BITAROO
BUILT FOR BITCOINERS

22 December 2020

Senate Select Committee
Financial Technology and Regulatory Technology
Department of the Senate
Parliament House
Canberra ACT 2600

Via email: fintech.sen@aph.gov.au

Dear Committee,

Fintech regulatory agencies around the world have clearly recognised that Bitcoin as well as other blockchain-enabled fintech products and payments infrastructure are borderless by their very nature as they are operating one protocol layer above the internet rather than via the traditional payment rails.

This realisation has led governments to take a coordinated approach to regulating this emergent technology through bodies such as FATF, IOSCO and the Financial Stability Board.

However, regrettably, it has become apparent that regulators lack a fundamental understanding of Bitcoin as well as open source blockchain technology in general. As a result, they continue to make poor decisions which, astonishingly, *increase* the risks to individuals while failing to adequately address both real and hypothetical threats arising from malicious actors that would seek to take advantage of this evolving technology.

Digital assets have unique properties that necessitate a more thoughtful regulatory regime

Bitcoin is unique and cannot be easily compared to legacy financial assets in a number of important ways.

Among many of its advantages, Bitcoin is decentralised (no single point of failure) and facilitates frictionless peer to peer 24/7/365 payments worldwide at extremely low costs.

Businesses and individuals are now leveraging these benefits to construct a more open and efficient financial and payments system online.

Within the cryptocurrency space, Bitcoin is the most established and reliable blockchain, with unparalleled settlement assurances, and a thriving ecosystem of developers and fintechs.

Media headlines tend to focus on its volatility and price (currently at all-time highs at the timing of writing) and neglect to mention that Bitcoin has experienced steady year-after-year growth in its hashing power, number of new wallets, and realised capitalisation – all indicating a healthy ongoing expansion of the network.

Bitaroo Pty Ltd supports a more sensible and effective approach to user protection

Bitaroo Pty Ltd has taken a principled decision to list only Bitcoin on its digital currency exchange. This is due to Bitcoin's superiority among cryptocurrencies in many aspects including but not limited to its guaranteed and auditable supply, fully decentralised network, and established track record of highest resilience against external shocks.

07 3185 0202
info@bitaroo.com.au
www.bitaroo.com.au
9/204 Alice St,
Brisbane QLD 4000

We believe that this is a responsible decision on behalf of Australian buyers and investors.

As a registered Digital Currency Exchange that is regulated by AUSTRAC we also support a sensible and measured approach by policy and regulatory agencies seeking to integrate digital assets into legacy systems - however, it is now becoming apparent that Australia's Government risks *destroying* the balance between innovation and regulation if it continues down its current path.

Government can do more to support blockchain-fintech without compromising standards

The key arguments of this submission are:

(1) Governments, including Australia's, are failing to sufficiently consider the risks to individuals arising from 'KYC honeypots' in the digital asset sphere;

(2) Governments, including Australia's, are imposing excess regulatory burdens on businesses due to their lack of technological literacy and moral panic over crypto-enabled entrepreneurship, and

(3) Australia's Government needs to do more as a sovereign nation to use its voice in international deliberations on blockchain regulation, rather than silently importing domestic policy regimes from foreign bodies such as FATF.

This submission makes *three key recommendations* that would help to improve the situation, supporting nascent fintech ventures and providing more choice to Australians. We hope to see these recommendations reflected in the Committee's critical work program going forward.

Kind regards,

Ethan Timor
Managing Director
Bitaroo Pty Ltd

SUBMISSION BY

Bitaroo Pty Ltd

FOR

Senate Select Committee on Financial Technology and Regulatory Technology
via email fintech.sen@aph.gov.au

—

Open source technology innovation is fundamentally different in nature to closed and proprietary ventures.

Open source projects contribute a sizeable share of innovation and growth to the digital economy, creating 30 million jobs for developers alone, and supporting a services industry on track to be worth US$33 billion by 2022 (CB Insights, Research Report, June 2020).

One critical area of rapid growth in open source software development is the newly emerging class of fintech projects backed by blockchain - most notably, Bitcoin, which many consider to be one of the most important, if not the most important, open source project under development worldwide.

