



Response to Token Mapping Consultation Paper

MARCH 2023

VIA EMAIL

Director - Crypto Policy Unit
Financial System Division
The Treasury
Australian Government

Our Response

Introduction and General Comments

TRM thanks the Treasury for sharing the results of its token mapping exercise and for the opportunity to respond.

The speed at which the exercise was concluded as well as the depth and breadth of its findings and the consultation questions reflects a serious and thoughtful effort by the Australian Government to introduce timely, fit-for-purpose regulation for crypto assets.

In particular, we are heartened by Assistant Treasurer Stephen Jones' assurance that Australia is committed to "get the balance right so [Australia] can embrace new and innovative technologies while safeguarding consumers." In this regard, we believe that the following considerations are highly relevant:

1. Clear and proportionate regulation

Keeping activity onshore enables governments to maintain regulatory oversight of crypto asset activities and better achieve consumer protection and other regulatory outcomes. However, given the borderless nature of crypto activities, it is impossible for governments to mandate that they remain onshore. Rather, governments can only encourage this with clear and proportionate regulation that achieves regulatory outcomes without placing an undue compliance burden on the industry. In this regard, it is important that the final crypto asset taxonomy makes clear the scope of regulated products and services, and that regulatory obligations take into account the unique characteristics of the digital assets and the blockchain technology that underpin it, borrowing from traditional finance regimes only when appropriate.

2. Public-private partnerships

The crypto asset sector is a relatively young one that is new to regulation compared to its traditional finance counterparts. At the same time, it is an extremely fast-moving space where innovators are constantly pushing the envelope of distributed ledger technology. Public-private partnerships ("PPPs") are essential in helping both policy and compliance keep up to speed. PPPs build a common understanding between policymakers and the industry, which will help to ensure that the industry is able to grasp regulatory objectives and implement best practices that not only comply with regulatory obligations but effectively achieve the underlying objectives. PPPs also equip policy makers, regulators and law enforcement with tools, training

and other expertise to move more quickly in achieving their aims. We hope that the Australian Government will remain open to more continuous, representative and inclusive PPPs across the entire crypto asset ecosystem, which will be beneficial to all involved.

3. Disruption of fraud, scams and other illicit activity

Consumer protection is front and center of many regulatory agendas following the events of 2022, and we note that this consultation also calls for suggestions to engender good consumer outcomes. In this regard, we would like to highlight that the traceability and immutability of the blockchain offers unique opportunities to fight fraud, scams and other illicit activities.

Blockchain intelligence demystifies the wealth of information on distributed ledgers and enables regulators, law enforcement and the crypto asset industry to identify and stop bad actors. Using regulatory and policy levers to encourage the use of blockchain intelligence as part of a comprehensive compliance programme for crypto assets will ensure that these tools are able to realize their full potential to fight illicit activity and help protect consumers.

We hope that the Treasury will consider these general principles as well as the responses below as it builds on this token mapping exercise to develop a regulatory framework for crypto assets in Australia.

Response to Consultation Questions

Consultation question

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

Governments play a dual role of driving economic growth and managing risks to both residents and the overall economy, and nowhere has the need to strike a balance been felt more keenly than in the crypto asset space.

The same qualities that make crypto assets a force for good - decentralized, permissionless, cross border value transfer at the speed of the internet - also make them attractive to illicit actors who seek to move funds across the globe at unprecedented speed and scale. At the same time, the failure of key global players in the last year have shown that the crypto ecosystem is exposed to some of the same vulnerabilities as traditional finance - poor corporate governance, as well as contagion and financial stability risks which could impact consumers.

The role of government in providing clear and proportionate regulatory oversight is essential in ensuring that the crypto asset sector realizes its potential for innovation and economic good while safeguarding consumers and the economy. We are heartened that governments around the world, including in Australia, have recognised the need to balance the two aspects in regulatory policymaking.

In this regard, we believe that public-private partnership (“PPP”) is fundamental to the development of timely and effective regulation for crypto assets.

