Response: Token Mapping Consultation Paper

15th March 2023

—

Australian DeFi Association

Overview

The Director, Crypto Policy Unit - Financial System Division

The Treasury

Langton Crescent, PARKES, ACT 2600

By email only: crypto@treasury.gov.au

Dear Director,

The Australian DeFi Association, a not-for-profit community focused on education and awareness of blockchain technology, is pleased to submit our response to the token mapping consultation. Our submission reflects a mix of thoughts and opinions from our members and community leaders who are actively involved in the development and growth of the DeFi ecosystem in Australia.

As a community, we are passionate about the potential of blockchain technology to disrupt traditional finance (and other industries) and create new opportunities for individuals and businesses. We believe that the development of a clear and effective regulatory framework is crucial to the continued growth and success of decentralised ecosystems and how they are evolving and integrating with traditional methods of commerce.

In our response to the consultation, we provide the thoughts and feedback from our community to these questions and share where the community responses were similar as well as where they differed (including, in particular, in relation to matters such as token classification, consumer protection, and regulatory sandboxes). We believe that our insights and expertise can help inform the development of a regulatory framework that balances the aspirations for technological innovation with the need for investor protection.

We thank the Treasury for the opportunity to provide our input and look forward to continuing to work with the Government and other stakeholders to promote the development of a thriving DeFi and web3 ecosystem in Australia.

Kind regards,

Australian DeFi Association

Part One - About Australian DeFi Association

The Australian DeFi Association (Aus DeFi) is a non-profit community organisation dedicated to increasing education and awareness of blockchain technology, specifically decentralised finance (DeFi) and web3-based projects. Our mission is to empower the Australian community with the knowledge and tools to participate in the decentralised economy and to promote the adoption and growth of blockchain technology in Australia.

While our name suggests a focus on DeFi, we cover a range of topics related to web3, including non-fungible tokens (NFTs), soulbound tokens, decentralised autonomous organisations (DAOs), and more. We were founded to provide a more grassroots approach to promoting blockchain technology compared to other industry-focused organisations in Australia, and have hosted a variety of events, including general community meetups providing education and updates as well as technical meetups with the likes of StarkWare and Chainalysis.

We are committed to building an inclusive and diverse community that is open to all who want to learn about web3. We have hosted events such as Women in Web3 and Female Leaders in Web3 to promote gender diversity in the industry, as well as an Indigenous NFT event called Canvas to Token. We are also supporting upcoming International Women's Day events around Australia.

Through our monthly meetups and events, we aim to educate and inform the Australian community about the benefits of blockchain technology and how it can be used to explore alternative business models and increase accessibility. We also aim to upskill local businesses and entrepreneurs to meet the needs of a more innovative economy.

As an organisation, we have built a strong following on various social media platforms, including Twitter, LinkedIn, Discord, and Meetup. Our organisation is supported by NotCentralised, a venture studio with the same founders, which builds within the Ethereum ecosystem and advocates for blockchain technology in its work.

Overall, we believe that promoting the adoption of blockchain technology is essential for driving innovation and creating new opportunities for growth and development in Australia. We are committed to being a leading voice in the blockchain industry and to advocating for a regulatory environment that fosters innovation and growth.

Responses to Token Mapping Questions

Question 1. What do you think the role of the Government should be in the regulation of the crypto ecosystem?

Across the variety of responses we received, there is a general consensus that the Government should aim to strike a balance between ensuring a proportionate, principles-based regulatory framework and fostering innovation, while also providing clarity and guidelines for the operation of crypto businesses. Some suggest that the Government should focus on regulating behaviour rather than technology, while others argue that the Government should be adaptive and take a leadership role in harmonising regulations with international partners. Additionally, reducing compliance costs and lowering the cost of remittances are mentioned as important considerations for maximising economic and consumer benefit.

Some of the common themes included

- **Balancing regulation with innovation**: There is a general consensus that the Government should strike a balance between regulation and innovation to avoid stifling the potential of the crypto ecosystem.
- **Providing clarity and guidelines**: The Government should provide clear guidelines and standards for the operation of crypto businesses, including licensing, disclosures, and KYC/AML requirements. Providing clarity and guidance can foster competition and innovation in the crypto ecosystem. A principles based approach is suggested by some respondents.
- **Reducing compliance costs**: Compliance costs can be prohibitively high for small businesses and startups, which can deter new entrants and potentially result in a lack of competition and higher prices for consumers. Therefore, the Government should explore options to reduce compliance costs and encourage new entrants to compete with established players.
- **International harmonisation**: The Government should take a leadership role with international partners to harmonise regulations, reduce costs for consumers, and potentially lower the cost of capital through international liquidity pooling for securities.
- **Focusing on behaviour rather than technology**: Some responses suggest that the Government's role should be to regulate behaviour rather than technology. They argue that the Government should focus on regulating businesses, activities, and behaviours, rather than the software used.
- **Providing sandboxes**: Providing regulatory sandboxes can allow companies to develop new innovations in collaboration with the Government, enabling regulation to evolve in lock-step.

- **Addressing evolving risks and trends**: The Government should monitor the crypto ecosystem to address evolving risks and trends while minimising compliance costs and maximising economic and consumer benefits. Some of these evolving trends include what is happening in the Decentralised Autonomous Organisation (DAO) space and open source communities.

Question 2. What are your views on potential safeguards for consumers and investors?

Across the range of responses we received, there were some common themes to this question and these include the following:

- **Education**: There is a general consensus that education is important in protecting consumers and investors from potential risks and scams in the crypto industry. This includes financial literacy, cybersecurity awareness, and awareness of the potential benefits and risks of crypto investments.
- **Regulation**: There is a range of opinions on the level of regulation needed to protect consumers and investors, with some suggesting a light-touch approach and others advocating for Government oversight and enforcement of rules and regulations. Some suggest that clear laws that are responsive, dynamic and specific on what is allowed and what is not allowed would be beneficial.
- **Differentiation of investors**: Some responses suggest that the term "investors" should be expanded upon further for the purposes of legislative safeguards. There are clear differences between large, sophisticated fund managers and solo retail investors, and different levels of safeguards may be necessary for these groups.
- **Application of existing laws**: Some responses suggest that existing laws and regulations should be applied to the crypto industry, such as financial services and banking licenses for smart contracts that act as financial instruments or bank accounts.
- **Technology**: The technology itself could be used to develop innovative and programmatic solutions that make financial markets more transparent, accessible, and secure.

There were also some differences in these responses covering the level of regulation, who provides education (Government or industry) and how active a role the Government should play in safeguarding consumers.

Overall, the responses suggest that a thoughtful approach is needed to protect consumers and investors in the crypto industry, taking into account the unique nature of this emerging technology and the needs of different types of investors.

Question 3. Scams can be difficult for some consumers to identify.

3.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?

There are several common themes that emerge across the responses, including:

- **Education and consumer awareness**: Many of the responses emphasise the importance of educating consumers about the risks and benefits associated with using crypto assets. This includes providing clear and comprehensive information, as well as encouraging consumers to have a foundational understanding of how crypto assets and blockchain technology work.
- **Regulation and oversight**: Several responses highlight the need for clear regulation and Government oversight to ensure appropriate safeguards are in place for the protection of consumers and financial stability. This includes disclosure requirements, standardised formats for disclosures, and third-party audits of a platform or asset's code where relevant. Some suggest that for certain parts of the market, this should be mandatory.
- **Industry self-regulation**: Some responses suggest that a level of self-regulation from within the industry can also be effective in safeguarding consumers. This includes the establishment of a self-regulating industry body that collates code auditing and other screening capabilities and the creation of an "allow list" of tokens under specific classifications.
- **Data analysis, transaction monitoring, and risk assessment**: Several responses recommend the use of data analysis, transaction monitoring and risk assessment tools to identify potential issues and provide risk warnings or ratings to digital asset users/investors. This includes private sector ratings agencies or researchers and online "red flag" tools and services.

While there are some common themes across the responses, there are also differences in the proposed solutions to safeguard consumers who choose to use crypto assets. Here are some of the key differences:

- **Trusted review site vs. self-regulating industry body**: One respondent suggests a trusted review site that collates information and provides a comprehensive overview of risks and benefits associated with various cryptocurrencies and blockchain-based products, while another respondent suggests a self-regulating industry body that collates code auditing and other screening capabilities.
- **Code auditing vs. plain English reproductions**: Another respondent suggests that advances in technology, particularly in translating code into plain English, can help reduce smart contract risk, while a different respondent suggests third-party audits of a platform or asset's code should be encouraged (where relevant).
- **Allow list vs. disclosure requirements**: One respondent recommends an "allow list" of tokens under specific classifications, while another suggests disclosure

requirements to ensure consumers are informed about the risks and benefits of using crypto assets.

- **Government regulation vs. private sector involvement**: emphasises the role of the Government in establishing a regulatory landscape that strikes the right balance between ensuring consumer protection and fostering homegrown innovation, while another group suggests private sector ratings agencies or researchers also help with mixed ownership between the Government and private sector, could disseminate risk warnings or ratings to digital asset users/investors.

These differences suggest that there is no one-size-fits-all solution to safeguarding consumers who choose to use crypto assets. Rather, a combination of approaches may be required, depending on the specific needs and circumstances of different stakeholders in the ecosystem. This includes education, regulation, industry self-regulation, and the use of data analysis and risk assessment tools.

3b) 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?

Based on the responses, there are several policy and regulatory levers that could be used to ensure that crypto token exchanges do not offer scam tokens and prevent consumers from being exposed to scams involving crypto assets. These include:

- **Licensing and registration requirements for centralised exchanges**, subjecting them to greater scrutiny and accountability.
- **Mandatory reporting requirements** and regular audits for centralised exchanges.
- Providing **access to on-chain data to regulators** to track and prevent scams.
- **Requiring centralised exchanges to conduct due diligence on crypto assets**, ensuring that consumers have all relevant information available to them when making an investment decision.
- **Requiring that consumers can reasonably rely on the disclosures provided by exchanges** and that the exchanges cannot simply remove their liability through broad disclaimers or indemnity provisions in their terms and conditions.
- **Requiring enhanced due diligence on teams behind a token being listed**.
- **Creating industry-wide standards** and best practices for token issuers and exchanges, including in respect of on-chain compliance and integrity systems.
- **Launching public education and awareness campaigns** to inform investors about the risks associated with investing in crypto assets and how to identify scams.

Overall, a combination of these levers could be used to ensure that consumers are protected from scams involving crypto assets while still allowing for innovation in the crypto ecosystem.

Question 4. The concept of 'exclusive use or control' of public data is a key distinguishing feature between crypto tokens/crypto networks and other data records.

4a) 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?

Based on the responses, it seems that the general consensus among the responses is that a definition of crypto tokens and networks for legislative purposes should consider the concepts of exclusive use or control of public data, custody, control, and the layers of a tech stack in a crypto ecosystem.

The responses included the following themes:

- The importance of understanding the concept of exclusive use or control of public data in defining crypto tokens and networks for legislative purposes.
- The need to consider custody and control when defining crypto tokens and networks for legislative purposes.
- The importance of distinguishing the layers of a tech stack in a crypto ecosystem.
- The difficulty in applying the concept of intermediaries to the crypto context, and the potential for adverse outcomes if it is broadly applied.
- The importance of ongoing consultation with the industry to address the limitations of the current regulatory framework, especially as blockchain technology is evolving.
- The use of an exclusive definition that is too narrow and which should consider businesses or multi-parties (aka multisig relationships) too.

4b) What are the benefits and disadvantages of adopting this approach to define crypto tokens and crypto networks?

