

AUSTRALIAN BITCOIN INDUSTRY BODY

Australian Bitcoin Industry Body response to:

Crypto asset secondary service providers: Licensing and custody requirements

<https://treasury.gov.au/consultation/c2022-259046>

Introduction

The Australian Bitcoin Industry Body (ABIB) welcomes the opportunity to provide input into the regulations being developed for licensing and custody requirements of Crypto Asset Secondary Service Providers (CASSPrs).

Bitcoin is a revolutionary innovation that allows for the self-custody of money by individuals using a unique mechanism of public and private keys. However, because of the nature of the way Bitcoin is stored and sent, ABIB recognises that the interaction of traditional business structures with the Bitcoin protocol presents significant challenges. It is for this reason that all ABIB members strongly recommend that their customers self-custody their bitcoin, thus removing the risk of a collapse or hack of an exchange which has custody of many customers' bitcoin or other crypto assets.

To help inform consideration of a licensing regime for CASSPrs, the Government seeks stakeholder feedback on the following questions:

1. Do you agree with the use of the term Crypto Asset Secondary Service Provider (CASSPr) instead of 'digital currency exchange'?

Lumping all businesses that interact with crypto assets into only one category will make it difficult to develop regulations that are appropriate for sub-sectors of the industry. We believe two specific sub-categories should be considered:

Custodial vs non-custodial service providers.

There are, and will be, many businesses which interact with the crypto ecosystem in a non-custodial manner, *i.e.* they are not providing custody for their customers' assets, or are only doing so for a period of hours or days, not months and years. Non-custodial businesses do not need the same level of regulation as custodial businesses, therefore having a distinction between the two is necessary.

Bitcoin only vs cryptocurrencies service providers

AUSTRALIAN BITCOIN INDUSTRY BODY

Bitcoin is a profoundly lower risk crypto asset than any other crypto asset. This is because Bitcoin is decentralised (*i.e.* not under the control of a centralised party). For the reasons outlined, Bitcoin should be defined as its own category. Further, Bitcoin has been recognised as a global macro-asset; the Chicago Mercantile Exchange (CME) offers Bitcoin futures, Bitcoin is legal tender in the sovereign nations of El Salvador and Central African Republic, and is on the balance sheet of several public companies including the S&P500 company Microstrategy.

Bitcoin is free open-source software (FOSS) and it is possible for anyone to copy the code to make their own cryptocurrency protocol (altcoin), or simply create a token on an altcoin platform. While altcoins may have distributed ledgers, they are still controlled by centralised parties, and therefore holders of these assets are exposed to additional risks which in most cases fall outside of the jurisdiction of the Australian legal system. These risks include, but are not limited to, on-chain hacks, changes to the token supply, 51% mining attacks, reversal of transactions and censoring of transactions or entire wallets.

Therefore, creating the distinction between Bitcoin Only service providers and those that also offer altcoins (*i.e.* including any crypto asset) will ensure that the level of regulation is appropriate to the risk in each category.

2. Are there alternative terms which would better capture the functions and entities outlined above?

As described in question 1, ABIB believes the following terms are appropriate:

- Non-custodial Bitcoin only secondary service provider.
- Custodial Bitcoin only secondary service provider.
- Non-custodial Crypto asset secondary service provider.
- Custodial Crypto asset secondary service provider.

3. Is the above definition of crypto asset precise and appropriate? If not, please provide alternative suggestions or amendments.

AUSTRALIAN BITCOIN INDUSTRY BODY

A “crypto asset” is defined by ASIC as: “...a digital representation of value or contractual rights that can be transferred, stored or traded electronically, and whose ownership is either determined or otherwise substantially affected by a cryptographic proof.”¹

It is proposed that one definition of crypto assets would be applied across all Australian regulatory frameworks. This definition will capture all possible crypto assets that may be subject to the AML/CTF regime, tax, financial and other regulation in Australia.

ABIB supports the avoidance of multiple definitions of crypto assets across the individual regulatory bodies. However, as mentioned in the response to Question 1, lumping all crypto assets into one category overly simplifies the ecosystem that has developed. Bitcoin is truly decentralised as it is not controlled by a central party, and is therefore censorship resistant. With respect to ownership, because it is sufficiently decentralised, ownership of a bitcoin unspent transaction output (UTXO – the units of bitcoin that are possible to own) is absolute. The person(s) who are able to send that UTXO (*i.e.* they have access to the required private keys and pass-phrase) are the absolute owners of that UTXO; it is not possible for any other party to send or impact that UTXO or its value (*e.g.* by modifying the token supply).

