Submission by

to the

Ministry of Justice

on the

Anti-Money Laundering and

Countering Financing of Terrorism Act 2009

3 December 2021

Contact:

Alison Mackie

Community Manager

BlockchainNZ

E| team@blockchain.org.nz **P|** +64 27 359 3938

3 December, 2021

AML/CFT Consultation Team
Ministry of Justice
SX 10088
Wellington 6140

BlockchainNZ Submission – Review of the AML/CFT Act

SUMMARY:

1. Blockchain NZ thanks the Ministry of Justice for the opportunity to submit on its Review of the AML/CFT Act consultation document. This submission is in response to sections relating to regulations and obligations of virtual asset service providers.
2. In response to the review, BlockchainNZ are aware of the Ministry's aspiration to make Aotearoa New Zealand one of the hardest places for money laundering to occur. However, BlockchainNZ stress the importance of balancing this aspiration, with the importance of enabling businesses and the wider economy to grow and prosper, particularly to counter some of the negative effects which the COVID-19 pandemic has had. Accordingly, we encourage the Ministry to explore and then enable the use of technological solutions which might achieve this fine balance.
3. BlockchainNZ is happy to engage further with you to discuss our submission in detail and provide further assistance.

BACKGROUND:

4. BlockchainNZ is a member of the New Zealand Tech Alliance (NZTech). NZTech is a group of independent technology associations from across New Zealand that work together with a common purpose to connect, promote and advance technology ecosystems and to help the New Zealand economy grow to create a prosperous digital nation.
5. BlockchainNZ itself is an association of organisations and individuals that represent the rapidly emerging business sectors being built using blockchain technology. These business sectors encompass IT, trade and supply chains, virtual asset service providers, financial services, and the public sector, to name a few. BlockchainNZ has taken a leading role in growing our country's ability to maximise opportunities enabled by blockchain technology and address key challenges.

COMMENT:

6. This submission is in response to sections relating to regulations and obligations of virtual asset service providers.

What is the right balance between prescriptive regulation compared with the risk-based approach?

7. BlockchainNZ encourages the Ministry of Justice to continue a risk-based approach to the regime. BlockchainNZ agree that a risk-based approach would continue to ensure an adaptable and flexible AML/CFT regime. In order for New Zealand to remain technologically competitive on the global stage, regulations need to allow innovation to flourish.
8. An effective risk-based regime can foster innovation while holding actors accountable and responsible when assessing the risks associated with what they're creating. This is especially relevant to the FinTech and Virtual Asset Service Providers (VASPs) sectors, where there is global market growth. If a regime were to be too prescriptive, it could hinder innovation and technological development, which would place New Zealand at a disadvantage in international markets. Another related issue of concern is that AML/CFT activity would still continue offshore, where New Zealand regulators have no jurisdiction.

Should there be an AML/CFT-specific registration regime which complies with international requirements?

9. BlockchainNZ recognises that there are international pressures from the Financial Action Task Force (FATF) for stricter AML/CFT registration and licensing regimes. BlockchainNZ believes that proper registration is needed. However, licensing may be unnecessary to ensure New Zealand's AML/CFT regime meets international requirements. Further, if a fit-and-proper process were to be established, it could discourage new entrants to confidently access the market.

10. Other jurisdictions have a more rigorous regulatory setting for virtual assets and VASPs than New Zealand. Some jurisdictions require VASPs to obtain a licence before operating. Jurisdictions operating VASP licencing regimes have been known to develop bottlenecks and backlogs within their regulatory organisations. This makes the licencing process more difficult to manage for all parties, and some licence applicants have withdrawn their licence applications as a result.

11. Theoretically, BlockchainNZ are conscious that a VASP licensing regime might give more credibility to the VASP industry. It is also possible that a VASP licensing regime could address some banks concerns with providing or continuing to provide banking services to VASPs. The theory being that a VASP licence would provide additional assurance to a bank, that a particular VASP has appropriate compliance and risk management frameworks, which would reduce the risk profile that VASP as a customer.

12. BlockchainNZ have confidence that the Department of Internal Affairs (DIA) would be able to track active participants by employing an effective registration system. However, if a licensing regime were to be employed, this could draw time and resources from the main cause, as it would require additional audit requirements. This in turn would make the licencing process expensive for new market entrants, and could increase de-banking risk.

Should we use regulations to ensure that all types of virtual asset service providers have AML/CFT obligations, including by declaring wallet providers which only provide safekeeping or administration are reporting entities?