The common themes across the responses provided include:

- Defining crypto tokens and networks in legislation can provide clarity and understanding of the concept.
- However, having a definition alone may not be enough to prevent people from losing their assets or having them stolen. It's important for people to educate themselves on the basics of cryptocurrencies to fully grasp the concepts and ensure their own protection.
- The current method of defining "crypto asset" in the consultation paper may not be compatible with the current and potential future use of crypto networks, and it differs from the approach taken by other jurisdictions.
- The valuable "asset" in any crypto network is the information recorded on the shared ledger, and a "crypto token" should correctly be the "asset" in the ecosystem, irrespective of the token system.

- The concept of "exclusive control" may limit the ability to describe certain concepts or functions in a crypto system, such as multi-sig wallets. Additionally, certain terms and conditions of token projects cannot be digitally expressed in a smart contract, as they rely on natural language and interpretation.

Overall, these responses suggest that while defining crypto tokens and networks in legislation can be beneficial, it's important to consider different perspectives and consult with industry experts to ensure that any regulations or definitions accurately reflect the nature and potential of crypto networks and tokens.

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

5a) What are additional supporting reasons or alternative views on the value of a bespoke taxonomy?

There were differing responses to this question but some common themes included:

- The crypto industry is constantly evolving and new projects and technologies are emerging all the time, which makes it difficult to create a comprehensive and up-to-date bespoke taxonomy for crypto assets.
- A functional approach that focuses on the resulting functions, outcomes, and risks associated with different token types may be more appropriate than a precise technical specification-based taxonomy.
- The importance of ensuring that regulatory frameworks remain flexible and adaptable to changing market conditions to avoid stifling innovation.
- The need for regular engagement between regulators and industry participants to ensure that any regulatory frameworks are effective and do not create unnecessary restrictions or confusion.
- The importance of distinguishing between different token types for the purposes of regulation, as different tokens have different functions, users, applications, and behaviours.
- The potential benefits of a bespoke taxonomy, such as providing regulatory certainty and making it easier for entrepreneurs to assess compliance across multiple jurisdictions, as well as potential drawbacks, such as the risk of becoming outdated quickly.

Given the differing responses on the value of a bespoke taxonomy for crypto assets, there are several pathways that could be considered:

- **Conduct further research and consultation**: Given the complexity of the issue and the differing opinions, it may be useful for Treasury to conduct further research and consultation with stakeholders to better understand the potential benefits and drawbacks of a bespoke taxonomy for crypto assets.

- **Explore a hybrid approach**: Given that some respondents suggest that a functional approach that focuses on outcomes, risks, and functions associated with different token types may be more appropriate, while others suggest that a bespoke taxonomy may have value, it may be useful to explore a hybrid approach that combines both approaches.
- **Focus on providing regulatory certainty**: Several respondents suggested that a bespoke taxonomy could provide regulatory certainty, making it easier for entrepreneurs to assess compliance across multiple jurisdictions. Thus, one pathway could be to focus on providing more regulatory certainty to support the growth of the crypto industry while ensuring that any regulatory frameworks remain flexible and adaptable to changing market conditions.
- **Emphasise engagement between regulators and industry participants**: Several respondents suggested that ongoing engagement between regulators and industry participants is essential to ensure that any regulatory frameworks remain effective and do not create unnecessary restrictions or confusion. Thus, one pathway could be to emphasise ongoing engagement and collaboration between regulators and industry participants to ensure that any regulatory frameworks reflect the needs of the industry and are effective in achieving their goals.
- **Develop education initiatives for developers**: Several respondents suggested that initiatives aimed at providing blockchain and token developers with a better understanding of the existing legal landscape could be useful. Thus, one pathway could be to develop education initiatives for developers to help them avoid inadvertent violations of the law and ensure that any regulatory frameworks are effective and understood by industry participants.

5b) What are your views on the creation of a standalone regulatory framework that relies on a bespoke taxonomy?

Overall, the responses suggest that any regulatory framework for digital assets should balance regulatory compliance with promoting innovation, provide clarity and certainty, be harmonised with international frameworks where possible, and clearly classify digital assets.

Responses can be grouped into the following categories:

- **Balancing regulation with promoting innovation**: Several respondents argue that any regulatory framework for digital assets should strike a balance between ensuring regulatory compliance and promoting innovation. They contend that overly burdensome regulation could stifle the growth of the industry.
- **Clarity and certainty**: Respondents stress the importance of clarity and certainty in any regulatory framework. They argue that a clear and predictable regulatory environment would be beneficial for businesses operating in the digital assets industry.

- **Harmonisation with international frameworks**: Some respondents suggest that any regulatory framework should be harmonised with international frameworks to reduce friction for Australian businesses operating in a multi-jurisdictional environment.
- **Classification of digital assets**: There is some disagreement among respondents on how digital assets should be classified and regarding how NFTs should be treated. Some argue that NFTs should be explicitly excluded from regulation if they have non-financial functions, while others suggest that exemptions from relevant regulatory requirements should be confirmed for NFTs with incidental financial elements.

5c) In the absence of a bespoke taxonomy, what are your views on how to provide regulatory certainty to individuals and businesses using crypto networks and crypto assets in a non-financial manner?

Overall, while there are some differences in the suggested approaches, all of the responses emphasise the importance of providing regulatory certainty to individuals and businesses using crypto networks and crypto assets in a non-financial manner.

Common themes across these responses are:

- The importance of providing clear guidance and practical education to users to help them make informed decisions and avoid scams and risky investments.
- The need for ongoing engagement and coordination between the public and private sectors to ensure regulatory certainty and minimise inefficiencies in the use of blockchain technology.
- Some mention the need for more dialog with ASIC as a way we could move towards better certainty.
- The suggestion that specific regulation should be implemented for clearly defined parts of the crypto ecosystem, such as exchanges and stablecoins, to provide further regulatory certainty.

Question 6. Some intermediated crypto assets are 'backed' by existing items, goods, or assets. These crypto assets can be broadly described as 'wrapped' real-world assets.

6a) Are reforms necessary to ensure a wrapped real-world asset gets the same regulatory treatment as that of the asset backing it? Why? What reforms are needed?

Based on the responses to this question, there were some common themes which include:

- **Education**: There is a consensus among the respondents that education is important in ensuring that individuals and businesses understand the technology and potential risks associated with wrapped real-world assets.
- **Need for legal clarity**: The respondents recognise that legal clarity is necessary to ensure that new technological methods of expressing existing property rights can be effectively enforced.
- **Treatment of tokenised versions**: There are different views on whether tokenised versions should be treated the same as the asset backing it or not. Some respondents believe that tokenised versions should be treated differently than the asset backing it while others believe that tokenised versions should be treated the same as the asset backing it.
- **Innovation**: Some respondents suggest that the current treatment of tokens as securities is prohibitive for innovation. There is a call for regulatory frameworks that encourage innovation in the space.

6b) Are reforms necessary to ensure issuers of wrapped real-world assets can meet their obligations to redeem the relevant crypto tokens for the underlying good, product, or asset?

The common themes across the responses were as follows:

- The need for education and understanding of the technology and potential pitfalls.
- The importance of sufficient safeguards, such as the involvement of legacy financial institutions, use of crypto tax software and on-chain data, and sharing of code audits.
- The need for disclosures and audits to confirm that issuers can meet their obligations.
- The potential for applying real-world obligations as is if relevant.

Question 7. It can be difficult to identify the arrangements that constitute an intermediated token system.

7a) 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?

Some common themes across these responses include:

- the need for transparency and clear information to be provided to users of crypto asset service providers, particularly centralised exchanges. This includes access to information about the arrangements underpinning crypto tokens, risk management policies, and the use of proof of reserve systems or allow lists to provide transparency and trust in the ecosystem.

- the responsibility of crypto asset service providers to protect their users and ensure they are aware of the risks associated with their investments.

7b) What are some other initiatives that crypto asset service providers could take to promote good consumer outcomes?

Across the responses received, we saw the following common themes:

- **Emphasis on consumer education**: Various responses highlight the importance of educating consumers about cryptocurrencies, DeFi exchanges, and potential scams or malicious activities in the crypto space. By offering guidance and resources, service providers can help users make informed decisions and avoid pitfalls.
- **Focus on transparency**: The responses also emphasise the importance of transparency in promoting good consumer outcomes. This includes making token unlock schedules clear and embedded in smart contracts, auditing smart contracts, and providing links to on-chain metrics that can help investors assess the progress of a token.
- **Advocacy for consumer protection measures**: The responses also suggest that crypto asset service providers should take steps to protect consumers, such as utilising systems that promote transparency and minimum standards. This can help build trust and increase consumer confidence in the crypto space.

Question 8. In addition to the functional perimeter, the Corporations Act lists specific products that are financial products. The inclusion of specific financial products is intended to both: (i) provide guidance on the functional perimeter; (ii) add products that do not fall within the general financial functions.

8a) Are there any kinds of intermediated crypto assets that ought to be specifically defined as financial products? Why?

Based on the responses provided, the majority agree that **existing laws that govern centralised exchanges are sufficient to regulate the industry**.

8b) Are there any kinds of crypto asset services that ought to be specifically defined as financial products? Why?

One response to this question focused on **services offered by centralised exchanges**. This response highlights the trade-off between ease of use and loss of control over assets. This suggests that there may be a need for regulation to ensure that users are adequately protected when using centralised exchanges.

Question 9. Some regulatory frameworks in other jurisdictions have placed restrictions on the issuance of intermediated crypto assets to specific public crypto networks. What (if any) are appropriate measures for assessing the suitability of a specific public crypto network to host wrapped real world assets?

Responses from our collective highlighted the following measures:

- High uptime and no known flaws in the code.
- A community to check if information is correct.
- Source data availability.
- Code audits from reputable audit firms.
- Robust security protocol that can withstand hacking attempts and other security breaches.
- Scalability to handle large volumes of transactions efficiently.
- Interoperability with other networks and protocols.
- Regulatory compliance with relevant frameworks.
- Transparent and decentralised governance structure that is accountable to its users.

These measures are important to ensure that the public crypto network is suitable and secure for hosting wrapped real world assets. As the space evolves, it is important to continually learn and watch for changes in the technology to ensure that the measures are up to date and relevant.

Question 10. Intermediated crypto assets involve crypto tokens linked to intangible property or other arrangements. Should there be limits, restrictions or frictions on the investment by consumers in relation to any arrangements not covered already by the financial services framework? Why?

We had a variety of responses to this question.

- Some felt that existing regulations and laws are already in place for intermediated crypto assets, such as on and off-ramp exchanges and individuals or entities' bank accounts, to protect investors.
- Others believe that investors should have knowledge of these regulations and laws to protect themselves, as there is no way to recall funds if they make a mistake, such as sending it to the wrong location.
- Another group highlights that digital assets or arrangements not covered by the financial services framework should not be restricted for consumer investment. They also go on to mention that retail investors are already allowed to engage in

risky activities in financial markets, such as equity and forex trading, even without having knowledge of the intrinsic value of the assets in question.

Question 11. Some jurisdictions have implemented regulatory frameworks that address the marketing and promotion of products within the crypto ecosystem (including network tokens and public smart contracts). Would a similar solution be suitable for Australia? If so, how might this be implemented?

Our responses highlighted some commonalities including the importance of striking a balance between protecting consumers and fostering innovation within the industry. Additionally, the responses also recognise the challenge of regulating an industry that is constantly evolving, and the need to consider the effectiveness of existing legislation before drafting new legislation. Finally, our responses acknowledge the importance of protecting consumers from scams and exploitation, while also fostering innovation within the industry.

