Australian Government
Attorney-General's Department

Token Mapping

Treasury consultation paper (February 2023)

The Attorney-General's Department and AUSTRAC submission

March 2023

Outline of the submission

The Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Attorney-General's Department (the department) welcome the opportunity to make a submission to Treasury's consultation on token mapping. Much of this submission build on AUSTRAC's submission in response to Treasury's consultation in 2022 on *Crypto Asset Secondary Service Providers Licensing and Custody Requirements*.

This submission provides broader context related to financial crime risks and global anti-money laundering and counter-terrorism financing (AML/CTF) standards for Treasury's consideration.

The submission is provided in three parts.

- Part 1 provides an overview of the department's and AUSTRAC, and regulation of digital currency exchanges under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.
- Part 2 address the international policy context for applying AML/CTF measures to the businesses providing services related to crypto assets.
- Part 3 provides specific responses to consultation questions.

Part 1: Overview

The department has responsibility for anti-money laundering and counter-terrorism financing (**AML/CTF**) policy. The department oversees Australia's AML/CTF regime, which establishes a regulatory framework for combatting money laundering (**ML**) and terrorism financing (**TF**), and other serious financial crimes. The AML/CTF regime comprises:

- the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (**AML/CTF Act**)
- the *Anti Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* (**AML/CTF Rules**)
- the *Anti-Money Laundering and Counter-Terrorism Financing (Prescribed Foreign Countries) Regulations 2018*, and
- the *Financial Transaction Reports Act 1988* (**FTR Act**).

The department also administers the *Proceeds of Crime Act 2002* which provides a scheme to trace, restrain and confiscate the proceeds of crimes against Commonwealth law.

About AUSTRAC

AUSTRAC is Australia's financial intelligence unit (**FIU**) and AML/CTF regulator.

As Australia's FIU, AUSTRAC provides financial transactions data and actionable financial intelligence to law enforcement, national security, human services and revenue agencies (AUSTRAC's partner agencies), as well as international counterparts. Partner agencies use this information to assist them to detect, prevent and disrupt ML/TF and other serious crime.

As a regulator, AUSTRAC oversees the compliance of more than 17,000 Australian businesses with the AML/CTF Act and associated AML/CTF Rules. AUSTRAC's regulated population (referred to as **reporting entities**) includes a broad range of businesses from across the financial services, gambling, bullion, remittance and digital currency exchange sectors. These businesses range from major banks and casinos to single-operator businesses, but all must comply with applicable obligations in the AML/CTF Act and implement effective AML/CTF systems and controls to identify and mitigate ML/TF risk.

AUSTRAC uses its knowledge of reporting entities, industry trends and ML/TF risks to direct our regulatory efforts towards vulnerabilities and high-risk entities, which increases resilience to criminal abuse within the financial sector. Our regulatory work and engagement with reporting entities improves the volume and value of financial intelligence provided to AUSTRAC and then subsequently disseminated to AUSTRAC's partner agencies.

AUSTRAC may take enforcement action against a reporting entity for serious and/or systemic non-compliance with the AML/CTF Act. In instances where reporting entities fail to meet their obligations, well-targeted and proportionate enforcement action can benefit reporting entities and the wider community by contributing to the broader integrity of the financial system.

AUSTRAC regulation of digital currency exchanges

Australia's AML/CTF regime adopts a risk-based and principles-based approach to regulation and recognises that reporting entities are best placed to identify, mitigate and manage their ML/TF risk.

Businesses that provide a designated service listed in section 6 of the AML/CTF Act are **reporting entities** and have certain regulatory obligations.

The designated service relevant to the digital currency exchange (**DCE**) sector is item 50A[1] in Table 1 of section 6 of the AML/CTF Act. Item 50A is the service of exchanging digital currency for money (whether Australian or not) or exchanging money (whether Australian or not) for digital currency, where the exchange is provided in the course of carrying on a digital currency exchange business.

