Mitchell Travers, Managing Director, Aus Merchant Pty Ltd

Website: ausmerchant.io

Submission on Notice: Means to stop de-banking through greater regulatory oversight.

Introduction:

The Senate has requested further submissions regarding regulation that would mitigate debanking to be provided on notice. Aus Merchant welcomes the opportunity to provide additional information on notice. Debanking was raised as a serious issue for crypto businesses in Australia. Chairperson Senator Bragg considered that with greater regulation, banks would not be as inclined to debank crypto businesses as a risk avoidance strategy. The following submission will provide our suggestions that would assist to decrease risks that banks face by servicing crypto businesses.

Suggestion 1 - Tailoring AUSTRAC DCE Registration

Tailoring DCE AUSTRAC Registration would assist to raise regulatory standards for DCE and reduce perceived risks from banking providers. The DCE AUSTRAC registration form is similar to a remittance registration form. The lack of specificity fails to address unique risk considerations and solutions available to DCE. The following questions and standards should be considered for DCE AUSTRAC Registration.

Questions:

How are private keys stored?

Private keys enable access to a user's wallet. It is standard practice for DCE to have possession of a user's private key in order to authorise transactions as a matter of convenience and safety for their clients. If a user or DCE loses their private key, they are permanently locked out of their wallet. There have been several notable stories of users locked out of their cryptocurrency

wallets.[1] Private key storage is a significant part of a DCE service. It is also closely related to digital asset custody, which is explored in Suggestion 2 below.

How are on-chain/layer 2 transactions monitored?

Transactions that occur on-chain are between wallet addresses, and if the wallet address sits outside the DCE's system, then the DCE may not know the identity of the holder. This is due to wallet addresses being pseudonymous. One of the key advantages of decentralised cryptocurrency is that all transactions are recorded on a public ledger. Transaction monitoring can identify money laundering/terrorism financing risks, where unknown users are sending/receiving cryptocurrency. Solutions for on-chain transaction monitoring are advantageous as they can identify risks posed by external wallets and flag suspicious transactions, however, they are also expensive. Further as these ledgers grow in size, the cost to add a transaction in the form of a new block to the chain increases. This has led to the development of 'layer 2' solutions, where transactions occur off the chain, then batched and recorded on the ledger.[2] Layer 2 solutions create difficulty to monitor transactions. Aus Merchant does not currently use a layer 2 solution to ensure strict segregation of client funds.

How are coin-swap or anonymous coins identified?

Some services have a high indication of illicit activity, such as coin-swaps or use of anonymous coins. A coin-swap service enables cryptocurrencies to be swapped between ledgers, for example a client receives Bitcoin from a coin swap service that has swapped Ethereum for Bitcoin. These swap services can conceal the origin of the swapped coin, in this case the Bitcoin, which has been swapped for an equivalent value in the user's Ethereum. Concealing the origin of the Bitcoin can raise concerns around money launder/terrorism financing. Similarly, anonymous coins or coin tumblers can also conceal the origin or account holder and raise similar concerns.

Is due diligence conducted for external wallets that are parties to transactions in DCE?

As noted above, wallets that are not within the ecosystem of the DCE may pose money laundering/terrorism financing risk as the identity of the of the wallet owner may not be available to the DCE. Some DCE may attempt to avoid this risk by blacklisting all external wallets, however, this is not a viable solution for a start-up DCE whose clients may want to send and receive cryptocurrencies from existing wallets.

Where is the cryptocurrency liquidity sourced from?

In order for a DCE to enable users to trade, they need to have reserves of cryptocurrencies to be traded. This liquidity can be sourced from DCE worldwide, including jurisdictions where AML/CTF

[1] https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html
[2]

risk is very high. Australian DCE should ensure that they are not incidentally laundering money or financing terrorism by purchasing cryptocurrency from high risk sources.

What due diligence is conducted for cryptocurrency liquidity providers?

Further to the above, DCE should detail how due diligence is conducted on cryptocurrency providers to ensure that money laundering/terrorist financing risk is avoided.