Question 12. Smart contracts are commonly developed as 'free open source software'. They are often published and republished by entities other than their original authors.

12a) What are the regulatory and policy levers available to encourage the development of smart contracts that comply with existing regulatory frameworks?

Despite proposing different approaches, there are some common threads in these responses.

- Firstly, all the responses acknowledge the **need for smart contracts to comply with existing regulatory frameworks**. They recognise that regulations such as the Austrac AML/CTF Act, ATO Income Tax Act, and the Goods and Services Act, provide sufficient oversight and guidance for the crypto system.
- Secondly, there is a **shared concern about stifling innovation through overregulation**. All the responses indicate that further regulation either may not be necessary or should be implemented with caution to avoid harming the competitiveness of the crypto system in the global market.
- Finally, there is a **focus on protecting retail investors**. The responses propose different methods of doing so, such as ensuring compliance with existing regulatory requirements, creating an "allow list" of tokens and facilitating user education.

12b) What are the regulatory and policy levers available to ensure smart contract applications comply with existing regulatory frameworks?

Overall, these responses demonstrate a range of perspectives and ideas for addressing the question of regulatory and policy levers for ensuring compliance with existing regulatory frameworks in smart contract applications. All the responses recognise the importance of ensuring compliance with existing regulatory frameworks. However, they differ in their approaches to achieving this goal.

- One response suggests that the current regulations are sufficient, and adding more regulation could stifle innovation.
- Another suggests a collaborative effort between the Government and industry stakeholders to establish clear guidelines and standards for smart contract development, third-party auditing or certification programs, and incentives for compliance.
- Another emphasises the importance of auditing smart contracts to ensure compliance.

Despite these differences, all the responses agree that it is important to ensure compliance with existing regulatory frameworks, and that a coordinated effort between industry stakeholders and Government could help achieve this goal.

Question 13. Some smart contract applications assist users to connect to smart contracts that implement a pawnbroker style of collateralised lending (i.e. only recourse in the event of default is the collateral).

13a) What are the key risk differences between smart contract and conventional pawn broker lending?

The responses suggest that the key risk differences between smart-contract and conventional pawn-broker lending are:

- **Trust**: Conventional pawn-broker lending requires trust in the lending service to hold the collateral over the period of time specified in the agreement, whereas smart-contract based DeFi lending uses self-custody escrow type mechanisms that cannot be corrupted by human error.
- **Immutability and transparency of the smart-contract system**, which reduces the risk of fraud or manipulation by the lender.
- **The ability to automate the entire loan process**, which reduces the time and cost associated with traditional loan applications.

- **Fungibility of cryptocurrency collateral**, which allows for greater price discovery but also leads to potential contagion risk if large lending positions are closed out simultaneously.

Overall, it seems that smart-contract lending offers significant advantages over conventional pawn-broker lending, particularly in terms of transparency, automation, and risk reduction. However, there are still some unique risks associated with lending in the cryptocurrency space, particularly around the volatile and rapidly changing value of collateral.

13b) Is there quantifiable data on the consumer outcomes in conventional pawn broker lending compared with user outcomes for analogous services provided through smart contract applications?

A common thread across the responses is the acknowledgement that **there is some quantifiable data available to compare consumer outcomes in conventional pawn-broker lending and smart contract applications**. However, there is also recognition that the data may not be directly comparable due to differences in the nature of the lending products.

Another common thread is the **importance of factors such as interest rates, repayment terms, default rates, and consumer protection** in assessing consumer outcomes for both types of lending. It is suggested that these factors could be used to compare the outcomes of smart contract applications and conventional pawn-broker lending.

Finally, there is a recognition that the **data available may not be completely useful for comparison at this time**, as DeFi loans are often over-collateralised on-chain and are not creating credit in the same way as traditional finance. However, it is noted that as DeFi continues to expand and evolve, this may change in the future.

Question 14. Some smart contract applications assist users to connect to automated market makers (AMM).

14a) What are the key differences in risk between using an AMM and using the services of a crypto asset exchange?

Based on the responses provided, the key differences in risk between using an AMM and using the services of a crypto asset exchange can be summarised as follows:

- Centralised crypto asset exchanges have operational risks, such as the potential for the business to go bankrupt, mismanagement or fraud by the exchange, while decentralised exchanges have smart contract vulnerabilities such as poorly written code or built-in back doors and admin keys that could be exploited or used against individuals interacting with such code.

- Both types of exchanges have risks related to sending crypto to the wrong address resulting in a permanent loss of assets.
- Centralised exchanges adhere to the AML/CTF Act, so when on- and off-ramping, the data is captured, while decentralised exchanges rely on on-chain data.
- AMMs expose users to liquidity dynamics driven by supply and demand of token buyers/sellers and liquidity providers, while centralised exchanges are able to be more dynamic during the provision of liquidity.
- Liquidity for centralised exchanges is typically provided by one or more centralised market makers, while AMMs have a permissionless environment where liquidity can be provided by market participants in exchange for a portion of trading fees collected.
- Centralised exchanges have counterparty risk, as customers trust them with deposited assets, while with AMMs, the same risk lies in the potential for underlying smart contracts containing errors in the code to be exploited by a malicious actor and the assets drained from that particular liquidity pool.

14b) Is there quantifiable data on consumer outcomes in trading on conventional crypto asset exchanges compared with user outcomes in trading on AMMs?

Based on the responses, it seems that quantifiable data on consumer outcomes is more readily available for AMMs than conventional crypto asset exchanges. This is because AMMs operate on public blockchains like Ethereum and information about transactions and outcomes of smart contract applications can be accessed through blockchain explorers like Etherscan. Financial reports from conventional crypto asset exchanges only show assets, liabilities, and equity, and the data is not as extensive.

Another response suggests directing the question to high-quality, on-chain data providers like Chainalysis, Dune Analytics, or Arkham Intelligence.

A further response highlights that price action is a common data point for both centralised exchanges and AMMs, which can be accessed through platforms like Tradingview. However, due to the open-source nature of AMMs, data from any transaction can be pulled permissionlessly into any new data aggregator or analytics platform, allowing users to get customised information that they wouldn't normally get from a centralised exchange.

Conclusion

The Australian DeFi Association, a not-for-profit community organisation focused on blockchain technology education and awareness, submits the above response to the token mapping consultation. The community members' various opinions on the topics discussed in the consultation reflect a desire to ensure consumer protection while continuing to encourage innovation in the digital asset space.

The submissions received indicate the need for flexibility in regulatory frameworks that focus on the underlying functions, outcomes, and risks associated with different token types. Instead of attempting to create a comprehensive taxonomy, the community suggests a more nuanced approach to regulation that adapts to changing market conditions and ensures that regulation is focused on protecting investors and promoting market integrity.

Respondents to the consultation agree that financial services regulation should not treat digital assets differently just because they operate on different technology. They urge the Government to work collaboratively with industry participants to develop regulation that strikes a balance between consumer protection and innovation. Members are committed to ongoing conversations with the Government to share their views proactively and to ensure that regulatory frameworks for digital assets are developed with due consideration for the unique features of the technology.

In conclusion, the responses to the Token Mapping Consultation highlight the importance of striking a balance between consumer protection and innovation and developing regulatory frameworks that support the growth of the digital asset space. Aus Defi looks forward to continued collaboration with the Government to help shape regulatory frameworks that promote the growth of the digital asset space and support innovation.

Appendix A - Contributors

We would like to acknowledge the following contributors (people and organisation) to this token mapping response

Appendix B - Community Responses

The following is a list of various responses from the community. It is from these responses that we have created our summarised views above. Whilst there are some differences, the responses were mostly in line with their views.

Response from NotCentralised

The response from NotCentralised is not shown here as it is already a submission to the consultation process. It can be found amongst all other responses listed by Treasury and will also be available on the NotCentralised blog under government submissions: https://medium.com/notcentralised/tagged/government

Responses from Immutable

Thematic observations: Government plays a role in ensuring appropriate safeguards are in place for the protection of consumers and financial stability. At the same time, the stance that the Government takes to crypto regulation will undoubtedly impact whether Australia is perceived as an attractive place for web3 innovation and investment, which in turn leads to opportunities, jobs and growth. There are Australian blockchain-based businesses that are global leaders and responsible innovators in their field and so Government must establish a regulatory landscape which strikes the right balance between (1) ensuring consumer protection and (2) fostering homegrown innovation. With the help of industry, it is incumbent on Government to educate itself about the vast spectrum of crypto use cases, so that regulation is fit-for-purpose, proportionate and sensible.

Functional approach: We generally agree with a functional approach to assessing tokens (particularly as the tech will continue to evolve beyond any laws). At the same time, this leaves the application of the law open to interpretation in circumstances where the current AFSL regime is already very broad. In turn, this breeds uncertainty which can be the enemy of innovation. Clarity and guidance upfront as to the application of the functional perimeter is key.

Token taxonomy: While we understand the 'token, token system, function' taxonomy is not necessarily intended to be a preview of the legislative terms, it requires quite a tortured analysis, and certainly one which most industry stakeholders are not equipped to assess themselves without the assistance of legal advisors. That shouldn't be the starting point. Business needs clarity upfront.

- Crypto networks shouldn't be caught as financial products. This bears out an important point about layers of a tech stack. There needs to be a clear understanding of and the distinction between the point at which a product or

service is offered vs. the mere provision of technology and infrastructure. While we are cautious of attempts to broadly label crypto use cases, we do think there is a distinction to be drawn between 'money-crypto' and 'tech-crypto', the former operating more closely to the established financial services perimeter and the latter, involving services more akin to the provision of software.

- NFTs
    - many have non-financial functions and such NFTs should be explicitly excluded (e.g. collectibles, NFTs purely for game play where no other financial elements are involved, digital representations of art, etc)
    - some have a non-financial primary functions but may have incidental financial elements. The use of the incidental exemption in the Corporations Act 2001 should be available here, with further guidance around its application to such NFTs
    - the fact that an NFT has value on a secondary market should not make it a financial product - you could say this about any item of value.

Intermediaries: Concept of intermediaries is an interesting one - is this is intended to be a hook for legislation and if so, how is the 'intermediary' concept intended to be applied in the crypto context? Custody and control are common concepts raised in this regard.

- We agree that the provision of custody will trigger financial service laws where financial products are involved and appropriate safeguards need to be in place for the protection of consumers. Conversely, a non-custodial provider of crypto-related services should not be caught, assuming no other regulated activities are conducted.
- Control is a much looser concept and could potentially lead to adverse outcomes if broadly applied. For example, a fully decentralised infrastructure running entirely programatically on smart contracts does not involve intermediaries. Is the coder of a smart contract an intermediary? Should it be? No doubt, the answer will be "it depends" but against what criteria is that assessment made?
- Reiterating the point above, we think it's important to distinguish the layers of a tech stack in a crypto ecosystem.

Responses from

Q1. Response

The role of the government in the regulation of the crypto ecosystem should be to balance regulation with innovation. By implementing measures such as KYC/AML, financial institutions and relevant agencies can monitor and track the movement of funds in and out of the crypto space. However, too much regulation can reduce trust in the crypto system, prevent the creation of new and innovative products and services, and discourage investment. The government should aim to strike a balance between regulation and innovation to avoid stifling the potential of the crypto ecosystem.

