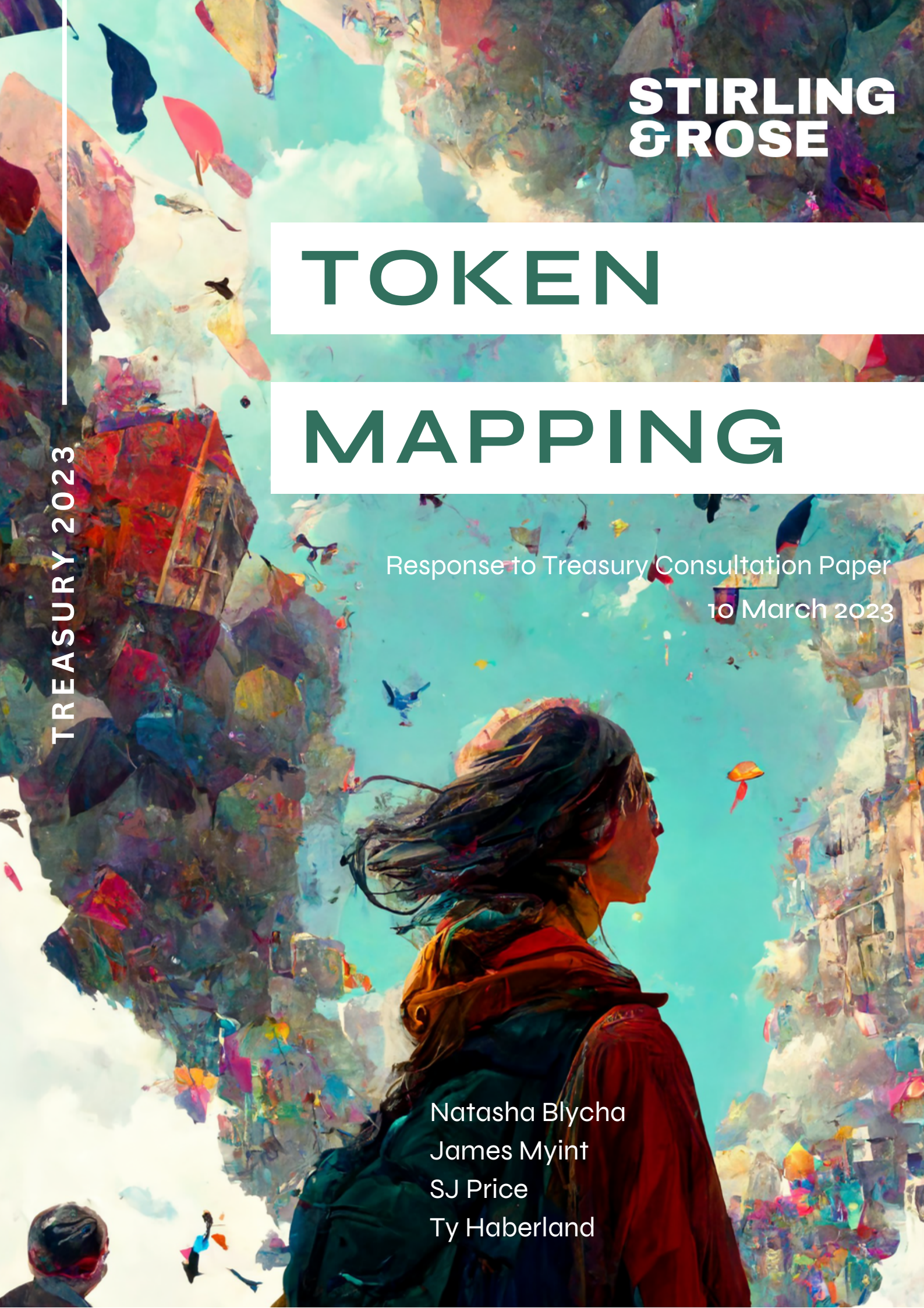

STIRLING & ROSE

TOKEN MAPPING

TREASURY 2023

Response to Treasury Consultation Paper

10 March 2023

Natasha Blycha
James Myint
SJ Price
Ty Haberland

Director
Crypto Policy Unit
Treasury
Langton Crescent
PARKES ACT 2600
By email: crypto@treasury.gov.au

STIRLING & ROSE

Dear Treasury,

Stirling & Rose welcomes Treasury's consultation paper and supports Treasury's comprehensive token mapping exercise, which seeks to build a shared understanding of crypto assets in the Australian financial system.

