KordaMentha

Token mapping

Response to Treasury consultation paper

March 2023

kordamentha.com

Contents

Introduction to KordaMentha

Introduction

KordaMentha welcomes the opportunity to provide this submission on Treasury's consultation on Token Mapping ('Consultation Paper') and assist in helping to shape the Australian regulatory landscape for crypto assets.

KordaMentha is an independent and trusted firm providing specialist expertise across forensic accounting, restructuring, cybersecurity, financial crime, performance improvement and real estate services. Our team of almost 400 specialists extends across Asia-Pacific and has experience ranging from finance and real estate to law enforcement and the c-suite.

Since 2002, our experts have been entrusted with some of the region's most complex and sensitive commercial situations. We work together to solve the challenges facing corporations, financiers, lawyers, private investors and government clients.

Through our experience restructuring high-profile crypto asset exchanges, commonly known as Digital Currency Exchanges ('DCEs'), such as FTX (50,000 customers) and Digital Surge (30,000 customers) in Australia and Zipmex in Singapore (250,000 customers), we have developed insights into the breadth of challenges facing crypto asset businesses and the regulatory challenges facing the broader industry.

The views provided in this submission are made on a general basis and limited to the Consultation Paper's token mapping exercise. As a technological and politically neutral firm, we support the development of regulation which offers clear guidance for business, enhanced consumer safeguards and opportunity for continued innovation and growth within the crypto asset industry.

We welcome continued collaboration with the Treasury as it progresses in the development of robust and effective regulatory policy for this continually evolving technology.

We have provided responses to a select number of questions asked in the Consultation Paper, which are set out below.

Background

Part A

Q1 – What do you think the role of Government should be in the regulation of the crypto ecosystem?

The role of Government should not be dissimilar to the role played in the traditional financial systems that currently exist today: promoting the integrity of financial markets, domestically and internationally, and ensuring that they achieve societal outcomes consistent with expectations held by all Australians.

Blockchain technology, financial disintermediation and decentralised financial systems offer unprecedented opportunity for innovation across global financial systems. Equally, unprecedented challenges are also emerging with respect to ensuring that appropriate and effective regulation, oversight and community protections are maintained. As such, there is scope for significant involvement by Government in the regulation of the crypto ecosystem. Given the current governance, risk and transparency issues across some areas of the crypto ecosystem, Government plays a critical role managing the competing interests of the free market, public interest, national security, competitive neutrality and financial services innovation.

Additionally, given the cross-border nature of the crypto ecosystem, Australia's alignment with existing international strategy and regulatory approaches will be essential for the purposes of interoperability, cross-border financial transactions and to ensure the crypto ecosystem at a global level can operate with integrity, trust and availability.

Government should seek to balance innovation, job creation and technological change with fairness, integrity and community protections when considering its approach to regulating crypto assets. If the right balance is achieved, a unique opportunity exists for Australia to become a global leader in a range of blockchain technologies.

Q2 – What are your views on potential safeguards for consumers and investors?

The ability to implement effective safeguards, regulatory requirements or similar protective measures for crypto assets is inherently challenging due to the significant degree of disintermediation and decentralisation within permissionless blockchain networks. In other words, decentralised finance and the borderless nature of many token offerings make implementing safeguards more challenging compared to traditional products.

Traditional protections are predicated on the ability of the Australian legal system to require individuals who offer products through a company structure to act in accordance with the law. However, when there are no individuals clearly identifiable (such as in the case of Decentralised Autonomous Organisations ('DAOs') or other types of code-based protocols), applying safeguards becomes difficult.

Enforcing broad prohibitions or restrictions at a network level can, therefore, be largely ineffective in dealing with illegal actors or services due to disintermediation of these networks. Accordingly, there will continue to be a level of risk of scams, fraud and similar schemes being present in these ecosystems and facing consumers or investors.

Despite the challenges brought about by decentralised activity, there are still numerous ways for Australian regulators to influence network activity by leveraging various levers aimed towards disincentivising or otherwise helping to limit the exposure of consumers to illegal activities or bad actors.