For altcoins, ownership is not absolute. For example, in some altcoin protocols, transactions have been reversed, the money supply has been changed, the blockchain has been hard-forked by decree or transactions have been censored. It is not accurate to say that the person(s) who can send an altcoin on-chain is the owner, because centralised parties have the ability to impact either transactions or the token supply and therefore have some ownership of all tokens on the protocol.

For the reasons outlined, as well as many other reasons, Bitcoin should be defined as its own category. The ownership aspect of the definition needs further clarification, and should ideally be defined differently for Bitcoin and altcoins.

4. Do you agree with the proposal that one definition for crypto assets be developed to apply across all Australian regulatory frameworks?

Yes, ABIB supports having one definition that applies across all regulatory frameworks.

5. Should CASSPrs who provide services for all types of crypto assets be included in the licencing regime, or should specific types of crypto assets be carved out (e.g. NFTs)?

¹ Australian Securities and Investment Commission, [Consultation Paper 343 - Crypto-assets as underlying assets for ETPs and other investment products](#), ASIC, 2021, accessed 1 March 2022.

AUSTRALIAN BITCOIN INDUSTRY BODY

Specific crypto assets should be carved out and be regulated appropriately for their respective risk profile. CASSPrs that only deal with Bitcoin should not have to comply with regulations that are only relevant to altcoins, for example interactions with copyright law which would only apply to NFTs.

Further, native blockchain tokens (*i.e.* the token that is built **into** the blockchain, *e.g.* bitcoin) should be regulated differently to tokens that are created **on** a blockchain (*e.g.* those aiming to be a digital representation of a real world asset such as US dollar stable coins or gold backed tokens).

6. Do you see these policy objectives as appropriate?

With respect to dot point 1 (minimise the risks to consumers...):

ABIB agrees that minimising risks to consumers is an appropriate objective. However, the most effective way to achieve this would be to:

- Educate consumers on the importance of self-custody of crypto assets (*e.g.* through the use of hardware wallets) and encourage consumers to do so, thus minimising the exposure of consumers to exchange hacks, theft etc.
- Provide clarity to consumers on the risk profile of different crypto assets by having separate and appropriate categories for crypto assets based on their risk profiles.
- Minimise regulation to ensure that there is a diverse offering of secondary service providers on the market. Over-regulating will lead to fewer, larger, secondary service providers which would serve to *increase* the risk as these large institutions would serve as a honey pot, attracting nefarious actors who can spend a large amount of resources in an attempt to steal the crypto assets under the custody of the large CASSPrs.

With respect to dot point 2 (support the AML/CTF regime...)

This regulation currently exists and is managed by AUSTRAC, there does not appear to be any reason to further complicate this structure.

With respect to dot point 3: (provide regulatory certainty about the policy treatment of crypto assets and CASSPrs...)

This is not deemed to be an appropriate policy goal. No amount of regulation will create a perfectly safe secondary service provider. All large institutions are susceptible to internal bad actors who may create back doors in the code to allow them to steal crypto assets. Crypto assets may also be lost due to human error. Providing a signal that a business is sound will give consumers a false sense of

AUSTRALIAN BITCOIN INDUSTRY BODY

security. In the long term, it would be far safer for consumers to assume that all businesses are *not trustworthy*, and take responsibility for their own crypto assets through self-custody.

7. Are there policy objectives that should be expanded on, or others that should be included?

Yes. More education is required so that consumers understand the importance of self-custody of crypto assets. Additionally, the terms *decentralised* and *ownership* need to be better defined. Decentralisation is the absence of centralisation. This distinction is critical to understanding the risk profile of different crypto assets. Further, *ownership* is only absolute in a *decentralised* crypto asset.

8. Do you agree with the proposed scope detailed above?

ABIB supports the aim to reduce the number of licenses required to operate a secondary service provider. Further, for CASSPrs offering crypto assets that are not financial products (*e.g.* Bitcoin only CASSPrs), minimising the need for additional licenses (*e.g.* by combining any additional requirements into the existing AUSTRAC process) would provide the best outcome for the industry.

9. Should CASSPrs that engage with any crypto assets be required to be licensed, or should the requirement be specific to subsets of crypto assets? For example, how should the regime treat non-fungible token (NFT) platforms?