Firstly, PPPs will help to build a common understanding of regulatory goals and how these can be achieved in the context of crypto assets. While crypto assets are vulnerable to many of the same risks as traditional finance, risk management techniques are often different due to the inherent nature of blockchain technology. Hence, PPPs play an important role in ensuring that the ultimate regulatory framework is fit-for-purpose and effectively addresses the underlying risks. They also engender a deeper understanding of policy objectives and make it easier for the industry to establish best practices in line with regulatory expectations.

Secondly, the private sector can offer tools, training and other expertise to help law enforcement, regulators, and policy makers move more quickly in achieving their aims. These tools also help compliance professionals – from small DeFi protocols and NFT marketplaces to large centralized exchanges – to monitor transactions and screen wallet addresses to effectively meet and exceed their compliance obligations, while providing actionable insights to regulators and law enforcement.

TRM welcomes this token mapping consultation as the first step in collaborative policymaking. As an international company operating in Australia, as well as in other key global markets, we look forward to providing global perspectives and contributing to the development of sound and effective regulation in Australia. We would be happy to engage further with the Treasury on this consultation and our responses, as well as any other related consultations.

Consultation question

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

Clear and proportionate regulation that encourages crypto asset activity to stay onshore will achieve better consumer protection outcomes. It ensures that Australian customers are able to access licensed crypto asset platforms, subject to appropriate regulatory requirements and oversight, and therefore deter them from seeking out unregulated or non-compliant platforms elsewhere.

One important aspect to consider in developing such regulation is the deterrence of unfair trading practices and market manipulation that often lead to adverse outcomes for consumers and investors by creating artificial price volatility. Strengthening market integrity has been identified as a priority in the IOSCO Fintech Task Force's [Crypto-Asset Roadmap for 2022-23](#), alongside investor protection, highlighting the inextricable linkage between the two. In identifying these priority areas, the FTF noted that the "recent market turmoil" resulting in "significant investor losses" was due to "inadequate regulatory protection and market safeguards." This view was echoed by the Monetary Authority of Singapore (MAS) in its recent consultation paper on crypto regulatory measures, which "encourages [...] platform operators to put in place good industry practices to detect and deter unfair trading practices."

Given the borderless nature of the crypto asset ecosystem, market integrity must be tackled on a global scale. MAS noted in its consultation paper that "a global consensus [...] would be needed to address market integrity concerns." We urge the Australian Government to leverage

Australia's strong reputation for regulatory rigor, and take an active role in establishing global principles for market integrity, in addition to domestic measures.

In this regard, it is important to recognise that the same blockchain technology that is exploited by bad actors also holds the power to identify and combat illicit activity through blockchain intelligence. We are heartened by increasing recognition of the power of blockchain intelligence in the regulatory community. In particular, the UK Financial Conduct Authority (FCA) had, in its recent feedback on good and poor quality applications under its crypto-asset regulatory regime, directed that applicants demonstrate "effective transaction monitoring and blockchain analysis" with "adequate coverage [...] of various types of currencies and transactions" and trained compliance staff with the "skills to carry out blockchain investigations" using these tools.

At TRM, we increasingly see both public and private sector clients leveraging blockchain intelligence. TRM enables real-time monitoring of on-chain funds flow across 1,000,000+ crypto assets and 26 blockchains -- including all ERC-20 tokens, popular stablecoins, DeFi tokens, which our clients can use to identify and take timely action on suspicious transactions.

Case Study: NFT Wash Trading

NFT wash trading is a method used by illicit actors to launder money or profit from market manipulation. Traditionally, wash trading has referred to a trader buying and selling a security for the explicit purpose of misleading the market and manipulating prices. Sometimes, a trader and a broker are colluding together, and other times an investor is acting as both the buyer and the seller. Either way, the goal is to quickly make money or potentially use the washing as a mechanism for money laundering.

NFT wash trading is becoming increasingly prevalent and therefore a concern for legitimate investors, collectors, and the general public because of inflated price comparisons and statistical outliers that reduce the integrity of the market.

