DIGITAL LAW ASSOCIATION

SUBMISSION

Third Issues Paper (Senate Select Committee on Australia as a Technology and Financial Centre)

July 2021

Disclaimer and Copyright

© The Digital Law Association (DLA)

Contents

ABOUT THIS SUBMISSION

The Digital Law Association is an organisation dedicated to the promotion of a fairer, more inclusive, and democratic voice at the intersection of law and technology.

Our mission is to encourage leadership, innovation, and diversity in the areas of technology and law by:

- bringing together the brightest legal minds in the profession and in academia to collaborate; and
- developing a network that promotes digital law, and particularly female leaders in digital law.

This document was created by the Digital Law Association in consultation with its members. In particular, the compilation of this submission was led by:

- Joni Pirovich
- Natasha Blycha
- Susannah Wilkinson
- Sarah Jacobson

This submission has been contributed to by the following Digital Law Association members:

- Greg Dickason
- Jenny Leung
- Jono Lim
- Kirsten Green
- Louis De Koker
- Louis Zetlin
- Michael Bacina
- Michael Daw
- Ravi Nayyar
- Soraya Pradhan
- Steve Vallas

In addition, the following have endorsed this submission:

- Holley Nethercote Lawyers
- Mycelium
- Piper Alderman

Submission Process

In developing this submission, our members have engaged through email correspondence, regular video calls, and worked in teams to conduct research and prepare briefing papers about the issues dealt with in the third issues paper.

Recommendation #1	*The Australian Government engage an independent body to properly and comprehensively assess the economic benefit of the opportunity within Australia of a digital asset policy framework.*
Recommendation #2	*The Australian Government prioritise and expedite the design and implementation of an Australian digital identity system that incorporates elements of decentralised digital identity (DID), also called self-sovereign identity (SSI[1]), and zero-knowledge proofs (ZKPs[2]) or the use of any other relevant technologies that balance security with individual consent and control (Privacy Enhancing Technologies - PET).*
Recommendation #3	*The introduction of a new authorisation class(es) within the Australian Financial Services licence explicitly designed to cater for digital assets and digital asset businesses as Financial Products & Services, and if required any changes to Pt 7 Corporations Act 2001 (Cth) to facilitate this new authorisation class. In addition, consideration of a Token Safe Harbour SEC style proposal for Australia.*
Recommendation #4	*As an interim measure before a digital asset policy framework is legislated, the Australian Treasury lead the preparation and release of a multi-agency working taxonomy of Digital Assets that sets out the Australian legal and tax implications of digital asset businesses and transactions, with input from multiple Australian regulators.*
Recommendation #5	*The Australian Treasurer instruct the Board of Taxation to undertake a comprehensive review of the federal, state and territory tax systems to recommend amendments required so the tax law does not produce anomalous outcomes to the economic intention of digital transactions, and for recommendations to be made by 1 April 2022.*
Recommendation #6	*The Australian Government consider the design and introduction of an opt-in micro tax for digital transactions that allows a tax amount to be collected from all digital transactions and automatically remitted to the Australian Taxation Office (ATO). Existing corporate tax, individual tax, GST regimes would then switch off.*
Recommendation #7	*The Australian Government consider introducing an opt-in designated service in the AML/CTF Act to capture the exchange of one digital asset for another digital asset, where a condition of opting in is that customer due diligence and KYC procedures are undertaken using PET.*
Recommendation #8	*The Australian Government consider introducing an opt-in designated service in the AML/CTF Act to capture custodial, depositary or agency services that involve the safeguarding of private cryptographic keys on behalf of a person to*

[1] *SSI promotes individual ownership and control of their digital identity.*

[2] *A ZKP is a cryptographic method to prove to a party that you possess some knowledge without actually revealing the underlying information.*

	hold, transfer and deal with digital assets where a condition of opting in is that customer due diligence and KYC procedures are undertaken using PET.
Recommendation #9	*The Australian Government consider introducing an opt-in designated service in the AML/CTF Act to capture selling a hardware wallet to a person, where a condition of opting in is that customer due diligence and KYC procedures are undertaken using PET.*
Recommendation #10	*The Australian Government consider introducing an opt-in designated service in the AML/CTF Act to capture digital asset reward pools, where a condition of opting in is that customer due diligence and KYC procedures are undertaken using PET.*
Recommendation #11	*The Australian Government devise a national ransomware strategy, including mandatory notification to the Australian Federal Police upon a ransomware event occurring, as part of its current Cyber Security Strategy and as a public-private collaboration.*
Recommendation #12	*The Australian Government and the Australian Prudential Regulation Authority (APRA) consider expanding and adapting the scope of CPS-234[3] to address digital asset businesses.[4] This necessitates extending the regulatory scope of APRA[5] to encompass and classify certain digital asset businesses as APRA-regulated entities, and to provide for the creation of tailored information security guidelines. Further, where an APRA-regulated entity's information assets are managed by a third party, measures for communicating and enforcing these standards upon digital asset businesses must be established.*
Recommendation #13	*The Australian Government legislate a requirement for directors and senior executives of digital asset businesses to undertake annual training programmes in organisational cyber resilience that are tailored to their organisational cyber risk profiles and that embody internationally recognised standards in assuring organisational cyber resilience like ISO/IEC 27032, the NIST Cybersecurity Framework and the Essential Eight.* *Digital asset businesses must be required to disclose whether their directors and executives have completed said programmes on their websites.*
Recommendation #14	*The ASD and ACSC, in conjunction with industry, author and institute a set of voluntary guidelines, directed toward improving the cyber resilience of digital asset businesses in relation to the development and use of Decentralized Applications (dApps), centring upon the underlying blockchain technologies dApps are commonly developed to interact with (e.g. smart contracts).[6] The contents of such guidelines should stress the adoption of a security-by-design approach within the development process - focused upon encouraging broad*

[3] *Australian Prudential Regulation Authority, Prudential Standard CPS 234 - Information Security (APRA, 2019) <https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf>.*

[4] *Department of Internal Affairs, 'Virtual Asset Service Providers' on Department of Internal Affairs (November 2019) <https://www.dia.govt.nz/AML-CFT-Virtual-Asset-Service-Providers>.*

[5] *Kate Marshall and Carl Buhariwala, ' CPS 234: the intersection of information security and data privacy' on KPMG (12 June 2019) <https://docs.google.com/document/d/1-L7mHQl9ciL8fi2gzeFqzJyBGQd6DizoTgbD4KxJd74/edit>.*