This question highlights the need to have sub-definitions of CASSPrs (specifically custodial and non-custodial) and appropriate categories of crypto assets (with Bitcoin in its own category) so that the various regulatory regimes can be applied appropriately. With these categories appropriately defined, a non-custodial Bitcoin only business may not require any additional regulation beyond AUSTRAC. Whereas an exchange that offers hundreds of crypto assets including stable coins, tokens deemed financial products or securities, NFTs, tokens that are backed by other tokens (*e.g.* a basket of NFTs similar to an ETF), etc. should probably comply with several different sets of regulations.

10. How do we best minimise regulatory duplication and ensure that as far as possible CASSPrs are not simultaneously subject to other regulatory regimes (e.g. in financial services)?

AUSTRALIAN BITCOIN INDUSTRY BODY

By having appropriate sub-categories of crypto assets and CASSPrs so that regulation will be applied only where it is necessary and only where it will add value.

11. Are the proposed obligations appropriate? Are there any others that ought to apply?

Regarding point 2: In addition, CASSPrs should be required to run a full node (*i.e.* a copy of the blockchain maintained on their own server which validates every transaction on the blockchain) for every crypto asset that they offer. This will ensure that CASSPrs minimise risk by not having to trust the version of the blockchain or the money supply of the protocol provided by another party's node that may lie in another jurisdiction.

Regarding point 5: All CASSPrs should be full reserve (*i.e.* no fractional reserve banking).

Regarding point 8: This is a worthy objective, and ABIB believes that CASSPrs should not falsely describe crypto assets that they offer as decentralised if they are not sufficiently decentralised (*i.e.* the absence of centralisation). Hence the need for a more accurate definition of the term *decentralised*.

Additionally, CASSPrs should independently verify the token supply of any crypto asset that they offer to their customers, using their own full-node, to ensure that the token supply matches that claimed by the cryptocurrency protocol or its owners.

Regarding point 11: ABIB deems it reasonable for independent external audits of businesses to occur to ensure that they are offering the services that they claim to offer. However, ABIB is against internal audits as they may reveal key security secrets and/or compromise established security protocols which puts the exchanges' digital assets at risk.

12. Should there be a ban on CASSPrs airdropping crypto assets through the services they provide?

Generally speaking, ABIB favours educating consumers rather than outright bans. That said, "Airdropping" can only be performed by a centralised party, which should be recognised as a centralised token.

Additionally, consumers should be made aware that tokens that are simply created from nothing have no long term value.

AUSTRALIAN BITCOIN INDUSTRY BODY

13. Should there be a ban on not providing advice which takes into account a person's personal circumstances in respect of crypto assets available on a licensee's platform or service? That is, should the CASSPrs be prohibited from influencing a person in a manner which would constitute the provision of personal advice if it were in respect of a financial product (instead of a crypto asset)?

Yes, financial planners and financial advisors should be properly educated on crypto assets (including the technical nature of what makes a crypto asset decentralised) and financial advice should remain in that domain, not within the CASSPr remit.

14. If you are a CASSPr, what do you estimate the cost of implementing this proposal to be?

There are not enough details available to accurately estimate the cost. Our position continues to be to favour self-regulation where possible.

15. Do you support bringing all crypto assets into the financial product regulatory regime? What benefits or drawbacks would this option present compared to other options in this paper?

No. Bitcoin is not a financial product and should not be regulated as such. It is more accurately categorised as property, commodity or money. Some other crypto assets are indeed financial products and should be regulated through the financial product regulatory regime if that would be deemed the most suitable option.

16. If you are a CASSPr, what do you estimate the cost of implementing this proposal to be?

There are not enough details available to accurately estimate the cost. ABIB's position continues to be to favour self-regulation where possible.

17. Do you support this approach instead of the proposed licensing regime? If you do support a voluntary code of conduct, should they be enforceable by an external dispute resolution body? Are the principles outlined in the codes above appropriate for adoption in Australia?

AUSTRALIAN BITCOIN INDUSTRY BODY

Yes, ABIB supports self-regulation of the industry, and ABIB is prepared to develop the regulations that will apply to the Bitcoin only industry in Australia. We believe this will create the best outcome of regulations that will protect consumers, as well as continue to allow innovation in the Bitcoin industry. ABIB has access to board members, members and sponsors, many of whom have extensive experience working directly with Bitcoin.