13. The virtual asset market is broadly (but not solely) operated by VASPs. VASPs deal in "virtual assets" and are an onramp and offramp for the virtual asset market to function. VASPs do this by providing a platform that enables the exchange of fiat currency or virtual assets for other virtual assets, and vice versa. According to the FATF, a "virtual asset" is a "digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes".[1]

14. Under the current AML/CFT Act, VASPs must comply the same way banks, other financial institutions and non-financial entities do. VASPs must conduct customer due diligence on all customers, which includes verifying their customers' identity. VASPs must also determine the source of funds or the source of wealth of high-risk users and trusts, report suspicious activities to the New Zealand Financial Intelligence Unit and lodge prescribed transaction reports. As VASPs are captured by the current AML/CFT Act, the risks of money laundering or financial terrorism using VASPs has been significantly mitigated.

15. VASPs generally fall under the DIA jurisdiction, although there is scope for VASPs to be within the Financial Markets Authority's (FMA) remit. The FMA requires VASPs to register on the Financial Service Providers Register in compliance with the Financial Service Providers Registration and Dispute Resolution Act 2008 . This has the effect of bringing virtually all VASPs within the FMAs jurisdiction. If underlying crypto-currencies services are not considered "financial products" under the Financial Markets Conduct Act 2013 (FMC Act), VASPs must still comply with the fair dealing obligations of financial service providers.

16. If a VASP is servicing virtual assets, which are financial products under the FMC Act, then that VASP will be regulated like any other service provider, requiring a licence, product disclosure statement, licensed supervisor, and/or financial obligations under the FMC Act, depending on the types of financial product involved.

17. Reading the recently released guidance by FATF on virtual assets and VASPs (FATF Guidance)[2], it appears that not all forms of digital assets fall within the FATF's definition of a "virtual asset". Only digital assets which are FATF virtual assets have the effect of making a digital asset business a VASP for regulatory purposes. For instance, certain digital collectibles in the form of non-fungible tokens

1 [1] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html.

2 Ibid.

(NFTs) are not virtual assets according to the FATF, if these digital collectibles are not capable of being used for payment or investment purposes. Blockchain NZ recommend that the Ministry engage with industry experts to provide more clarity and guidance on the types of digital assets and digital asset business which are caught by the AML/CFT Act – i.e. what types of digital assets are "virtual assets". Providing this clarity to the industry will have flow-on effects in helping to determine which digital asset businesses are VASPs for the purposes of the FMC Act, the AML/CFT Act and the FSP Act.

18. If regulations were to capture all VASPs, including those that only provide safekeeping or administration as reporting entities, there needs to be more consideration of the implications of the trade-off between costs and benefits (with benefits including the mitigation of money laundering / terrorism financing (ML/TF) risks). A clear understanding needs to be established as to what and how much ML/TF risks are mitigated by capturing all VASPs under the same regulations, as well as the associated costs for individuals, businesses, and society. To anticipate no further compliance costs is not clear enough, and further investigation into these costs, both financial and time-cost, is imperative.

Would issuing regulations for this purpose change the scope of capture for virtual asset service providers which are currently captured by the AML/CFT regime?

19. Virtual asset service providers are covered under current laws, as New Zealand has an adaptive regulatory regime, which allows VASPs to work within AML/CFT guidelines. BlockchainNZ encourages the inclusion of continuing adaptive regulations, as the nature of the technology evolves frequently and faster than regulations can adapt to. BlockchainNZ suggests regulations are based upon set objectives and principles, rather than specific and set compliances to ensure businesses continue to meet new and proposed regulations as technology evolves.
20. BlockchainNZ foresee that the Ministry, in consultation with New Zealand's supervisors of the AML/CFT Act, specifically the DIA, the FMA, and the Reserve Bank, will consider whether to enforce the "travel rule" recommended by the FATF. The travel rule will further enhance the visibility and identity of VASPs, which should have the flow on effect of making money laundering or financial terrorism more difficult to achieve using virtual assets and VASPs. BlockchainNZ do not have an opinion on whether the travel rule should be introduced and enforced into the new AML/CFT Act. However, anecdotally that jurisdictions with more mature ML/F regulatory regimes than New Zealand's struggle to enforce the travel rule.
21. If new regulations are set to become stricter to mitigate local and international AML/CFT risk, this may negatively impact technological innovation within New Zealand. Users within New Zealand may become more inclined to seek external and overseas financial services due to restrictive regulations. Rather than exporting our services internationally, restrictive regulations may see further exporting of talent. We need to ensure New Zealand is positioned to be a technological hub where regulations facilitate innovation, job creation, and host economic benefits. BlockchainNZ urge regulators to ensure the regime allows responsible and dedicated users to comply and conduct business and not deter potential participants.
22. BlockchainNZ is aware that the Select Committee on Australia as a Technology and Financial Centre recently published a report to the Australian Senate, which explored, among many things, the regulation of virtual assets and VASPs under the Australian Anti-Money Laundering and Counter-Terrorism Financing Act 2006.[3] BlockchainNZ recommends that the Ministry follow the developments in Australia.