Standards for DCE that we suggest may be considered:

Multi Factor Authentication

Multi-factor authentication (MFA) is a standard security measure to access accounts across a variety of services, and should be utilised by DCE to sign transactions for wallets in custody. As noted above, cryptocurrency transactions are signed by a private key. This private key is commonly held by the DCE, who provides custody for their client's digital assets. Access to private keys should be protected by MFA. MFA is an accessible standard for DCE. Further considerations on custody standards will be discussed in Suggestion 2.

Use of on-chain monitoring services

On-chain monitoring services are a powerful tool to monitor transactions and prevent money laundering/terrorism financing risk, however, can be a significant cost for a start-up business. Aus Merchant currently uses an on-chain transaction monitoring service to monitor and review transactions. It may be prudent for on-chain monitoring services to be considered a voluntary standard for DCE under a specific transaction volume and mandatory for DCE with transaction volume above that designated level. There are alternative means to prevent risk posed by external wallet addresses, anonymous coins and tumbling services, which are discussed below.

Whitelisting external wallet addresses

Whitelisting external wallets means that external wallets are subject to a due diligence process and then permitted to transact with wallets within the DCE. This is in opposition to blacklisting, where an individual wallet address is banned from transacting. In a whitelisting process, all external wallet addresses are prevented from transacting until they have passed due diligence thresholds. Whitelisting creates significant control over the DCE ecosystem and minimises money laundering/terrorism financing risk posed by external wallets. Aus Merchant employs a whitelisting process for all external wallets.

Banning/limiting anonymous coins/coin-swap services/tumbling services

DCE should have processes to identify the use of anonymous coins, coin-swap services and tumbling services. DCE have the capability to prevent anonymous coins to be received/sent on their exchange. On-chain transaction monitoring services can identify when coin swap/tumbling

services have been used. Enhanced due diligence measures can be triggered by the use of such services, and the source of funds then determined. DCE should prepare how they plan to address these risk and what mitigation strategies they have in place.

These additional questions and standards create clear expectations for DCE in regards to their infrastructure and processes required. AUSTRAC would need to engage with industry to ensure that any additional requirements are realistic, current and accessible for start-ups.

Suggestion 2 - Custody Standards for Digital Assets

The development of a tailored license for digital asset custody will raise overall regulatory standards for digital asset service providers and create further evidence of regulatory compliance to banking providers. Currently, custodians of financial products are subject to AFSL requirements. Digital assets have unique technological features and risks that mean current custody regulations are inadequate. In ASIC's Consultation Paper 343 (CP343), ASIC also recognised the need for a specific digital asset custody license that reflected these technological requirements.[3] Aus Merchant already employs some of the custody standards put forward by ASIC in CP343.[4] We agree with the below standards suggested by ASIC for digital asset custody:

- Specialist expertise and infrastructure for digital asset custody;
- Segregation of crypto assets on blockchain - unique public and private keys for each client;
- Private key generation and storage in a way that minimises risk of unauthorised access
- Multi-signature or sharding based storage;
- Practices for receipt, validation, review, reporting and execution of instructions; and
- Robust cyber and physical security practices.

In light of potential regulatory change, it is important to emphasise that any change must reflect market realities. Genesis Block has advised that potential change to digital asset custody regulation may include requirements for digital assets in custody to be stored in Australia.[5] Digital asset custody is not suitable for on shore storage. This is due to the lack of experienced digital asset custody providers with sufficient technological capabilities based in Australia. Digital asset custody is a developing area, with international companies spearheading the development of robust technology and safe services. These companies have high regulatory standards and maintain compliance in multiple jurisdictions. Our custodial service provider, Fireblocks, has offices in the UK, Hong Kong, Israel, Singapore, France, Germany and Switzerland.[6] Requiring digital asset custody to be hosted in Australia would create difficulty to ensure high quality custody of digital assets and severely impact the ability for Australian companies to provide custody of digital assets to their clients. Access to private keys and transfer instructions are ultimately

[3] ASIC CP343 p.20 [53]
[4] ASIC CP343 p. 19 [C1]
[5] Genesis Block provided this advice during the course of the engagement with Aus Merchant for consultant services.
[6] https://www.fireblocks.com/about/

managed by the head of compliance, who is domiciled in Australia. This key person is subject to police checks, staff due diligence and Australian law, even if the assets are held internationally. Creating a regulatory environment that encourages and supports digital asset custody could entice these international companies to establish offices in Australia. Communication between regulators and industry can ensure that further regulation is well informed and able to increase the quality of services provided.