Example: Wash Trading of a CryptoPunk NFT

In late 2021, someone bought a CryptoPunk NFT from themselves with borrowed money and repaid the loan in the same transaction. The purchase price was over 124k ETH, which was worth \$532M at the time. Prior to the wash trading/flash loan, the same CryptoPunk had been trading for closer to \$300-400K. The anomaly was so large that it led to a Tweet from the NFT creator stating that bids like these could not be accepted and that enhanced filtering would be created to avoid wash trading in the future.

Combating NFT Wash Trading

The most effective way to mitigate NFT wash trading is to make it difficult for illicit actors to sell NFTs involved in such schemes to unsuspecting parties. Blockchain intelligence allows buyers to conduct risk assessments of NFTs by identifying any outliers or other suspicious activity in the transaction history of the NFT. Using both on and off-chain data, investors can assess the token and creator provenance, as well as current ownership of an NFT. The buyer can look at whether the current owner has an unusually tight transaction network or if the NFT appears to have been traded amongst the owner with discrepancies in the bid, sale and floor price. The same blockchain technology that is being used to manipulate the market can provide a wealth of historical data that can provide unique insight into the integrity of an NFT. This is impossible in the traditional art, antiquities and collectible markets today in which provenance is often opaque. We are seeing more and more NFT issuers and marketplaces use blockchain intelligence to monitor transactions and screen wallet addresses to ensure that they are not sending an NFT to an illicit actor and mitigating their risk of sanctions exposure.

Consultation question

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?
 - 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?

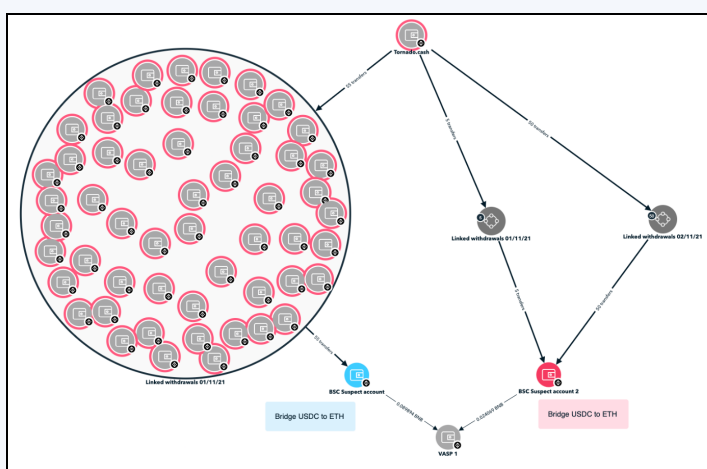
In most instances, scam tokens are not maliciously offered by crypto token exchanges, nor do they actively seek to expose customers to scams, as this would be counterproductive for business growth. Rather, it is the lack of adequate controls and monitoring tools that often result in exchanges being utilized for scams. Using regulatory levers to encourage stronger controls and use of effective tools (e.g. the UK FCA's directive described above) will help to safeguard consumers from scams.

Blockchain intelligence can help to identify operating patterns for common scams and prevent successful laundering of scam proceeds.

Case Study: Squid Game Scam

In October 2021, scammers launched a tradable SQUID token on the back of the global frenzy around the South Korean drama Squid Game. Within weeks of SQUID's launch, its price surged by over 40,000%. But when holders rushed to realize their gains, they were locked out by the smart contracts underpinning the tokens. These, it turned out, allowed only the creators to sell. When the creators cashed out, SQUID's price collapsed from USD 2,862 to a fraction of a cent – pulling the rug out from under investors' feet. Within moments, the anonymous scammers walked away with millions.

TRM's capability to trace complex cross-chain swaps using our Forensics tool enabled investigators to follow the flow of these stolen funds. TRM's analysis also helped link the scammers behind SQUID to two other similar "rug pulls". Although the total value obtained from the three scams is difficult to determine due to the complexity of the laundering process, research by TRM estimates it to have been at least 35,025 BNB (approximately US\$19.3m at the time of the events).