[6] Nikita Savchenko, 'Decentralized Applications Architecture: Back End, Security and Design Patterns' on freeCodeCamp (2 April 2019) <https://www.freecodecamp.org/news/how-to-design-a-secure-backend-for-your-decentralized-application-9541b5d8bddb/>.

	adherence with recognised information security standards, and advancing due diligence measures.[7]
Recommendation #15	*The Australian Government establish mechanisms, to be led by ASD and ACSC, for the real-time sharing of threat intelligence between Commonwealth agencies and digital asset businesses that serve Australian customers, whether or not they have a physical presence or other facilities in Australia. These mechanisms should be led by ASD and ACSC. The specific form of said mechanisms should be explored by the Committee in partnership with ASD, ACSC, the Department of Home Affairs and the Parliamentary Joint Committee on Intelligence and Security.*
Recommendation #16	*The Committee consider and make recommendations on how regulators and supervisors can best ensure that banks undertake appropriate and comprehensive risk assessments in relation to individual customers, before an account opening application or banking services is denied based on AML/CTF risk, and how information about risk management expectations of banks can best be conveyed to current and prospective customers.*
Recommendation #17	*The Australian Government introduce a new type of legal entity in the Corporations Act 2001 - DAO Limited, informed by, but not a wholesale adoption of the COALA DAO Model Law.*
Recommendation #18	*ASIC update Regulatory Guide 172 to provide guidance about the licensing regime and regulatory obligations for DAO-run financial markets like Uniswap.*

[7] Andre Kudra, 'Smart Contract Security – Expect and Deal with Attacks' on dotmagazine (July 2018) <https://www.dotmagazine.online/issues/blockchain-e-government/blockchain-security/smart-contract-security-expect-and-deal-with-attacks>.

1 Regulation of Cryptocurrencies and Digital Assets

1.1. Valuing the economic benefit of the opportunity within Australia of a digital asset policy framework

Recommendation #1

The Australian Government engage an independent body to properly and comprehensively assess the economic benefit of the opportunity within Australia of a digital asset policy framework.

Intended outcomes

- A comprehensive and robust valuation of the economic benefits of a digital asset policy framework would assist government and policy-making departments in understanding and prioritising policy-making resources to the areas that will derive most economic benefit for Australia.

Reasons

Our preliminary research shows that digital asset policy -- in either or both of new and amended legislation -- should be made in the following areas, in order of priority of potential economic benefits:

Asset Class	Global Opportunity
Stablecoins and financial services based on stablecoins / central bank digital currencies	Opportunity at least $2 trillion USD, based on 10% of the existing financial industry's size.
Digital assets generally	Centralised exchanges alone process $1.1 trillion USD per annum of digital asset transactions, plus other markets are evolving for customer due diligence and custodianship.
Blockchain based security tokens (natively digital assets)	Small current market at $700 million but projected to reach $8 trillion USD by 2025.
Tokenised real world assets (tangible and intangible)	Small existing market but with real estate value in the Australian market alone, already over $8 trillion AUD, has potential to grow rapidly
Non-fungible tokens	NFT market is $2 billion in Q1 2021. A much larger opportunity exists to enable the programmatic and atomic transfer of real world assets.

Our fuller research is available at Appendix A. Industry bodies and industry members have volunteered an enormous amount of time and effort over the last 5 years to assist government and policy-makers. However, the lack of a single, consolidated and comprehensive assessment has meant government and policy-makers have not had an accessible resource from which to understand and prioritise policies in this area. Such an important and severely overdue assessment should be funded by the Australian Government and undertaken by an independent body.

1.2. Digital identity

Recommendation #2

The Australian Government prioritise and expedite the design and implementation of an Australian digital identity system that incorporates elements of decentralised digital identity (DID), also called self-sovereign identity (SSI[8]), and zero-knowledge proofs (ZKPs[9]) or the use of any other relevant technologies that balance security with individual consent and control (Privacy Enhancing Technologies - PET).

Intended outcomes

- Australia will be a leading technology and financial centre in its design and implementation of a digital identity system that incorporates SSI, ZKPs and/or other PET.
- Australia's digital identity system will be 'fit for the digital economy', 'private by design' and provide a reliable and independent source of electronic data for AML/CTF purposes, where personal information is not received, stored and managed by multiple parties and is shared with read only access on a permissioned basis.
- Australia's digital identity system would propel the attractiveness of Australia as a centre from which to launch and operate technology and financial businesses.
- Australian commercial banks will be strategically positioned to adapt their service offering to 'digital identity and data custodian and consent management services', where Australian commercial banks performing this service would have cyber security standards and practices expected of national critical infrastructure providers and to protect against stolen or fraudulent digital identities. If Australians initially choose an Australian commercial bank to assist with their digital identity and consent management, high cyber security requirements will contribute to a broader national culture of cyber resilience.
- Contextualised and practical scrutiny of the Australian Consumer Data Right regime as a temporary measure until an Australian digital identity system that includes SSI, ZKPs and/or other PET is implemented.

Reasons

Digital identity will be the most important digital asset in the digital economy.

Digital identity should not repeat or inherit the mistakes of our legacy (centralised) identity systems because SSI and ZKPs and other PET have introduced a paradigm shift to traditional trade offs that needed to be made between privacy and transparency. The recently released proposed legislation by the Digital Transformation

[8] *SSI promotes individual ownership and control of their digital identity.*

[9] *A ZKP is a cryptographic method to prove to a party that you possess some knowledge without actually revealing the underlying information.*

Agency does not clearly address decentralised identity (or SSI) or ZKPs, and in its current form will leave Australia lagging behind.

We strongly recommend that the design of Australia's digital identity system take reference from latest research on SSI and ZKPs, including Pieter Pauwels' paper "zkKYC: A solution concept for KYC without knowing your customer, leveraging self-sovereign identity and zero-knowledge proofs" (July 2021).

1.3. Suggested changes to existing laws/implementation of new laws

Recommendation #3

The introduction of a new authorisation class(es) within the Australian Financial Services licence explicitly designed to cater for digital assets and digital asset businesses as financial products and services, and if required any changes to Pt 7 Corporations Act 2001 (Cth) to facilitate this new authorisation class. In addition, consideration of a Token Safe Harbour SEC style proposal for Australia.