The principles in the example codes given are not appropriate for industry wide adoption in Australia. For example, Blockchain Australia's 37 page *Australian Digital Currency Code of Conduct* does not mention any requirements for businesses to run their own nodes or even mention the word *node* once. The *Global Digital Finance Principles for Token Trading Platforms* also fails to mention nodes.

Nodes are an essential component of a decentralised cryptocurrency. Hence, ABIB believes it necessary to develop a Bitcoin specific voluntary code of conduct which is written in consultation with technical Bitcoin experts.

In the interest of protecting consumers, ABIB supports an external dispute resolution body that can adjudicate on matters specifically relating to CASSPrs.

18. If you are a CASSPr, what do you estimate the cost and benefits of implementing this proposal would be? Please quantify monetary amounts where possible to aid the regulatory impact assessment process.

Per previous questions, ABIB cannot estimate the cost of implementation without more specific details. ABIB will require a once-off outlay of time to develop the voluntary code of conduct. However, it is not expected that implementation of the code of conduct will be onerous.

19. Are there any proposed obligations that are not appropriate in relation to the custody of crypto assets?

Yes. Additionally, we reiterate our point that self-custody is the safest way for consumers to protect themselves from loss of crypto assets by CASSPrs:

(21) *holding assets on trust for the consumer*

AUSTRALIAN BITCOIN INDUSTRY BODY

Given how the security of assets operates in Bitcoin and other crypto assets, holding crypto assets on trust would offer no protection to consumers. Therefore, it is recommended that this point be removed.

(2) ensuring that consumers' assets are appropriately segregated

This is not feasible or value-adding. In the example of an exchange, the assets of the business and the consumer are constantly being exchanged off-chain (*i.e.* within the accounts of the exchange). To “segregate” these on-chain would add significant friction to businesses while providing no additional security for consumers because the same party (*i.e.* the CASSPr) would have responsibility for the private keys of both the consumer’s crypto assets and that of the business.

(3) maintain minimum financial requirements including capital requirements

CASSPrs should be operating on a full reserve basis.

(8) independent verification of cybersecurity practices

ABIB would support independent auditing of cybersecurity practices if the independent party was using only public access (*i.e.* a standard customer account or accessing the website or app without a login) to the CASSPrs website to perform white-hat penetration testing.

However, if the intent is for the auditor to have super-user or administrative access (*i.e.* the ability to observe internal processes including private key management) then ABIB would strongly oppose this proposed obligation. A CASSPr’s processes for securing their crypto assets should *never* be shared outside of the organisation. Should this become an obligation, it is likely that a few companies will audit the industry. These auditors would collectively have the knowledge required to take the crypto assets of the *entire* Australian crypto industry. Apart from the risk to the businesses, the individual auditors may be creating a safety risk to their own lives and that of their families, should nefarious actors realise the valuable secrets held by these auditors.

(9) processes for redress and compensation in the event that crypto assets held in custody are lost

Bitcoin transactions are immutable; they cannot be reversed. Any form of insurance that is implemented would be incredibly expensive and hamper Australia’s global competitiveness. It is better to approach this problem understanding that crypto assets that are lost are irretrievable, and develop processes that better deal with this new reality (*e.g.* self-custody).

AUSTRALIAN BITCOIN INDUSTRY BODY

20. Are there any additional obligations that need to be imposed in relation to the custody of crypto assets that are not identified above?

All CASSPrs should consider the following scenarios and implications. ABIB will include these in its voluntary code of conduct:

- The death or incapacitation of an employee of a CASSPr that is a required signer of on-chain transactions (*i.e.* is the only person who has access to a private key that is required to send the CASSPr's crypto assets).
- The death or incapacitation of two (or multiple) employees of a CASSPr whose private keys collectively are required to sign the organisation's multi-signature transactions (*e.g.* several employees may be travelling to a conference together who may hold the quorum in an n-of-m multi-signature wallet).
- The resignation of an employee of the CASSPr that is a required signer of on-chain transactions (*i.e.* ensuring that this person no longer has access to the CASSPrs private keys).

21. There are no specific domestic location requirements for custodians. Do you think this is something that needs to be mandated? If so, what would this requirement consist of?

It would seem prudent to ensure that a quorum of private keys will be required to send significant amounts of the crypto assets out of CASSPr regardless of the location of the individuals involved. Bitcoin is, by nature, borderless.

