Blockchain Australia

c/o Hall & Wilcox

L 11 South Tower, Rialto

525 Collins Street, Melbourne VIC 3000

28th February 2023

Senate Standing Committees on Economics

PO Box 6100

Parliament House

Canberra ACT 2600

economics.sen@aph.gov.au

Dear Committee Secretariat,

Thank you for the opportunity to respond to the Senate Economics References Committee Inquiry into international digital platforms operated by Big Tech companies. We are appreciative of the government's efforts in this regard.

In responding to this consultation, Blockchain Australia, on behalf of its members, seeks to ensure that any changes proposed by government support the following objectives:

- Encourages innovation and ongoing investment into blockchain and other emerging technologies
- The regime facilitates the adoption and use of blockchain
- Provide appropriate investor protection

Given the mandate of Blockchain Australia and the makeup of our membership, we have restricted our responses to those questions pertaining to the metaverse, cryptocurrencies and digital assets.

In preparing this submission, the association would like to acknowledge and thank Dr Jane Thomason for her input and articulation of the potential legislative impacts the metaverse brings.

We would welcome the opportunity to meet with the Senate Senate Economics References Committee to discuss any matters in our submission or the broader cryptocurrency evolution.

Please direct any questions you may have to:

Gordon Little

Policy Lead, Blockchain Australia

Policy@blockchainaustralia.org

Or

Amy-Rose Goodey

Head of Operations, Blockchain Australia

Members@blockchainaustralia.org

About Blockchain Australia

Blockchain Australia is the peak industry body representing Australian businesses and business professionals participating in the digital economy through blockchain technology. Blockchain Australia 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
- Art
- Banking
- Building & Construction
- Cyber Security
- Development
- Digital ID
- Education
- 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, employs approximately 11,600 people (Source) and with support from government and natural market growth, these figures could increase to AU$68.4 billion and over 206,000 people employed in the sector. To ensure Australia realises these opportunities, we seek a fit-for-purpose, technology-neutral, regulatory framework with clear guideposts for consumers and a focus on driving innovation and Investment.

Blockchain Australia

CONSULTATION QUESTIONS:

Market Concentration:

Question 1: What impact does the market power of big tech companies have on the economy, society and small businesses?

With Big Tech investing hundreds of billions of dollars in VR and AR products and services, it is reasonable to predict that the metaverse will impact the lives of billions of people within the next decade, driving a global transition from flat media to immersive media as the primary means by which users access digital content. This will greatly impact the public sphere, giving even more control to platform providers than current technologies. With the industry heading in this direction, it's prudent to assess the potential dangers of the metaverse and propose viable regulatory solutions.

Of greatest concern to the members of Blockchain Australia is the ability of these large firms to stifle innovation in Australia by deploying marketing and sales tactics that impact investment into startups in Australia. An example of this is the threats by Apple over a year ago to add a buy now pay later capability to Apple Pay. This has greatly impacted the development of an industry that started in Australia and had potential to grow internationally. Apple has still not gone live, but the threats have had the desired impact.

Our members also have concerns about the increased dependency they have to get their messages out to clients and the ability of the owners of those companies to change charging models for ads or modify their algorithms to negatively impact the reach Australian business can have via these channels.

Question 2: What regulatory measures could be put in place to address the adverse impact of big tech companies? What other non-regulatory interventions could governments take to reduce the market power of big tech companies?

Potential measures could include:

1. Minimum deployments of capital back into the local tech industry to contribute to the growth and development of the domestic technology sector.
2. A requirement for companies to make their infrastructure available to local organisations to build on.
3. Establish a percentage-based requirement for research and development spending in Australia. This could be based on a percentage of sales to Australians or a similar metric to incentivise investment in local talent.

Question 3: Do Big Tech companies have any special dispensations from the rules that govern all other companies? If so, should these be removed, and why?

It is important that a balance be reached in enhancing big tech companies' willingness to deploy capital and build capability in Australia with the need to ensure innovation and small business investment is supported. Tax and R&D rules that favour big tech companies with complex offshore business models need to be reviewed and changed where needed to create a level playing field for local firms.