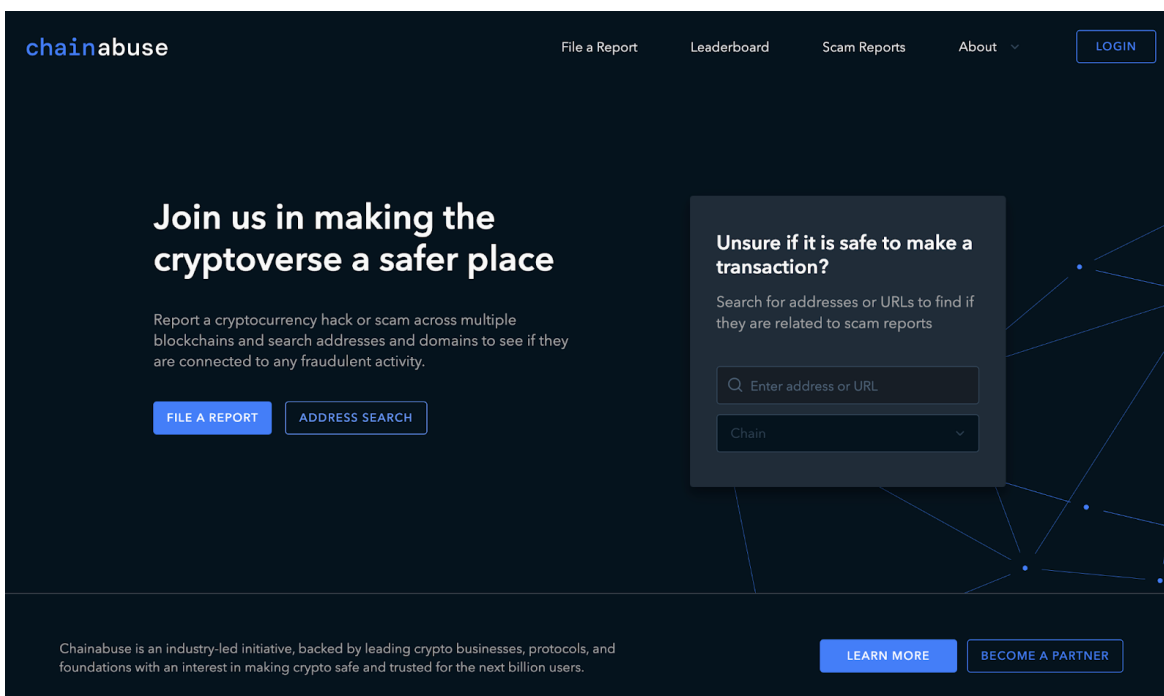
To launder their ill-gotten gains, the scammers sent most of the [proceeds to Tornado Cash, a notorious mixing service used to obscure cryptocurrency origin. The funds deposited into Tornado Cash were quickly withdrawn and consolidated. On 1 November 2021 alone, 55 deposits were made into Tornado Cash and then sent into a single address. The scammers then used bridge

applications to move the funds onto the Ethereum network. Ultimately, the scammers consistent behavior patterns, and their decision to cash out a significant portion of proceeds via two VASPs with poor KYC controls, left a breadcrumb trail of errors for investigators.

More information is available on [our website](#).

That said, prevention is even better than cure. Aside from tracing the flow of funds after the fact, the public nature of blockchains means that the industry can also collaborate to enable greater information sharing between consumers and the industry, enabling them to act together to protect the ecosystem from scams, hacks, and fraud. Through crypto fraud-reporting tools like Chainabuse.com, which is operated by TRM, members of the public can increase visibility of notable schemes and limit further victims by reporting the scams they come across. Victims can also choose to report scams and fraud directly to law enforcement.

Since its launch, the Chainabuse platform has received close to 350,000 reports of wallet addresses and URLs that are linked to frauds and scams involving cryptocurrencies. These reports allow Chainabuse to crowdsource a network-community driven reliable multi-chain real-time database of scams in web3 worldwide. In doing so, a resource is created where users can quickly check addresses and entities they interact with to understand whether they might be exposed to illicit activity.