Stirling & Rose (**S&R**) is a boutique emerging-technology firm with deep experience in the subject matter of digital assets, artificial intelligence, smart legal contracts and autonomous organisations (including their sub-set decentralised autonomous organisations). We advise major investors (hedge funds, VC funds, and lenders) and enterprise blockchain architects on major real-world application and enforcement of all the above. We have done so at an international level as the executive team of a major international law firm since the inception of the space. Our partners have backgrounds in international regulatory law and disputes, insolvency and personal property law, asset and structured financing as well as ICT contracts and machine learning. We are currently leading Australia's Responsible Contracting Project in respect of smart legal contracts together with Nooriam Pty Ltd and The Commonwealth Scientific and Industrial Research Organisation (**CSIRO**) the Australian Government agency responsible for scientific research.

As discussed with Treasury in the initial consultation on 1 March 2023, S&R believes that mapping the lifecycle of a token in various real-world situations against the existing regulatory perimeter is a worthwhile exercise. S&R is in the process of finalising this and is looking forward to sharing with Treasury.

We again extend a hearty congratulations and warm thanks to the Treasury for its work in this Token Mapping consultation.

Yours sincerely,
Stirling & Rose

Part 1: Initial Comments

S&R is supportive of the comprehensive token mapping exercise undertaken by Treasury and set out in the Consultation Paper. We also support a regulatory approach that balances the opportunities of the crypto ecosystem alongside prudent risk management, while being informed by international approaches to crypto ecosystem regulation.

In agreement with Treasury, S&R acknowledges that the Consultation Paper does not address all the risks of investing in crypto-assets, but maps the ecosystem against specific portions of the financial services regulatory framework and that a complete overview of the crypto ecosystem is beyond the scope of this submission.

S&R supports and agrees with the application of the functional perimeter i.e. which captures any 'facility' through which, or through the acquisition of which, a person does one or more of: (a) makes a financial investment; (b) manages financial risk; and (c) makes non-cash payments (together, the 'general financial functions').

Part 2: Answers to Consultation Paper

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

a. **Dynamism**: The Government through the Australian Securities and Investments Commission (**ASIC**) should enforce the functional perimeter in respect of crypto-assets in a technology agnostic way. This enforcement should be timely, appropriate and take account of the dynamic nature of tokens – i.e., that they may change in function, form, rights and obligations over time. Relevantly, crypto-assets may by their digital nature fall in and out of the functional perimeter at a velocity greater than conventional assets.

b. **Future proofing**: The Government should exhibit caution in providing responses or mappings that over emphasise status quo public permissionless infrastructure terminology and current smart contract methodologies. To date, many smart contract methodologies, tools and platforms have been intentionally designed to avoid governmental oversight and do not work well with a number of fundamental legal principles, corporate duties and traditional markets. To date this has not been fatal as many of these assets have been simplistic generation one digital products that have not been whole of economy critical. In the future, (as a by-product of mass digitalisation and a greater preponderance of legal products and platform) digital assets will become an increasingly complex form of property associated with enumerate economic dependencies (see more on smart legal contracts below).

c. **Tax leakage**: The Government should through the Australian Taxation Office, the Department of Social Services and the Department of the Prime Minister and Cabinet (and other relevant departments) recognise the not significant impact on the money supply and leakage of taxation revenues and hidden revenues (impacting for example family court outcomes) that are achievable via the use of cold wallet solutions as well as platforms like Ethereum and popular decentralised "peer to peer" exchanges. This is not just a "money laundering risk".