Intended outcomes

- Signal clarity and certainty from regulators to anyone who would like to do business involving digital assets in Australia.
- Meet s760A Corporations Act objectives including for confident and informed decision making by consumers of Financial Products and Services, while promoting efficiency, flexibility and innovation in the provision of those products and services.

Reasons

Our member legal practitioners are reporting an increasingly frustrated cohort of otherwise law-abiding digital asset client businesses unwilling to become embroiled in regulatory test cases, but crying out for clear direction and legal processes.

Notwithstanding that ASIC has issued Information Sheet Info 225 which makes clear that digital assets are not exempt from regulatory oversight and will be subject to regulatory action if non-compliant, it is currently unclear how to practically license and register digital asset products and services. This is because increasingly complex, new and creative methods of economic interaction, from fractionalised fundraising to yield farming, or from tethering and stable coins to wrapped non-fungible tokens (NFT), are yet to be successfully reconciled neatly to the traditional regulatory process and in particular the current Financial Product & Service classes of security, managed investment scheme, derivative or non-cash payment scheme.

The flow on effects arising from the introduction by ASIC of a bespoke digital asset friendly classification category for financial products and services, would be greater certainty for those requiring market licences that need to extend to cover digital asset financial products and services, as well as positive impacts on both traditional stock exchanges and digital exchanges, where there is considerable uncertainty as to the regulatory implications of listing tokens or platform providers that are not licensed.

If Recommendation #3 or something similar to it is not instituted within the next 12 months, a "safe harbour" provision similar to that currently being discussed in the US by the SEC may need to also be instituted in Australia given the increasing number of digital asset financial products & services that are currently not being regulated or prosecuted for lack of clear regulation. In addition, practical issues such as the lack of availability of insurance or licenced digital asset custody providers will need to be considered and accounted for so that compliance with such a license is not rendered impossible. This could be achieved by, for example making clear that custody of digital assets may be provided by existing licensed custodians.

Recommendation #4

> ***As an interim measure before a digital asset policy framework is legislated, the Australian Treasury lead the preparation and release of a multi-agency working taxonomy of Digital Assets that sets out the Australian legal and tax implications of digital asset businesses and transactions, with input from multiple Australian regulators.***

We begin with a number of caveats in developing any useful taxonomy. These include:

(a) The most useful taxonomy of Digital Assets will be one that is developed *after* the development of new and clear authorisation classes for Digital Asset Financial Products (see #Recommendation 3 above). This is a key and pivotal step that will have waterfall implications across the digital landscape.

We should not mistake what are currently commonly issued token features, (or combinations of features) to be demonstrative of the types of tokens business would like to deal in. Rather they are very often demonstrative of development undertaken to avoid regulatory oversight (e.g attempts to stay within the feature setlist often identified as a "Utility Token"). If regulatory oversight was simplified and ASIC could provide clear categories of acceptable licensed behavior, we anticipate that token businesses would evolve their products to meet those authorisation class requirements.

(b) Tokens can change characterisation over time. The analysis of whether a digital asset is offered or sold for example as a security is not static.

(c) There is a great deal of overlap between classification classes. Modifying a token's function (even in a small way) may move a Digital Asset from one classification category into another classification category, and/or dictate that it straddles more than one category.

(d) How a token should be classified and therefore regulated, is also a product of the relationship that token has with other digital assets, or its milieu of operation. For example an NFT in isolation is its own class set out below, if however it is wrapped or tethered to a security token, that will likely change the nature of the NFT such that it also should be a regulated token.

If a taxonomy of digital assets is required now without changes as per the above caveats, the following classification schema is useful. We do not recommend the use of this list as a long term solution, as we anticipate many of these categories will collapse for regulatory purposes.

(e) Cryptocurrency (other terms include payment tokens, exchange tokens), which is natively digital and can be used like money but can be held as a speculative asset.

(f) Crypto(graphic)-assets (other terms include virtual assets, digital assets), which may be natively digital or tokenised representations of real money or property. Categories include:

(i) Utility tokens, which represent a right to access goods, services or information and may be 'closed loop' (i.e. only exchangeable within its own network) or without restrictions, and can be held as a speculative asset.

(ii) Tokenised securities, where the equity, debt or property is registered with the traditional legal system and the interest exists in parallel as a 'tokenised' asset.

(iii) Security tokens, which are natively digital assets and where the features, rights or obligations of the token mean the token is classified as a security or other financial product (examples could include governance tokens, liquidity provider tokens and certain non-fungible tokens).

(iv) Stablecoins, which may be fiat-, crypto- algorithmic- or hybrid-collateralised.

(v) Non-fungible tokens, which may represent the original or licenced literary and artistic works of an author or authors or the unique contractual terms between parties.

(vi) Sovereign digital currencies, including central bank digital currencies and government-issued or government-mandated cryptocurrencies.

(vii) Privacy coins, which may display one or more features of the categories of digital assets above but also conceal the sender and/or recipient details to a digital asset transaction.

(viii) Credentials, including digital identity and verifiable credentials.

(ix) Vaults, including curated data vaults and tokenised data.

(x) Smart legal contracts, legal documents that are machine readable and include natural language and coded instructions.

(xi) Multi-characteristic tokens, which include features from one or more categories of digital assets above and where there may be multiple concurrent intentions and uses of the token.

(xii) Multi-tiered token economies, whereby the second tier token is only accessible by holding a first tier token.

Intended outcomes

- Signal clarity and certainty from regulators to Australians and Australian businesses to operate with the benefit guidance whilst a policy is being formulated.
- A working document to allow for ease of updating to reflect the fast pace of developments in emerging technology.
- Develop a common language and understanding to facilitate discussions among and between business and government.
- Make a clear distinction between the digital asset and the information required to access and deal with the digital asset (i.e. the private keys).

Reasons

There is no globally agreed taxonomy or set of definitions for digital assets and this creates confusion for policy-makers, regulators, investors and consumers. A multi-agency working taxonomy of Digital Assets will allow for prompt guidance from regulators, attraction of business and investment to Australia, and clear delineation of what matters require involvement from policy-makers.

1.4. Tax

Recommendation #5

The Australian Treasurer instruct the Board of Taxation to undertake a comprehensive review of the federal, state and territory tax systems to recommend amendments required so the tax law does not produce anomalous outcomes to the economic intention of digital transactions, and for recommendations to be made by 1 April 2022.