The screenshot shows the Chainabuse website homepage. The header includes the logo 'chainabuse' and navigation links: 'File a Report', 'Leaderboard', 'Scam Reports', 'About', and a 'LOGIN' button. The main content area features a large heading: 'Join us in making the cryptoverse a safer place'. Below this, a sub-heading reads: 'Report a cryptocurrency hack or scam across multiple blockchains and search addresses and domains to see if they are connected to any fraudulent activity.' There are two buttons: 'FILE A REPORT' and 'ADDRESS SEARCH'. A modal window is open with the title 'Unsure if it is safe to make a transaction?' and the text 'Search for addresses or URLs to find if they are related to scam reports'. The modal contains a search input field with the placeholder 'Enter address or URL' and a dropdown menu labeled 'Chain'. At the bottom of the page, there is a footer with the text: 'Chainabuse is an industry-led initiative, backed by leading crypto businesses, protocols, and foundations with an interest in making crypto safe and trusted for the next billion users.' and two buttons: 'LEARN MORE' and 'BECOME A PARTNER'.

By encouraging entities under their remit to contribute to such industry-wide initiatives, as well as raising awareness of such platforms amongst the general public, governments can help to increase the comprehensiveness and reach of these essential fraud-fighting tools in safeguarding consumers from crypto scams.

Consultation question

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?
 - 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?

Longevity and clarity are the cornerstones of an effective taxonomy. In this regard, we appreciate the Treasury's considerations against creating an exhaustive bespoke taxonomy for crypto assets given the breadth of functions and the fast-changing nature of the industry.

That said, it is important for any taxonomy and the regulatory frameworks that are built on them to provide clear criteria on what is likely to fall in or out of scope of regulation. In this regard, there may be room for the Treasury to build on the examples and high-level taxonomy outlined in the consultation paper to provide further clarity.

In achieving both longevity and clarity, the Treasury may consider the approach taken by other key jurisdictions like the UK and Singapore (summarized in the table), which depend on the characteristics of a particular token. The scope of regulated activities in relation to such tokens are then further defined either in relation to a bespoke framework for said tokens, or to an existing regulatory regime.

Jurisdiction	Summary of Taxonomy
Singapore	<p>MAS classifies regulated tokens into digital payment tokens and digital tokens which constitute capital markets products:</p> <ul style="list-style-type: none"> • Digital payment tokens refer to “any digital representation of value that is expressed as a unit; is not denominated in any currency, and is not pegged by its issuer to any currency; is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of a debt; and can be transferred, stored or traded electronically.” (Source: Section 2(1) of the Singapore Payment Services Act (“PS Act”)) • Digital tokens which constitute capital markets products: “MAS will examine the structure and characteristics of, including the rights attached to, a digital token in determining if the digital token is a type of capital markets products under the Securities and Futures Act. This includes, but is not limited to a share, a debenture, a unit in a business trust, a securities-based derivatives contract, or a unit in a collective investment scheme, as defined under the Securities and Futures Act.” (Source: MAS Guide to Digital Token Offerings) <p>It further specifies the types of activities that would be regulated under the payments regime and capital markets regimes.</p> <ul style="list-style-type: none"> • Digital payment token services, defined as dealing in or facilitating the exchange of digital payment tokens, attract regulatory obligations under the PS Act. The activities of “dealing in” and “facilitating the exchange of” are further defined in the PS Act specifically in relation to digital payment tokens. (Source: Part 3 of the First Schedule of the PS Act) • Issuance and offering of digital tokens attract regulatory obligations under existing securities laws if they constitute capital market products (Source: MAS Guide to Digital Token Offerings)

