# ACS Response to Token Mapping Treasury Consultation Paper

## March 2023

**Australian Computer Society Inc. (ACT)**
ARBN 160 325 931
**National Secretariat**
Tower One, 100 Barangaroo Avenue, Sydney NSW 2000
PO Box Q534, Queen Victoria Building, Sydney NSW 1230
T +61 2 9299 3666 | F +61 2 9299 3997
E info@acs.org.au | W www.acs.org.au

**To The Treasury of the Australian Government**

# ACS response
# Token Mapping Consultation Paper February 2023

3 March 2023

Dear Sir or Madam

Thank you for the opportunity to contribute to this critical issue.

The Australian Computer Society (ACS) is the peak professional association for Australia's information and communications technology sector. We represent over 35,000 members working in all sectors and across the nation.

The ACS works to grow the technology sector while making sure IT professionals act ethically, responsibly, and in keeping with the best interests of not only their employers, but the wider community.

The crypto sector is one of the most vibrant and fastest growing in Australia and the world. It's characterised by incredible innovation but also by opportunists and scammers, and we're very glad Treasury is taking these steps to start the process of integrating it into the broader economy.

Regulation is something most of the industry has been asking for – so long at is sensible, fair and doesn't overreach. It's a chance to focus on the opportunity as well as the risk of crypto, and we hope that this contribution can help Treasury and the Australian Government reach a reasonable balance.

In the following pages we have provided some answers to the questions posed in the paper. We'd be happy to discuss it further – especially since we have a large number of blockchain developers and professionals among our membership and advisory boards.

## Token mapping response

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

The crypto industry is one of the most dynamic and exciting in the world, with unrealised potential to significantly shake up finance, identity, resource tracking, contracts and public information. However, in order to realise its full potential, regulation is unquestionably necessary.

Fair, reasonable and balanced regulation in Australia can change the narrative on crypto, and enable the kind of innovation in Australia that drives multi-billion dollar industries.

It is certainly true that many of the current issues in crypto – scams, fraud, misappropriation of customer funds, market manipulation, and much more – are issues that are also present in the traditional financial sector, and have been washed through centuries of practice and legislation.

In that respect we support Treasury's work to properly map cryptocurrency products to existing financial regulations, but have concerns about the applicability of many such regulations to crypto.

Crypto has unique characteristics that will make 1:1 mapping a challenge, an attempt to fit a square peg into a round hole. Notably, some of the key challenges include:

- **Accountability.** It's not always feasible to identify accountable parties, which will make 'traditional' enforcement difficult if not impossible. Organisational units like Decentralised Autonomous Organisations (DAOs) add a further level of complication.
- **Jurisdictional.** Crypto is borderless and stateless. There is limited scope for an Australian government alone to impact the sector. Instead, impact can best be achieved through harmonized action by major players. Australia should seek to align regulation with the EU, for example.
- **Anonymity.** The pseudonymous nature of most blockchain accounts makes tracing activity challenging at best, especially combined with jurisdictional issues and decentralised exchanges that offer on/off ramps without know your customer (KYC) tracking. Wash trading (and 'pump and dump'), for example, is extremely common but also very difficult to stop, especially given the availability of new service models such as flash loans.
- **Rapid evolution.** New tokens, applications and services can spring up very quickly on a blockchain, and disappear just as quickly. A pump-and-dump scheme or rug pull might be executed and complete before a financial

regulator even becomes aware of it. Much like the internet itself, crypto is unlikely to be 'contained'.

Given these challenges, bespoke laws for cryptocurrency seem required and inevitable.

That being said, Treasury and the Australian Government should try to avoid laws that stifle innovation or make Australia "unfriendly" to blockchain and crypto enterprises. We have the potential to be a leader in the sector, and overly restrictive legislation will quash that potential.

In particular, there is a strong desire among businesses and blockchain developers for more certainty with respect to crypto asset regulation. Uncertainty around regulation is a major barrier to the technology right now. Australian businesses expect their government to provide a safe and stable regulatory environment, that protects them from fraud and also allows for innovation with reduced red tape where feasible.

Consumers would be more willing to engage if they had more guidance on what is and isn't safe, and had a more sensical tax environment that doesn't require opening up a spreadsheet to calculate tax every time they spend or move their cryptocurrency.