22. Are the principles detailed above sufficient to appropriately safekeep client crypto assets?

No.

No amount of regulation or procedures will keep client's crypto assets perfectly safe. There will always be the possibility that a bad actor or actors within a CASSPr will disappear with a client's crypto assets. There will always be the possibility of human error. There will always be the possibility of the unexpected death of a private key holder who has not made appropriate back up preparations. These scenarios will always exist. Therefore it is safest for all crypto asset holders to self-custody their assets with their own private keys. Then, when one of the above scenarios occurs, the loss is minimised to the individual asset owner.

AUSTRALIAN BITCOIN INDUSTRY BODY

23. Should further standards be prescribed? If so, please provide details.

No. ABIB favours self-regulation as will be discussed in the next set of questions.

25. Is an industry self-regulatory model appropriate for custodians of crypto assets in Australia?

Yes, particularly for Bitcoin-only businesses because ABIB's members, board members and sponsors represent the foremost Bitcoin technical experts in Australia.

26. Are there clear examples that demonstrate the appropriateness, or lack thereof, a self-regulatory regime?

ABIB member's businesses have been operating for up to eight years (which is a significant amount of time given Bitcoin only launched in 2009) with none of these businesses collapsing or performing an exit scam or shutting down unexpectedly.

27. Is there a failure with the current self-regulatory model being used by industry, and could this be improved?

ABIB is not aware of a failure in the way the current Bitcoin only industry operates within Australia, particularly with the exclusive focus on Bitcoin, encouraging customers to self-custody and educating customers on Bitcoin, and with each business running its own full node to ensure the accuracy of transactions.

Additionally, ABIB's board members, members and sponsors voluntarily meet at least once a year in person or via video to share knowledge of the latest developments in Bitcoin, such as Taproot and implications for multi-signature.

28. If you are a CASSPr, what do you estimate the cost of implementing this proposal to be?

AUSTRALIAN BITCOIN INDUSTRY BODY

Implementing industry self-regulation would be by far the best cost/benefit option for Bitcoin only businesses as:

- The regulations would be specifically tailored to Bitcoin only businesses and not have any friction associated with other crypto tokens.
- The regulations would be developed by the foremost Bitcoin technical experts in Australia, and would ensure that security practices keep pace with developments in the Bitcoin Core software as well as new hardware wallet products.
- The Bitcoin industry in Australia has already implemented critical security practices such as using multi-signature wallets, securing private keys with hardware wallets and generating private keys offline (*i.e.* not on an internet-connected computer).

29. Do you have any views on how the non-exhaustive list of crypto asset categories described ought to be classified as (1) crypto assets, (2) financial products or (3) other product services or asset type? Please provide your reasons.

Bitcoin should not be categorised as a financial product. It could potentially be categorised as money, a foreign currency (given its legal tender status in the sovereign nations of El-Salvador and Central African Republic), property or a commodity.

Additionally, please refer to the answer to question 30.

30. Are there any other descriptions of crypto assets that we should consider as part of the classification exercise? Please provide descriptions and examples.

A distinction should be created between native crypto tokens (*e.g.* Bitcoin, which is integral to the blockchain and is only created through mining), and other tokens (*e.g.* an Ethereum ERC20 token) which can be created at no cost without mining (*i.e.* without proof-of-work).

A distinction should be made between decentralised crypto assets (*i.e.* those that have no centralised controlling party and allow users to run their own node) and centralised crypto assets. The key factor here is not whether or how much a protocol's blockchain is distributed, but whether a central party can reverse transactions, censor wallets, modify the token supply, turn off the protocol or be regulated by bodies in other jurisdictions (*e.g.* the US based Securities and Exchange Commission).

Using these categories, Bitcoin would be a decentralised crypto asset, while altcoins would be categorised as centralised crypto assets.

AUSTRALIAN BITCOIN INDUSTRY BODY

31. Are there other examples of crypto asset that are financial products?

Yes, including but not limited to:

- Crypto assets that launched with an ICO
- “De-Fi” tokens
- Governance tokens

32. Are there any crypto assets that ought to be banned in Australia? If so which ones?

Banning would only encourage consumers to bypass regulation and be more susceptible to scams that manage to sneak through regulation. ABIB continues to favour educating consumers on how Bitcoin actually works to empower them to make their own educated decisions.