d. **Critical digital infrastructure**: The Government through the Federal Attorney General's department should consider whether additional grants and legislation are required to support the digitisation of legal contracts (smart legal contracts) and what impact this has on a need for critical digital infrastructure. National digital infrastructure is likely to become a matter of national security and competitive advantage, as data and smart legal contracts increasingly represent a digital twin of the national economy. See also our response to our **Question 11** below.

e. **DAOs and AOs**: The Consultation Paper sets out a clear explanation of decentralised autonomous organisations (**DAOs**) in paragraphs 177 to 183. In

furtherance of this, the Government should follow the Token Mapping exercise with a follow-on consultation by Treasury that considers the Responsible Machine Problem see here and whether appropriate legislation/regulation is required to give machines / AI / algorithms legal status as a "person" under the law see here. We set out how the Responsible Machine Problem relates to digital assets in the June 2022 CASSPR submission as below:

> *(Crypto assets) ..."includes assets with autonomous elements that exist independently of a responsible person or 'person in the loop'. This is problematic because* ***all existing legislation is predicated on rights, responsibilities (custody) and penalties for non-compliance to ultimately be placed on or with a 'person' (not a machine or an algorithm).*** *This problem (the Responsible Machine Problem) will need to be addressed by the Australian government many times over the next decade and will impact all areas of the law. For example, the notion of a 'responsible person' is difficult in the context of some crypto assets where the Responsible Machine Problem is already at play. It cannot be correct that where no responsible person can be identified, a crypto asset should not be regulated if the crypto asset would be considered a financial product or service, but for the substitution of an algorithm or a machine for a responsible person. A clear example of legislative decisions that will ultimately revolve around this problem, is the regulation of decentralised autonomous organisations or (DAOs);"*

f. This latter point is directly relevant as to whether DAOs are the better consideration under the law as compared to the more agnostic artificial intelligence concept of Autonomous Organisations (**AOs**). That is, going beyond the "crypto" specific context, the "D" in DAO may be less significant from a technological, market and regulatory perspective, than the existence of organisations that operate autonomously in general: AOs.

S&R has extensively researched and authored on this subject. To assist Treasury, we have set out the relevant extracts of our response to the Law Commission of England and Wales Call for Evidence on DAOs below.

> *Notwithstanding that the "D" in DAO stands for decentralised – the broader notion of an autonomous organisation entirely run by (centralised) AI (where AI is eventually recognised as falling within the definition of person in a legal sense) is likely to outlive the decentralised nature of the underlying infrastructure that supports it.*
>
> *The AO of the future is increasingly likely to have AI style director capability closely mimicking centralised human governance, but with superior recourse to a corpus of more expansive data from which to make real time governance decisions.*

We observe that there is a continuum in the degree of autonomy in AOs with governance delivered via a combination of executing code and human decision-making. We expect the pathway to fully autonomous AOs to be an ongoing expansion of the matters handled autonomously i.e., without human intervention. For this reason, we use the term AO to includes organisations which have a differing degree of governance discharged by code.

Our observation is that at present, the primary motivation for humans setting up an autonomous organisation regularly involves the potential for financial reward to be gained by the founder(s) through majority positions as "Software Protocol token holders" and traditional external investment. To date, in practice the majority of AOs end up running in a very similar fashion to an established class of corporate structure, particularly as token holders tend to not have or not exercise active participation in governance decisions relating to the particular protocol, and the public facing founders increasingly make the majority of decisions in relation to the AO. Further, simply replacing shareholder meetings and shareholders agreements with operating code is more a technical implementation difference to traditional corporations rather than a substantive legal one.

Having an identifiable founder(s) is legally useful. When there has been some aberration in the operation of the AO that the software protocol is inadequate to moderate (through the deterministic nature of potential coded premediated actions, or unwieldly and unrealistically large quorum requirements unsuited to most strategic and risk decisions), an identifiable human is still key to consumer, third party and other software protocol token holders' protections. Unless a way is found to make code responsible for aberrant legal actions (see the Responsible Machine Problem,) it is prudent for the law to continue to both recognise and appropriately hold accountable humans who participate in (and perhaps benefit from) leadership in AOs. The humans directing and managing the AO should still be liable as they would be under existing law.