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

As a practical matter, the on-ramp (and often sole point of engagement) for most crypto users right now is centralised exchanges, where they can exchange fiat currencies for crypto assets – but also in very many cases use the exchange as they would a bank, leaving crypto assets in exchange custody instead of using personal wallets or dedicated custodial services. Some exchanges will even securitise those assets on the customer's behalf, putting them into (for example) staking protocols and yield farms.

Aside from laws regarding KYC, anti-money laundering and counter-terrorism financing (AML/CTF), and reporting for taxation purposes, such entities have largely been allowed to run amok, creating enormous consumer risks as demonstrated by the FTX collapse. Some common practices have included:

- running fractional reserves of custodial assets
- blending customer funds with their own investment funds, risking customer assets
- abuse of their privileged access to order books
- front running new crypto listings
- providing extremely risky leverage products to inexperienced customers
- enabling wash trading
- denying withdrawals during runs (often because of running fractional reserves)

- losing customer money to data breaches without compensation.

Given that, stronger regulation of exchanges and other custodial entities operating in Australia is one of the most impactful actions that an Australian government can make. Some of the measures to regulate them could include:

- requiring audits of assets *on-chain* to match customer funds
- banning the investment of customer funds without explicit and informed permission
- enforcement of a 'Chinese wall' between the exchange and investment operations
- enforcement of custodial requirements around breach accountability.

One of the most compelling elements of the EU's Markets in Crypto Assets (MiCA) regulation is the inclusion of Market Abuse Rules that are designed to ensure that exchanges serve as neutral market makers. We would recommend similar here, perhaps modelled on the ASX regulatory framework.

Beyond exchanges, it will be difficult for the Australian government alone to protect consumers. As noted above, however, international harmonisation can give bad actors fewer places to hide.

**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? 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?**

An important distinction needs to be made here between 'scams' and 'extreme high risk assets'. Not every crypto project that goes under is a scam, in that they don't derive from malicious intent. A scam should be characterised by malicious and deliberate intent on the part of the creator (a rug pull, for example). A project that fails should not automatically be considered a scam.

That being said, we think it would be valuable to develop a risk register or guidance to help Australian consumers. While this would not have legislative power, helping Australian consumers and investors understand the risks and requirements of a given class of crypto asset service will hopefully serve to reduce losses due to fraud and mishandling.

In practice, this could work similarly to DFAT's Travel Advisory system, providing Australian consumers with advice on the level of risk associated with a specific class of service.

This could be readily combined with a voluntary certification/tick scheme for individual projects. In such a scheme individual projects could submit projects to government for inclusion on the risk register, at which point ASIC (or some other regulatory body) performs an analysis of both risk and legal compliance and publishes the results.

Much like the Travel Advisory, it would require a principles-based underpinning to avoid having 'judgement calls' on projects being made by Australian Government employees. Such principles could include the nature of the service, legal compliance, project longevity, degree of decentralisation, the availability of white papers, whether the code is open source, project governance and tokenomics, and whether the project founders/maintainers are anonymous or known entities.

With respect to b), there are several options that could be considered. One is a consumer right, where exchanges that sell questionable tokens are governed by the same Australian Consumer Law (ACL) principles that apply to retailers of faulty products. While financial products are not currently covered by the ACL, a similar principle could be applied to tokens, which currently exist in a nebulous space outside of consumer law or the *Corporations Act*/ASIC (a fact the discussion paper acknowledges). In effect, an exchange would be liable for compensating users for any genuine 'scam' token sold on its platform.

Another option is a take down system, that allows potential scams or extreme high risk tokens to be reported to a responsible government entity. Following a principles-based investigation, the entity could issue a take-down notice which would be required of all Australian exchange providers. Penalties and compensation for users might also be applied.

In principle, this could even be extended to a system wherein new listings require regulatory authority (similar to the new EU regulations around Crypto Asset Service Providers). However, we would argue against such a model, since it will risk creating gridlock in a fast-moving industry.

**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?**

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

That is one model, but perhaps a broader definition of digital asset is required to cover both current and future use cases. The value and regulatory framework of a digital asset should not change depending on the nature of permissions or public accessibility of the storage and certification platform.

A DLT platform is not (or should not be) "special" in a legislative sense. If you define crypto tokens and crypto assets by the network on which they reside or the method by which they are secured, then you run the risk of having to repeat this process for every exception that appears.

**Levels of decentralisation and ownership**

At a fundamental level, a blockchain or other DLT could be considered to be 'owned' by its validators, since those validators collectively have control over the network and can collectively accept or reject changes to the code even when they are made by the organisation "in charge" of the DLT code (whether that's a singular business or a collective). They are providing a service – data storage, authentication, transaction processing and smart contract execution – for the benefit of their users. In some cases they are paid directly by those users; or they are compensated by the network itself in the form of newly minted tokens.

