Blockchain Australia

PROMOTING BLOCKCHAIN INNOVATION IN AUSTRALIA

Blockchain Australia – Submission to Attorney General Consultation

Modernising Australia's anti-money laundering and counter-terrorism financing regime

June 2023

Table of Contents

1. Blockchain Australia 3

2. Executive Summary 4

3. Detailed Response 6

1. Blockchain Australia

This submission is made by Blockchain Australia, in collaboration with its members and industry stakeholders.

Blockchain Australia is the peak industry body representing Australian businesses and business professionals participating in the digital economy through blockchain technology. Blockchain Australia is non-partisan and encourages the responsible adoption of blockchain technology by the government and industry sectors across Australia as a means to drive innovation and create jobs in Australia.

The Blockchain Australia membership base consists of 120+ leading cryptocurrency and Blockchain centric businesses and 100+ individuals across multiple verticals including:

- Accounting and Taxation
- Artificial Intelligence
- Banking
- Cyber Security
- Art
- Development
- Building & Construction
- Digital ID
- Energy and Resources
- Entertainment
- Gaming
- Health and Wellbeing
- Insurance
- Investment
- Legal
- Professional Services
- Recruitment
- Real Estate
- Risk and Compliance
- Supply Chain
- Venture Capital

The sector contributes AU$2.1 billion and employs approximately 11,600 people (Source) and with supportive reform these figures could increase to AU$68.4 billion and over 206,000 people employed in the sector.

In responding to this and other government consultation we seek a fit-for-purpose, technology-enabling regulatory framework with clear guideposts for consumers and a focus on driving innovation and Investment while protecting consumers.

We thank you for taking the time to consider our submission.

Gordon Little

Policy, Blockchain Australia

2. Executive Summary

Blockchain Australia is grateful for the opportunity to provide its response to the Attorney General Consultation - Modernising Australia's anti-money laundering and counter-terrorism financing regime.

We endorse the government's collaboration with industry to streamline AML/CTF obligations, thereby eliminating the current redundancies and incongruities, and aligning them with globally accepted standards. In particular the distinction between Part A and Part B of the AML/CTF program is complex and there is a lack of explicit statements regarding risk assessments.

Our members place significant emphasis on the acknowledgment that digital (Crypto) payments will progressively gain prominence, necessitating the adaptation of AML/CTF obligations to accommodate these practices. We strongly advocate for fostering innovation and stimulating growth within the Australian sector.

With that objective we are conscious that the use cases and operating models for Digital Assets are still evolving and over regulation will stifle the sector forcing developers and organisations to move offshore outside the Australian regulatory environment.

We are also conscious that the current media narrative on digital assets is negative and may lead to regulators and governments believing the risks associated with the sector are greater than our research would indicate. Recent research from Chainalysis shows the following global trends.:

- The share of all cryptocurrency activity associated with illicit activity has recently risen for the first time since 2019, from 0.12% in 2021 to 0.24% in 2022.
- A large proportion (43%) of these illicit volumes came from activity associated with sanctioned entities, such as Garantex (a Russian-based high risk exchange), which has significantly skewed the trend.
- Although scams were the second largest component of the illicit activity, making up $5.9b worth of illicit activity, crypto scam revenue fell significantly in 2022, from $10.9 billion the year prior. However there continues to be a number of highly successful scams, the top being Hyperverse with nearly $1.3 billion in revenue.
- Ransomware attackers extorted at least $456.8 million in digital assets from victims in 2022 - a substantial reduction on the $756.6 million the year before, but still a significant sum no less.

The FATF has noted that ransomware attackers tend to receive and launder their ransoms in the form of digital assets. We acknowledge that there are certain features of digital assets that can make them attractive to illicit actors.

However, equally, the transparency of the public ledger offers important tools in the fight against illicit finance, which AUSTRAC should consider as it develops industry-specific guidance as well as its own work programme. As detailed in the Coinbase response to this consultation there are a number of organisations developing tools to assist DCE's and regulators to meet AML/CTF obligations.

We would also draw your attention to our submission to Treasury on De-Banking[1] in 2022, and reiterate that access to banking and financial services can no longer be seen as a privilege. Individuals and organisations can no longer operate on a cash basis with access to government services, utilities and many other essential services now requiring a bank account.

It is critical that any modification to AML/CTF obligations ensures that organisations cannot unreasonably withhold services and reasons for being de-banked must be clearly articulated and provide valid commercial reasons for not being willing to provide the service. We recommend that the obligations around transparency and fairness are mandatory and enforceable.

Finally we would add that this consultation is being undertaken in parallel to consultations on the licensing of exchanges and custodians as well as a Board of Taxation review which is due in September. Any changes to the AML/CTF obligations need to be developed in parallel to the other digital asset legislation that is being developed.