Having said that, while we support personal liability being attached to any humans that direct and manage the AO, there are practical and legal challenges with relying on strict human responsibility alone. With respect to an AO, the universe of potentially liable persons are the founders, token holders (particularly where a single or small group of token holders control a majority of voting tokens) and the developers. In the case of civil or criminal actions which require mental intent (such as fraud) it may be difficult or even inappropriate to attribute the requisite intent to a particular individual.

Such a cause of action against a human actor may not be sufficient recourse for an injured party.

Further, a responsible human may be too far removed from an actual decision or action of the AO to attribute fault to the human. The realistic possibility of code alone being responsible for making an aberrant decision or action which founders, token holders and developers are not reasonably able to foresee, draws a crucial distinction between an AO and a corporation, or any other traditional non-human legal personality. A corporation, partnership or unincorporated association ultimately depends on a human in the loop to make a decision, whereas the code underpinning an AO may be able to independently make decisions for itself with limited or no human direction.

For these reasons, there may be merit in potentially granting legal personality to protect internal and external stakeholders interacting with the AO. To iterate:

1. *the development of machine learning will mean that greater management of an organisation for day-to-day functions by code becomes feasible and widespread;*
2. *an AO presents potential improvements over a human-led organisation. The capacity to review more relevant information quicker, undertake more efficient decision making, and be prone to less biases than human counterparts means that there may be productivity gains from AOs. Individuals and investors may prefer to be token holders in an AO than shareholders in a human led corporation; and*
3. *from the perspective of third-party protection, if the above two propositions are accepted, then the AO itself should have legal personality to be subject to legal sanction not only for the benefit of injured parties but also to empower regulators to deter aberrant behaviour. This provides an additional avenue of relief to the extent that action against individuals is not appropriate.*

Granting legal personality to an AO should not be unconditional. Bare requirements are necessary to recognise that an AO is a separate organism that may functional independently of founders, token holders and developers, but, that at the same time, any legal personality construct must recognise that regulating humans does not readily translate to regulating code. A suggested list of conditions may include the following:

1. ***Registration**. All AOs should be registered with the appropriate local and international agencies and should have their own unique identifier (such*

as a registration number or digital fingerprint). We would propose that there should be a dedicated governmental authority to regulate AOs and monitor the register.

2. ***Identification as an AO**. All AO should have a signifier in their names such that they are readily identifiable as an AO in all interactions. Much the same way companies are identified by "Ltd", "Inc.", "LLC" or other signifiers of their corporate status, AOs should also be identifiable as an AO – for example ACME AO Ltd.*

3. ***Functional AO test**. An AO must be able to provide reasonable evidence of its capability to discharge de minimus functionality, i.e., those things necessary to discharge the AO's legal obligations. For example, paying annual AO registration fees. This evidence would need to be provided as a condition to registration of the AO, but also possibly on a periodic and ongoing basis to confirm the continued functionality of the AO in what is a dynamic and rapidly evolving arena where consumer harm in interacting with an AO (or at least with an early generation AO) may be elevated.*

4. ***AO sanctions**. Economic risk allocation does not solve the role of 'skin in the game' whereby personal liability and the potential for adverse action against an individual incentivises alignment of interests and actions. Even with limited recourse vehicles, there is still a responsible person (in the case of a company, directors still owe director duties to the company, and in certain circumstances to, or are personally responsible for harm inflicted on, third parties e.g., misleading, and deceptive conduct). The applicable governmental authority regulating AOs should be conferred with powers to suspend the operation or terminate an AO and exercise rights of forfeiture against AO assets. While it is impossible to imprison an AO, suspension, or termination of all active operation of an AO is required to provide a meaningful regulatory stick. To prevent AO sponsors "phoenixing" a sanctioned AO, there would have to be a means of identifying the code of a phoenixed AO from the underlying code of one that has been sanctioned. We reiterate that even if AOs had legal personality and could be separately held liable, it remains prudent to hold individuals accountable: (a) to the extent that the private citizens are engaged in directing the AO; (b) to the extent that it is difficult to properly censure an AO to ensure that there is 'skin in the game' and there is sufficient deterrence from bad behaviour.*