Therefore, a smart contract chain could readily be considered largely analogous to a public cloud service like Amazon Web Services or Microsoft Azure Cloud, with the primary difference being ownership of the service going from a single entity to an amorphous group of validators. The key challenge for regulators is that those validators don't have individual initiative, only collective, which makes accountability an issue.

There is an important distinction to be made here. Not all DLTs are highly distributed. In some cases a single entity or small cabal has enough validating power to be considered the 'owner' of that network. Ripple or Binance Smart Chain, for example, are largely controlled by a single company. Many proof of stake networks also have highly concentrated validating authority, to the point where an individual company or cabal can override consensus.

There may be a desire to treat such DLTs differently, since in one case there is effectively an entity that can be held accountable to the activities (and failures) of the blockchain.

**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 agree with Treasury that a principles-based model is more useful in the long term than a bespoke taxonomy of crypto assets.

a) The strongest argument *for* a bespoke taxonomy is that is provides more certainty around specific projects. A principles-based model risks potential situations where legalistic parsing of exact wording will be required to figure out where a specific project lands on the regulatory spectrum.

b) However, as noted above, we agree with Treasury that ultimately, a principles-based framework is a better model for a rapidly developing industry.

c) In the absence of a bespoke regulatory taxonomy, the Australian Government does need to provide clear on unequivocal guidance on where specific classes of tokens and services lie within the current regulations. That will ensure that businesses and consumers have no doubts about the legality and compliance requirements of a given service or class of services.

   That includes revamping current advice services (such as those offered by ASIC) to be more definitive in their advice to developers of blockchain products. Right now, for example, requests for legal advice from ASIC are often responded to with a list of laws and statutes that a *might* apply to a project, but almost never with a definitive "yes this is legal under current law" or "no it is not".

   In contrast, blockchain developers should be able to get a clear tick on a project in advance of setting it up, rather than having to roll the dice on whether ASIC or some other agency will decide to come after them.

**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?**

**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?**

a) Yes. A clear recognition in law of asset-backed tokens would be necessary, including the obligations of the holder and the receiver. In effect, asset backed

tokens function like bearer bonds, with the token acting as a contract between issuer and current holder (who may not be the original holder).

b) Yes again. An issuer of a wrapped/tokenised asset should legally and enforceably hold an obligation to redeem that asset per the original contract at time of issuance (whether that is an informal contract written on a website or coded into a smart contract). This may require some kind of government register (perhaps ASIC) or recognised "source of truth" on the issuance of such bonds that holds the contract. It could even be a blockchain itself.

**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?**

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

a) Absolutely. Issuers of tokens should be obligated to detail precisely the operating conditions and redemption value of the token, as well as any requirements around its redemption, with a clear understanding that those terms are sustained through secondary markets.
That obligation should also persist through misadventure or breach (such as cyber hacks) – the onus should always be on the issuer to redeem the token or at least provide compensation equal to the value of the token, except in cases where compliance with law enforcement prevents such (as in the instance of stolen assets). In the case of bankruptcy or company failure, token holders should be considered creditors to the defunct organisation.

b) Providing clear and simple consumer information about the nature of the asset and its associated conditions. Consumers cannot be expected to read or understand the code of smart contracts, so there needs to be a reasonable obligation to provide simple, human readable, information about the asset: where and how it can be traded, where and how it can be redeemed, any special conditions or requirements.
This information should also be included in any secondary market listing, possibly with a link back to the original issuer's contract.

**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?**

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

In some ways this takes us back to the original question in this discussion paper, about the need for bespoke regulation. There are of course numerous crypto assets and crypto asset services that *could* be considered financial products. For example, crypto asset lending services have become quite common on smart contract chains. Services that securitise real-world assets, such as real-estate tokenisation/fractional ownership services[1] could also be considered financial products.

The question is: would it be valuable to do so? That would create a fractious regulatory regime where different crypto products are governed by different laws and agencies, some of which might not have the tools to understand crypto assets.

It would also be valuable to be consistent about where these products sit within the regulatory regime and how they interact with the tax code. ASIC often wants to treat crypto assets as financial products, but the ATO treats them like goods. A single regulatory understanding is needed.