Suggestion 3 - Greater Education

Debanking may also be reduced through educating the banks on the AML/CTF regulations for DCE. Chairperson Senator Bagg noted that the AUSTRAC DCE registration was essentially useless in a decision to cancel banking services to a DCE for AML/CTF risk. Achieving the requisite standard from AUSTRAC and providing proof of that compliance to a bank should safeguard banking services from the risk of being debanked. If banks had greater knowledge of the compliance required for DCE and their relevant process and procedures, there would be less perceived risk of banking a DCE. AUSTRAC advised the Committee that DCE requested that the DCE registration list to not be made public, to prevent being automatically debanked. Making the DCE registrar public should mitigate risk of debanking by demonstrating compliance with AUSTRAC. DCE cannot achieve a high regulatory standard if they are unable to access banking services. Greater collaboration and communication to increase education amongst industry, banking providers and regulators will be needed to ensure a high standard of regulatory compliance. Where banking providers require further information as to the nature and process of DCE transactions industry providers, such as Aus Merchant, would welcome the opportunity for greater communication and collaboration.

Suggestion 4 - Balancing Regulation with Innovation

The benefits of additional regulation must be balanced against potential negative impacts. Regulation must be fit for purpose; it should be tailored to the specific technological and market requirements of digital assets. It is clear that through this consultation process, Australia is well positioned to ensure new regulations will be relevant to the digital asset industry and congruous with achieving fair, orderly and transparent digital asset services. Jurisdictions that have taken a litigious approach to regulation, such as seen with the SEC's enforcement of Coinbase[7] are relying on regulations that when drafted, could not conceive the technological capability of cryptocurrencies. Regulation by litigation is an expensive exercise, both for industry and the regulator. The crypto industry in Australia is currently driven by disruptive start-ups, and regulation should not create a barrier of entry which is too high for start-ups. This is especially important as established and institutional companies enter into the crypto industry. Established businesses not only have a financial advantage over startups but also have existing relationships with banking and insurance providers. One example where the need for regulation to be both fit for purpose and not pose a barrier to entry is in relation to prospective market licenses for digital currency exchanges. DCE have similar functions and features to OTC trading. Any potential introduction

[7] https://blog.coinbase.com/the-sec-has-told-us-it-wants-to-sue-us-over-lend-we-have-no-idea-why-a3a1b6507009

of market licenses for DCE should reflect the features and technology of DCE, as a market license is a large undertaking for a start-up. The regulator's approach to Buy Now Pay Later ('BNPL) regulation highlights the benefits of enabling a low barrier to entry. BNPL operated in a regulatory 'grey zone' and were able to build successful and respected services.

In order to ensure that regulation is achieving the desired goals, new regulation should be subject to regular reviews by the regulator in partnership with industry. These reviews can ascertain whether new regulation is achieving the desired outcome. Regulations introduced for the purpose of preventing debanking should be measured against debanking outcomes. This provides an opportunity for education amongst both the industry and regulators. A collaborative approach to regulation ensures that the regulator is aware of industry movement, and able to address regulatory needs efficiently and effectively.

Suggestion 5 - Support of Current Proposals

In addition to the above recommendations, Aus Merchant would also like to emphasise support for existing proposals raised by the ACCC for a debanking appeals process and in the Farrell Review for tiered payments licensing.