5. ***Economic reserves**. It may be feasible to improve the economic risk of AOs to counterparties by imposing some form of credit support. This could be in the form of actual asset backing (i.e., collateralisation) to meet potential claims or guarantees provided by individuals or legal entities of*

substance or insurance (such insurance to be for a sufficient level of cover for the AO's activities and incurred obligations and with no material exclusions). A counterargument to this is that without some form of collateralisation, an AO represents a similar risk profile to external counterparties as corporate or other limited liability vehicles which have minimal asset backing e.g., shell companies. In which case, it is a matter of caveat emptor for parties that fail to do their due diligence (assuming that the AO is registered and identified as an AO pursuant to conditions 1 and 2 above).

6. ***Intent of an AO**. As referred above, causes of actions and offences which presuppose mental intent will need to be adjusted for AOs, given there may not be a governing 'mind' in the legally understood sense. This may involve abolishing or adjusting the requirement of mental intent from such causes of actions and offences where an AO is the defendant or relying on a completely objective (and possibly expert determined) test to determine what the AO should have done. Corporations attribute intent to their directors and officers. We do not think this presumption should automatically apply to AOs, but it should be available as a continuation of our liability continuum comment above, to the extent that a founder or other human actor is a shadow director or is otherwise involved in the material decision making.*

7. ***Minority token holder protections**. Minimum protections may be granted to minority token holders (e.g., no compulsory transfer or extinguishment of minority tokens). This, in conjunction with the evidence required to establish a functional AO, may comprise the base governance protections to minority token holders to avoid potential fraud on the minority.*

g. **Licensing**: The Government through ASIC (and appropriate legislation / regulation if required) should consider the introduction of a third-tier style market licence which is a lighter touch market authorisation that can be applied for in a similar manner to a "fill in a form" Australian Financial Services Licence (**AFSL**). A form (which currently does not exist) would help guide market participants to satisfy their regulatory obligations, and avoid incurring unnecessary legal and other costs which may not necessarily reduce the fundamental risk exposure to investors.

h. **Regulator resourcing**: The Government should resource ASIC appropriately to moderate new and emerging users of platforms and markets catalysed by the digitalisation of traditional assets by non-traditional financial market participants and stakeholders who lack familiarity when consuming ASIC

services. This increase in digitalised property will only increase and will be used as Complex Money see here.

i. **Regulatory equivalence**: The Government should work with other global regulators to ensure maximum International Organization of Securities Commissions (IOSCO) style regulatory equivalence. This is perhaps the largest on-the-ground change that would encourage innovation in Australia and inflow of innovative companies. If a financial market or AFS licence could be obtained in Australia and that licence(s) could assist innovators in more easily securing equivalent licences in other foreign markets - this would have immediate and direct financial impact in the hundreds of millions of dollars of regulatory relief. Likewise, it would encourage prudent foreign entities to provide services to Australian users within the tolerance range of Australian regulations rather than avoiding Australia as a "too hard and too small" market.

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

Between existing consumer protection laws, AML / CTF laws, the *Corporations Act 2001* (Cth), the *Banking Act 1959* (Cth) and state and federal gambling laws, at this stage we can see no additional law that is required to regulate crypto-assets, other than a law governing artificial intelligence / autonomous organisations, which may have tangential impact.

Existing laws are sufficient to cover the space from a crypto -asset perspective. The airgap may be perceptions or awareness that such spectrum of laws have already been developed.