We look forward to working with the Attorney General's office and AUSTRAC on the program to modernise the Australian AML/CTF regime.

Michael Bacina

Chair, Blockchain Australia

Gordon Little

Policy, Blockchain Australia

[1] https://blockchainaustralia.org/wp-content/uploads/2022/12/Treasury-Policy-Response-to-DeBanking.pdf

3. Detailed Response

Questions for all entities

1. ***How can the AML/CTF regime be modernised to assist regulated entities address their money laundering and terrorism financing risks?***

   We are supportive of the government's effort to update Australia's AML/CTF regime to ensure it is fit-for-purpose, responds to the evolving threat environment, and meets international standards set by the Financial Action Task Force, the global financial crime standard-setter.

   We are encouraged by the government's approach to work closely with industry to both learn from and educate organisations on AML/CTF best practice. The practicalities and challenges of implementing effective AML/CTF programs are impacted by a range of internal and external factors that are often outside a single organisation of government to control.

   As such it is important that as part of the consultation process real world examples are documented and analysed to determine the best approach to regulation and implementation of controls by organisations.

   We represent a broad range of organisations in terms of size, geographical footprint and sector that are impacted by AML/CTF obligations. As a consequence changes to the regime need to ensure that:

   a. The expansion of AML/CTF obligations should not apply a "one size fits all" approach to all digital currency service providers regardless of business model. For example, service providers who engage solely in the business of long-term custody of digital currency for solely Australian clients, where transfers in and out of custody are infrequent, may pose a lower AML/CTF risk than other types of business. Digital currency service providers should in all cases be left to identify, assess, and measure risks, and apply controls that are most appropriate for their business model. In particular all obligations should be scaled such that what is required of an organisation depends on the size, nature and complexity of the organisation and its money laundering and terrorism financing risks.

b. The legislation is consistent with global best practice and the timing of complying with the legislation takes into consideration the challenges of operating in markets where not all counterparties are obliged to comply with similar requirements.

c. The obligations are clear, consistent and able to be implemented without adding unnecessary cost and or introducing risk/liability that could impact the ability for these organisations to operate and receive funding.

2. ***What are your views on the proposal for an explicit obligation to assess and document money laundering and terrorism financing risks, and update this assessment on a regular basis?***

   We are supportive of the explicit obligation for all organisations to assess and document AML and terrorism financing risks. Having clarity of this process is important to those who provide services into the digital economy.

   Based on the assessment and risk profile it would be useful to have guidelines for organisations providing input into minimum expectations of AML/CFT programs for different risk levels.

3. ***For currently regulated entities, to what extent do you expect that a simplified AML/CTF program obligation would affect your AML/CTF compliance costs?***

   Our members anticipate that simplified AML/CTF obligations would reduce cost or at a minimum be cost neutral.

   We are however concerned and have evidence from other geographies that the introduction of additional obligations on VASPs (Digital Currency Exchanges) has increased compliance costs primarily as a result of the travel rule and sunrise challenge.

4. ***What kind of entities would you propose to include in a designated business group if membership were no longer limited to regulated entities, and what volume of AML/CTF information would you seek to share?***

   The definition of eligible entities should be wide, leaving it up to the reporting entity to ultimately decide. The reporting entity(ies) within the group should be required to

apply a risk-based methodology for restricting who within the group should be allowed what information including suspicious matter information.

Trying to document all eligible group structures or a particular volume of AML/CTF information is overly prescriptive and unhelpful. AUSTRAC could provide guidance on what it thinks is a reasonable risk assessment. For example, Officers and other senior management within a group that may not constitute Related Bodies Corporate but which shares a common logo should have access to information they need to discharge their responsibilities, which include complying with the law and operating a risk-based AML/CTF framework.

5. ***How will a flexible approach that allows an AML/CTF program to incorporate all related entities within a designated business group affect your AML/CTF compliance and risk mitigation measures?***

   Having a flexible approach to incorporate all related entities within a designated business group would simplify the reporting process for our members affected by this.

6. ***What are your views on the proposal to expressly set out the requirement for entities to identify, mitigate and manage their proliferation financing risks?***

   We are supportive of expressly setting out requirements, on the basis that these are consistent with FATF and generally accepted international standards. Our members do not anticipate this will have much impact beyond updating AML/CTF programs to also include proliferation of financing risks which is a FATF recommendation and already seen in other jurisdictions.