The potential transformative benefits of this type of innovation cannot be overstated.

The digital asset industry has already drawn in hundreds of billions of dollars of capital in recent years, and according to the Government's own National Blockchain Roadmap, blockchain is expected to deliver annual business value in excess of US$3 trillion by 2030.

This is in addition to the significant benefits that will accrue to ordinary citizens that are increasingly looking to leverage open protocols for remittances, micropayments, non-fungible art and a host of other uses.

However, in order to realise the enticing possibilities that digital assets offer, businesses require an enabling regulatory environment that is mindful to the unique features of this still poorly-understood technology.

—

KYC regulations pose additional risks to digital asset users relative to other financial assets

Bitcoin, and to a lesser degree some other cryptocurrencies, is unique relative to other financial assets in a number of important ways.

One of the key differentiating features of Bitcoin is that it is a *bearer instrument*, meaning that it is controlled entirely by its custodians.

This is different to financial assets that Australians traditionally own, such as shares.

In the case of a share portfolio, one can rely on a share registry or stockbroker to keep records of their legal ownership, without the risk that if the share registry's records are leaked, the underlying assets will also be at risk.

Similarly, Australians can keep their savings in an account with an Authorised Deposit-taking Institution (ADI) such as a bank, and know that if their bank card is stolen, the ADI can reverse or otherwise remedy the situation.

This is not at all the case with Bitcoin where possession is really ten-tenths of the law, and where transactions cannot be blocked or reversed.

This is because both ownership and control are entirely a function of maintaining personal possession of the cryptographic keys of the asset.

Each cryptographic private key is derived from a unique string of random binary numbers represented by common English words (usually 12 or 24 words) and there is no limit on the total financial value that this string of words can potentially protect and control.

To be clear, this means that an individual or business could potentially custody their entire life savings or financial reserves within a string of 12 random words, and if this list of words (aka 'seed') is as much as *seen* by a malicious party, the funds can immediately and permanently be stolen without recourse as the inner workings of the protocol do not allow for censorship or reversal.

It is important to note that funds are being transferred by cryptographically signing transactions. Thus, the entity who has knowledge of these confidential words has the power to move them by applying mathematics to this information. In essence, a user's wallet is nothing but a collection of words and math.

Keeping the seed secure from prying eyes as well as from theft, loss, or damage while also keeping the location of it secret is therefore of paramount importance to all bitcoin holders, and is far more of a grave and urgent task relative to the need to keep in confidence other personal financial information, such as which stocks you own, who you bank with, or what your superannuation balance is.

Revealing, inadvertently or not, the cryptographic private keys has devastating real-world consequences.

It is for this reason that the Bitcoin community generally advocates for '*Not your keys, not your bitcoin'* principle. This short phrase is meant to capture the seriousness of secure custodianship practices in the digital asset world.

While it may seem like a good idea to circumvent these risks by encouraging second-party custody of crypto-assets by digital currency exchanges, recent experiences internationally demonstrate that this is not a desirable strategy.

At Bitaroo Pty Ltd, we regularly remind our users that self-custody is an important responsibility. Our users are adults and we believe that they themselves should be responsible for the safe keeping of their assets, instead of trusting us or any other third party.

However, some still choose to trust us and that is within their rights. We strongly believe that this is a right and should not be forced as an obligation.

Our analysis shows that those that chose to hold their bitcoin with us could be divided into 3 main groups: traders; those who wish to sell in the near future; and those that trust us as custodians more than they trust themselves.

As Bitaroo is a custodian of bitcoins that belong to such users, we undertake rigid and costly security practices to safeguard those assets.

Due to the honey pot nature of our service, we consider that using Bitaroo, or any other custodial, as a long-term wallet solution is not best practice as the cryptocurrency industry globally has been affected numerous times by enormous hacks and theft for the entirety of its existence to date, including across North America, Europe, Asia and even New Zealand.

In addition, phishing attacks and similar scams continue to target digital exchanges, businesses and individual bitcoin holders, and these attacks are further enabled by the 'Know Your Customer' (KYC) regulations imposed on various blockchain businesses.