Q5) This paper sets out some reasons for why a bespoke 'crypto-asset' taxonomy may have minimal regulatory value.

a) What are additional supporting reasons or alternative views on the value of a bespoke taxonomy?

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

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?

We broadly support Treasury's rationale to avoid reliance on a bespoke 'crypto-asset' taxonomy.

In summary, this includes because:

a. a functional rather than taxonomic approach is more appropriate and sufficiently flexible and rigorous to deal with crypto-assets for the reasons given by Treasury;

b. a taxonomic approach may simply encourage regulatory arbitrage which may defeat the consumer protection policy objectives, this is particularly so given the dynamic nature of crypto-assets (see more in **Question 1** above); and

c. given technological development, a taxonomic approach may only deal with simplistic 'Generation One' crypto-assets and without constant updating may miss subsequent developments in crypto-assets (see more in **Question 12** below).

Q11) Some jurisdictions have implemented regulatory frameworks that address the marketing and promotion of products within the crypto ecosystem (including network tokens and public smart contracts). Would a similar solution be suitable for Australia? If so, how might this be implemented?

To the extent this question is referring to MiCA-style European legislation, the answer is no. Please refer to our response to **Question 2** above in this respect.

This does not mean that we do not expect to see changes to the existing laws, for example, we anticipate that in may be helpful for the *Corporations Act 2001* (Cth) (in particular Chapter 7) to explicitly refer to crypto-assets to the extent that they fall within the functional perimeter, and also the converse: given the dynamic nature of crypto-assets, they may at some point in time(s), legitimately fall outside the functional perimeter.

We would also think the definition of a person under Australian laws will need to be amended to incorporate the concept of an autonomous agent or algorithm / machine as discussed elsewhere in this submission.

We consider the *Security of Critical Infrastructure Act 2018* (Cth) and Part XIC of the *Competition and Consumer Act 2010* (Cth) may need to be amended (or an equivalent style provision that also seeks to include smart legal contract infrastructure as a listed service for the purposes of such legislation) to accommodate increasing use of smart legal contracts as critical digital assets in the future. We draw a distinction here and in all of our material between smart legal contracts (digitised forms of legal agreements) and smart contracts (as broadly understood i.e., self- executing code on a block chain).

We are happy to provide further comments on all of these points.

Q12) Smart contracts are commonly developed as 'free open-source software'. They are often published and republished by entities other than their original authors.

a) What are the regulatory and policy levers available to encourage the development of smart contracts that comply with existing regulatory frameworks?

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

We anticipate that many responses to the token mapping exercise may have in contemplation what we call 'Generation One' tokens (aka generation one smart contracts).

We consider that an over emphasis on these speculative assets that are currently operating on public permissionless layer one protocols is ultimately a short to medium term technical solution. This is because part of the attraction of these assets and systems to holders and users is that they believe these assets and systems exist outside of existing legal perimeters and nation state perimeters. Once governments audit and understand the economic and regulatory leakages that are occurring, regulatory action will reduce the attractiveness of these platforms and assets, particularly as speculative asset classes.

That is not to say that the technology of digital assets is not obsolete, quite the contrary, digital assets will only increase in usage, volume and real-world use cases. As such, regulatory frameworks will need to focus on regulated infrastructures which can accommodate later generation digital assets.

Q13) Some smart contract applications assist users to connect to smart contracts that implement a pawn-broker style of collateralised lending (i.e. only recourse in the event of default is the collateral).

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

b) Is there quantifiable data on the consumer outcomes in conventional pawn-broker lending compared with user outcomes for analogous services provided through smart contract applications?

Aside from the potential practicalities in respect of cold wallets and the nature of crypto-assets, in our view, legally the main (and larger) question would be the treatment of such crypto-assets in the context of secured lending arrangements.

In this context, there is persuasive case authority[1] for the proposition that crypto-assets should be personal property for the purposes of section 10 of the *Personal Property Securities Act 2009* (Cth) (**PPSA**) (and is relevantly, not excluded under section 8 of the PPSA).