The ACCC Foreign Currency Conversion Services Inquiry, published in 2019, identified de-banking of non-bank International Monetary Transfer ('IMT') suppliers as damaging to innovation and competition.[8] Although the ACCC did not find that the banks were engaging in anti-competitive behaviour, they recommended that banks and IMT suppliers engage in a due diligence scheme that involved a review process.[9] Similarly, in their submission to the Senate, ACCC representatives affirmed their support for a review/appeals process for debanked individuals/entities. We support this proposal and believe it would open communication and clarify compliance expectations from banks.

We also support the Farrell Review's proposal for tiered licensing for payment service providers.[10] This tiered form of licensing could account for the specific needs of smaller businesses who offer cryptocurrency payment solutions through to larger more established cryptocurrency payment service providers. By enabling a means for smaller, less established businesses to access licensing, the perceived risk of non-compliance will be reduced. This is particularly relevant where more established, larger businesses begin to provide cryptocurrency payment services, such as Zip-Pay[11] or even banks. Larger businesses will have pre-existing relationships with their banking providers and are not likely to be subject to debanking resulting from their cryptocurrency payment services. This poses a risk to creating an anti-competitive environment and potentially stifling innovation. Aus Merchant supports these proposals as a means to introduce regulation that mitigates debanking.

---

[8] ACCC Foreign currency conversion services inquiry, Final Report, July 2019, p. 57 [2.4]
[9] ACCC Foreign currency conversion services inquiry, Final Report, July 2019, p. 64
[10] Farrell Review, Recommendation 9.
[11] https://www.afr.com/companies/financial-services/zip-unveils-plan-to-jump-on-bitcoin-bandwagon-20210914-p58rha

Suggestion 6 - Travel Rule

The risk of debanking may further be influenced by the introduction of a requirement to comply with the FATF travel money rule. The Select Committee questioned the utility of the travel money rule and the capability for cryptocurrency service providers, also known as virtual asset service providers, to comply with the requirements. The FATF Second 12 Month Review on Virtual Asset and Virtual Asset Providers ('the Second Review) affirms the FATF's position to increase compliance with the travel money rule.[12] However, the Second Review acknowledges there is a lack of universally accepted travel money rule solution to virtual asset service providers.[13] Internationally, companies are conducting research and development for blockchain specific solutions.[14] Market participants, such as Aus Merchant are in the best position to technically evaluate these proposed solutions as well as provide additional feedback and support for Australian specific compliance standards. Compliance with the travel money rule is particularly difficult for virtual asset service providers due to friction between the technology and the information required to be shared. For example, wallet addresses are different to bank accounts as they are pseudonymous, and there is difficulty to identify the owner of the wallet. In order to comply with travel money rule, both payer and beneficiary information needs to be attached to the transaction for the respective institutions to collect.[15] Aus Merchant is exploring how to add identifiers to wallets hosted in custody on behalf of customers for the purpose of travel money rule compliance information sharing obligations. Two proposed solutions include the use of NFT technology or alternatively working with a blockchain analytics company to develop a permissioned and independently verifiable database of customer details and transactions for the purpose of information sharing between counterparties. We encourage a collaborative approach for the introduction of the travel money rule in Australia.

Suggestion 7 - DeFi as a New Class of Financial Products

Regulation of Decentralised Finance ('DeFi') products would be assisted by the creation of a targeted licensing regime. Aus Merchant and other DCE registered with AUSTRAC have the ability to deal and issue DeFi products without breaching AML/CTF obligations. Some of these products act in a similar manner to traditional financial products. However, the range, scope and continued development of DeFi products create difficulty to apply existing financial regulations, such as AFSL requirements. We suggest the development of a targeted DeFi licensing regime to adequately address the unique technological considerations of DeFi products. This DeFi license regime should draw on existing key principles and standards in the current AFSL for regulatory consistency. Key principles regarding some of the following features (without limiting the scope)

[12] FATF Second 12-month Review Of The Revised Fatf Standards On Virtual Assets And Virtual Asset Service Providers p. 40 [140 b.]
[13] FATF Second 12-month Review Of The Revised Fatf Standards On Virtual Assets And Virtual Asset Service Providers p. 17 [54]
[14] See: https://shyft.network/, https://blog.chainalysis.com/reports/chainalysis-notabene-travel-rule-integration
[15] Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (Report, October 2019), 17(16)

such as custody, lending, fixed/variable interest rates, collateral requirements, capital requirements and key persons requirements would provide the basis for regulation. DeFi authorisation can be further tailored based on the DeFi product being issued/dealt to retail/wholesale clients. For example, additional requirements may be placed on DeFi lending, staking or other DeFi products. We also include the below suggestions regarding this new DeFi regulation regime.