Like all reporting entities, DCEs providing item 50A services must:

- enrol with AUSTRAC;
- establish and maintain an AML/CTF program to help identify, mitigate and manage the ML/TF risks the business faces;
- conduct initial and ongoing customer due diligence;
- report certain transactions, including notifying AUSTRAC of suspicious matters and, threshold transactions; and
- keep records.

DCEs must also register with AUSTRAC before providing digital currency exchange services. Failure to do so is a criminal offence. Registration is intended to reduce the risk that criminals and their associates enter the DCE provider sector and the key consideration is whether registering the person would involve a significant ML/TF or other serious crime risk.

AML/CTF obligations for DCEs commenced on 3 April 2018.

[1] Designated service item 50A focuses on the fiat-digital currency on and off ramps, i.e. the exchange of fiat currency for digital currency (i.e. crypto asset) and vice versa.

Part 2: International AML/CTF context

Australia is a founding member of the Financial Action Task Force (**FATF**)[2], the global AML/CTF standard-setting body. The department, supported by AUSTRAC, leads Australia's engagement with the FATF. As a FATF member, Australia has committed to the full and effective implementation of the FATF Recommendations and is publicly reviewed for its compliance with the FATF's international best practice standards (**FATF Standards**), through the FATF's peer-review process, known as a Mutual Evaluation.

Where a country is found to have poor compliance and implementation of the FATF Standards, a range of escalating consequences can be applied to the country by the FATF. This can range from letters to ministers and high-level visits from the FATF, to referral to the FATF's International Cooperation Review Group for formal monitoring, and public statements identifying a country as being under increased monitoring (commonly known as 'grey listing'). 'Grey-listing' carries significant economic and reputational consequences.

FATF Recommendation 15 in relation to virtual assets and virtual asset service providers

Australia implemented AML/CTF obligations for the DCE sector domestically in April 2018. In October 2019, the FATF adopted new global standards for regulating the sector.

The FATF standards require countries to apply AML/CTF regulation to five categories of 'virtual asset service provider' (VASP) services. These services are set out under the FATF's definition of 'virtual asset service provider', which is the international equivalent of 'digital currency exchange' under the AML/CTF Act.

> Virtual asset service provider (VASP) means any natural or legal person who is not covered elsewhere under the FATF Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
>
> i. exchange between virtual assets and fiat currencies;
>
> ii. exchange between one or more forms of virtual assets;
>
> iii. transfers of virtual assets;
>
> iv. safekeeping or administration of virtual assets or instruments enabling control over virtual assets;
>
> v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Australia currently regulates the first activity listed in the definition—the exchange between virtual assets and fiat currencies—for AML/CTF purposes. AUSTRAC registration requirements, and other AML/CTF measures, do not currently apply to the remaining activities in the FATF definition unless they incidentally involve the exchange between virtual assets and fiat currency.

[2] Refer to https://www.fatf-gafi.org/ and the FATF Recommendations

FATF VASP licensing/registration requirements

The FATF requires that VASPs undertaking any of the five activities in the FATF's definition to be licensed or registered by a competent authority that takes measures to prevent criminals and their associates from owning, controlling or managing a VASP.

- VASPs are expected to be supervised or monitored by a competent authority (not a self-regulatory body), which should conduct risk-based supervision or monitoring.
- Supervisors are expected to have powers to impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's licence or registration, where applicable.

The FATF does not require that VASPs be subject to a bespoke AML/CTF licensing or registration regime—a licensing framework that applied to a broader range of financial services providers including VASPs would be sufficient if it achieves the purpose of keeping criminals out of the sector (e.g. through fitness and propriety checks).

Part 3: Responses to consultation questions

The department and AUSTRAC consider that financial crime risk and AML/CTF regulation need to be considered in the development of a framework for the regulation of crypto assets. The FATF's standards on the regulation of virtual assets for AML/CTF purposes provide the globally accepted minimum standards, of which many jurisdictions have implemented as the basis of their regulatory regimes. Accordingly, we consider that Treasury should adopt a similar approach in its development of a regulatory framework for crypto assets, by utilising basic concepts from these standards to ensure harmonisation across Australia's existing regulatory frameworks, and to limit the potential for regulatory duplication or inconsistency that could increase compliance costs for business.

