it may not be possible to back the smart lending protocols with natural language contracts entered into with a central clearing counterparty – in that context it may even not be clear who the appropriate respondent to any court proceedings would be. Finally, ordinary contracts are "persistent" in that (generally) rights and obligations do not cease to exist merely because the paper they are written on is torn up or the .pdf deleted (though there are obvious evidentiary issues). By contrast the existence of "rights" under a smart contract is contingent upon the smart contract protocol continuing to exist and operate. It is not clear how the law would deal with the scenario where there is an interruption to such rights part way through a transaction – for example, whether failure of the smart contract mid-loan meant the borrower did not need to finish making repayments. The effect of this is to introduce significant uncertainty as to the enforceability rights and obligations of the parties.

- Given there is no clear position on whether crypto assets are property – see paragraphs [123]–[129] – it follows that it is not clear whether the interests of a party in crypto assets, even if legally recognised, are "proprietary". A number of key features of the modern lending market depend on the ability to take proprietary interests in assets by way of security. Some, like the "self-help" nature of enforcement remedies, may not be relevant due to the way in which smart contracts automatically execute. However others, like the fact assets subject to security are ring-fenced on insolvency of the security provider and appropriated to satisfy the debt owed to the secured financier, or the ability to appoint a receiver or receiver and manager (rather than triggering a fire sale of collateral), may not be available when using smart contracts. The unavailability of such legal technique may result in credit not being extended to borrowers of certain credit risk profiles, or may result in credit becoming more expensive due to the risk that financiers will not be able to rely on their security in the event of borrower insolvency.

- The automated lending market described in paragraph [190] does not provide financiers with any discretion as to whom they lend (provided the borrower is

admitted to the platform). A couple of risks follow from this. First, the financiers are effectively required to outsource any anti-money laundering or know-your-customer checks to whomever operates the platform (or, in the case of a true DAO, to the checks built into the protocol (if any)). Financiers will similarly be unable to verify the use of proceeds of the borrower. Second, financers are unable to include any credit risk spread in the case of different borrower risk profiles, meaning that borrowers of higher credit quality in the smart contract pool effectively subsidise borrowers of poorer credit. Finally, financiers are unable to differentiate between borrowers based on metrics outside the smart contract protocol – for example, preferential pricing for ESG-linked borrowings. This has the effect of limiting the utility of smart contract protocols for regulated lending institutions.

- It is not possible (at law) to hold or convey property solely using software. Even if smart contracts adequately manage handling of crypto assets, transfer of funds or "real" securities require instructions be given to financial custodians and banking institutions. It is not clear how the interface between smart contracts and such counterparties will be managed, and even if there is no question as to the authority / validity of such instructions, using smart contracts in this fashion does not obviate the need to take performance risk on the traditional banking network. A different, but conceptually related, risk is that the existence of smart contract protocol is somehow affected, varied or interrupted, altering the rights of the parties. This could be in the form of performance risk on a trusted counterparty who is responsible for managing the protocol, but also could be as a result of a fork in the smart contract protocol or agreed amendment. There are means to limit this risk – see paragraphs [173]–[176] regarding immutability and upgrade risk – but the equivalent risk in the context of ordinary legal contracts (potential change in law) is less material. As a result, there remain interface risks which are at best already present in the traditional banking network, and at worse exacerbated by use of a smart contract protocol.

(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?

AIMA does not have any data on consumer outcomes in this context.

(14) 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?

AMM can be described as the decentralised version of a crypto asset exchange, which usually is operated by an identified and centralised entity. There are certain differences in the way AMM is governed and operated compared to a crypto asset exchange, leading to several differences in their risk profiles, including:

- Price volatility risk: Both AMMs and crypto asset exchanges are subject to price volatility risk. However, AMMs may be more volatile because their prices are determined by supply and demand, rather than being set by an order book.

- Liquidity risk: AMMs and crypto asset exchanges may have different levels of liquidity. An AMM typically provides liquidity using a reserve pool, which means that large trades can cause slippage or price impact. In contrast, a crypto asset exchange with a deep order book may be able to handle large trades without significant price impact.

- Counterparty risk: When using a crypto asset exchange, there is a risk that the exchange itself may be hacked or that the counterparty may default on their obligations. In contrast, an AMM does not have a counterparty risk because trades are settled directly on the blockchain.

- Regulatory risk: AMMs tend to operate without a license or anti-money laundering or know-your-customer provisions.

- Impermanent loss risk: AMMs may be subject to impermanent loss, which is the temporary loss of value that can occur when a liquidity provider provides funds to an AMM pool. This happens when the price of the tokens in the pool changes, causing the liquidity provider's share of the pool to change in value. Crypto asset exchanges do not have this risk.

- Smart contract risk: AMMs operate through smart contracts, which are software programs that run on the blockchain. If there are vulnerabilities in the smart contract code, there is a risk that funds could be lost or stolen. Crypto asset exchanges also use software, but the risk of smart contract vulnerabilities is lower.

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

While there are not many peer-reviewed studies on consumer outcomes in trading on each of these venue types, partly due to lack of credible or usable data, an industry-wide common source of liquidity ('total value locked') can be found at DeFiLama.[11]

* * *

[11] *See*, https://defillama.com