ASX Submission to the Senate Select Committee on Financial and Regulatory Technology

Opportunities and risks in the digital asset and cryptocurrency sector| 16 July 2021

Department of the Senate
PO Box 6100
Parliament House
Canberra ACT 2600

fintech.sen@aph.gov.au

Dear Committee,

Thank you for the opportunity to respond to the matters raised in the third issues paper. ASX will focus on comments in relation to section the 2(h) of the Issues Paper being the "opportunities and risks in the digital asset and cryptocurrency sector".

ASX has a perspective on this both as an operator of markets and securities settlement facilities, including operating as a central securities depositary, and as a pioneer in the adoption of distributed ledger technology in financial markets. This gives us a view of some of the challenges facing digital assets on public blockchain platforms.

At the same time we see the benefits that technological innovation can bring to financial markets, and the way that innovation in crypto-currency has contributed to the development of distributed ledger technology. In saying that, we would distinguish the technology, which we see as potentially transformative, from specific use cases such as crypto-currencies.

We comment below on some of the risks that we see associated with crypto currencies, with a particular focus on some of the challenges in relation to custody arrangements. However, we emphasise that we do not seek to comment on issues outside our experience or expertise, and so, for example, we do not provide any views on specific technologies, given the broad range of blockchain technology use cases, or on the role of crypto-currencies as a store of value or mechanism for payment.

Digital assets on public markets

ASX is mindful that ASIC is currently consulting on the appropriateness of crypto-assets as underlying assets for exchange-traded products and other investment products, and how product issuers might ensure that these are compliant with Australian financial products and services regulation. ASX will participate in ASIC's consultation and share our thoughts with the Committee at that time.

Custody of digital assets

It is worth considering whether investors understand the risks and benefits of owning digital assets through a custodian or an exchange operating as a custodian.

On major blockchain platforms such as Bitcoin and Ethereum, digital assets are associated with a user through an address. Whoever can access the address is effectively the custodian of the digital assets in that address. The user's address is a mathematical derivation of their private key, which in turn is derived from a random seed. The user must keep their random seed secret to prevent other users from deriving their private key and accessing the address associated with their digital assets. In effect, access to the private key of an address will confer custody of the underlying assets in that address. In that sense, access to the private key can be likened to legal title.

The fact that access to the private key determines access to a user's digital assets raises some risks including, importantly:

- Many users are leaving their digital assets on a crypto exchange, with the private key held by the exchange, leaving the user vulnerable to security breaches on the exchange or to the risk that their assets may be dealt with in an undisclosed or unauthorised manner
- Challenges in the secure storage and management of private keys by crypto exchanges.

In most cases the custodian of the underlying digital assets is the exchange itself, and the user does not have access to their private key unless they choose to transfer their digital assets to an address away from the exchange, and for which they directly manage the private key.

Crypto exchanges can provide a user experience which is attractive to many Australians who wish to invest in crypto assets, including the experience of a password-based login. However, as others have noted, there are risks in these custodial arrangements for digital assets. Many of these risks are associated with the management of private keys. A parallel can be made between management of user passwords and user private keys, however, we note below an important difference.

Crypto exchanges can also be vulnerable to cybersecurity risks, and there have been some prominent examples of this. In this sense they are no different to other businesses that may be subject to this risk, and investors commonly use third parties to hold assets in custody and safekeeping. However it is important that these decisions can be made in the confidence that the custodian is appropriately regulated, well capitalised, carries appropriate insurance, maintains data and operational systems in accordance with industry best practice security standards, and so on.

It is also true to say that users who choose to manage their private keys directly are vulnerable to risks. If using a 'hot wallet', which remains connected to the internet, they open themselves up to some of the security risks faced by cryptocurrency exchanges, but potentially without the benefit of the systems, insurances and so on that may be maintained by a crypto exchange. If using a 'cold wallet', which is kept offline, the user risks physical theft, loss or destruction with limited avenues for recovery other than through law enforcement in appropriate cases.

The risks associated with custody arrangements through crypto exchanges could be a matter for the Committee to consider and recommend measures to address, including in relation to:

- Disclosure requirements in relation to crypto assets, including disclosure of the terms of custodial arrangements (whether through a crypto exchange or otherwise) and the key risks to users
- Core standards and requirements for digital asset custodians, including in relation to capital, technological, operational and governance matters
- Independence assurance requirements for digital asset custodians, in relation to core matters such as legal title to crypto assets left on the exchange.

In saying this, we also note that crypto assets and crypto exchanges are subject to inconsistent, and in some cases minimal, regulation globally. Any measures such as those canvassed above would need to be considered in the context of the broader regulatory framework considered appropriate, in view of the nature and risks associated with these assets and activities.

ASX welcomes the opportunity for continued dialogue with the Senate Select Committee if requested.

Yours sincerely,

Dan Chesterman
Group Executive, Technology and Data and CIO