Q2. Response

Investing in new companies, including those in the cryptocurrency market, involves financial loss, risks to other companies that work with them, and the risk of new products being riskier than traditional ones. Education and awareness about potential scams and risks are the best safeguards for consumers and investors, as opposed to heavy regulation. It's important for individuals to educate themselves about the market to make informed decisions and protect their investments. Criminals do not follow the law, so holding those who committed fraud accountable under existing laws is also important.

Q3a. Response

The solution to safeguarding consumers who choose to use crypto assets is a trusted review site that collates information and provides a comprehensive overview of the risks and benefits associated with various cryptocurrencies and blockchain-based products. This can help users make informed decisions and avoid scams or security threats. However, it's important to note that with the rapid pace of technological change and the emergence of new security threats, it can be difficult to keep track of everything. That's why it is equally important for consumers to educate themselves and have a foundational understanding of how crypto assets and blockchain technology work. This will help them make informed decisions and minimise their risk, even as new threats emerge.

Q3b. Response

Regulators should focus on centralised exchanges as a priority for ensuring the prevention of scams involving crypto assets. The centralised exchanges, like FTX, have been indicted for fraud, money laundering, and campaign finance offenses, which highlights the need for regulation in this area. By providing access to on-chain data, regulators can better track and prevent these types of scams. Additionally, educating consumers on the basics of cryptocurrency through websites and resources that offer information and insights can also help create a more informed and aware crypto community, reducing the risk of exposure to scams.

Q4a. Response

Defining crypto tokens and networks for the purpose of legislation requires a clear understanding of the concept of exclusive use or control of public data. This is a key characteristic that distinguishes crypto assets from other data records. In order to ensure that individuals are protected in the world of cryptocurrencies, it is important for them to be educated about the basics of how these assets work. This includes understanding that if they do not control their private keys, they do not control their crypto assets. A good way to ensure this understanding is to promote education and awareness about cryptocurrencies, including the dangers of entrusting control of crypto assets to centralised exchanges. This will help individuals make informed decisions and protect themselves from negative outcomes, as seen in the case of FTX in the past.

Q4b. Response

"The benefits of defining crypto tokens and crypto networks in legislation are that it provides a clear understanding of the concept. However, having a definition alone will not prevent people from losing their assets or having them stolen. It's important for people to have knowledge and understanding of the network or blockchain the token is on, how it works, and the risks involved in order to protect themselves. Definitions and regulations can provide a foundation for understanding, but it's crucial for people to educate themselves on the basics of cryptocurrencies to fully grasp the concepts and ensure their own protection."

Q5a. Response

The creation of a specific taxonomy for crypto assets may not have significant value in regulation due to the current focus on random updates rather than understanding the on-chain data analysis of past transactions. This lack of understanding and knowledge of on-chain data by the public is a major obstacle that needs to be addressed before any new taxonomy can be effective. However, as more people gain a better understanding of the crypto industry and the importance of on-chain data analysis, the process of creating and implementing a taxonomy that provides regulatory value will become easier. Additionally, a taxonomy that offers reduced capital gains incentives or exemptions may encourage innovation in the crypto industry and make it more attractive to investors. Furthermore, it is possible that a bespoke taxonomy may not even be required, as sufficient coverage may already exist. Crypto tax software can still be useful for tracking transactions, while DeFi remains unaffected and centralised exchanges would remain as they are.

Q5b. Response

I only support the creation of a standalone regulatory framework for cryptocurrency if it is more favorable for the industry. This could include reduced tax rates for capital gains, or treating cryptocurrency as an asset where people only pay taxes when they sell and make a profit. There is already enough guidance and tools, such as on-chain data analysis, crypto tax accounting software, and centralised exchange data, to track transactions and catch bad actors. However, compared to some countries, the current level of regulation and taxation is too high. Countries like Germany, Belarus, El Salvador, Portugal, Singapore, Malaysia, Malta, Cayman Islands, Puerto Rico, Switzerland, and Georgia are good examples of how to lead in this space by having less regulation.

Q5c. Response

A government-run program could provide clear guidance and warnings on current scams, smart contract code issues, and exchange ratings. This information would help individuals make informed decisions, similar to how Coinbase offers lessons online. There are already regulations in place for centralised exchanges, and there is enough on-chain and centralised exchange data when moving fiat in and out of the system. To ensure a positive

experience, it is crucial to educate the public about good habits, such as avoiding paid shills that promote risky crypto derivatives trading. Instead, individuals should prioritise choosing technology with well-written code, no exploits or bugs, and 100% uptime, as well as understanding the importance of secure asset management.

Q6a. Response

Reforms may not be necessary to ensure that wrapped real-world assets receive the same regulatory treatment as the assets backing them. However, it is important to educate individuals and businesses on the technology and potential risks associated with wrapped real-world assets to ensure they make informed decisions.

Q6b. Response

Reforms are not necessarily required to ensure the issuers of wrapped real-world assets meet their obligations. However, educating the public on the technology and potential pitfalls is important. The use of crypto tax software and on-chain data, along with the involvement of legacy financial institutions, provides sufficient safeguards for those who understand the underlying technology. To prevent scams, continuous education and the sharing of code audits within the industry can help maintain the integrity of the system.

Q7a. Response

Crypto asset service providers, such as centralised exchanges, should be required to ensure their users have access to information that allows them to identify the arrangements underpinning the crypto tokens they trade. This can be achieved by requiring centralised exchanges to release on-chain data, making it subject to public scrutiny, similar to DeFi. If centralised exchanges are protected from disclosing information due to company secrets, a proof of reserve system could provide assurance to users who want to surrender control of their assets. Personally, I prefer not to participate in centralised exchanges, except for on and off ramping purposes.

Q7b. Response

Crypto asset service providers could promote good consumer outcomes by taking several initiatives, such as offering guidance and educational resources to their users. For example, providing information about different crypto currencies, trusted DeFi exchanges, and teaching users how to take control of their own assets can help prevent scams and malicious activity. Additionally, a government-led initiative providing basic education and updated information about new types of scams and developments in the crypto space could benefit both novice and experienced investors.

Q8a. Response

I don't think additional regulations are necessary, as long as businesses in the industry operate in accordance with existing laws, such as those governing centralised exchanges that offer traditional financial products, which can easily be identified.

Q8b. Response

Crypto asset services can be broadly categorised into two options: using a centralised exchange or interacting directly with decentralised smart contracts. Centralised exchanges provide ease of use, but result in the loss of control over one's assets. On the other hand, interacting directly with smart contracts offers the advantage of full control over one's assets, but with increased contract and security risks. As a result, the safest option for storing crypto assets is to use a personal wallet.

Q9. Response

This could be subject to change as technology develops say a once efficient chain fills up and becomes expensive to use it may no longer be the best, a good start would be 100% up time and no known flaws in the code, maybe with a community behind it to be able to check if information is correct etc. and where to find source data from. Code audits are also held in high regard from reputable audit firms. Again this all comes down to learning and watching as the space evolves.

Q10. Response

There is already enough regulation and laws in place for intermediated crypto assets, such as on and off ramp exchanges and individuals or entities' bank accounts. It's important for investors to have knowledge about these regulations and laws for their own protection, as there is no way to recall funds if they make a mistake, such as sending it to the wrong location.

Q11. Response

"The implementation of additional regulations in the marketing and promotion of crypto products may hinder innovation in the field. Regulations can add barriers to entry, which can restrict the growth of new and innovative ideas and technologies. In addition, the crypto industry is constantly evolving, and it may be challenging for regulators to keep up with the pace of change. Therefore, it's crucial to strike a balance between protecting consumers and fostering innovation within the industry. Education about the different products and their risks and benefits can be more beneficial in promoting responsible practices and reducing the risk of scams or exploitation."

Q12a. Response

Smart contracts are subject to existing regulations such as the Austrac AML/CTF Act, ATO Income Tax Act, and the Goods and Services Act, before fiat can enter the crypto system. The regulations provide sufficient oversight and guidance for the crypto system, and all data related to smart contracts is recorded on the blockchain for transparency and accountability. Further regulation may stifle innovation and harm the competitiveness of the crypto system in the global market.

Q12b. Response

The existing regulations such as Austrac AML/CTF Act, ATO Income Tax Act, and Goods and Services Tax Act, provide sufficient oversight and guidance for the operation of smart contract applications. The data recorded on the blockchain is publicly accessible and transparent, adding a level of accountability. Adding additional regulation may stifle innovation and detract from the competitive advantages of the crypto system.

Q13a. Response

"In Australia, if a conventional pawn-broker business goes bankrupt, the process of getting your collateral back would depend on the specific circumstances and the rules and regulations in place at the time of the bankruptcy. According to the Australian Securities and Investments Commission (ASIC), consumers may be able to get some of their money back from the National Guarantee Fund (NGF) if the lender was a member of the NGF and the loan was covered by the NGF. However, this may not always be the case, and it is always best to research and choose a reputable conventional pawn-broker lending business to reduce the risk of losing your collateral in the event of a bankruptcy.

Regarding smart contract applications, understanding well-written immutable code is crucial to reducing the risk of loss in the event of bankruptcy or any other issue. It is important to note that smart contracts are self-executing and rely on the underlying code to determine the outcome of a transaction, so it is essential to thoroughly research and understand the code before engaging with a smart contract application."

Q13b. Response

Yes, there is quantifiable data available on the public blockchain for open networks, which can be used to assess the outcomes of smart contract applications and compare them to conventional pawn-broker lending. Additionally, conventional pawn-broker lending in Australia is regulated by ASIC, providing additional data and information on consumer outcomes.

Q14a. Response

"With a centralised crypto asset exchange, the risks include the lack of on-chain data and the operational risk of the business potentially going bankrupt or in some cases, mismanagement or fraud by the centralised exchange. These exchanges do adhere to the AML/CTF Act, so when on- and off-ramping, the data is captured.

On the other hand, when using an AMM (decentralised exchange), the risk is related to smart contract vulnerabilities such as poorly written code or built-in back doors and admin keys that could be exploited or used against individuals interacting with such code. Additionally, when on- and off-ramping with traditional financial markets, these are typically conducted through centralised exchanges, and the data is picked up then.

It is worth noting that regardless of whether you use a centralised or decentralised exchange; there is a risk of sending your crypto to the wrong address, resulting in a permanent loss of your assets.

A risk for both is education about which exchange an individual chooses to engage with and where the individual wants to send their assets."

Q14b. Response

Quantifiable data is more readily available on the public blockchain for AMMs, such as Ethereum, than for conventional crypto asset exchanges. A blockchain explorer like Etherscan can provide in-depth information about the transactions and outcomes of smart contract applications on the blockchain. On the other hand, financial reports from conventional crypto asset exchanges only show assets, liabilities, and equity, and the data is not as extensive.

Responses from

Q2. Response

I think the laws should start from a goal, with the goal being to:

1. Protect consumers (to a reasonable but not prohibitive extent)

2. Encourage local innovation

3. Encourage a crypto brain drain into Australia

Unlike most places, the law should try to be:

1. Quick in response (so not take 5 years to draft basic things)

2. Extremely clear on what is allowed and what is not allowed

This is a pain point in pretty much most jurisdictions where clarity is lacking and regulation is done by enforcing web2 laws that just end up being unnecessary court time - that could have been solved easily through clarity

Maybe something interesting would be a 'Bureau of Web3 Standards' that consults stakeholders from the industry, legal, technical and government to draft standards/ guidelines that Web3 can follow and know they are safe from legal issues

That would save the industry heaps of legal costs and doubts if there was a '10 commandments' sort of standards they knew they could stay within

And laws could even stem from those standards (and take their time in being drafted, since we all know that government is pretty slow).