Blockchain Australia

The Cloud

Question 1: With respect to the cloud, what regulation that currently exists in other countries that could be of benefit to Australia?

Question 2: Should new assessments and oversight protocols for cloud computing products be implemented to bolster security of the cloud? If yes, how should cloud computing products be regulated?

Question 3: Would government regulation increase confidence in cloud services and provide greater clarity on accountability and have an impact on the benefits this technology?

Question 4: What regulatory challenges are associated with the use of cloud services, particularly where data and information is stored in other jurisdictions? How might these regulatory challenges be addressed to ensure that consumers using cloud services are protected?

Question 5: What can be done to promote competition in the cloud space rather than attempt some form of protection in this market?

Blockchain Australia

Algorithm transparency

Question 1: Akin to the Federal Trade Commission in the US, should an oversight body be established in Australia to undertake similar regulatory activities?

Question 2: Are there useful ideas in the proposed US legislation that are applicable in Australia?

Question 3: Similarly, are there other jurisdictions, such as the UK, EU and Japan, that also have applicable concepts that could be usefully incorporated into Australian law?

Blockchain Australia

Data and privacy

Question 1: What benefits would arise from introducing a legal mechanism to allow people to seek compensation for privacy breaches in Australia (e.g. establishment of a statutory tort for serious invasion of privacy)?

Question 2: Would stronger penalties levied by government regulation act as an effective disincentive to prevent data leaks and hacks in the future? What should be the scope and size of any such penalties?

Question 3: Do further changes to privacy laws in Australia need to be made to better protect Australians and change corporate attitudes regarding data collection and management?

Blockchain Australia

Children's safety

Question 1: How effective is the current legislative framework in protecting children and preventing online harm from occurring?

Question 2: What more can be done to enhance online safety for child protection in Australia?

Other organisations and individuals are better placed to advise the government on the specific impacts this technology has to children and potential changes to legislation.

We do, however, have members who are building technology, tools, platforms and services within the blockchain industry that can contribute to the safety of children online. These kinds of tools should be considered for those building frameworks and regulations as minimum requirements for those creating products in the metaverse.

An example of this are authentication and self sovereign ID (SSI) projects that aim to enhance the transparency and auditability of interactions between individuals. With Self Sovereign ID a game company targeting children could verify participants' age against an SSI chain to ensure only children are allowed to interact with one another.

Blockchain Australia

The Metaverse

Question 1: Given the currently ambiguous status of the Metaverse and its development, is it necessary to begin regulating it now, or should authorities wait in order to understand better how it will function?

Regulating the metaverse is a complex issue, as it is a new and evolving technology, and there are currently no established regulations specific to the metaverse. However, it is likely that existing laws and regulations will be applied to the metaverse, such as:

1. Data protection laws: The metaverse will need to comply with data protection laws, such as the General Data Protection Regulation (GDPR) in the EU, and the California Consumer Privacy Act (CCPA) in the US, to protect users' personal and financial information.

Intellectual property laws: The metaverse will need to comply with intellectual property laws to protect the rights of creators and owners of virtual content and assets.

2. Consumer protection laws: The metaverse will need to comply with consumer protection laws to protect users from fraud and other forms of deception.

3. Tax laws: The metaverse will need to comply with tax laws to ensure that virtual transactions are properly taxed.

4. Cybersecurity laws: The metaverse will need to comply with cybersecurity laws to protect users' personal and financial information and prevent unauthorised access.

5. Gambling laws: If the metaverse includes virtual gambling activities, it will need to comply with gambling laws.

6. Copyright law on ownership of rights

7. Intellectual property law on data ownership

8. DeFi, or crypto asset services provided in a “fully decentralised manner without any intermediary.” raises the question of which of the existing DeFi protocols would meet this definition. If they don’t, they may likely be subject to Regulatory requirements. Even for those “fully decentralised” services, the government can begin work on an assessment of the development of DeFi, token mapping and impact of web3, and new layer blockchain protocols and whether the regulatory treatment of these new applications is adequate.