Intended outcomes

- Australian tax system that is fit for purpose in a digital and decentralised economy, which does not disincentivise digital asset business models which will include fractional security and fractional real property interests -- and the trading of those interests -- in the near future.
- Update ESVCLP[10], CSEF[11], AMIT[12] regimes to clearly include digital asset businesses.

Reasons

Australia's tax settings are outdated, are not fit for purpose in the digital and decentralised economy and are not technology neutral. The current Australian tax settings do not make Australia an attractive jurisdiction to launch, undertake or participate in digital asset businesses. The ATO is not sufficiently resourced to produce timely guidance that deals with the complexities of digital asset transactions, particularly DeFi transactions.

Since early 2019, multiple tax recommendations have been made to the Treasury and the Senate Select Committee in relation to the tax issues of issuing, holding and transacting with digital assets but the issues and recommendations have not progressed to legislative amendments at a cost to the attractiveness of Australia as a place for digital asset business activity. These tax issues and recommendations can be found in the following submissions (which do not reflect the tax issues related to DeFi which have become apparent since January 2021):

- Submission to Treasury's consultation on initial coin offerings, dated 1 March 2019, available at: https://treasury.gov.au/sites/default/files/2019-07/attachment_-_hw_submission_-_treasu.pdf
- Submission to Second Issues Paper, dated 14 December 2020, available at: https://www.millsoakley.com.au/wp-content/uploads/2020/12/Mills-Oakley-submission-to-2nd-Issues-Paper-SSC-on-FinTech-RegTech-14-Dec-2020-.pdf.

[10] Early Stage Venture Capital Limited Partnership

[11] Crowd-sourced Equity Funding

[12] Attribution Managed Investment Trust

Recommendation #6

The Australian Government consider the design and introduction of an opt-in micro tax for digital transactions that allows a tax amount to be collected from all digital transactions and automatically remitted to the Australian Taxation Office (ATO). Existing corporate tax, individual tax, GST regimes would then switch off.

Intended outcomes

- Signal tax certainty and simplicity to global markets to attract founders working on digital business models to Australia, as well as investment capital.
- Learn from and transition to a tax model fit for the digitalised and decentralised global economy.
- Certainty of tax revenue collection and amount of tax paid by taxpayers.
- ATO compliance efforts become proactive to ensure micro-tax is implemented correctly into technology design, rather than reactive identification of non-compliance which is costly and time consuming to enforce.

Reasons

As countries move to connect digital identity with digital money, digital micro-taxing will become a necessary mechanism to collect taxes effectively, efficiently and fairly in a digital economy.

Australia's tax settings are neither competitive nor simple to administer. In addition, international tax settings are struggling to keep pace with the digital economy and digital and decentralised business models. The work being undertaken as part of the OECD's BEPS Action 1 (Addressing the Tax Challenges of the Digital Economy) project is ongoing, is highly political and does not deal with a number of taxation issues that arise because of the digitalisation and decentralisation of business models.

1.5. AML/CTF

Recommendation #7

The Australian Government consider introducing an opt-in designated service in the AML/CTF Act to capture the exchange of one digital asset for another digital asset, where a condition of opting in is that customer due diligence and KYC procedures are undertaken using PET.

Intended outcomes

- The blockchain and digital asset industry is still maturing therefore opt-in regulation or self-regulation should be encouraged to support the protection of consumers and investors while encouraging innovation.
- Regardless of the regulatory classification, decentralised exchanges (**DEXs**) and other dApps that permit trading or exchange of digital assets and operate autonomously through self-executing smart contracts could opt-in to AML/CTF obligations that are appropriate and adapted for the pace, scale, decentralised and autonomous nature of their operation.
- Smart contract standards that handle the zkKYC obligations and report directly to the regulator should be developed by industry in close consultation with regulators like AUSTRAC and regularly reviewed by AUSTRAC to ensure the smart contracts are working appropriately. DeFi services that are no longer operated by an entity or individual(s) should be dealt with in this way because the entity or individual(s) no longer have control or admin keys to the smart contracts or have ceased to maintain or operate the DEX or dApp.
- Where there is an operator or person involved in the oversight of the DEX, this measure could capture peer-to-peer, non-custodial, DeFi services where an entity or individual(s) is providing an ongoing service of facilitating digital asset to digital asset transactions and where that entity or individual has actual control over the digital asset exchange.

Reasons

Some of our members noted that regulating digital asset to digital asset exchanges and transactions would bring Australia in line with other jurisdictions such as the U.S. and one step closer to FATF's Recommendations and thatthis would reduce the effect of regulatory arbitrage which is an unavoidable consequence of decentralized and distributed technologies. Following on from a period of self-regulation, we note that this issue and approach may need to be revisited.

Most consumers, investors and businesses might understandably think that digital assets are unregulated due to the lack of enforcement action taken by ASIC and AUSTRAC against issuers of digital assets that are characterised as securities or other financial products or where customer due diligence and KYC procedures have not been undertaken. Providing an opt-in regulatory regime for digital asset to digital asset exchanges and transactions would bring Australia a step closer to FATF's

Recommendations and reduce the effect of regulatory arbitrage, while allowing the industry to mature in its understanding of risks, risk mitigation and best practices.

Per the Pauwels paper referred to above, "With no central party in full control of a DeFi service, the set of smart contracts of a DAO could perform the role of Verifier… The zkKYC [zero-knowledge KYC] concept could also facilitate undercollateralised or even uncollateralised lending, given the DAO could verify a zero-knowledge proof of a credit score from a trusted Issuer."

Recommendation #8

> ***The Australian Government consider introducing an opt-in designated service in the AML/CTF Act to capture custodial, depositary or agency services that involve the safeguarding of private cryptographic keys on behalf of a person to hold, transfer and deal with digital assets where a condition of opting in is that customer due diligence and KYC procedures are undertaken using PET.***

Intended outcomes

- The blockchain and digital asset industry is still maturing therefore opt-in regulation or self-regulation should be encouraged to support the protection of consumers and investors at the same time as encouraging innovation.
- Clear recognition of the lack of possessability of digital assets and that the service being provided involves the safeguarding of private keys that allow for the control, access and dealing with digital assets.
- Regardless of regulatory classification, custodial, depositary or agency service providers could be subject to AML/CTF obligations that are appropriate and adapted for digital assets.