Responses from

Q1. Response

"The role of the government in regulating the crypto ecosystem should be to provide clarity, strike a balance between innovation and safeguards, minimise compliance costs, and monitor the ecosystem to address evolving risks and trends. To maximise economic and consumer benefit the government should also attempt to be adaptive where the transparency of the blockchain, on-chain metrics and open source protocols can improve traditional compliance. In addition, the government should take a leadership role with international partners to harmonise regulations. Finally, government should work to reduce international remittance costs.

For example, blockchain/smart contracts can improve speed, transparency and lower compliance costs as several stages in traditional finance can be disintermediated. Siemens cited that using the blockchain and taking advantage of local legislation to issue a bond on blockchain meant it did not require a central clearing house or a bank to operate as intermediary. The diagram below shows the large number of parties in a securitisation – many of these functions are repetitive and indeed less transparent than blockchain.

It is also essential to consider the cost of participation in the ecosystem, especially for small businesses and start-ups. If compliance costs are prohibitively high, it could deter new entrants from entering the market, resulting in a lack of competition and potentially higher prices for consumers. Therefore, the government should explore options to reduce compliance costs and encourage new entrants to compete with established players. Where licencing/regulation is deemed necessary if compliance costs are high perhaps there are options to explore initiatives similar to the AFSL sandbox to encourage new entrants and competition.

The government should engage internationally to harmonise regulations to reduce costs for consumers. This includes potentially lowering the cost of capital through international liquidity pooling for securities.

Importantly it should consider working with local partners to lower the cost of remittances. At 5.8% as at September 2022, Australia has the opportunity to reduce this cost significantly. This burden is often borne by people sending money home to family.

Q2. Response

Information asymmetry that can be used to the detriment of consumers needs to be closely looked at. That said, consumer protection needs to be viewed in the modern light where retail investors are a greater part of the market as shown below, and wish to have more control over their financial future. An overly paternalistic approach to managing consumer risk is not in touch with contemporary thinking especially limiting opportunities to wholesale investors. The emphasis should be on education and financial inclusion. Financial disclosure requirements should also reflect the changing nature of investors.

Q3a. Response

"Advances in technology, namely the ability to translate code into plain English, can be used to reduce the “technology risks” cited at 111 (a). This can lower smart contract risk.

Historically, smart contract risk has been more problematic for users not proficient at reading code. This enables malicious code to be inserted into the contract unbeknownst to the user. The significant recent advances in LLM (such as ChatGPT) can facilitate plain english reproductions of the contract. The interpretation should include which wallet funds are being sent to, but also outline specifically if the smart contract gives any ongoing permissions or authorities."

Q3b. Response

"Licensing and registration requirements for centralised exchanges*: The Government could require crypto token exchanges to obtain licenses and register with regulatory bodies, subjecting them to greater scrutiny and accountability. This could include mandatory reporting requirements and regular audits. (see question 7 and the NYFDS guidance on custody for more).

Generally more information should be available to prospective investors to enable them to make better informed decisions. Specifically, token unlock schedules should clear and embedded in smart contracts so they cannot be manipulated. In addition, smart contracts should also be audited. An interesting possibility is to require CEX to provide links to on-chain metrics that can help individual investors assess the current progress of a token such as its Total Value Locked (TVL), current users etc. There is exciting potential for real-time information transparency in the crypto space.

Public Education campaigns: launch public education and awareness campaigns to inform investors about the risks associated with investing in crypto assets and how to identify scams. This could include providing information on how to conduct due diligence, how to spot red flags, and how to report suspicious activities.

Encouragement development of Industry bodies for improved self-regulation: creating industry-wide standards and best practices for token issuers and exchanges. This could include establishing codes of conduct, implementing transparency measures, and developing guidelines for token issuers to follow. "

Q5a. Response

Advantages of a bespoke taxonomy include increasing harmony with the international community and providing more regulatory certainty. It would be more efficient and economically advantageous for Australian entrepreneurs to be able to quickly assess compliance across Australian and international regulations. The European Union's MiCA framework that was finalised in October 2022 will be applied throughout 27 member nations (representing approximately one-sixth of the global economy). The government should aim to reduce friction for Australian businesses operating in a multi-jurisdictional environments in order to maintain competitiveness.

Q5b. Response

See above.

Q5c. Response

Ongoing public-private engagement to ensure that digital asset stakeholders can regularly meet and co-ordinate on arising issues. Clear worked examples could also provide useful practical guidance for users. For example, working through and outlining under what jurisdiction and regulatory requirements would a Siemens type bond be applied to in Australia? Proactively discussing how can industry and the public sector can minimise inefficiencies using blockchain will improve Australia's competitiveness and potentially lower the cost of capital for Australian businesses.

Q7a. Response

Clear risk management policies should be available for review by users. Some of the losses caused in 2022 were due to the intermediator taking on significant and correlated risk positions that were opaque to the consumer. Similarly, players took large positions in illiquid assets (such as StETH) that would (and did) become an issue if there was a run on redemptions. It was not obvious to retail users that the yield they were earning was based on these practices.

Regarding centralised exchanges (CEX) the guidance NYDFS issued in January 2023 on custodial structures for consumer protection is a good starting point. Coinbase claims it has already complied with these rules. JonesDay summarises these rules as follows: The

Guidance sets forth NYDFS's expectations in four areas:

- Segregation of and Separate Accounting for Customer Virtual Currency: NYDFS expects that VCE Custodians will hold the virtual currency of customers in either ""separate on-chain wallets and internal ledger accounts for each customer"" or omnibus wallets containing only customer virtual currency held by the VCE Custodians as agents or trustees. That is, VCE Custodians should not commingle proprietary digital assets with customer assets. If a VCE Custodian holds customer virtual currency in an omnibus wallet—comingling customer assets with other customer assets only—it must uphold appropriate recordkeeping and internal audit trail procedures such that it is able to promptly and accurately identify each customer's beneficial interest.
- VCE Custodian's Limited Interest in and Use of Customer Virtual Currency: The Guidance restricts a VCE Custodian's interest in the assets under its control, directing VCE Custodians to ""structure their custodial arrangements in a manner that preserves the customer's equitable and beneficial interest in the customer's virtual currency."" Further, the Guidance advises VCE Custodians to treat all customer assets under their control as solely the property of the customers, and to avoid handling customer assets as if they were the property of the VCE Custodians. NYDFS expects that customer assets will not be used to secure or guarantee an obligation of, or extend credit to, the VCE Custodian or others.

- Sub-Custody Arrangements: VCE Custodians may enter into sub-custody arrangements with third parties, provided that they conduct appropriate due diligence and obtain prior approval from NYDFS.
- Customer Disclosure: VCE Custodians must disclose their terms of service to customers, including their procedures for segregating customer assets, what property interest customers will retain, and how the VCE Custodians can use the virtual currencies they hold. VCE Custodians must also obtain customers' acknowledgment of such terms. For VCE Custodians that offer digital asset staking and lending programs, more clarity may be needed on how these disclosure provisions interact, if at all, with NYDFS's expectation that VCE Custodians will not make extensions of credit using customer assets.

Q7b. Response

As noted earlier - generally more information should be available to prospective investors to enable them to make better informed decisions. Specifically, token unlock schedules should clear and embedded in smart contracts so they cannot be manipulated. In addition, smart contracts should also be audited. An interesting possibility is to require CEX to provide links to on-chain metrics that can help individual investors assess the current progress of a token such as Total Value Locked (TVL), current users etc. There is exciting potential for real-time information transparency in the crypto space.

Q9. Response

Security: The security of the public crypto network is paramount. The network should have a robust security protocol that can withstand hacking attempts and other security breaches. The security measures should also cover the process of wrapping and unwrapping the real-world assets.

Scalability: The public crypto network should be able to handle large volumes of transactions efficiently. The network should have high throughput, low latency, and low fees to ensure that the transactions are processed in a timely and cost-effective manner.

Interoperability: The public crypto network should be interoperable with other networks and protocols to facilitate the movement of wrapped assets across different platforms. This will help to increase liquidity and reduce counterparty risk.

Regulatory compliance: The public crypto network should be compliant with relevant regulatory frameworks in the jurisdiction where the assets are being wrapped. This will help to ensure that the assets are legally recognised and can be traded in a compliant manner.

Governance: The public crypto network should have a transparent and decentralised governance structure that is accountable to its users. This will help to ensure that the network is managed in a fair and democratic manner.

Q10. Response

Not necessary at this stage.

Q11. Response

Not necessary at this stage.

Q12b. Response

To foster a conducive environment for the development and use of smart contracts, the government could engage in a cooperative effort with industry stakeholders. This partnership could involve the establishment of unambiguous guidelines and standards for smart contract development, with a focus on compliance with existing regulatory frameworks. As part of this collaboration, third-party auditing or certification programs could be implemented to monitor and ensure adherence to regulations.

Furthermore, the public and private sectors could collaborate in research and development efforts to create innovative solutions that comply with regulations. To incentivise this cooperation, the government could provide funding or other incentives, such as tax breaks or grants, to facilitate the development of compliant smart contracts.

Overall, a coordinated effort between the government and industry stakeholders can help ensure that smart contracts are developed and used in a manner that complies with regulations and is beneficial to society. The government can provide guidance and incentives, while industry stakeholders can contribute their expertise and resources to create compliant and innovative solutions.

Q13a. Response

Smart Contracts offer many important advantages over pawn shops or rent-to-buy loans – critically by reducing the human ability to cause harm to the consumer. A couple of examples are below – these are not supposed to be exhaustive but simply illustrate why concepts like immutability do matter in the real world.

- Immutability: The terms of the loan are embedded in the smart contract and cannot be changed against the consumers' wishes. As an example - according to the Consumer Action Law Centre, Cash Converters have artificially extended the term of loans:
    - The amount of repayments under some loans are inexplicably reduced (stepped down) after 6 months without the consumer requiring this. This extends the repayment period to 12 months and maximises the amount of fees that Cash Converters can obtain under the Small Amount Credit Contract regime. Had the repayments been maintained at the original amount, the loans would be paid off faster and at less expense to the Consumer.

- Equality of access /lack of discrimination: The smart contract is not discriminating against individuals or a class of persons. A pawn shop owner or rent-to-buy or type lender can do so. A 2015 ASIC report found that Centrelink recipients were charged more and noted, “Of particular concern is that the most financially vulnerable consumers in Australia are paying the highest lease prices for basic household goods. For two year leases, half the Centrelink recipients in our study paid more than five times the retail price of the goods.”
- Efficiency: Smart contracts can automate the entire loan process, reducing the time and cost associated with traditional loan applications. Smart contracts can also eliminate the need for intermediaries, such as banks or loan officers, reducing the cost and complexity of the loan process.
- Transparency: Smart contracts are transparent, meaning that all parties involved in the contract can see the terms and conditions clearly. This transparency ensures that there are no hidden clauses or unfair terms that can be used to exploit one party or the other."

Q13b. Response

Currently the data is probably not overly useful. This is because the majority of current Defi loans are over-collateralised on chain and it is not really the creation of credit in the same way as in traditional finance. To quote Jump Crypto, “In the world of DeFi, the “credit” offered by decentralised lending protocols generally means something quite different: rather than access to more money, the primary use case is exposure to a different asset mix.” Naturally this is expected to change in the future as Defi expands.

As Jump Crypto points out in the same paper, for this loan product (eg identity based) the key aspect that governs the value of this kind of service to the borrower is the cost of capital. The implication is that Defi would only succeed in offering this credit product if it could offer it at a better price to consumers. The reasons why this might be the case are varied – but an obvious one is access to a larger pool of liquidity for the lender. Interestingly, consumers of this credit product might at other times offer liquidity to the lending pool and thus have access to also profit from this product (if this is not regulated against of course!).