While we have been fortunate in Australia that there have been no known major hacks of Digital Currency Exchanges, there have been 'disappearances' as well as data breaches.

A prime example would be the Exchange ACX, which in January 2019 abruptly stopped allowing withdrawals from its exchange and to this date does not reply to support tickets or enquiries via social media channels. Although even today the exchange appears to be online, its users are unable to retrieve assets held on the exchange. It is suspected that the owners have performed what the Bitcoin Community refers to as an 'exit scam'.

More recently, earlier this month the exchange 'BTC Markets' accidentally leaked their entire database via a bulk email distribution, revealing full names and email addresses of approximately 270,000 KYC verified Australian customers.

For Bitcoiners, the implications of KYC honeypot leaks are more severe than the equivalent risk outside of the cryptocurrency world, but this is not addressed by regulators when they impose KYC requirements.

Once a potential attacker becomes aware that an individual or an email address is associated with a particular cryptocurrency holder, the affected individuals will continue to be (probably for the rest of their lives) more vulnerable to physical attacks, commonly known in the Bitcoin community as '$5 wrench attacks', and/or phishing scams, creating real personal and financial risks.

Even for blockchain businesses that are not digital currency exchanges, harsh lessons are being learned about the consequences of storing Personally Identifiable Information (PII).

This is playing out now in real time for customers of Ledger, a hardware wallet manufacturer, who are continuing to report incidences of their assets being irreversibly stolen due to personalised phishing scams following a PII database hack in June 2020 which affected over *1 million individuals*, exposing over 250,000 physical addresses and phone numbers among which over 11,000 are Australians.

In addition, recent studies have shown that KYC is not only a huge burden on companies (both financially and otherwise), it also does very little to actually stop money laundering and terrorism funding, all while adding identity theft and other risks to law abiding citizens.

Despite the lack of evidence that these regulations are stifling criminal activity, it is evident to us as a business that they do effectively hinder economic activity in the ecosystem.

For example, we notice that many of our users are so concerned about potential identity theft via database leak that they opt out of increasing their AUD deposit limit due to onerous compliance hurdles associated with 'enhanced KYC'. This results in smaller sized purchases than they would have otherwise chosen.

We urge the committee to ensure that Australia sends out a strong beacon of hope to those who value their freedom, their rights and their privacy and ensures that it remains a desired place to live in. Otherwise, we may see an exodus of high value and/or high net worth individuals moving away from here and migrating to other locales that have friendlier regulatory environment that also treasure these important values.

Recommendation #1

Reduce 'Honey Pot' sizes by advocating the paramount importance of self-custody to buyers and investors, by avoiding the imposition of regulations that would deter self-custody and by revisiting the current KYC regime.

Virtual Asset Service Providers (VASPs) worldwide will continue to be targets for hacks and theft of both crypto-assets, and PII of crypto-asset owners. Retaining the ability of individuals to self-custody their digital assets is crucial to minimise the value of assets held by VASPs, and thus reduce the incentives to attack these funds.

To maximally protect individuals from risks associated with 'KYC honeypots' **VASPs should also be able to use external identity verification, and should not be required to store legal names of their customers**.

This has already been proposed to financial institutions more broadly, including in the National Blockchain Roadmap (Use Case #3, KYC information sharing) to prevent the repeat collection and storage of sensitive information. However, the Government has so far failed to act on this aspect of the Roadmap.

—

Regulators lack in depth technological literacy while rushing to act

It is becoming apparent that in many cases, both domestically and abroad, regulators lack understanding of crypto-assets. This lack of understanding, combined with a sense of urgency in wanting to regulate the industry, is a recipe for a tragic loss of potential innovation and growth.

As explained by Jeremy Allaire of US-based fintech company Circle, in an open letter to Secretary Mnuchin (December 2020) [emphasis added]:

"I am aware of the fact that the administration, including Treasury FinCEN, are working towards new rule-making that would effectively attempt to "plug a hole" by significantly constraining how financial intermediaries can interact with public blockchain networks, via so-called unhosted or self-hosted wallets. With all due respect, I believe the proposal would inadequately address the actual risks that are at issue, would significantly harm industry and American competitiveness, would continue to yield economic and industry advantage to Chinese firms, and would have significant unintended consequences around the broader use-cases for this technology. In my view, the kinds of approaches I've heard that are being discussed would be ***taking a sledgehammer to a problem that needs precision tools*** and could materially curtail the much more significant potential for public blockchains to transform many industries."