Jurisdiction	Summary of Taxonomy
United Kingdom	<p>The UK FCA defined crypto assets under its Money Laundering and Terrorist Financing Regulations (“MLRs”) for the purpose of AML/CTF regulation:</p> <ul style="list-style-type: none"> • Cryptoasset means a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically (Source: Regulation 4(7)(3)(a) of the UK Money Laundering and Terrorist Financing (Amendment) Regulations 2019) <p>Aside from AML/CTF regulation which applies to all crypto assets, the UK FCA has issued guidance on specific types of crypto assets and how these might be subject to further regulation under existing regulatory frameworks:</p> <ul style="list-style-type: none"> • Security tokens: These are tokens that amount to a ‘Specified Investment’ under the Regulated Activities Order (RAO), excluding e-money. These may provide rights such as ownership, repayment of a specific sum of money, or entitlement to a share in future profits. They may also be transferable securities or other financial instrument under the EU’s Markets in Financial Instruments Directive II. These are subject to the same regulatory obligations as their traditional counterparts in the RAO. • E-money tokens: These are tokens that meet the definition of e-money¹ under the Electronic Money Regulations (EMRs), including stablecoins that meet this definition. Such tokens are regulated under the EMRs.

¹ That is:

- electronically stored monetary value that represents a claim on the issuer
- issued on receipt of funds for the purpose of making payment transactions
- accepted by a person other than the issuer
- not excluded by regulation 3 of the EMRs

Jurisdiction	Summary of Taxonomy
United Kingdom (continued)	<ul style="list-style-type: none"> ● Exchange tokens: These are tokens such as Bitcoin, Litecoin and equivalents, and often referred to as ‘cryptocurrencies’, ‘cryptocoins’ or ‘payment tokens’. These tokens are usually decentralized and designed to be used primarily as a medium of exchange. They are currently regulated only for AML/CTF purposes. ● Utility tokens: Those tokens that provide consumers with access to a current or prospective product or service and often grant rights similar to pre-payment vouchers. They currently fall outside of the regulatory perimeter. <p>Source: UK FCA PS19/22 Guidance on Cryptoassets</p> <p>As the UK seeks to introduce a comprehensive regulatory framework for crypto assets, HM Treasury has proposed the inclusion of a definition of crypto assets in the UK Financial Markets and Services Act that is similar to its current definition in the MLRs:</p> <ul style="list-style-type: none"> ● Any cryptographically secured digital representation of value or contractual rights that— (a) can be transferred, stored or traded electronically, and (b) that uses technology supporting the recording or storage of data (which may include distributed ledger technology).” <p>The consultation paper also proposes an expansion of existing regulatory frameworks to eventually cover all crypto assets.</p> <p>Source: UK HMT Consultation on Future financial services regulatory regime for cryptoassets</p>

With regard to a standalone regulatory framework vs extending the existing financial services regime to crypto assets, we encourage the Treasury to consider that the inherent characteristics of crypto assets and blockchain technology mean that the path to achieving the same regulatory outcome could differ significantly from traditional finance. For example, verifying the ownership of a crypto asset wallet, which is attached to an on-chain address rather than a legal person per se, requires a completely different process and toolset to verifying the ownership of a bank account.

These differences could be accounted for regardless of which approach Australia ultimately chooses for crypto asset regulation, by detailing specific requirements for crypto asset compliance that account for the unique risks and characteristics of this asset class where beneficial. At the same time, we note that it may be appropriate in some instances to borrow or extend existing requirements to crypto assets where the underlying risk and risk management requirements are similar. As such, the process of reviewing where existing requirements make sense in the unique context of crypto assets, and where bespoke requirements might add value, is an invaluable step in designing a regulatory framework that is fit for purpose.

For example, in Singapore, digital payment tokens are regulated as part of a broader payment services regime. However, MAS has issued requirements that are specific to digital payment tokens, such as specific AML/CFT requirements for digital payment tokens vs other fiat payment services (see [MAS Notice PSN01](#) for fiat vs [MAS Notice PSN02](#) for digital payment tokens). On the other hand, the same [cyber hygiene requirements](#) have been applied to both digital payment token service providers and other payment service providers. These requirements also broadly mirror those applied to other financial institutions.

Consultation question

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?
 - 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?