The development of any future regulatory framework for crypto asset service providers should build on Australia's commitment to implement FATF standards and the existing AML/CTF regime. This ensures that vulnerabilities of the crypto eco-system can be comprehensively considered in the context of its potential abuse by criminal actors for ML, TF and other financial crimes. Anonymity-enhancing technologies and other characteristics of some crypto assets can enable the obfuscation of the origins of financial flows that may be the proceeds of crime.

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

From a financial crime regulation perspective, there are broadly two levels at which regulation of the crypto ecosystem could usefully achieve a range of policy objectives:

- at the ecosystem level, including regulation of governance bodies (entities that establish or participate in the establishment of rules governing crypto networks) for economically significant crypto tokens (e.g. payment stablecoins), and
- regulation of financial intermediaries providing crypto asset services to customers.

Crypto network level regulation

Regulation at the ecosystem level could be considered analogous to regulating payment systems. As with payment systems, the design of a 'crypto network', notably the underlying distributed ledger technology and ongoing rules by which it operates, can significantly affect its vulnerability to misuse for financial crime.

For example, the FATF has at various times highlighted the following characteristics that could affect tokens' attractiveness for misuse by criminals:

- the potential for 'mass-adoption' or the extent to which a token is used—as noted by the FATF report to the G20[3] in relation to the potential for mass adoption of stablecoins:

> 'Criminals' ability to use a virtual asset as a means of exchange depends on it being freely exchangeable and liquid… [C]riminals tend to make use of the more widely-adopted or popular virtual assets in their illicit activities.'

[3] Virtual Assets – FATF Report to G20 on So-Called Stablecoins, June 2020

- the inclusion of anonymity-enhancing technologies in the design of the crypto network, and the extent to which the underlying technology facilitates the use of mixers and tumblers, decentralised platforms and exchanges, privacy wallets, and other types of products and services that enable or allow for reduced transparency and increased obfuscation of financial flows,
- whether the crypto network is permissioned or permissionless—in a permissioned network the governance body can apply due diligence to participants in the network to assess whether they undertake appropriate customer due diligence and other AML/CTF measures,
- whether the crypto network permits the use of self-hosted wallets or peer-to-peer transfers, which reduces the need for token holders to interact with regulated businesses who might apply AML/CTF measures.

While none of the above features in isolation is necessarily indicative of significant financial crime risk, each of them is relevant to assessing any systemic vulnerability to misuse by criminals. As such, any regulation of crypto ecosystems at the network level should ideally take account of such risks and empower the appropriate regulator to determine whether or not to approve an economically significant crypto network on the basis of financial crime risk.

Regulation of financial intermediaries

As noted previously[4], AUSTRAC considers that regulation of the crypto ecosystem should ultimately bring crypto asset businesses into line with other sectors regulated by AUSTRAC. Licensing of financial intermediaries is undertaken by ASIC, APRA or other authorities, while AUSTRAC supervises the AML/CTF compliance of licence holders. Such a licensing framework would ideally replace the existing AUSTRAC registration requirement for digital currency exchanges, since the primary reason for registration (keeping criminals and their associates out of the sector) could be fulfilled by the broader licensing framework. As such, in addition to regulating for consumer protection and investor confidence, licensing should include the policy objective of protecting the Australian community from the harm of criminal enterprises becoming involved in the crypto assets sector.

To achieve this objective, certain baseline requirements should be considered as part of any licensing framework:

1. the licensing framework should cover all activities specified in the FATF VASP definition, specifically all businesses which conduct one of the following activities (VASP services) on behalf of a customer:
    a. exchange between virtual assets and fiat currencies,
    b. exchange between one or more forms of virtual assets,
    c. transfer of virtual assets,
    d. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets, and
    e. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset, and

[4] AUSTRAC submission in response to the Treasury consultation on 'Crypto asset secondary service providers: Licensing and custody requirements', May 2022.