Accordingly, for secured lending arrangements, a security interest over crypto-assets could be perfected by registration under section 12(1) of the PPSA.

However, there are a number of caveats, which may warrant further legislative review.

First, perfection by other means to registration, such as by possession or control under Part 2.3 of the PPSA is less clear.

Ostensibly, a cold wallet (such as a USB stick) may be subject to possession, however there is a query whether under a reading of possession under section 24, this would be "actual or apparent possession" of the underlying crypto-asset.

In respect to control, crypto-assets are not a designated form of personal property under Part 2.3 that could be subject to perfection by control. Namely, they would unlikely fall under the categories of:

1. an ADI account;
2. an intermediated security;
3. an investment instrument;
4. a negotiable instrument that is not evidenced by a certificate;
5. a right evidenced by certain types of letters of credits; or
6. satellites or other space objects.

Interestingly, the most likely (if at all) categories for perfection by control that would apply to most 'Generation One' crypto-assets, would be intermediated securities or investment instruments. However, this would involve a characterisation (which is the scope of Treasury's current review) that such crypto-assets are:

- in the case of intermediated securities as defined in section 15 of the PPSA, securities operated by an intermediary with an AFSL. We observe the challenge may be that most such intermediaries do not have an appropriate AFSL; and
- in the case of investment instruments as defined in section 10 of the PPSA, such crypto-assets would likely either need to be characterised as a

[1] Cf *David Ian Ruscoe And Malcolm Russell Moore v Cryptopia Limited (in liquidation)* [2020] NZHC 728.

derivative, a financial product as prescribed by the relevant regulations, or be a financial product traded on a financial market operated in accordance with an Australian market licence (which runs into the same problem with respect to intermediaries as referred in bullet point one above).

The consequence is that even if practically a person (such as a secured lender) would have possession or control to address the policy rationale behind the PPSA ie to overcome the "*illusion of apparent wealth*" (which some may say is ironic in the context of less scrutable crypto-assets), they would not be able to achieve perfection for the purposes of the PPSA. Accordingly, given the nature of possession and control of crypto-assets (in the practical sense) does not align with possession and control (in the PPSA sense), perfection by registration under section 21 remains the only viable means of perfection.

In our view, this impairs lenders obtaining perfected security over crypto-assets and accordingly, impairs meaningful secured lending of crypto-assets in Australia (if ever achievable – there are broader questions, which are not necessarily insurmountable, but are tied to legal recognition of crypto-assets and regulation of providers of crypto-assets, which need to be addressed e.g. insurance, credit risk etc– S&R are happy to discuss our research in this space if helpful – at its core, from a legal perspective, it is the same central issue facing Treasury and governments around the world: what S&R calls the Responsible Machine Problem and discussed earlier in this submission). Accordingly, an interesting tension has been that advocates of no / lite regulation for crypto-assets have limited (under the current wording of the PPSA) viable funding and investment in the Australian crypto-asset industry.

While this may seem academic (as perfection by registration is still available), the legal question invariably intersects with the practical given the nature of enforcement and insolvency. In a practical sense, perfection by registration may be moot compared to having control of the crypto-asset (such as being in control of private keys to a digital wallet) or possession (the holder of a physical cold wallet) – which is exactly the issue the PPSA is/was trying to resolve. Conversely, a secured party with control or possession of crypto-assets which are pledged as collateral, would want to have regulatory certainty in the legal enforceability of any security interest they may impose at law.

Perfection is the most obvious air gap with respect to secured lending arrangements. There are complex technological characteristics of crypto-assets which may need accommodation for other sections of the PPSA, such as commingling and taking free rules alongside the treatment of financial products within that legislation (but this may narrow if the functional perimeter proposed by Treasury applies).

We would suggest legislative amendments to accommodate this. S&R has extensively considered the treatment of crypto-assets in the context of security arrangements and the PPSA. We would be happy to discuss this further if that is helpful or with any governmental departments who may be interested, such as the Australian Financial Security Authority or the Attorney-General's Department.