Smart Contract Auditing

To gain authorisation from ASIC to deal or issue a DeFi product, a digital asset service provider should have the smart contract audited, either through by a third party or internally prior to issuing/dealing in the product. This ensures that the smart contract conforms with the features of the services listed to ASIC.

Database of DeFi Product Standards

As digital asset service providers are authorised by ASIC to issue/deal DeFi products, these smart contract standards should be collected by ASIC. The database of smart contract standards would ensure any forthcoming products would meet or exceed existing standards and prevent the same DeFi products being issued or dealt with different standards.

We acknowledge that creating new licensing standards is a large undertaking, however, DeFi products are ill suited to existing regulatory frameworks. In order for regulation to provide consumer protection, it will need to address the specific nature of DeFi products. The potential cost from harm caused will outweigh the cost of implementing proactive regulations.

Suggestion 8 - Recognition of Uses and Benefits of Blockchain Technology to Regulators

The benefits of blockchain/distributed ledger technology extend to government and regulatory uses. Regulators, and the government more broadly, have an opportunity to understand and benefit from blockchain technology to achieve greater compliance efficiency and effectiveness. The below will outline triple entry accounting, DeFi standards and blockchain signatures to enable regulator verification. By engaging with this technology, the government can regulate more effectively and increase overall knowledge and skill in the industry.

Triple Entry Accounting

Blockchain technology provides an opportunity for ‘triple-entry accounting,’ a significant breakthrough in accounting standards. Double entry accounting, which is the separation of debit and credit books, created incredible economic improvements and fostered innovation. The improved level of accuracy from double entry accounting over single entry accounting increased trade activity, particularly international trade, and subsequently increased economic activity. Triple entry accounting is where the blockchain keeps an independently verifiable record of debit

and credit, reconciling debit and credit recordings of two parties.[16] This distributed ledger may be only available to view by the parties or publicly available, depending on its design. Triple entry accounting reduces the mistakes and inconsistencies found in double entry accounting. It also significantly decreases the ability to falsify accounting records. Triple entry accounting has the potential to be a powerful tool that increases the standard of financial record keeping.

Blockchain Signatures for Regulator Verification

Regulators can also use features of distributed ledger technology to improve efficiency and accuracy of compliance due diligence. Blockchain signatures enable the verification of wallets, and the funds under management, without revealing the associated private key. A regulator, such as ASIC or AUSTRAC could set up their own wallet address for the purpose of verification. Cryptocurrency service providers, such as DCE, can generate a cryptographic signature to demonstrate ownership of wallets in custody, which is then sent to the regulator's wallet address. This enables a quick, easy and efficient auditing process for regulators that can then inform compliance with custody regulators or other such regulations as relevant. In order to implement this strategy, regulators will need increased education and knowledge. This increase in education will assist regulators to understand the technology and industry it regulates. Engaging with the technology will assist regulators to act in an informed manner that reflects market concerns and industry capabilities.

Conclusion

Aus Merchant is invested in the growth of a stable and safe cryptocurrency industry that yields broad economic benefits. We support the creation of smart regulation that assists the industry to grow and develop. The Select Committee's commitment to engaging industry feedback highlights the value of collaboration. The above suggestions provide a tangible way to approach debanking and regulation more generally. We hope that as industry experts, we are able to assist and educate regulators.

Sincerely,

Mitchell Travers
Managing Director
Aus Merchant Pty Ltd

[16] https://medium.com/uclcbt/is-bitcoin-really-triple-entry-accounting-df14e26ae3e7