**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?**

Referring back to our answer to question 3, it is possible to 'rate' public networks on a range of criteria, including project longevity, degree of decentralisation, the availability of white papers, whether the code is open source, project tokenomics, project governance and whether the project founders/maintainers are anonymous or known entities.

A rating system based on these metrics provided by Treasury, ASIC or another entity could provide a basis for evaluating 'safe' platforms for issuance of crypto assets. A

[1] See https://www.herox.com.au/tokenization for an example.

voluntary certification model, as noted in our response to that question, could be applied.

It should be noted here, however, that a 'safe' network does not necessarily mean a safe product, and it should be made clear to consumers and business that the network and the application are not equal. There are plenty of problematic projects launched on Ethereum!

**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?**

We don't believe so, no. Current law already has provisions for requirements of sophisticated investors, so no additional law would be required.

While there are plenty of 'dodgy' assets and arrangements sold and traded on cryptocurrency networks, we don't believe it is in the interests of the Australian people for the Australian Government to decide what is and isn't a legitimate crypto asset or to restrict access to certain types of asset or arrangement. Room should be kept open for innovators in the field, and this aligns with supporting a principles-based model.

That being said, there is an opportunity to provide some sort of guidance or guarantee or 'Tick' for those crypto businesses that can adhere to a stronger regulatory framework, as noted in our response to question 3.

**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?**

Australian Consumer Law already covers obligations and requirements for companies when advertising or promoting products. If the question is "should marketing for crypto products be specially regulated the same way that, say, medical products, cigarettes and legal services are?" then we would suggest no. Companies that make obviously false or outrageous claims should be held to account by the ACCC, but we do not believe that there is, at this time, a need to carve out special exceptions for crypto products.

**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?**

An organisation that publishes a smart contract to the network should have an obligation to the outcomes as well as the regulatory compliance of that smart contract, whether or not they coded it themselves, employed a third-party contractor to develop the code or copied and pasted open source or other code.

That includes responsibility for custodial arrangements within that contract, such as when a contract holds funds in escrow or locks them for bridging purposes to other crypto networks. In the past few years, 'bridge' hacks have become one of the largest sources of crypto losses, wherein hackers have exploited flaws in smart contracts that wrap assets for transfer to other networks. The publishers of those smart contracts should be liable for such breaches.

However, a company *should not* be liable for third party use of assets created by a smart contract, any more than a road operator is liable for the actions of drivers on that road. Digital assets used in criminal activity, for example, should not be the responsibility of the creators of those digital assets, since they have no control over the actions of that third party.

**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?**

a) Such contracts are usually automated through the smart contact code, and often activate instantly and automatically without 'human care' for impacts or extenuating circumstances. This is sometimes maliciously exploited through manipulation of asset values and other techniques to push loans (even momentarily) past certain thresholds and trigger their contract conditions (such

as instant, automated liquidation). These contracts do not typically have any kind of release valve or human grace to moderate such manipulations.

Crypto loan protocols also enable certain kinds of loans that are not present in traditional finance. 'Flash loans' for example, are a completely new kind of loan enabled by automated asset recovery through smart contracts. A flash loan is a loan with an expiration period that may be measured in microseconds, in which the loan, the spend and the repayment all occur within the course of a single smart contract transaction. Their primary and initial use was to take advantage of instant arbitrage opportunities, but they have also been heavily used for the purpose of market manipulation and wash trading – sometimes to laughable degrees, such as NFTs being 'bought' (wash traded) for hundreds of millions of dollars acquired through a flash loan to inflate their perceived value.

b) We are not aware of such data. It is, as far as we know, a vanishingly small market right now and we have not seen quantitative data on the subject.

**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?**

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

a) There are a number of key differences:

- poor explainability: they are often controlled by very opaque rules, acting as "black boxes" without understanding of the operations by the user. This is exacerbated when multiple market makers and products are put together and large numbers of smart contracts start interacting in ways that are difficult to trace or understand
- there are no human controls that oversee decentralised exchanges (whether they are AMM or order book based) and many other AMMs
- their entirely online and decentralised nature means there is often no recourse in case of error or mishap
- this is where the most risky assets tend to get listed, since there are no checks and balances over listing, while most centralised exchanges do at least do some due diligence. This is a consumer risk for users of AMMs –

though we would suggest that anyone with the know-how to use an AMM (at least right now) is also cognisant of the risks

- liquidity providers might not understand the risks, such as impermanent loss
- they are not typically subject to any domestic regulation, including KYC/AML.

b) Not that we have been made aware of.

ENDS