Responses from Adiuvo Legal

Q1. Response

We believe that the overarching role of the Government with regards to regulation of the crypto ecosystem is balancing the need for innovation and development with the need for consumer protection and the prevention of illicit activities.

Government regulation should establish clear guidelines and standards for the operation of crypto businesses, including, but not limited to, requirements for licensing, disclosures required, KYC (know-your-customer) and AML (anti-money laundering).

Such regulation and its requirements should be simple and straightforward to foster competition and innovation in the crypto ecosystem.

Q2. Response

"We believe the there are two potential safeguards:

1. Government oversight - this can help ensure that the crypto industry operates in a transparent and accountable manner. Oversight would involve things like the monitoring of exchanges and other crypto businesses and the enforcement of rules and regulations; and
2. Balanced education - this is essential to ensuring that consumers and investors are aware of the risks and opportunities associated with the crypto ecosystem. Education initiatives could include campaigns to help promote financial literacy, cybersecurity awareness and to raise awareness of the potential benefits and risks of crypto investments.

Q3a. Response

Yes, in addition to clear regulation, government oversight and education initiatives discussed above, disclosures and code auditing can be useful in safeguarding consumers.

Disclosure requirements help ensure that consumers are informed about the risks and benefits of using crypto assets. They also allow them to make more informed decisions about their investments. Disclosures should be required to be clear and comprehensive, including information like the blockchain address of the asset, method of purchase, estimated return and details of the development team behind the asset.

Further, it would be helpful if disclosure were in a standardised format (similar to, say, consumer medicines information sheets in medication packets) making it easier for consumers to identify the relevant information they need.

Code audits, although helpful, involve human intervention and so cannot always identify all vulnerabilities in the asset. Accordingly, we believe that third-party audits of a platform or asset's code should be encouraged (where relevant) but should be an obligation.

Q3b. Response

Crypto token exchanges should be required to conduct due diligence on each crypto asset they list. This due diligence should, at a minimum, ensure that they have all relevant disclosure information available to provide to consumers. This would ensure that consumers have all relevant information available to them when making an investment decision.

Additionally, to encourage exchanges to conduct proper due diligence, regulation should require that consumers can reasonably rely on the disclosures provided and that the exchanges cannot simply remove their liability through broad disclaimers or indemnity provisions in their terms and conditions.

Q4a. Response

We suggest the following definitions:

1. Crypto token - a digital representation of information:
    a. over which a person or group has exclusive use or control;
    b. that has value and or grants some right to that person or group; and
    c. which may be transferred, stored or traded electronically, using technology supporting the recording or storage of that information, including, but not limited to, distributed ledger technology.
2. Crypto network - a distributed computer network system connected via the use of a shared cryptographic protocol and used to maintain a shared ledger of crypto tokens.

Q4b. Response

The above definitions follow trends in how to define crypto assets in the UK and EU. We believe that the method of defining “crypto asset” in this paper is incompatible with the current (and potential future) use of crypto networks and also differentiates from the approach taken by other jurisdictions.

We submit that the valuable “asset” in any crypto network is the information recorded on the shared ledger. Accordingly, using the paper’s own terminology, a “crypto token” should correctly be the “asset” in the ecosystem, irrespective of the token system.

Q5a. Response

We believe that there is limited benefit in creating a bespoke taxonomy for two main reasons:

1. Difficulty in keeping up with innovation. The crypto industry is constantly evolving and new projects and technologies are emerging all the time. It will be very difficult to keep a bespoke taxonomy up-to-date and relevant as the industry evolves, which can lead to outdated or incomplete classifications. As an example, the classification of the Bitcoin network in this paper as a cryptocurrency network may already be in doubt with the development of Ordinals (can be thought of as a Bitcoin NFT) within the last few weeks.
2. Lack of an agreed standard. A bespoke taxonomy requires widespread adoption and should be an agreed standard across the industry. Given the global nature of the crypto ecosystem, it is likely that jurisdictions will have varying taxonomies, leading to confusion and inconsistency in how different projects, tokens and technologies are classified and understood.

Q5b. Response

As we do not agree with a bespoke taxonomy, we are of the view that a standalone regulatory framework would not assist in balancing regulation with promoting innovation.

Q5c. Response

We believe that specific regulation should cater for one or more parts of the crypto ecosystem that can be clearly defined e.g. exchanges, stablecoins, disclosures, etc.

Q6a. Response

We do not believe that the tokenised version should be treated in the same way as the asset backing it. That conflates a digital information with the real world asset. The digital information is simply a right, most likely in contract, to the real world asset and should be treated accordingly.

Q6b. Response

A degree of reforms are necessary. Reform should focus on requiring disclosures to inform consumers and audits to confirm to consumers that an issuer can meet their obligation.

Responses from

Q14a. Response

For the most part, an on-chain, smart contract-based exchange such as an AMM has very similar risks to a centralised exchange (colloquially "CEX"). However, the key differences lie in how these risks arise.

One example of this is liquidity risk. Both can suffer from price slippage on certain assets offered for exchange if there is insufficient liquidity. However, common difference between the two is the source of liquidity for those markets can vary. Most CEXs will engage and sign agreements with one or more centralised market makers to provide liquidity to certain order books. In this scenario, the liquidity is permissioned. While some projects may also engage with market makers to provide liquidity for their tokens, AMMs have the advantage of a permissionless environment where by liquidity can also be provided by market participants, in exchange for a portion of trading fees collected.

Another example of risks shared by both sides is the potential for loss of assets from technical bugs. Losses from a CEX commonly occur when a team member is successfully attacked by a malicious actor and gains access to the assets of the exchange but can be mitigated by good hot-cold wallet OpSec practices. Because a customer of the CEX is trusting them with deposited assets, this risk comes across in the form of counterparty risk. With an AMM, however, the same risk lies in the potential for the underlying smart

contracts containing errors in the code being exploited by a malicious actor and the assets drained from that particular liquidity pool.

Q14b. Response

The most common data points for both CEXs and AMMs can be found in price action. Depending on the asset, this can be easily accessed through platforms like Tradingview. Due to the open-source nature of AMMs, data from any transaction can be pulled permissionlessly into any new data aggregator or analytics platform. AMMs tend to have their own siloed analytics pages but there are also products like Dune and Arkham that aggregate data from various different AMM platforms (among many other on-chain data points) that allow users to get customised information that they wouldn't normally get from a CEX.

Responses from

Q1. Response

Supporting Innovation with digital assets as a technology platform supporting multiple use cases.

Q2. Response

Warning on potential loss of funds when funding digital asset network through fiat on ramps. Consumers have enough agency to conduct themselves in gambling venues so its arguable they have enough agency to conduct themselves in the digital asset space.

Q3a. Response

A self regualting industry body that collates code auting and other screening capabilities, like the LSEG digital assets screening methodology used to screen digital assets for inclusion in FTSE Russell Indices - this screening is required to comply with EU and UK index regulations. See https://research.ftserussell.com/products/downloads/Guide_to_the_Vetting_of_Digital_Assets_and_Digital_Asset_Exchanges.pdf

Q3b. Response

Require exchanges to conduct enhanced due diligence on teams behind a token being listed. Transparency on listin rules (e.g fees / token swaps required), conduct screening similar to the FTSE Russel digital asset screening methodology - https://research.ftserussell.com/products/downloads/Guide_to_the_Vetting_of_Digital_Assets_and_Digital_Asset_Exchanges.pdf

Q5a. Response

Using a taxonomy aligned with the financial services (e.g. the LSEG FTSE Russel taxonomy) ensures the digital asset industry is aligned with the financial services. This supports future invesment from the institutional services and a foundation for future regulation if some assets are deemed as security-like. The LSEG FTSE Russell taxonomy is a core part for the Eikon platform taxonomy sitting alongside global industry classifications like the Reuters Instrument Code (RIC), Global Industry Classification Standard (GICS), ISIN, CUSIP, SEDOL and PermId identifiers.

Q5b. Response

digital assets are classified seperately to equities in LSEG systems today. As a technology, the range of digital asset use cases is broad and many are not suitable for LSEG to classify as another investment class (e.g. equity, fixed Income). Formation of a new regulatory framework to manage digital assets seperately from the institutional grade instruments is prudent, enabling innovation at the same time as grading digital assets into the correct instrument type over time.

Responses from

Q1. Response

regulation should simply be applicable to the type of token, its application and use, and locality.

In the first instance, there are use cases for crypto that matches existing legislation, let those apply, i.e. shares/equity, commodities, cash

In the second instances, there will be use cases that cannot map to these use cases. The government should provide a sandbox as they do for normal financial products, which allows companies to develop these new innovations, collaborating with the government to allow regulation to be evolving in lock-step.

Also see Q2, potential safeguards.

Q2. Response

It depends on the application of the tokens:

If the tokens represent shares/equity for a local company, then it should apply regulation that currently applies to shares/equity.

If the tokens are used as a payment mechanism such as cash, it should have the light touch regulation that currently applies to cash.

If they are used as a store of value, similar to gold, then similar regulation should apply.

There are also smart contracts that act as financial instruments/bank accounts, if these originate in Australia, they can also be regulated as such, requiring financial services /banking licences.

It is fairly simple to look at the smart contract code to classify/verify a classification of a token and or smart contract.

Q3a. Response

I recommend an "allow list" of tokens under 4 classifications. Some tokens can be allow-listed to start with, such as USDC, and there should be a process by which a token/smart contract can apply to be added to such an allow list with appropriate vetting.

Code can be audited to confirm whether the token does what the application says, and it can refer to a specific smart contract address (assuming it is not an upgradeable contract).

The 4 classifications would be:

1. payment token - similar to cash
2. Shares/equity - tokens that represent shares that are consider to be publicly listed, and that carry the same responsibilities and disclosure requirements as companies that are listed on the ASX.
3. commodity tokens - similar to buying gold.
4. financial contracts - similar to bank accounts that offer interest paid on deposits.

There can be minimum standards for what a smart contract has to contain to be easily allow-listed - such as a function that allows tokens that were accidentally transferred to be returned.

Allow lists should only apply to exchanges - which themselves would need AFSL licences to operate, and they can facilitate retail investors to purchase allow-listed tokens or interact with allow-listed smart contracts.

As part of their responsibilities to keep their licence, exchanges/onramps would need to explain to users that transferring tokens to their own wallets and exchanging them for non allow-listed tokens represent a great risk.

This would provide a reasonable framework for retail investors to be protected, but also allow retail investors to acknowledge and accept the risk of moving outside of that protected world, enabling them to support innovation much like the USA crowd funding."

Q3b. Response

See A. Scams happen outside of crypto also. Having a framework - to clearly identify vetted tokens/contracts, and require explicit acknowledgement of the risks when venturing outside of that framework - can protect against scams the same way having regulations and frameworks to guard against scams by publicly traded companies.

Q5a. Response

Each application of a smart contract can be understood, and if it acts as equity/shares, or any other known application, it can be regulated as the current industry is regulated.

If it falls outside that, it can be clearly identified as something new and therefore be fostered as innovation whilst managing consumer risk collaboratively.

Q5b. Response

Refer to answers 2 and 3.

Q6a. Response

Currently all tokens are treated as security, it is prohibitive for innovation to classify tokens that wrap assets that are not securities, as such.

Q6b. Response

Real world obligations should just be applied as is if it is relevant.

Q7a. Response

see question 3 A, allow list could also require an easy to understand PDS.