> **...there are still numerous ways for Australian regulators to influence network activity, ... disincentivising or otherwise helping to limit the exposure of consumers to illegal activities or bad actors.**

Centralised DCEs should be the first place for the Government to focus its attention, given these entities impact a far greater number of consumers than DAOs or other code-based protocols.

For the purposes of this consultation response, we have set out a broad view as to the potential solutions available for implementing or developing safeguards below. Once a regulatory pathway is selected by Government, further detailed consultation should be sought to develop specific polices for implementation.

We have provided five key areas for consideration in developing and implementing safeguards for consumers and investors.

01: Education

We have engaged with a wide variety of customers and creditors whilst conducting the restructure of Australian and Singaporean cryptocurrency exchanges through the Voluntary Administration process. From these interactions, it is clear that many customers do not understand the fundamental principles of interacting with a DCE. We have experienced significant customer confusion regarding concepts such as custody and the implications on customers in an insolvency scenario. Terms and conditions are often not read by customers of DCEs, which is in part due to their length and complexity and in part because DCEs can be opaque on key issues such as custody and control.

Educating consumers about the risks of investing in crypto assets and the various ways consumers can interact with centralised exchanges or centralised finance protocols should be an important element in safeguarding consumers and investors.

The development of educational resources, analyses, case studies or similar material could assist consumers in gaining a greater understanding of the broader risks, limitations and challenges facing crypto assets as well as specific risks relating to certain products, providers and/or schemes.

02: Licensing framework of crypto asset exchanges and other intermediaries

Globally, specific regulatory frameworks for crypto assets remain in early stages of development with policy initiatives being considered across leading international economies, such as the United States, United Kingdom, Middle East and Europe. The development of robust policy and regulatory frameworks will provide broader protections for those engaged in the crypto asset sector or part of the broader community.

As noted in the Final Report by the Senate Select Committee on Australia as a Technology Financial Centre, released in October 2021, the establishment of a market licencing regime for DCEs in Australia is a priority and critical to ensuring the future success the crypto asset industry.

The following considerations should be included as part of broader policy development and in respect of developing consumer safeguards:

- Requirements for the disclosure of crypto asset custody arrangements.
- Mandatory requirements for maintaining asset or capital reserves and reporting.
- Standardised token due diligence requirements or procedures for popular tokens.
- Standardised guidelines for operational risk management practices.

Treasury may also consider the utility of licensing regimes for crypto asset intermediaries (i.e., non-exchange entities) which set out a clear framework for compliance under a differential reporting regime, in a manner similar to the European Union's Market in Crypto Assets ('MiCA') regulation.

Our response to Question 7 provides further suggestions on the regulation of DCEs.

03: Safe harbour and sandboxing

The safe harbour concept has been proposed and supported by several industry participants[1] to serve as a transparent and risk-weighted approach to enabling operation of crypto asset businesses with reduced compliance concerns.

The safe harbour initiative is broadly specific regulatory environments (or subsets) which offer eligible businesses reduced compliance requirements or immunity to regulatory enforcement measures. The safe harbour initiative is designed to promote flexibility, innovation and growth where certain eligibility requirements and conditions apply.

04: Industry standards

Industry associations or self-regulatory organisations could develop standards for projects, developers or token issuers and other intermediaries offering crypto asset products to follow, such as best practice guidelines and procedures.

Government funding to industry bodies could bolster the ability of industry organisations to develop greater regulatory approaches or codes of conduct for its members, similar to the way the Australian Restructuring Insolvency and Turnaround Association ('ARITA') requires its members adhere to the ARITA Code of Professional Practice.

05: Market-driven solutions

Deteriorating asset prices, declining consumer sentiment and recent large insolvency cases have prompted strong demand from consumers for greater transparency and assurance across the crypto asset sector.

As a result, many crypto asset service providers, including DCEs, have turned to unique market-driven solutions to satisfy consumer needs, differentiate service or product offerings and strive to develop competitive advantage within the sector. Some of the most prevalent market-driven solutions include smart contract auditing and security assessment, token economics (or 'tokenomics') reviews, protocol audits, due diligence and security reviews and similar third-party independent verification or assurance solutions.