Are the standards of verification and the basis by which verification of identity must be done clear and still appropriate? If not, how could they be improved?

23. BlockchainNZ suggests the proof-of-address requirement should be changed from "verification" to "collection". The Ministry of Justice would be wise to consider the inclusion of "digital" components where possible, particularly where the entity can collect the IP address of a user who accesses your site to perform a transaction. The main issue is the costs versus benefits, specifically in relation to identification verification, the AML process as a whole, as well as the trade-off between privacy and

[3] https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/AusTechFinCentre/Final_report.

transparency.

24. In relation to identity verification, BlockchainNZ considers the current verification process and customer due diligence requirements through the AML/CFT regime is a necessary process, however it comes at a cost - not only for businesses but also for the consumer, as sometimes customers have to pay to have their identity verified. It creates an economic benefit through employment and jobs, however it does create costs across sectors and duplication costs, which disproportionately affects small and medium sized businesses. There is also additional risk of personal information and identity being disclosed to unwanted parties through the current regime.
25. In relation to privacy and Transparency, BlockchainNZ considers a level of transparency is needed for an effective AML/CFT regime to function. Most market participants are honest actors who set out to conduct legitimate business. They deserve the right to privacy and to conduct business without interference. New Zealand has privacy laws, however, this is often in conflict with what the AML/CFT Act states.

Are there any identity documents or other forms of identity verification that businesses should be able to use to verify a customer's identity?

26. With the implementation of a digital identity framework, with zero-knowledge proof, individuals do not have to disclose information about themselves or their identity. However, they will still be able to be an active participant. A sound digital identity framework will ensure businesses and users are meeting compliance lines and their requirements without having to endure unnecessary risk or invasion of privacy.
27. Through the implementation of a decentralised electronic ID verification system, digital identity providers can ensure high levels of identity assurance. As trust is seen as a human construct, not a technical one, a decentralised system will ensure individuals have full ownership and control over their data. A decentralised system for ID verification will allow for new market actors, reduced costs, and ensures we focus on our trust in privacy.

Are there any obligations we need to tailor for virtual asset service providers? Is there any further support that we should provide to assist them with complying with their obligations?

28. BlockchainNZ encourage the development of industry standards for the custody of virtual assets to ensure user assets are protected from theft and negligence and that regulatory standards mitigate the risk of ML/TF. The inherent visibility and traceability of virtual assets within blockchain protocols, as well as the work of many blockchain analytic companies (such as Elliptic and Chainalysis), who work with VASPs and law enforcement to trace the movement of illicit or stolen virtual assets across blockchain addresses.
29. BlockchainNZ recommend that the Ministry and government agencies work collectively and holistically with the industry around the regulatory settings for virtual assets and VASPs as they relate to security laws, anti-money laundering and counter financing of terrorism law, and financial service provider law. New Zealand regulatory settings for virtual assets and VASPs should be aligned with the resources and internal expertise available within New Zealand's regulators of virtual assets, to ensure that the regulatory settings are fit for purpose.
30. BlockchainNZ encourage the Ministry to recognise the importance of balancing the mitigation of risks associated with virtual assets and VASPs against the importance of preserving a legal and regulatory environment that does not stifle New Zealand innovation or prevent willingly compliant enterprises from operating. Achieving this balance would likely have a positive flow on effect on the wider economy, such as growth in the New Zealand tax base and employment, consumer protection and an overall reduction in ML/TF risk.

If so, should the threshold be set at NZD 1,500 (in line with the FATF standards) or NZD 1,000 (in line with the Act's existing threshold for currency exchange and wire transfers)? Why?

31. To align with global FATF standards and improve competitiveness for New Zealand companies, BlockchainNZ believe that increasing the wire transfer threshold to $1,500 would be beneficial. Our

members also believe that there is no need to redefine "wire transfer" as there have been significant developments in payment methods since the wire transfer provision was initially set out.

Are there any other issues with the definitions that we have not identified?

32. BlockchainNZ NZ has identified Issues regarding the definitions of VASPs:
33. Under current FATF definitions, general VASP activity is sufficiently captured. However, given the speed of innovation within the VASP space, BlockchainNZ encourage the Ministry of Justice to develop a strategy for addressing new risks as they emerge. In particular, BlockchainNZ recommends adding "Decentralised Autonomous Organisation" (DAO) alongside natural or legal persons. For a DAO to be considered a VASP, it needs to be clear that these activities are conducted by an individual user, and that a person who provides the platform for someone to take his/her action does not become a VASP.

CONCLUSION:

5. Thank you for the opportunity to provide feedback. BlockchainNZ is happy to engage further to discuss our submission and provide any further assistance.

6. If you have any further queries do not hesitate to contact me.

Yours sincerely,

Alison Mackie

Community Manager

BlockchainNZ

E| team@blockchain.org.nz **P**| +64 27 359 3938