Reasons

Digital currency custodians can be a significant source of systemic risk, are not subject to the Financial Claims Scheme, and are notoriously difficult and expensive to insure. The consequences of a cyber-attack, money laundering and employee fraud can be quite significant given the large values that are typically custodied at digital currency custodians around the world and the irreversible nature of such transactions.

Because of their role in the storage and movement of digital currencies, digital currency custodians are in a position to collect, request, and store valuable information. In other words, they represent a point in the digital currency ecosystem that could provide significant visibility of the ecosystem for governments as well as high "honeypot" risk for cyber-attacks. For this reason, privacy enhancing technologies such as zkKYC are extremely important before bringing digital currency custodians into the AML/CTF regime.

Providing an opt-in regulatory regime for digital asset custodians would bring Australia in line with other jurisdictions such as the E.U. and one step closer to FATF's

Recommendations, while allowing the industry to mature in its understanding of risks, risk mitigation and best practices.

Recommendation #9

> ***The Australian Government consider introducing an opt-in designated service in the AML/CTF Act to capture selling a hardware wallet to a person, where a condition of opting in is that customer due diligence and KYC procedures are undertaken using PET.***

Intended outcomes

- The blockchain and digital asset industry is still maturing therefore opt-in regulation or self-regulation should be encouraged (including involving industry group level accreditation) to support the protection of consumers and investors at the same time as encouraging innovation.
- Provide AUSTRAC with greater visibility within digital asset ecosystems.
- Through interagency data sharing arrangements, AUSTRAC can provide the ATO with information about taxpayers that have purchased hardware wallets to facilitate the ATO's collection of information when assessing whether all income and gains have been reported by taxpayers.

Reasons

Since issuing an open-loop stored value cards to a person is a designated service under item 21 of table 1 at section 6(2) of the AML/CTF Act, and hardware wallets mimic open-loop SVCs in the way they enable users to transfer value internationally, the Australian government should consider providing an opt-in regulatory regime for the sale of hardware wallets.

Recommendation #10

The Australian Government consider introducing an opt-in designated service in the AML/CTF Act to capture digital asset reward pools, where a condition of opting in is that customer due diligence and KYC procedures are undertaken using PET. The amendments may involve the following:

insert the proposed definitions at section 5:

> ***'digital asset reward recipient' means a person who receives digital assets as a reward or consideration for performing a specific activity or activities required to validate digital asset transactions in accordance with a software protocol.***
>
> ***'digital asset reward recipient pool' means a network operated by a person or persons (the relevant operator or relevant operators) and where the network:***
>
> ***(a) is comprised of digital asset reward recipients that have organised themselves into that network (the organised recipients), such as (but not exclusively) by each organised recipient entering relations (contractual or otherwise) with the relevant operator or relevant operators; and***
>
> ***(b) exists for the dominant purpose of bringing together the computational and / or digital asset resources of the organised recipients in order to increase the likelihood of, collectively, the organised recipients receiving digital assets as a reward or consideration for performing a specific activity or activities required to validate digital asset transactions in accordance with a software protocol; and,***
>
> ***(c) where the relevant operator or relevant operators may distribute the digital assets received to one or more of the organised recipients and their associates.***

insert proposed item 50D into table 1 of section 6(2), so that the provision of a designated service is stated as:

> ***'if registered with AUSTRAC, operating a digital asset reward recipient pool where the relevant operator or relevant operators provide digital asset rewards to one or more organised recipients',***

where the customer of the proposed designated service is the 'organised recipient' or 'organised recipients' that may receive digital asset rewards.

The providers of this designated service should be required to:

- ***conduct CDD under part 2 of the AML/CTF Act;***
- ***keep records of their CDD procedures under part 10 division 3 of the AML/CTF Act, including the address or addresses the digital asset rewards will be or have been sent to; and***

- ***report suspicious matters under section 41 of the AML/CTF Act.***

Intended outcomes

- The blockchain and digital asset industry is still maturing therefore opt-in regulation or self-regulation should be encouraged to support the protection of consumers and investors at the same time as encouraging innovation.
- Provide AUSTRAC with greater visibility within digital asset ecosystems and enable AUSTRAC to identify P2P digital currency transactions when the relevant units of digital assets were distributed among members of mining or staking pools.
- Further consideration is required with industry as to whether all digital asset reward recipients should be required to at least register with AUSTRAC.

Reasons

In order to properly risk assess, identify and prosecute criminal and other suspicious activity, governments need greater understanding and visibility into how digital assets are created and distributed through consensus mechanisms like Proof of Work and Proof of Stake as well as tokenomics models that have other means of creating and distributing new digital assets.

Given the global reach of digital asset mining, active cooperation and information sharing between industry, governments and agencies is critical before a unified approach can be legislated in AML/CTF legislation.

Recommendation #11

The Australian Government devise a national ransomware strategy, including mandatory notification to the Australian Federal Police upon a ransomware event occurring, as part of its current Cyber Security Strategy and as a public-private collaboration.

Intended outcomes

- Raise awareness and education in digital asset businesses, whether or not they provide designated services under the AML/CTF Act, about the risks of digital assets being abused by criminals and terrorists and risk-mitigation strategies.
- Establish and reinforce existing frameworks for Commonwealth agencies and the digital asset sector to share intelligence concerning money laundering which involves digital assets and ransomware.
- Close collaboration and information sharing between the Australian digital asset sector, law enforcement and the National Intelligence Community to prosecute cyber and other national security risks stemming from ransomware.

Reasons

The role of the digital asset sector in the fight against the ransomware threat arises because the ransoms demanded by attackers can be denominated in digital assets.[13]

[13] European Union Agency for Law Enforcement Cooperation, *Internet Organised Crime Threat Assessment 2020* (Report, 5 October 2020) 17.

By necessity, the sector must be part of the counter-ransomware policy response.[14] As part of the ransomware strategy, businesses, especially blockchain forensics providers, should educate government and agencies on how they can better identify and prosecute financial crime risk in digital asset ecosystems in order to counter the ransomware threat. NIC agencies like AUSTRAC — given its role as Australia's Financial Intelligence Unit and the coordinator of the Fintel Alliance —[15] must take the lead on such campaigns and build relationships with the digital asset sector. This would be synchronous with the nature of AML/CTF regulation as a public-private partnership, as enshrined in AML/CTF Act.