It is encouraging to see that many industry participants have taken their own initiative to self-regulate and develop better practices. We expect this will continue regardless of any additional regulation developed by the Government.

Ultimately, the development of any regulatory approach within the above categories may ultimately comprise a combination of optional, mandatory, or an otherwise mixed or differential compliance regime.

Given the unique characteristics of many tokens, protocols and service offerings, we discourage the Government from taking a 'one size fits all' approach to regulation.

1 Refer to Blockchain Australia proposal dated 13 June 2022. Available at https://treasury.gov.au/sites/default/files/2022-12/c2022-259046-blockchain_australia.pdf.

Q3 – Scams can be difficult for some consumers to identify.

a) Are there solutions (e.g., disclosure, code auditing or other requirements) that could be applied to safeguard consumers that choose to use crypto assets?

Yes – please refer to our response at Item 2 and additional commentary below.

In a regulatory sense, there are significant limitations to completely safeguarding consumers against losses due to scams, fraud or similar misconduct due primarily to the decentralised nature of permissionless networks, as set out in our response to Item 2 and identified in the Consultation Paper. With greater education, consumers should be able to better discern between platforms that are 'unprotected' compared to those that adopt any regulation implemented by the Government in the coming months.

Despite the limitations present at a network level, the more centralised or intermediated aspects of permissionless networks can be leveraged for regulatory purposes and provide an opportunity for safeguards to be developed. These centralised aspects are comprised primarily of institutions, DCEs or similar service providers which offer payment settlement, trading, exchange or other crypto asset products and services.

> Despite the limitations present at a network level, the more centralised or intermediated aspects of permissionless networks can be leveraged for regulatory purposes and provide an opportunity for safeguards to be developed.

As detailed in our response at Item 2, there are various solutions available to regulators in developing greater consumer protections and safeguards. These solutions may vary in levels of compliance requirements, and solutions available may be subject to differential compliance or reporting regimes based on the extent of centralised or intermediated risk exposure and/or level of public interest.

We also note the emergence of market-driven solutions to consumer safeguarding concerns being developed within the industry by businesses seeking to increase reporting standards, transparency and trust, including:

- Smart contract auditing and security assessment.
- Token economics (or 'tokenomics') reviews.
- Protocol audits.
- Due diligence and security reviews.
- Similar third-party independent verification or assurance solutions.

b) What policy or regulatory levers could be used to ensure crypto token exchanges do not offer scam tokens or more broadly, prevent consumers from being exposed to scams involving crypto assets?

Please refer to our response at Item 2 and additional commentary below.

In our experience, some customers of DCEs have limited knowledge of the crypto assets they hold. DCEs could be required to provide information on each token offered in the form of a detailed fact sheet to enable customers to make better informed decisions.

This information could be issued by the Government in consultation with industry bodies and experts, with the same information being available across all Australian DCEs. Whilst there are thousands of tokens available, information could be provided for the most popular tokens, noting the top 20 tokens represent approximately 87% of crypto assets' total market capitalisation. The information should be in the same format for each token and identify areas of risks, where appropriate.

To the extent that sufficient information is not available, DCEs could be required to provide warnings to consumers prior to purchasing certain crypto assets.

We note that the provision of additional information will not prevent scams. However, it may highlight the risks involved with specific tokens to allow consumers to make better informed decisions before purchasing tokens.

Token mapping: terminology and concepts

Part B

Q4 – The concept of 'exclusive use or control' of public data is a key distinguishing feature between crypto tokens/crypto networks and other data records.

a) How do you think the concepts could be used in a general definition of crypto token and crypto network for the purposes of future legislation?

It is challenging to attempt to define an ecosystem that, by its very nature, exists to challenge traditional/existing financial/other ecosystems. Currently, crypto assets with clear financial functions lack the robust governance and risk management frameworks required by traditional financial institutions and vehicles.