7. ***What guidance would you like to see from AUSTRAC in relation to AML/CTF programs?***

   The following would be beneficial to our members.:

   a. Expanded training (educational visits).
   b. Clear examples of the types of risks and expected AML/CTF measures expected from an organisation to mitigate them.
   c. Clarity on what constitutes ‘grounds for suspicion’ for DCEs and therefore when an SMR needs to be lodged. The 2021 guidance provides good

guidance and practical examples for banks and other financial institutions however we require more specific guidance.

d. A helpline for DCEs to call when they have questions about SMR information and lodgement process.

e. Greater public-private and industry-wide information sharing arrangements on evolving typologies of financial crime, as well as on suspicious addresses. AFCX[2] is one example of this.

Customer due diligence

8. What are your views on the proposed simplification of the customer due diligence obligations as outlined?

Without seeing the updated guidance on how obligations are to be met it is difficult for our members to assess the impact of the proposed changes. We note that the proposed changes as described in the Consultation Paper would:

a. seek to require reporting entities to assess every customer relationship for risks associated with channel, product, geography and customer risks, rather than more broad identification requirements currently required by the safe-harbour process.

b. require the collection of additional information, and to conduct dynamic risk assessments that are affected by the customer's activity.

Increasing the complexity of identifying customer risks and introducing dynamic risk assessments may have a negative commercial impact on many reporting entities, especially for smaller entities.

Accordingly, any such changes should be sufficiently detailed to minimise the impact on a reporting entity's ability to comply with the regulations in an affordable manner. To assist members, the provision of case studies that provide detailed examples of how small to large businesses could successfully meet their obligations would be beneficial.

9. Do you have suggestions on other amendments to customer due diligence obligations?

[2] https://www.afcx.com.au/

In determining the data types and documentation required to identify and assess a customer, the government needs to balance the need to see and retain sensitive data with the risks associated with saving and storing this data to demonstrate organisations have met their obligations.

The increased risk of cyber crimes means that organisations need to adopt a minimalist approach to storing and retaining sensitive data. Legislative changes need to include provisions to allow for organisations to rely on self sovereign ID providers to verify the identity of consumers.

Examples of this could include a situation where a user allows Services NSW or My Gov to verify a user and then to make that acknowledgement known to the organisation conducting due diligence with minimum data transferred to the organisation. A record of the interaction with the government being sufficient evidence that the identity was verified.

Our international members' experience with Singpass (Singapore's equivalent of Australia's Mygov) has been positive. For the purposes of streamlined eKYC, Singaporean businesses can integrate with Myinfo (govt tech KYC solution) enabling businesses to pre-fill digital forms with data from Government sources via Singpass. The onboarding process is almost instant which is a great user experience.

Amending the tipping-off offence

10. ***Are there aspects of the tipping-off offence that prevent you from exchanging information, which would assist in managing your risks?***

    Our members note that there have been problems with sharing data with AFCA where a complaint is lodged regarding the rationale for the offboarding of a customer. It is unclear what information can be or should be provided to AFCA without breaching the tipping off provisions. Members seek clarity on what information can and cannot be provided to AFCA in these situations.

    We would also appreciate clarity on the ability to share data in court cases where data has been subpoenaed.

11. ***What features would you like to retain or change about the current tipping-off offence?***

We are supportive of the intention to focus on not compromising an investigation, however, the proposed reforms should take care not to follow other jurisdictions blindly. For example, the UK requires transactions deemed suspicious to be frozen until approved by the NCA. We understand that, in practice, this has been incredibly difficult to achieve without the customer realising that something is wrong, and has proven to be costly to implement effectively, greatly impacting the customer experience.

We would also like to ensure that proposed changes do not add to the current challenges with de-banking of individuals and organisations in the digital asset sector. We are concerned that organisations are hiding behind the tipping off obligations as a basis to withhold services. We would like to see changes to the effect that unless the organisation has alerted authorities and raised an SMR that they cannot withhold banking services due to tipping off.

12. ***What safeguards are needed to protect against the disclosure of SMR-related information? Has the current tipping-off offence achieved the right balance between protecting against the risk of leaked SMR information and disclosures which help manage shared risks?***

Our members have not raised any concerns with regard to sharing of SMR data.

Digital currency sector

13. ***What are the benefits and challenges of expanding the AML/CTF obligations to a broader range of digital currency-related services?***

We support the proposal to increase supervision of digital currency exchanges (DCEs) and believe it will reduce the risks of ML/TF in Australia.

For our members that have implemented AML/CTF programs we do not believe the inclusion of these additional services will have a large impact on their operations and may reduce AML/CTF risk in interacting with other DCE's in Australia knowing that they all have to comply with these obligations.

Our members are also supportive of the Swyftx recommendation in their response that "additional concepts could be explored, such as considering whether 'designated services' is still the most effective model to use. In this regard, we note that the UK and New Zealand focus on types of businesses subject to the regulations, rather than

the services offered. This prevents the need for introducing new designated services to keep up with ML/TF trends."