Q8a. Response

There are smart contracts that specifically act as financial products, by managing loans that require interest payments, that pay interest on deposits etc. These can and should be treated as financial products.

Q12a. Response

Compliance would make it easier for a smart contract to be allow-listed. Similar to answer 3 A)

Q12b. Response

Smart contracts can be audited to confirm that they do what is stated in the PDS

Q13a. Response

It is more transparent what a smart contract does. A pawn broker can operate outside of the law by keeping certain activities "off the books", where all activities on chain are visible and transparent.

Responses from Scio Consulting / MakerDAO

Q1. Response

The government has a responsibility to protect the weakest, most vulnerable and lesser informed sectors of society with regards to risk taking and understanding of risks affecting both households and businesses.

It is expected therefore that the government take a guiding and principled approach, so that the technology can evolve while ensuring some level of reassurance for the weakest sectors of society e.g. uninformed consumers. For example, establishing clear guidelines and regulations regarding the use and exchange of crypto assets, especially regarding anti-money laundering (AML) and counter-terrorism financing (CTF) regulations as well as guard rails for fraud prevention that impact consumers and by extension confidence in the markets are a good start for virtual asset providers.

Beyond that, providing a principles-based approach to regulation of financial service providers and financial markets that allows room for technology development is certainly advisable. There is a significant amount of innovation using the technology that might lead to the development of financial products that currently have no existing parallel in the marketplace. Establishing a sandboxed approach to newer services where service providers, industry bodies and regulatory agencies can collaborate, validate, monitor evolution and design policy that is fit for purpose and functional to these newer products would provide the best outcome for both the marketplace, consumers, businesses and market actors. All in all, for such evolution and innovation to flourish, basic principles on guardrails and an interaction framework should be in place so innovators know what, when and how they can approach authorities when developing solutions without the operational and consumer risks associated with an abrupt end in operations.

Last but not least, any functional and principles-based approach developed by the government should take into account new forms of organisation of innovation e.g. DAOs and open source communities. This is the key novelty in this interaction to which traditionally regulators were not exposed. Traditional financial service providers interacted with regulators through the umbrella of centralised entities (LPs, Trusts, Incorporated Societies etc). In a world where the core of the innovation is being driven by globally-distributed open source communities such as DAOs, there needs to be a different framework for engagement to ensure the same levels of guardrails applied to fraud protection, market abuse protection, consumer protection is also reflected in the organisational setup and interaction framework.

In summary, the role of government in the regulation of the crypto ecosystem should strike a balance between promoting innovation, and how innovation happens, while protecting consumers and maintaining the integrity of the financial system.

Q2. Response

The principle of same function, same regulation and same safeguards should be applied when it comes to consumer and investor protection, so long as the functions are appropriately mapped to similar services.

Some potential safeguards for consumers and investors could include:

1. Regulation: Governments could either introduce or reiterate existing policies and regulations to protect investors and consumers from unethical and fraudulent activities. This would give market confidence and democratise access to financial services at lower costs, which is one of the benefits of crypto assets, while also embedding into existing service providers obligations and discipline to dealing with consumers and unsophisticated investors. This could include more regular background checks, financial audits or other monitoring activities on companies providing services and products in the marketplace. However, such monitoring and operational compliance should follow similar principles applied to financial services institutions i.e. the bigger and more systemically important players also require higher levels of safeguards and surveillance.

2. Transparency: Companies could be required to provide clear and comprehensive information and disclosure about their products and services, including risks and benefits on a like-for-like basis with regulated operators. This would help consumers and investors make informed decisions. Additionally, operators would be nudged into enforcing transparency by design through for example exposing smart contract parameters in order to prove diligence and transparency to both regulators and the public. This programmatic transparency would reduce their compliance risks and operational costs, therefore enabling innovation.

3. Education: Investors and consumers should be educated about financial products, services, and investment strategies by operators. Financial literacy (or lack thereof) is one of the core reasons for consumer losses in risky asset classes. Designing principles into policy that nudges providers to educate communities, particularly where novel products are developed, would significantly reduce the risks of unexpected losses.

4. Technology: The technology itself could be used to develop innovative and programmatic solutions that make financial markets more transparent, accessible, and secure. For example, within the appropriate frameworks, blockchain technology could be used to promote good decentralised, peer-to-peer financial systems and best practices within operators. An example would be using a (or set of) labelling mechanisms for cybersecurity of peer-to-peer contracts that have been thoroughly tested and whitelisting those for use by regulated financial providers over less audited solutions.

Overall, there are many potential safeguards that could be put in place to protect consumers and investors. Ultimately, the goal should be to create a fair and transparent financial system that benefits everyone.

Q3a. Response

Yes, there are a few solutions that could be applied to safeguard consumers who choose to use, store, invest or trade in crypto assets:

1. Mandatory Disclosure: Enforcing disclosure of relevant information about digital assets by financial operators benefiting the most from market trading volumes (e.g. on-ramp, off-ramps) could be implemented. Such disclosures would enforce a level of sophistication into operators that is currently very variable operator to operator. Disclosures could include things such as understanding and communicating about tokens and contracts code audits, legal and financial disclosure on risks of underlying assets. Crypto service providers such as exchanges would be required to thoroughly investigate, monitor technological developments and disclose important details about the crypto assets products offered to their end consumers before listing them. Disclosure could include things such as features, contract ownership, security and financial risks associated with the underlying products.

2. Code Auditing: Regular audits or at least higher focus on code security outcomes could be applied to frontend operators such as DeFi UI providers and exchanges offering tokens to purchase. Crypto ecosystems are constantly developing and smart contracts are constantly being integrated, creating composability risks (i.e. money legos). Higher transparency and visibility on code security of these contracts would guarantee higher probability of consumer protections through front end websites. Without going as far as enforcement, regulators could work with the industry to rank code auditing firms on their capabilities and depth of testing abilities for critical contracts and transparently guide frontend companies on the level of trust that should be given to particular audits. In a certain way, similar to the way the regulators indirectly recommend a set of ratings agencies for financial services.

3. Regulatory Requirements: Regulators could require crypto-related businesses dealing with consumer investors to meet specific security and consumer protection standards. These regulations could go beyond the existing Know-Your-Customer and Anti-Money Laundering guidelines to include additional requirements, such as requiring exchanges to disclose their insurance policies or utilise independent asset's management solutions.

4. Insurance Protection: Insuring digital assets to protect against loss, theft, or other risks is a solution that is growing in popularity with many insurance companies offering such services. This would provide an additional layer of protection for the consumer in the event of a catastrophic loss. There exist both DeFi and centralised solutions in the marketplace. The big question is then guardrailing the insurer to avoid excess risk taking similar to the GFC scenarios on CDS/CDOs.

Overall, a combination of disclosures, code auditing and quality review, appropriate insurance protection, and consumer education could go a long way in safeguarding consumer interests in the crypto asset ecosystem.

Q3b. Response

As stated previously, with a few additions, a set of options could be considered on the regulation of exchanges:

1. Licensing and Registration: Governments can require crypto token exchanges to register and obtain licences to operate that are relevant to the function of the services they provide. Exchanges must meet specific criteria, including security measures such as anti-money laundering (AML) and know-your-customer (KYC) policies.

2. Disclosure and Transparency: Crypto token exchanges must disclose information to users about risks involved with buying and investing in tokens, including complete information on the token issuer and its finances, project details, financial and non financial risks.

3. Anti-Fraud Measures: Exchanges must have efficient monitoring and surveillance systems to counter illegal activities and fraudulent activities.

4. Education: Governments and regulatory bodies can focus on educating, or partnering with private sector businesses, to educate the public about the risks involved in investing in cryptocurrencies and scams associated with crypto investments. This includes consumer education campaigns highlighting what to look out for when investing in tokens, ICOs or newer variations of offerings.

5. Legal Framework: Establishing clear legal regulations for the trading, buying, and selling of cryptocurrencies and tokens. This includes creating legal ways that consumers can seek recourse in case of fraudulent token offerings. A robust legal framework combined with transparency and consumer education would act as a deterrent to scams.

Q4a. Response

One possible way to define crypto tokens and crypto networks for the purposes of future legislation is by emphasising the concept of "exclusive use or control" of a public record or data (i.e. token). Specifically, a crypto token could be defined as a digital representation of a specific asset or utility that is recorded on a blockchain or distributed ledger system, and that provides its holder or contract with exclusive rights to use or control the underlying asset or utility.

In our view, however, the consultation paper uses an “exclusive” definition that is too narrow as it focuses on a “person”. In reality, the concept of “exclusive use or control” should be broadened to include businesses or multi-parties (e.g. multisig relationships) as well as smart contracts (i.e. applications). A smart contract application can actually be an exclusive owner and controller of assets. There are many examples of such applications where the code (i.e. smart contract) has ownership rights over tokens with rights to distribute assets, if needed or intended, but no obligation (e.g. Tokens created as staking rewards).

Similarly, a crypto network could be defined as a decentralised system that uses cryptographic protocols and consensus mechanisms to enable secure and exclusive access to shared data or resources running on the network.

In summary, by emphasising the concept of exclusive use or control but broadening its scope of ownership and exclusivity, future legislation could aim to create clear rules and standards for the issuance, trading, and governance of crypto tokens and networks, while also protecting the interests of users, investors and innovators.

Q4b. Response

Benefits:

1) It allows for decentralised control and ownership of data (or system of records) in the form of tokens with a "registrar" that publicly records to the rightful owner(s) of assets and their actions.

2) It promotes transparency, auditability and accountability as all transactions on the network are recorded on a public ledger.

3) It creates a unique value proposition for investors and users, as they have a stake in the network and therefore become co-owners and, to an extent, "citizen auditors" of the underlying networks where their assets are recorded.

4) It can incentivise developers, contributors and entities (e.g. companies, foundations, academia) to continuously improve and innovate on the network while maintaining its security and attractiveness to entrepreneurs building applications.

Disadvantages:

1) It can create regulatory challenges and uncertainties, as governments may view such networks as potential threats to monetary and financial stability, if poorly understood.

2) It can create barriers to entry for new entrants and incumbents in financial institutions, as they need to speed the rhythm of innovation to catch up with existing players that adopted the technology earlier and now have a moat.

3) It can create privacy breaches and litigation challenges for lawmakers and companies as private information is recorded publicly on crypto networks without the consent of rightful data or token owners.

4) It can lead to concentration of power and influence among a small group of individuals or entities who hold a significant percentage of the crypto token supply at either the network level or the smart contract protocol level. This could have an impact on network/protocol security but also on governance when it comes to change to the contracts (e.g. upgradeability, parameter changes, risk appetite etc). This could therefore impact owners or application builders while not giving them a "say" into those changes.

Q5a. Response

At this stage, we are of the opinion that a fully bespoke taxonomy is not required for crypto assets. We understand that a high-level, principles-based and functional based approach is appropriate so long as it does leave space for sandboxed innovation where the assets or functions observed cannot be directly mapped to an existing financial product as defined in the paper. As an example, the fractionalisation of ownership in the digital arts industry might not be covered by mapping to existing products.

Should the Government consider a more detailed taxonomy, here are a few supporting reasons for the value of a bespoke crypto asset taxonomy:

1. Clarity and Consistency: A well-defined taxonomy can provide clarity and consistency across different regulatory jurisdictions, making it easier for businesses and individuals operating globally, as is the case for many digital asset service providers, to understand and map out regulatory requirements across borders and be responsive to policy makers.