Given the decentralised and international nature of crypto tokens and crypto networks, any legislative framework, and associated definitions domestically, should leverage and align with definitions agreed by Australia's strategic partners, including the G20 and other international jurisdictions already progressing legislation in this space. This will reduce resulting regulatory arbitrage/burden.

> **...any legislative framework, and associated definitions domestically, should leverage and align with definitions agreed by Australia's strategic partners, including the G20 and other international jurisdictions already progressing legislation in this space.**

Under the international Financial Action Taskforce ('FATF') Standards, Australia's AML/CTF regulator (AUSTRAC) currently regulate DCEs, and any broadening of the regulatory regime should align with this approach[2].

2 Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (fatf-gafi.org)

Q5 – This paper sets out some reasons for why a bespoke 'crypto asset' taxonomy may have minimal regulatory value.

b) What are your views on the creation of a standalone regulatory framework that relies on a bespoke taxonomy?

KordaMentha has considered and agrees with the views set out in the Consultation Paper that an exhaustive, bespoke taxonomy may not be the best option. Doing so may lead to regulatory inefficiencies and uncertainty in the market. The existing framework could apply where the service falls within the definition of a financial product. Where that is the case, there is value in the Government providing further clarity in addition to the Australian Securities and Investment Commission's Information Sheet 225.

If products or services do not fit within the existing framework (for example, some decentralised finance protocols), then Government could respond with an alternative arrangement.

The Government, in consultation with industry, could consider the development of a taxonomy for more popular tokens (for example, the top 20-50 by market cap) to provide regulatory clarity for Australian consumers. This would include a determination on whether a popular token is regarded by the Government as a financial product, or otherwise. However, this approach should be measured and considered on a case-by-case basis.

> "The Government, in consultation with industry, could consider the development of a taxonomy for more popular tokens (for example, the top 20-50 by market cap) to provide regulatory clarity for Australian consumers."

Working with industry partners, the Government could prepare a document on popular tokens, providing information on the token in a standardised form, including if the Government views the token as a financial product. This information sheet could be provided to DCEs and consumers could be required to acknowledge they have read the information sheet before purchasing the product.

Intermediated token systems

Part C

Q7 – It can be difficult to identify the arrangements that constitute an intermediated token system.

a) Should crypto asset service providers be required to ensure their users are able to access information that allows them to identify arrangements underpinning crypto tokens? How might this be achieved?

Yes, users of any crypto product or service should be given sufficient information about the product they are engaging with.

The challenge facing the Government is the vast array of providers that are accessible to Australian consumers, which may never be captured within an Australian regulatory framework. For example, it is difficult to see how the Government could restrict an Australian-domiciled customer from staking their crypto assets to an overseas platform that has no Australian subsidiary. Therefore, the Government should focus on ensuring that Australian entities are encouraged to provide sufficient levels of information to users. In particular, the Government should focus on products offered by AUSTRAC registered DCEs, given these are the most widely accessible on-ramps to purchase crypto assets.

Further clarity is needed over what protocols are deemed as financial products and what are not. KordaMentha is not in a position to recommend which products should be defined as financial products. However, for those protocols determined to be financial products in the coming months, the requirement for an AFSL (including product disclosure statements) will provide sufficient information to users. Some providers may cease to offer products if they are unable to obtain an AFSL.

For products not determined to be financial products, the Government could consider introducing short form product disclosure statements that provide sufficient information to users without the additional and costly regulatory compliance that comes with an AFSL. The requirement to provide such appropriate documentation could be made a condition of DCEs maintaining their AUSTRAC registration, for example.

b) What are some other initiatives that crypto asset service providers could take to promote good consumer outcomes?

Many crypto asset service providers have adopted clear and transparent approaches to promote good consumer outcomes. Others appear to be intentionally vague or make it difficult for consumers to understand key elements of how the service provider works.

As noted in Item 7a, the Government should focus on improving the conduct of AUSTRAC registered DCEs.