With regard to part (b) of this question, the regulation of stablecoins is particularly pertinent. We note that in its standards for the [prudential treatment of banks' cryptoasset exposures](#), the Basel Committee on Banking Supervision (BCBS) had classified crypto assets with effective stabilization mechanisms (i.e. qualifying stablecoins) separately from unbacked crypto assets, with the two categories attracting different capital treatments. The criteria for the former classification as set out in Basel Framework [SCO60](#) parts 60.11 and 60.12 are:

- Designed to be redeemable for a predefined amount of referenced assets
- Stabilization mechanism designed to minimize fluctuations in the market value of the crypto asset relative to its pegged asset
- Stabilization mechanism enables risk management similar to that of traditional assets, based on sufficient data and experience
- Sufficient information for banks to verify the ownership rights of the underlying reserve assets
- Asset issuer must be supervised and regulated by a supervisor that applies prudential capital and liquidity requirements
- Reserve assets are sufficient to enable the crypto asset are redeemable at par at all times

In their stablecoin regulatory regimes, MAS, the Hong Kong Monetary Authority (HKMA) and the New York State Department of Financial Services (NYDFS) have both proposed qualifying criteria for stablecoins that broadly mirror the BCBS standards.

- [MAS' proposed regime](#) focuses on standard-setting and regulation of Singapore-issued single currency stablecoins. These must be backed 100% by cash or equivalents and be redeemable at par in a timely manner, as well as fulfill certain disclosure, prudential and asset segregation requirements. Other non-qualifying stablecoins will be regulated as digital payment tokens alongside other cryptocurrencies.
- [HKMA's proposed regime](#) covers all stablecoins pegged to a fiat currency, which are required to be fully backed with high quality, liquid assets and be redeemable into the reference fiat currency at par. The proposed regime regulates a broader scope of activities than Singapore, including for stablecoins issued outside of Hong Kong, and prohibits Hong Kong firms from dealing in stablecoins that do not meet the qualifying criteria, such as algorithmic stablecoins.
- [NYDFS' guidance](#) requires stablecoins issued in the state to be fully backed by segregated reserve assets. These reserves must be held in custody with the state, federally chartered depository institutions and/or asset custodians, and monthly attestations on their value and adequacy by an independent Certified Public Accountant are also required.

In considering any regulatory reforms in relation to stablecoins, it may be useful for the Treasury to reference the BCBS standards and other jurisdictions' regulatory treatment of this asset class.

Consultation question

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

With regard to part (b) of this question, we would again like to highlight the importance of PPPs and industry-wide initiatives, such as Chainabuse (discussed in our response to question 3), in promoting good consumer outcomes.

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

As outlined in our response to question 5, longevity is important in any legislated definition of an asset class, and this is particularly pertinent in the fast moving crypto asset space. In this regard, should the Treasury decide to scope crypto assets/services into or out of the definition of financial product, it may consider doing so based on a set of characteristics rather than scoping in/out specific products that exist on the market today.

Consultation question

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?
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?

In balancing consumer access to crypto assets against potential consumer harm, clear and proportionate regulation that encourages crypto asset activity to stay onshore will achieve better outcomes. It ensures that Australian customers are able to access licensed crypto asset platforms, subject to appropriate regulatory requirements and oversight, and therefore deter them from seeking out unregulated or non-compliant platforms elsewhere.

In particular, we note that outright bans on marketing and promotion, or overly punitive consumer access measures, may impact service providers' appetite to serve retail customers thereby resulting in fewer onshore, regulated options for consumers looking to participate in the crypto asset space.

The UK FCA has taken the [approach](#) of applying promotion rules to crypto assets "in the same way as promotions of other financial services products with similar levels of risk." This limits financial promotions of crypto assets to registered and authorized persons, including crypto asset businesses registered with the FCA for AML/CFT purposes. In the same way, Australia could consider applying existing obligations on advertising of financial products and services to crypto assets which are scoped into the definitions of financial products and services. This would provide a level playing field with other regulated financial products and services.

No comment

We do not have comments on questions 4, 9, 12, 13 and 14 of the consultation.