The full letter can be read at https://www.circle.com/hubfs/AllaireLetterUSTreasurySecretary.pdf

While this is a complaint targeting proposed American laws, it reflects a broader trend globally of the creeping fog of regulation that threatens to stifle innovation in blockchain-based fintech.

Given that the US exports much of its policy to the rest of the world via bodies such as FATF, this trend is highly disturbing.

Our concern is that proposals such as the "STABLE Act" could have far-reaching implications for citizens and businesses to engage in even basic activities such as validating the authenticity of transactions, and could also have spill-over effects for non-blockchain fintech activates such as the ability for firms to offer non-cash payment facilities without a banking charter.

For Australian regulators to be able to appreciate the implications of new regulation, they should engage more closely with industry and not just accept the proposals made in foreign jurisdictions, where the policymakers making new proposals may not necessarily have a better understanding.

Recommendation #2
The agencies that represent Australia in FATF deliberations on digital assets should engage in regular and genuine consultation with the private sector.

Given that regulators generally lack technical competence in this field, it is imperative that policy makers and regulators work far more closely with a diverse cross-section of the industry to prevent unintended harms from arising to individuals, and excess regulatory burdens and ineffective policies from being applied to businesses.

It is important to note that moving to regulate the ecosystem before it has had a chance to fully develop will severely limit the innovation and productivity gains that can be delivered.

—

To our detriment Australia lacks voice in international deliberations on critical regulation

Australia has traditionally prided itself on having strong market integrity while also positioning itself as a global champion of innovation, openness and progress.

Sadly, our government has not been taking a holistic view with respect to Bitcoin and to other blockchain-enabled fintech.

Some regulators have been moving ahead of others, leaving gaps that actually create more risks for individuals and businesses, as in the case of KYC risks already described above.

Another good example would be FinCEN's proposition to FATF in 2019 that the "Travel Rule" compliance threshold be lowered from $3,000 to $250, a significant reduction, requiring all VASPs and banks to undertake additional reporting on transactions, whether using fiat or digital assets.

This places many fintech businesses at a competitive disadvantage to large institutions such as banks due to the higher relative compliance burden that start-ups face.

Further, a policy like this does not take into account the unique circumstances of Australian consumers. Australians are known to bulk buy purchases to save on shipping costs and shipping times, so our international purchases would tend to be higher than the $250 threshold, including on purchases where privacy is important for the reasons outlined earlier (e.g. if importing a couple of hardware wallets to set up a best practice multi-signature bitcoin wallet).

The Prime Minister has said that he wants Australia to be a "brain gain" nation when it comes to Fintech, however our ability to innovate and grow will be significantly affected by the attitudes of regulators domestically as well as the policies we choose to import from overseas.

Recommendation #3
Australia should make its voice heard in global standards-setting bodies such as FATF, positioning itself as a voice in support of open source fintech innovation.

—

Summary of Recommendations

This submission makes three recommendations to remedy the above-described failures and inadequacies of the current regulatory approach to digital assets.

1. **Reduce 'Honey pot' sizes by encouraging self-custodianship of digital assets and by allowing VASPs the use of external identity verification services**, removing the need for each VASP to store the legal names of their customers, as proposed in the National Blockchain Roadmap.

2. **Policy makers and regulators should work far more closely with a diverse cross-section of the industry to prevent unintended harms** from arising to individuals, and excess regulatory burdens and ineffective policies from being applied to businesses. In particular, we request that the agencies that represent Australia in FATF deliberations on digital assets to engage in regular and genuine consultation with the private sector.

3. **As a sovereign nation, Australia should use its voice in global standards-setting bodies such as FATF to defend the benefits of innovation and entrepreneurship**. We should not blindly import regulations that are not effective, that do not have a net benefit, or that will impose undue restrictions on the growth of the sector.

Thank you for your consideration and for the opportunity to voice our concerns.