From our experience in the turnaround and restructure of DCEs in Australia and Singapore, good consumer outcomes would be aided by DCEs being required to disclose key information relevant to the commercial and legal arrangements underpinning their offering, including:

- Clear descriptions on private key/custody policies and procedures – plainly, and not buried in the terms and conditions.
- Private key/asset custody arrangements.
- Details of asset ownership and use rights (for example, who holds legal title and ownership of assets).
- Conditions, procedures and guidelines for insolvency events.
- For global DCEs, clarity on where assets are held (i.e. if they are held offshore) and the jurisdictional implications this brings.
- Publishing proof of reserves, or otherwise clearly describing how customer funds are being used.
- Publishing details on liabilities alongside proof of reserves. It is no use showing proof of reserves if a lender has first-ranking security over reserves in an insolvency scenario.
- External audits of reserves by firms that have the necessary technological capability to provide appropriate assurance.
- Clear guidance around the conversion of fiat currency to stablecoins and transparency on reserves used to back stablecoins.
- Details of any insurance policies for custody or loss events.
- For derivative products, clear details regarding hedging requirements and policies (as required under an AFSL) and regularly published statements showing net tangible asset positions.
- Conducting internal cybersecurity audits and gaining recognised cybersecurity certification and accreditation.
- Engaging independent financial assurance and audit experts (separate from proof of reserve audits).
- Providing detailed information on governance and risk management policies and procedures.
- Providing educational assets and material to promote customer understanding.
- Conducting due diligence on product offerings.

> **"... good consumer outcomes would be aided by DCEs being required to disclose key information relevant to the commercial and legal arrangements underpinning their offering..."**

Public token systems

Part D

Q14 – Some smart contract applications assist users to connect to automated market makers (AMM).

a) What are the key differences in risk between using an AMM and using the services of a crypto asset exchange?

There are significant differences between AMMs and typical DCEs spanning across technical design, functionality, perceived risk, degree of decentralisation and liquidity. The extent of any difference between the platforms can vary immensely, but typically differ in large part due to the trading mechanisms and procedures implemented.

AMMs are typically entirely decentralised (i.e., peer-to-peer) protocols which utilise mathematical algorithms based on liquidity to determine asset pricing at any given time. Users engaging with AMMs typically trade directly with the protocol but gain access to the protocol assets through liquidity providers. Accordingly, typical differentiators for AMMs are the increased level of disintermediation between users and liquidity providers, transparency in the AMMs design and trading algorithms and a perceived lesser extent of counterparty risk in comparison to DCEs.

In contrast, traders engaging with centralised exchanges typically rely on the exchange to fulfill orders through central order books or asset reserves. In addition, DCEs typically also offer greater variability in products, services and trading tools which may otherwise not be available in AMMs.

In most instances, transactions with DCEs operate in a centralised manner and result ordinarily in a higher degree of exposure to counterparty risk when compared to decentralised AMMs. This is typically driven by a range of factors which may be present and vary in any given scenario, such as custody arrangements, central treasury functions, asset reserves, liquidity, transparency and various additional factors.

It should be noted that the majority of insolvencies in Australia and around the world have been centralised DCEs, whereas AMMs have largely performed according to their underlying smart contracts.

> The extent of any difference between the platforms can vary immensely, but typically differ in large part due to the trading mechanisms and procedures implemented.

Conclusion

Conclusion

We appreciate Treasury providing the opportunity for industry participants to provide input to the development of regulation for crypto assets.

KordaMentha looks forward to participating in Treasury's next Consultation Paper proposing a licensing and custody framework for crypto asset service providers, due for submissions in mid-2023.

Key contributing authors

Brian Wood
Partner
Brisbane

Paul Hewson
Director
Sydney

Grace Mason
Executive Director
Sydney

Tony Vizza
Executive Director
Sydney

Mitchell Grimmond
Senior Executive Analyst
Brisbane

KordaMentha

Contact us

Brisbane
+61 7 3338 0222

Jakarta
+62 21 3972 7000

Melbourne
+61 3 8623 3333

Perth
+61 8 9220 9333

Singapore
+65 6593 9333

Sydney
+61 2 8257 3000

Townsville
+61 7 4724 9888

For more information visit
kordamentha.com