1.6. Comparable/leading jurisdictions and elements which could be leveraged from in Australia

We have prepared a table of legislation, key definitions used within the legislation, and commentary with respect to the legislation from jurisdictions leading the way with blockchain and digital asset policy, or jurisdictions that are comparable with Australia but more advanced than Australia in their blockchain and digital asset policy.

The table is provided at Appendix B.

1.7. Cyber-resilience

Recommendation #12

The Australian Government and the Australian Prudential Regulation Authority (APRA) consider expanding and adapting the scope of CPS-234[16] to address digital asset businesses.[17] This necessitates extending the regulatory scope of APRA[18] to encompass and classify certain digital asset businesses as APRA-regulated entities, and to provide for the creation of tailored information security guidelines. Further, where an APRA-regulated entity's information assets are managed by a third party, measures for communicating and enforcing these standards upon digital asset businesses must be established.

Intended outcomes

- APRA leads a dialogue between digital asset businesses and relevant government agencies - especially the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) - in improving board-level awareness of emergent cyber threats, and undertake adaptive measures concerning the information

---

[14] *Combating Ransomware* (n) 14.

[15] 'Fintel Alliance', *AUSTRAC* (Web Page, 11 May 2021) [1] <https://www.austrac.gov.au/about-us/fintel-alliance>; 'Intelligence', *AUSTRAC* (Web Page, 3 September 2020) [1] <https://www.austrac.gov.au/about-us/intelligence>.

[16] *Australian Prudential Regulation Authority, Prudential Standard CPS 234 - Information Security (APRA, 2019) <https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf>.*

[17] *Department of Internal Affairs, 'Virtual Asset Service Providers' on Department of Internal Affairs (November 2019) <https://www.dia.govt.nz/AML-CFT-Virtual-Asset-Service-Providers>.*

[18] *Kate Marshall and Carl Buhariwala, ' CPS 234: the intersection of information security and data privacy' on KPMG (12 June 2019) <https://docs.google.com/document/d/1-L7mHQl9ciL8fi2gzeFqzJyBGQd6DizoTgbD4KxJd74/edit>.*

security role and responsibilities within digital asset businesses. This requires mandating an information security capability commensurate with the size and extent of threats to a digital asset business's information assets, implementing information security controls to protect information assets, and the timely issuing of notifications to APRA concerning material cyber security incidents.

- Improved adoption and compliance rates with CPS-234 standard among digital asset businesses will elevate organisational resilience vi-a-vis information security incidents, and the maintenance of an information security capability by digital asset businesses which is commensurate with information security vulnerabilities and evolving cyber threats.[19]

- The formulation of collaborative measures between government and digital asset businesses to address the growing threat of emergent cyber threats to Australia's banking, lending, payments, insurance and superannuation industries, arising from the continuing absence of defined and targeted information security guidelines for digital asset businesses. This will contribute to the safety and soundness of financial institutions and digital asset businesses, and promote community confidence in their ability to meet financial commitments under all reasonable circumstances.

- Encouragement of digital asset businesses to undertake proactive measures to prohibit malicious practices surrounding digital goods and services, to improve the reporting of significant cyber incidents to relevant authorities, and in reducing the liability and threat of legal action against compliant digital asset businesses.

- The establishment of tailored and interoperable information security standards concerning digital asset cyber security for APRA-regulated entities and digital asset businesses - extending APRA's supervision and influence to the broader ecosystem of associated third-party suppliers and providers.

Reasons

APRA's supervisory authority, outlined across several legislative instruments,[20] encompasses approximately 680 financial entities. Consequently, the developing intersection between these entities and digital asset businesses necessitates the broader application of CPS-234 in establishing an information security benchmark, and safeguarding Australia's financial system amid the increasing incidence of material cyber incidents targeting Australia's critical infrastructure. Financial institutions remain a key target for malicious actors, with the finance sector being the second largest source for data breaches.

Consequently, with a growing number of Australians investing in digital assets, this elicits concerns surrounding organizational information security guidelines existing

---

[19] ***Abi Tyas Tunggal, 'How to Comply with CPS 234' on Upguard (16 June 2021) <https://www.upguard.com/blog/cps-234-compliance>.***

[20] *Banking Act 1959; Insurance Act 1973; Life Insurance 1995; Private Health Insurance (Prudential Supervision) Act 2015; and Superannuation Industry (Supervision) Act 1993.*

across digital asset exchanges, startups, and projects.[21] The requirement for regulated entities and digital asset businesses alike to demonstrate basic cyber-hygiene, and for such requirements to extend to associated third parties, is crucial in minimising the likelihood and impact of incidents on confidentiality, integrity or availability of information and information systems.[22]

Recommendation #13

The Australian Government legislate a requirement for directors and senior executives of digital asset businesses to undertake annual training programmes in organisational cyber resilience that are tailored to their organisational cyber risk profiles and that embody internationally recognised standards in assuring organisational cyber resilience like ISO/IEC 27032, the NIST Cybersecurity Framework and the Essential Eight.

Digital asset businesses must be required to disclose whether their directors and executives have completed said programmes on their websites.

Intended outcomes

- Fluency of directors and senior executives in 'cyber resilience'.
- Digital asset businesses better able to interrogate their organisations' management of cyber risk, including by asking proper questions of lower-level executives responsible for implementing organisational strategies and developing products and services about the cyber risks.[23]
- Promotes 'a strong "cultural" focus [on cyber resilience] driven by the board and reflected in organisation-wide programs for staff awareness, education and random testing, including of third parties'.[24]
- Competitive advantage for the Australian DASP sector, given the greater regulatory focus worldwide on user privacy,[25] the growth in cybercrime (targeting DASPs)[26] and wider acknowledgement of the importance of assuring cyber resilience during the current pandemic.[27]

Reasons

As above, lax cyber resilience of digital asset businesses and poor fluency among management thereof can be a source of reputational risk for them and undermine the

---

[21] *Aleks Vickovich, 'Four million Aussies set to buy into crypto' on Australian Financial Review (8 June 2021) https://www.afr.com/companies/financial-services/four-million-aussies-set-to-buy-into-crypto-20210608-p57z2g.*

[22] *Michale Caplan and Mark Furgeson, 'CPS 234: 8 things you didn't know about APRA's new cybersecurity standard' on Lexology (25 June 2019) <https://www.lexology.com/library/detail.aspx?g=75990000-3101-4499-8c9c-4b778bf2a267>.*

[23] Ibid.