2. the licensing framework should apply fitness and propriety checks to any owner or controller of a business providing VASP services, and their key personnel, to ensure criminals and their associates do not enter the market and any licence can be revoked swiftly when this is identified.

Given the near universal commitment by jurisdictions to implement the FATF standards, they form the basis of many comparable overseas regimes for regulating the VASP sector. Therefore, building on these standards offers efficiencies in ensuring greater harmonisation with the legal frameworks of comparable jurisdictions with potential benefits to businesses operating in multiple jurisdictions.

In addition to the definition of VASP services, we note that the FATF standards may have some broader implications for possible approaches to regulation arising from the current token mapping work:

- the FATF standards do not require a separate licensing framework for virtual asset service providers if they are subject to a broader licensing framework—it is therefore open to countries to incorporate VASPs into existing licensing frameworks;
- the definition of virtual asset is a broad one:

> 'A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations'.

The reference to virtual asset being used 'for payment or investment purposes' may align somewhat with Australia's functional definition of 'financial product'. However, the FATF definition does not require that there be a 'facility', and this concept does not form part of the definition of 'digital currency' in the AML/CTF Act. It remains an open question for AUSTRAC whether, and in which circumstances, the requirement for a 'facility' will be met for VASP services involving unbacked tokens, such as Bitcoin and Ethereum, or for tokens with an algorithmic or smart contract-based value stabilisation mechanism. Regardless of whether such services involve financial products or services, all VASP services must be subject to licensing to ensure that criminals and their associates are kept out of the sector.

AUSTRAC does not ultimately take a position on what tokens or related services should be 'financial products', but considers that any regulatory approach should:

- apply rigorous licensing requirements to businesses providing VASP services involving tokens regardless of whether the token meets the financial product definition or not; and
- if separate licensing frameworks apply to VASP services involving tokens that are financial products and those that are not, the delineation between the two licensing frameworks should ideally be clear and easy to understand both for regulators (to avoid delays in taking regulatory action) and businesses themselves (to reduce compliance costs).

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

Globally, countries are moving to implement the FATF 'travel rule'[5], which involves the transfer of information about the payer and the payee between licensed businesses involved in the transfer of crypto assets on behalf of customers.

If Treasury moves towards licensing of economically significant crypto networks and crypto asset service providers, it would be timely to consider how a licensing framework can assist global implementation of the FATF travel rule. For example, if the list of licensees permitted to provide VASP services in Australia were publicly available (at least in searchable form)[6].

In addition to the potential consumer protection benefits of a public register, the travel rule, requiring the sending of information between licensed financial institutions or crypto asset businesses and a public register of licensees, could assist with discoverability. Some countries have also taken steps either to prohibit transfers where the travel rule cannot be applied, or are moving to require that such transfers be considered a high financial crime risk. It would therefore assist Australian crypto asset businesses to deal with their overseas counterparts if their licensed status could be verified based on public information.

Q3) Scams can be difficult for some consumers to identify.

a) Are there solutions (e.g. disclosure, code auditing or other requirements) that could be applied to safeguard consumers that choose to use crypto assets?

Nil comment.

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

While AUSTRAC is not a conduct or consumer protection regulator, we note that the AML/CTF contains a risk-based approach that could potentially be adapted to prevent consumers from being exposed to scams. Under the AML/CTF Act and Rules, regulated businesses (including digital currency exchanges) are required to identify, mitigate and manage the ML/TF risk arising from:

- all new designated services prior to introducing them to the market, and
- all new or developing technologies used for the provision of a designated service prior to adopting them[7].