We would draw your attention to the 5th additional service being, "Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset". Clarification on the meanings of "participation in" and "financial service" is required, noting that the definition of "financial service" is not consistent with Chapter 7 of the corporation's law. There is a need to ensure this definition evolves in line with the changes being proposed under the token mapping exercise.

Failure to align the definitions would result in our members having to assess tokens against two different definitions to determine if they have regulatory obligations.

14. ***How can definitions under the Act be amended to integrate digital currency activity in payment-related obligations, such as activities associated with credit, debit and stored value cards and general transfers?***

Changes to definitions should accommodate new technology infrastructure for payments and associated services and align to the definitional changes resulting from other digital asset regulatory reform under way.

More specifically we would draw your attention to the response from Coinbase that provides examples of where definitional changes would be appropriate.

Financial institutions, remittance & digital currency sector

15. ***What are the benefits and challenges for financial institutions in applying the existing travel rule obligations?***

We support efforts to apply the Travel Rule to VASPs, as it provides valuable assistance to law enforcement and regulatory agencies in detecting, investigating, and prosecuting money laundering and other financial crimes by creating and preserving an information trail about persons sending and receiving large sums of money through the funds transfer system. But because the Travel Rule was designed many years ago, it understandably does not contemplate digital assets nor does it specifically accommodate for the nuances presented by blockchain technologies. As a result, the Travel Rule construct presents several novel compliance challenges for VASPs, these include:

a. Interoperability
b. Sunrise Challenge: if other countries haven't implemented a travel rule then they are outside the regime.
c. Discoverability issue with finding out who the counterparty is - is it a VASP? Is it a reliable VASP?
d. Identification of a secure method of transmitting applicable Travel Rule data which cannot be included on the public blockchain. This requires a secure separate network to transmit this data on.
e. Ensuring/verifying that the travel rule data is sent concurrently or prior to the transaction data is complicated by the validation process of public ledgers whereby the transaction is published in the ledger but the Travel Rule data is sent via a private network and may not occur concurrently.
f. Transaction eligibility where the transaction thresholds between countries can vary - e.g. For a particular transaction, a sending VASP needs to comply with their country's travel rules triggered by the set $1,000 threshold but the receiving VASP need not comply with their country's travel rule for this transaction as their threshold is $3,000
    i. Inconsistent regulator treatment
    ii. Inconsistent treatment by exchanges in foreign jurisdictions - if you are applying for a license you have to have ability to work with countries entities on the travel list. Could we whitelist of approved exchanges/markets
g. Increased compliance costs whereby members have needed to increase their compliance costs 3-5x to deal with increased volumes in geographies where this has been implemented.
h. We also have concerns about including the physical address in data collection in order to protect consumers from physical crime in the event of a wide scale data breach.

We would draw to your attention that the industry has been working to overcome these problems. An example of this is that a large group of VASPs over the last few years have worked on the development of TRUST—a Travel Rule solution that allows VASPs to accurately identify their counterparties and securely exchange required data. VASPs around the world are already using the solution to exchange information required under the Travel Rule.

TRUST's rapid growth since its launch in 2022 is a testament to the industry's commitment to solving complex compliance challenges. All VASPs who join TRUST undergo comprehensive evaluations to help ensure that their security protocols are equipped to prevent unapproved access to sensitive customer data shared by TRUST participants.

Further, TRUST was designed so that no customer personally identifiable information is stored on a centralised database but is instead only shared directly between counterparty VASPs via encrypted, peer-to-peer channels, reducing the risk of hacking or improper access. These and other features have been critical to TRUST's growth to become the world's leading Travel Rule solution.[3]

16. ***Would the proposed model assist in addressing these challenges?***

Aligning the proposed model with FATF would assist our members in having a globally consistent program. However, we do have concerns that FAFT requires the capture (albeit not validating) the identity of the receiver of the transaction. In situations where a DCE allows customers to transfer crypto to private wallets, the identity information of the recipient is not always available for capture beyond the public keys of the recipient. We would welcome the opportunity to work with AUSTRAC on this problem.

We note that the current FATF obligations require VASPs to capture both sender and receiver information. Our members are concerned that they will be in breach of personally identifiable information obligations (or in breach of internal policies) if they are asked to send details of receivers to the transactions initiating party.

We also recommend an appropriate transition period of at least 12-18 months to allow the industry to make the required changes and to accommodate jurisdictions whose regulations are still evolving.

Exemption for assisting an investigation of a serious offence

17. ***Are there any additional issues that would not be addressed by the proposed approach for exemptions for assisting an investigation of a serious offence?***

We are supportive of this proposal.

[3] *See Coinbase, The Standard for Travel Rule Compliance: Travel Rule Universal Solution Technology, https://www.coinbase.com/travelrule (describing the TRUST platform and listing VASPs who have joined the TRUST coalition).*