[24] Ibid [21].

[25] Gartner, 'Gartner Says by 2023, 65% of the World's Population Will Have Its Personal Data Covered under Modern Privacy Regulations' (Press Release, 14 September 2020).

[26] European Union Agency for Law Enforcement Cooperation, *Internet Organised Crime Threat Assessment 2020* (Report, 5 October 2020) 17 ('*IOCTA 2020*').

[27] OECD, *Dealing with Digital Security Risk during the Coronavirus (COVID-19) Crisis* (Paper, 3 April 2020).

competitiveness of the Australian digital asset sector as a whole. Suboptimal cyber resilience will undermine 'the size and scope of the opportunity for Australian consumers and business from Australia growing into a stronger technology and finance centre' and thus the achievement of one of the missions of the Committee.[28]

Furthermore, suboptimal cyber resilience encourages a serious category of operational risk for Australian digital asset businesses because of their business models' dependence on the security of interconnected computer networks not least because the digital assets they handle are native to cyberspace.[29]

Recommendation #14

> ***The ASD and ACSC, in conjunction with industry, author and institute a set of voluntary guidelines, directed toward improving the cyber resilience of digital asset businesses in relation to the development and use of Decentralized Applications (dApps), centring upon the underlying blockchain technologies dApps are commonly developed to interact with (e.g. smart contracts).[30] The contents of such guidelines should stress the adoption of a security-by-design approach within the development process - focused upon encouraging broad adherence with recognised information security standards, and advancing due diligence measures.[31]***

Intended outcomes

- The imposition of a security-by-design approach will enable organizations to automate data security controls and formalize the design of infrastructure, thereby enabling integrating security into its IT management processes. This will help digital asset businesses and dApp designers anticipate and prevent the occurrence of material cyber incidents, summarise and apportion responsibilities for security controls, and automate security baselines based upon reliably coded security and governance.

- The integration of a security-by-design approach will be founded upon advancing broad adoption of internationally recognized information security standards by digital asset businesses, including ISO/IEC-27000 and NIST information security standards.[32] This provides a common and established baseline from which digital asset businesses may increase the reliability and security of dApps systems and information, and the effect of which will improve customer and business partner confidence and spur the wider utilization of dApps for commercial benefit.[33]

---

[28] 'Select Committee on Australia as a Technology and Financial Centre', *Parliament of Australia* (Web Page, 18 March 2021) [3] <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology>.

[29] See eg Marco Iansiti and Karim R. Lakhani, 'The Truth About Blockchain: It Will Take Years to Transform Business, but the Journey Begins Now', *Harvard Business Review* (Article, 15 January 2017) [43] <https://hbr.org/2017/01/the-truth-about-blockchain>; Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press, 2018) 18, 20; *Report 429* (n) 18.

[30] Nikita Savchenko, 'Decentralized Applications Architecture: Back End, Security and Design Patterns' on freeCodeCamp (2 April 2019) <https://www.freecodecamp.org/news/how-to-design-a-secure-backend-for-your-decentralized-application-9541b5d8bddb/>.

[31] Andre Kudra, 'Smart Contract Security – Expect and Deal with Attacks' on dotmagazine (July 2018) <https://www.dotmagazine.online/issues/blockchain-e-government/blockchain-security/smart-contract-security-expect-and-deal-with-attacks>.

[32] ISO, 'ISO/IEC 27000:2018' on ISO (2021) <https://www.iso.org/standard/73906.html>.

[33] Manar Abu Talib et al., 'Guide to ISO 27001: UAE Case Study' (2012) 7 *Issues in Informing Science and Information Technology 335.*.

- Emphasis upon due diligence concerns the need for comprehensive analysis in the design of dApps, including analysis of the dApp technology stack and careful review of source code.[34] This is necessary in cultivating a security-oriented culture/mindset within digital asset businesses, helping determine the most suitable blockchain(s) for a dApp, and in minimizing the presence of vulnerabilities by encouraging responsible and secure coding practices.

Reasons

dApps are digital applications or programs that operate from logic written into a smart contract, and therefore require careful design and thorough testing to ensure persistent and continuing intended functionality.[35] A security-by-design guideline and process for dApps provides a preferable preventative path for digital asset businesses and dApps designers to improve their cyber resilience.

Factors driving the development and implementation of dApps by digital asset businesses include the zero downtime enabled by a decentralized network, privacy where Personally identifiable information (PII) is not required in deploying or interacting with a dApp, resistance to censorship, data integrity, and trustless computation.[36] This underscores the commercial potential for dApps across the digital asset market, gaming industry, advertising space, transportation sector, and financial industry.[37]

As digital asset businesses and associated third parties move to embrace the use of dApps, it is critical to have appropriate monitoring and data leak prevention controls to ensure that sensitive information and PII are not at risk if digital identity and privacy enhancing technologies are not yet available or legislated.

Recommendation #15

The Australian Government establish mechanisms, to be led by ASD and ACSC, for the real-time sharing of threat intelligence between Commonwealth agencies and digital asset businesses that serve Australian customers, whether or not they have a physical presence or other facilities in Australia. These mechanisms should be led by ASD and ACSC. The specific form of said mechanisms should be explored by the Committee in partnership with ASD, ACSC, the Department of Home Affairs and the Parliamentary Joint Committee on Intelligence and Security.

Intended outcomes

- Commonwealth and the digital asset sector to gain a stronger understanding of the nature of the threat landscape.

- A better, more targeted response by the Australian government to malicious cyber activity targeting Australian networks, including ransomware attacks involving

---

[34] Kudra, above n27.

[35] Ryan Grunest, 'Introduction to dapps' on Ethereum (12 June 2021) <https://ethereum.org/en/developers/docs/dapps/>.

[36] Valid Network, 'Decentralized Applications: The good, the bad, and why should enterprises care?' on Valid Network (19 August 2020) <https://valid.network/post/decentralized-applications-the-good-the-bad-and-why-should-enterprises-care>.

[37] Lucas Mearian, '10 top distributed apps (dApps) for blockchain' on ComputerWorld (30 December 2019) <https://www.computerworld.com/article/3510457/10-top-distributed-apps-dapps-for-blockchain.html>.

digital assets.

- The specific form of threat intelligence sharing mechanisms should be explored by the Committee in partnership with ASD, ACSC, the Department of Home Affairs and the Parliamentary Joint Committee on Intelligence and Security.