The onus is therefore on the regulated business to understand and implement systems and controls to mitigate the ML/TF risks. Failure to do so can lead to civil penalties. An analogous approach could

[5] FATF Recommendation 15.
[6] To date, AUSTRAC has not published the register of digital currency exchange providers for a range of reasons, but recognises that the global move towards travel rule implementation may require consideration of alternatives to permit external parties to verify a digital currency exchange's registration status.
[7] Among other things, see Rules 8.1.5(5) and 9.1.5(5) of the Anti-Money Laundering and Counter-Terrorism Financing Rules.

require businesses offering crypto asset services (whether involving financial products or not) to understand and mitigate the potential risks to consumers, fraud risks etc.

Q4) The concept of 'exclusive use or control' of public data is a key distinguishing feature between crypto tokens/crypto networks and other data records.

a) How do you think the concepts could be used in a general definition of crypto token and crypto network for the purposes of future legislation?

The concept of exclusive control would need to be carefully defined to avoid potential loopholes. It should be sufficiently broad to capture both unilateral control and control through multi-signature arrangements.

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

As noted above, the approach to defining crypto tokens and crypto networks should cover all 'virtual assets' that fall within the FATF definition, at the very least. While AUSTRAC recognises that some regulatory obligations may turn on whether something is a financial product, crypto tokens should not be defined exclusively in terms of being financial products given that the requirement for a financial product to be a 'facility' could possibly exclude some things commonly understood to be crypto tokens (which are also captured by the AML/CTF Act definition of 'digital currency').

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?

Nil comment.

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

Nil comment.

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?

As noted above, some form of licensing should be applied to all businesses providing VASP services in relation to crypto assets, including where such services do not meet the definition of 'financial product' or 'financial service'.

Q6) Some intermediated crypto assets are 'backed' by existing items, goods, or assets. These crypto assets can be broadly described as 'wrapped' real world assets.

a) Are reforms necessary to ensure a wrapped real-world asset gets the same regulatory treatment as that of the asset backing it? Why? What reforms are needed?

Nil comment.

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?

Nil comment.

Q7) It can be difficult to identify the arrangements that constitute an intermediated token system.

a) Should crypto asset service providers be required to ensure their users are able to access information that allows them to identify arrangements underpinning crypto tokens? How might this be achieved?

Nil comment.

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

Nil comment.

Q8) In addition to the functional perimeter, the Corporations Act lists specific products that are financial products. The inclusion of specific financial products is intended to both: (i) provide guidance on the functional perimeter; (ii) add products that do not fall within the general financial functions.

a) Are there any kinds of intermediated crypto assets that ought to be specifically defined as financial products? Why?

The department and AUSTRAC do not take a view on what crypto assets should constitute financial products. However, as a regulator with responsibility for supervising AML/CTF obligations for many crypto asset service providers, it will be important for AUSTRAC that the type of licence(s) a particular business requires should be a simple and straightforward as possible to determine. We could envisage challenges in enforcement of a range of regulatory obligations if the type of licence a business requires remains uncertain, particularly if it leads to delays in taking regulatory action while the question is determined.

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

Nil comment.

Q9) Some regulatory frameworks in other jurisdictions have placed restrictions on the issuance of intermediated crypto assets to specific public crypto networks. What (if any) are appropriate measures for assessing the suitability of a specific public crypto network to host wrapped real world assets?

As noted in the response to question 1, public crypto networks that incorporate or allow the use of anonymity enhancing technologies may be used in an effort to obfuscate the origin of crypto or real world assets that are the proceeds of crime. Any token or wrapped asset that combines relative price stability with enhanced anonymity could prove attractive to criminals unless appropriate risk mitigations are built into the design of the crypto network itself.

Q10) Intermediated crypto assets involve crypto tokens linked to intangible property or other arrangements. Should there be limits, restrictions or frictions on the investment by consumers in relation to any arrangements not covered already by the financial services framework? Why?

For the reasons set out in the response to question 1, such businesses should be subject to licensing where they provide VASP services in relation to the intermediated crypto asset.

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?

Nil comment.

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?

This response will consider parts (a) and (b) of the question together. Ultimately, regulation will be most effective where there is an identifiable person or entity providing services by way of the smart

contract. Regulating the bare act of coding a smart contract itself would present challenges, and the FATF recognises that this is not required for AML/CTF purposes[8].