Where Decentralised Finance (DeFi) is integrated in a metaverse, then key regulatory bodies need to agree on definitions and harmonise principles and technical standards for digital assets, including:

- Regulatory Technical Standards
- Supervisory policies and procedures
- Information exchange requirements
- Regulatory and license criteria and guidelines

9. NFTs are outside the scope of regulation. However, the "fractional parts of a unique and non-fungible" token, as well as those tokens issued in a large series or collection, should be considered as an indicator of their fungibility. Clarity on the meaning of the indicator of fungibility is essential. Those NFTs and NFT platforms falling within this definition would then need to comply with financial and non-financial regulatory requirements.

It is likely that as the metaverse develops, new regulations specific to the metaverse will be developed to address any unique challenges and risks associated with this new technology. Regulations for the metaverse are still in an early stage, and may vary depending on the jurisdiction, as different countries have different laws and regulations. Authorities should begin developing a framework for regulation of the Metaverse and keep abreast of what is happening in other jurisdictions.

Our members are also conscious that DOA's offer the ability to address shared ownership and equitable governance issues associated with Big Tech and monopolies organisations. DAOs enable shared ownership and equitable governance, however, the lack of clarity in legal and tax treatment of DAOs, aggressive enforcement actions and emerging global policy environment are each inhibiting the growth of these natural competitors to Big Tech companies. Please refer to the submission from BADAS@L for more information on this.

Question 2: What regulatory frameworks are required both internationally and in individual jurisdictions to address the risks associated with the Metaverse?

We are unaware of any formal regulatory frameworks to address risks associated with the metaverse. However, a number of industry associations are forming with the intention of leading dialogue on regulations, policy and standards. For example:

World Metaverse Council (wmetac.com)

https://metaverse-standards.org/

https://metaverseassociation.co/

https://metaversesafetyweek.org/

Question 3: How would any regulatory frameworks encompassing the Metaverse be enforced?

This will be a difficult challenge due to jurisdictional issues. There will be a need for legislative agreements across borders.

A key component will be intelligence gathering and collaboration with the tech firms involved in developing these experiences. This emphasises the need to build partnerships with Telco companies, which possess the infrastructure through which attacks are perpetrated.

Developers must be included in the security process and need precision training on the vulnerabilities that they are likely to face.

Governments need to start developing approaches to defend against threats now, such as the controls to remove bad actors and user education.

International

Question 1: How can Australia best approach regulating the increasing number of foreign owned tech companies that have established themselves in Australia?

Question 2: How should western democracies approach the data collection activities of companies based in countries whose political systems are more authoritarian and who may demand access to said data?

Question 3: How should Australia and other countries approach regulation of cryptocurrency, including the CBDCs of other countries?

The global nature of businesses operating in the Web3/Crypto space and the ability of customers of those businesses to access the services without going through an Australian regulated business makes regulating these organisations difficult. Regulatory arbitrage opportunities and the ability for unscrupulous actors to interact with Australian consumers avoiding tax and other obligations, is a concern.

To this end, Blockchain Australia is working closely with the government on the token mapping consultation process, which we believe is crucial to determining the regulatory changes required across Tax, Custody and licensing of DCE's and other AFSL holders. It is critical that these consultations and resulting legislative changes continue on the timeline outlined by government.

Blockchain Australia

Big Tech disinformation

Question 1: Is the current regulatory framework governing disinformation and misinformation meeting community expectations and industry? Does it appropriately balance concerns about misinformation with freedom of expression?

Question 2: Should the Australian Code of Practice for Disinformation and Misinformation, which is currently voluntary, be enshrined into the law (as has been done in the EU)?

Question 3: Does the former government's Social Media (Anti-Trolling) Bill 2022 adequately address online safety and, if so, should it be reintroduced to the Parliament?

Question 4: Does the current regime of registering US (and other countries') companies adequately ensure that US Big Tech companies adhere to their corporate responsibilities in Australia?