Reasons

The formation of public-private partnerships to fight cyber risk is best practice in the counter-cybercrime policy context.[38] Such partnerships are integral to Australia's Cyber Security Strategy, which is built on the joint role of the Commonwealth, private sector and civil society in tackling cyber risk.[39] In this regard, threat intelligence sharing is one of the planks of the Strategy.[40]

[38] See eg Institute for Security and Technology, *Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force* (Report, 30 April 2021) 24, 68 ('*Combating Ransomware*'); *IOCTA* (n) 7.

[39] Commonwealth, *Australia's Cyber Security Strategy 2020* (Report, 6 August 2020) 8, 18 ('*Strategy*').

[40] Ibid 6.

2 Issues relating to 'debanking' of Australian FinTechs

Recommendation #16

The Committee consider and make recommendations on how regulators and supervisors can best ensure that banks undertake appropriate and comprehensive risk assessments in relation to individual customers, before an account opening application or banking services is denied based on AML/CTF risk, and how information about risk management expectations of banks can best be conveyed to current and prospective customers.

Intended outcomes

- Promote a broader perspective on bank risk management practices informing de-banking and supervisory practices to ensure that the risk management processes are reasonable, fair and comply with international standards to assess the risks posed by individual customers.
- Consider the relevance of the solution proposed by the Australian Competition and Consumer Commission for International Money Transfers (IMTs) in *Foreign Currency Conversion Services Inquiry - Final Report* (2019) in relation to the de-banking of IMTs and progress with the solution to date.

Reasons

Australian banks are very reluctant to provide services to Australian FinTechs in the blockchain and digital asset space. Large banks have adopted policy decisions not to have such businesses as customers, and smaller banks and financial institutions have followed suit.

These policies are presented as positions taken after an assessment of money laundering, terrorist financing and proliferation financing risk posed by the sector. There is however no convincing evidence that appropriate risk assessments were undertaken as required by international standards adopted by the Australian government.

The FATF is the global inter-governmental body that sets international regulatory and supervisory standards of money laundering, terrorist financing and proliferation financing risk. Australia is a member of FATF and the Australian government is committed to ensure that Australian laws and practices meet the FATF standards. These standards require banks to perform risk assessments, but they have also warned consistently, after de-banking practices became evident, that:[41]

> *"Regulators and supervisors should also ensure that financial institutions are taking a risk-based approach to implementing AML/CTF measures, without prejudice to rules-based measures such as targeted financial sanctions.*

[41] FATF, 'FATF Takes Action to Tackle De-Risking' Statement, Paris, 23 October 2015.

> *Implementation by financial institutions should be aimed at managing (not avoiding) risks.*
>
> ***What is not in line with the FATF standards is the wholesale cutting loose of entire countries and classes of customer, without taking into account, seriously and comprehensively, their level of money laundering and terrorist financing risk and applicable risk mitigation measures for those countries and for customers within a particular sector**." (own emphasis)*

The experience of smaller FinTechs in Australia is that Australian banks do not comply with these standards. They generally refer to standing policy decisions that banks will not engage with businesses involved in cryptocurrency. Individual risk assessments may be undertaken in relation to large FinTechs but in the majority of cases FinTechs are not even given an opportunity to provide information about their business model and risk control measures. The refusal to consider the risk and risk control information of an individual applicant does not meet the international standards of a serious and comprehensive risk assessment that should precede a decision to refuse an application for a bank account. The result is that businesses who genuinely wish to comply with bank requirements have found their accounts frozen or have been asked to bank elsewhere.

The Australian Competition and Consumer Commission investigated de-banking of non-bank providers of International Money Transfers (IMTs) in Foreign currency conversion services inquiry - final report. The report acknowledged competition concerns relating to de-banking of competitors:[42]

> *"From a commercial perspective, there can be little incentive for a bank to supply banking services to an IMT supplier who is possibly going to win IMT business from that bank. HiFX alludes to this in its submission: …. a residual risk to larger non-bank providers that banks look to secure a larger % [share] of the overall market by making it harder for, or refusing to provide services to, non-bank providers."*

[42] Australian Competition and Consumer Commission, Foreign Currency Conversion Services Inquiry - Final Report (2019) 11. In 2017 Louis de Koker, Supriya Singh and Jonathan Capal, 'Closure of Bank Accounts of Remittance Service Providers: Global Challenges and Community Perspectives in Australia' (2017) 36(1) University of Queensland Law Journal 119 investigated de-banking of Horn of Africa remitters in Melbourne. As solutions, they authors suggested collaborative public-private management of public policy risks; recognising the legal right to access the payment services of a bank; and regulatory and supervisory reform in relation to remittance service providers to ensure broader and more balanced regulation of non-AML/CFT aspects of the remittance industry too.

3 Instances of corporate law holding back investments

Recommendation #17

The Australian Government introduce a new type of legal entity in the Corporations Act 2001 - DAO Limited, informed by, but not a wholesale adoption of the COALA DAO Model Law.

Intended outcomes

Generate responsible DAO development in Australia, with responsible models of decentralised governance.

Reasons

DAOs will increasingly feature as a business model in the digital and decentralised economy and must be given legal recognition, the clear ability to hold property and contract, as well as limited liability. We note the submission provided by Mycelium, which sets out key features of the COALA DAO Model Law and the increasing prevalence and importance of DAOs.

Recommendation #18

ASIC update Regulatory Guide 172 to provide guidance about the licensing regime and regulatory obligations for DAO-run financial markets like Uniswap.

Intended outcomes

- DeFi market protocols that observe and uphold security and integrity of financial market infrastructure that supports transparency, price discovery, etc.
- ASIC should prepare the update in close consultation with industry. In this regard, we note the submission by Paul Derham of Holley Nethercote Lawyers that calls for the assembly of the right people to work with government and regulators.

Reasons

RG 172 is not appropriate nor adapted for DAO-run financial markets and should be updated as soon as possible for ASIC to meet its obligations in ensuring financial market stability and protection against systemic risks. The longer that DeFi continues without any or adequate oversight by the financial market regulator and the greater the amount of value locked and transacted in DeFi the greater the potential systemic risks to the Australian financial market.

FIND US AT

@digitallawassociation

@DigitalLawAssoc

@digitallawassociation

@DigitalLawAssoc

CONTACT US

info@digitallawassociation.com