However, where a person or entity provides services by way of a smart contract or decentralised application, the person or entity should be legally responsible for meeting all regulatory requirements in relation to those services just as all other service providers are.

Given the novelty and diversity of many decentralised arrangements, the question of whether there is an identifiable person or group of people behind the provision of services should be a question of fact and not based on the (lack of) legal structure or the marketing terms used to describe the arrangement[9]. For this reason, AUSTRAC notes the potential limitations of using a narrow test based on traditional legal concepts of ownership or control. A factual test such as the 'sufficient influence' test used for some tax purposes[10] could potentially be adapted to cover the provision of services via a smart contract, e.g. a person could have regulatory responsibility for the operations of a smart contract where that smart contract might reasonably be expected to operate in accordance with the wishes of that person or entity.

While it may not always be easy to determine whether a person or entity has such influence over a decentralised arrangement (whether to allow it to operate or to affect its design), it should be possible for regulators to take action in those cases where such persons or entities can be identified.

In future, consideration of legislative options might provide greater clarity about the control and operation of smart contracts or decentralised applications could also provide an incentive toward regulatory compliance for those person or entities that desire to minimise legal risk and provide additional assurance to their customers/users.

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?

Nil comment.

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?

Nil comment.

---

[8] See also analysis by the FATF in *Updated Guidance: A Risk-Based App roach to Virtual Assets and Virtual Asset Service Providers* (2021), at paragraph 76.
[9] See also analysis by the FATF in *Updated Guidance: A Risk-Based App roach to Virtual Assets and Virtual Asset Service Providers* (2021), at paragraph 67.
[10] See for example s 318 of the *Income Tax Assessment Act 1936*.

Q14) Some smart contract applications assist users to connect to automated market makers (AMM).

a) What are the key differences in risk between using an AMM and using the services of a crypto asset exchange?

The term automated market maker, or AMM, encompasses a range of services that give rise to possible financial crime risks, including decentralised exchanges (DEX) and marketplaces operated by centralised exchanges.

AUSTRAC does not currently regulate DEXes as it is not possible for DEXes to provide services exchanging fiat currency for crypto assets. However, we observe a few likely financial crime vulnerabilities for DEXes:

- AML/CTF measures such as customer due diligence are difficult to implement or enforce in the absence of an identified service provider, unless some mechanism is implemented such as requiring approval by an intermediary or outsourced service provider as a condition of participating,
- AUSTRAC is unaware of effective mechanisms by which DEXes can themselves undertake meaningful ongoing customer due diligence (which involves understanding a customer's individual risk profile and flagging unusual transactions for further review),
- the automated nature of the services seem to create inherent challenges around ongoing customer due diligence, and seem to limit the scope to apply enhanced customer due diligence, including making decisions about whether or not provide services in circumstances where there a high financial crime risk is identified,
- in the absence of the above AML/CTF systems and controls, and an identified service provider, it is unclear how effective reporting of suspicious matters to AUSTRAC can practically occur.

Centralised exchanges are, on the other hand, capable of applying the same AML/CTF systems and controls as other regulated businesses. Depending on the design of the AMM, where the AMM is subject to the governance of a centralised exchange, AUSTRAC would expect the exchange to implement measures to allow compliance with all applicable AML/CTF obligations.

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

Nil comment.

Conclusion

The department and AUSTRAC welcome the draft token mapping taxonomy and recommends that any future licensing framework for crypto asset related services considers financial crime risks at both the crypto network and for financial intermediaries providing crypto asset related services, noting that some aspects of the design of crypto networks and tokens that were not referred to in the consultation paper can affect financial crime risk.

The department and AUSTRAC encourages continued consideration of possible regulatory responses to the risks arising from the delivery of services via smart contracts, including through decentralised applications. We will continue to engage with and support Treasury on their work on licensing and customary reforms for crypto assets, and are happy to provide further information on any of the points raised in this submission.