2. Risk Management: A bespoke taxonomy can help regulators identify and categorise the various types of crypto assets as a helpful internal exercise. This would allow government agencies to be proactive in distributing mandates for oversight according to an existing mapping exercise. The downside to such exercise is the extra operational requirements on the regulators to keep up pace and maintain a constant adaptation of the taxonomy to keep up with the opensource evolution of these protocols.

3. Investor Protection: A clear classification system can help inform and protect investors by providing them with consistent and accurate information about the underlying assets of a crypto asset, as well as their rights and protections under law. This could reduce the possibility of fraud by market operators. However this is also achievable in a non-bespoke setting.

In the case of a non bespoke taxonomy, here are alternative views on the value of a bespoke crypto asset taxonomy:

1. Lack of Standardisation: One could argue that the lack of standardisation in the crypto asset market makes it difficult to create a consistent and meaningful taxonomy that can be applied across different jurisdictions. It would therefore make the ongoing work of regulators domestically more challenging as it would require a constant adaptation of their taxonomy.

2. Limited Impact: A bespoke crypto asset taxonomy may have limited impact, as many crypto assets are designed to operate internationally, often outside the remit of domestic financial regulatory frameworks. The impact could therefore be limited to what the paper calls intermediated token systems, operating domestically.

3. Regulatory Overreach: Some critics argue that attempts to regulate the crypto asset market through a bespoke taxonomy could be seen as regulatory overreach and may stifle innovation of market operators. This will be particularly acute in areas where the mapping

of existing financial products may not be applicable to new kinds of tokens, protocols or forms of coordination e.g. DAOs.

Q5b. Response

As stated in the previous section, in our view the creation of a standalone regulatory framework that relies on a bespoke taxonomy may not be effective in regulating the fast-evolving crypto industry. A principles-based and functional approach, as outlined by the paper, seems more fitting for a constantly evolving ecosystem.

While a clear and concise categorisation of crypto assets can aid in understanding their underlying features and risks to regulators and the public, regulatory measures must also take into consideration the unique features and use cases of each asset on a functional basis. A one-size-fits-all approach may not be practical in such a diverse and complex industry. Therefore, a holistic and functional approach combining fit-for-purpose assessments, and coordination between regulators and industry stakeholders could offer more value in formulating a regulatory framework that evolves alongside other financial services.

Q5c. Response

When it comes to financial uses of crypto networks and assets, regulatory certainty can be achieved by using mostly regulatory frameworks that are already in place for other types of assets such as commodities, securities, or property. Such frameworks cover areas such as consumer protection, tax compliance, property rights, and data privacy.

For non-financial use cases, such as digital identity portability or provenance tracking, certain frameworks covering existing financial products, such as consumer protection and data privacy could be leveraged as well. They would provide an additional layer of clarity and consistency from regulatory bodies on how existing laws and regulations apply to crypto networks but also provide assurances to individuals and businesses leveraging that technology when providing new solutions.

Lastly, it will be important for the regulator to collaborate with the industry and observe the changing nature of certain types of crypto assets. While assets can be initially categorised as “non-financial”, the financialisation of assets can lead a crypto asset to “become” a product. Therefore any assessment will need to take into account the changing nature and characteristics of its use with time. For example, a governance token in a DAO might initially have characteristics of identity for voting purposes. With time the same token could be financialised and traded as a product.

Q6a. Response

Wrapped real-world assets or “tokenised” real-world assets are widespread in the cryptocurrency market as they offer the benefits of blockchain technology (e.g. fast settlement, reduced counterparty costs, automation) while still being backed by assets,

securities, goods. However, there are concerns about the regulatory treatment of these assets compared to the ones they are backing.

Oftentimes they lack the same level of consumer and investor protection associated with their underlying assets. This is particularly clear in the biggest class of real-world assets, fiat-backed stablecoins, where different types of arrangements and guarantees abound across issuers.

Another potential issue is that the regulatory treatment of wrapped assets may vary across different jurisdictions, leading to regulatory uncertainty for investors and issuers alike. For example, should a holder of a wUSD token have redemption rights guaranteed in the USA via FDIC insurance would the same be applicable in Australia? If the underlying asset is regulated in a particular way, it may be necessary to ensure that the wrapped asset follows suit.

Similarly, should the same guarantees be applicable to wrapped real-world assets and underlying assets, it is also expected that similar obligations follow suit. In the case of stablecoin issuers for example, they might be subject to similar regulatory requirements as financial institutions providing deposit taking services.

Other reforms that may be applicable, depending on the type of real-world asset:

Oversight over issuers, custodians and other counterparties: In the case of stablecoins for example the lack of oversight may raise questions about potential fraud, manipulation, and custody of the assets. One possible reform could be to establish a clear and harmonised legal framework and oversight mechanism that covers the issuance, trading, and custody of wrapped assets.

Disclosures enforcement: An enhanced framework would need to ensure that investors have transparent information about the underlying assets, their custody, and the process for unwrapping the assets. Additionally, it would need to set out clear standards for audits and risk management to reduce the risk of fraud and manipulation.

Building on existing frameworks: Another potential reform could focus on strengthening the existing regulatory framework for traditional asset-backed securities, which might apply to some wrapped real-world assets. This would involve requiring higher standards of disclosures, transparency, data reporting and supervision, as well as imposing penalties for any breaches of these standards.

Overall, it is crucial to ensure regulatory clarity and consistency for wrapped real-world assets to promote investor protection and market integrity, and to increase the likelihood of widespread adoption of these instruments given the market efficiencies they create.

Q6b. Response

As mentioned above, we believe that enhancing existing frameworks where similar guarantees and rights applicable to issuers of wrapped assets should come hand-in-hand with obligations. In the case of wrapped real-world assets backed by traditional securities, this could involve implementing stricter regulations and oversight, as well as requiring

issuers to have adequate reserves or insurance to cover any potential defaults or counterparty risks (e.g. bank run). In exchange for increased oversight and stricter obligations, such counterparties might be eligible for government insurance for example.

This framework however might prove too strict for other types of wrapped real-world assets e.g. event tickets or coupons. Ultimately, it will depend on the specific circumstances and risks involved with each type of wrapped asset.

Q7a. Response

In our view, crypto asset service providers should ensure that their users can access information that helps them identify the arrangements underpinning crypto tokens, particularly for wrapped assets. This is important to ensure transparency and protect users from fraud, misrepresentation and other financial risks.

To achieve this, crypto asset service providers could use at least two strategies:

First, they should provide clear and easy-to-understand documentation on how their token systems work, including details on any intermediaries involved. They can also provide access to third-party audits or certifications that verify the legitimacy of their token systems. This documentation and risk statement disclosure should be as widely available as possible to users and holders of these assets, regardless of whether they are the contracted counterparty or an investor that has acquired the wrapped assets through the secondary market.

Second, a more technologically sophisticated means to ensure information is widely distributed, whether assets are accessed through primary or secondary market, would be to enforce asset service providers to embed disclosure statements within the metadata of the wrapped tokens themselves. Therefore, any user at any stage in the asset cycle would have access to equal information (i.e. contracts, audits, certifications etc).

Additionally, regulators can require crypto asset service providers to disclose certain information about their token systems, such as the identity and roles of intermediaries, transaction fees, and security measures. This would enable users to make informed decisions about the risks and benefits of using specific token systems.

Q7b. Response

Some initiatives that crypto asset service providers could take to promote good consumer outcomes include:

1. Transparency: The service providers can disclose all their operation details in a clear and concise manner. They can provide information about the fees, risks, and benefits of using their platform and wrapped assets offered therein.

2. Security measures: The providers can take best-in-class security measures to protect the consumer's assets. This can include implementing clear separation between entities

trading and the ones hosting assets, multi-factor authentication, use of multi-signature wallets, cold wallets, multi-party computation.

3. Arm's length relationship: Maintain clear distance between asset service providers and their counterparties for accountability and transparency. This relationship would avoid the commingling of assets between related parties e.g. FTX, Alameda. A clear separation of entities avoids any conflicts of interest or engaging in any activities that could compromise the service provider objectivity, integrity and misuse of consumer assets. To ensure the arm's length, asset service providers would make use of independent legal and financial advisors, and periodic evaluations of the relationship between counterparties.

4. Regulatory compliance: The service providers can comply with all the existing applicable laws and regulations relative to the financial products offered. Also, service providers should be licensed appropriately according to the activities they carry out. Both would help build trust with the consumers and avoid any legal scrutiny.

4. Customer support: Crypto asset service providers can offer prompt customer support to address any queries and ensure that their consumers have an appropriate experience, in pace with the industry where they operate in. Given these markets operate non-stop, asset service providers would require support 24/7.

5. Education: The providers can educate their consumers about the risks and benefits of both the wrapped assets as well as the underlying asset class being tokenised. This would help consumers to evaluate their portfolios better as well as become more sophisticated investors e.g. in the case of tokenised securities

Q8a. Response

Some intermediated crypto assets, such as security tokens and asset-backed tokens, may warrant specific definitions as financial products.

Although such asset-backed tokens often possess key characteristics of the underlying financial products, including offering ownership or rights to assets, returns or profit-sharing, they are frequently not perceived as subject to similar regulations and investor protections by holders. This leaves asset holders at the mercy of market dynamics and facing a variety of asset-backed offerings that from an unsophisticated eye may appear similar and guarantee similar obligations and guarantees. But in reality follow a wide spectrum of setups.

Better defining these intermediated asset-backed crypto assets as financial products would provide greater clarity and regulatory oversight, potentially mitigating risks for investors and promoting greater market stability.

Q8b. Response

In general, we believe most intermediated crypto asset services can be defined within the remit of existing regulation defined under the Corporations Act, such as making financial investments or managing risk for customers.

Given the technology enabled by smart contracts and the reduction in the cost and need of some types of intermediary services (e.g. settlement, clearing, account management), we believe some obligations might need to be enhanced to ensure appropriate processes are in place at issuers of wrapped assets. This might include things such as greater smart contract security and auditing of internal operations. Now certain services that used to be carried out by third parties are carried out by technology. This requires asset service providers to be on top of those obligations to guarantee market integrity and confidence to consumers. We believe enhancing existing rather than rewriting obligations to be more appropriate here.

Q9. Response

There are several factors to consider when assessing the suitability of a specific public crypto network to host wrapped real-world assets. Wrapped real-world assets such as stablecoins or asset-backed securities address by their own nature significantly bigger markets than existing crypto assets. Therefore it is expected they will attract in the longer run significantly more liquidity and trading activity than existing crypto assets. That raises financial stability and market integrity considerations in the medium to long-term. Should the bulk of the liquidity for these assets be hosted natively on immature or historically unproven public networks, financial stability risks are raised in our view. This does not mean however that certain public networks should be specifically banned, but possibly caps should be considered while such networks are under a “testing” phase, until they can be considered suitable for greater liquidity.

Some factors to consider include:

1. Security: A key consideration is the security features of the network, such as its consensus mechanism, governance structure, and level of decentralisation. Since wrapped real-world assets have real-world value in their underlying assets, it is important to ensure that the network hosting them is secure and resilient to collusion or attacks.

2. Performance: The network’s performance metrics such as transaction speed and capacity are also important to ensure that it can handle the volume and speed of transactions required for wrapped real-world assets. The performance requirements here will be dependent on the nature of specific real-world assets. For example, the number transactions on stablecoins have a higher throughput than investments in asset-backed securities, though the volume might be lower.

3. Compliance: Compliance with relevant regulations and laws is crucial, especially for assets that have regulatory requirements, such as securities or other financial instruments. Here it is important to have a parallel to implementations occuring in other jurisdictions to avoid real-world asset liquidity to be “trapped” in certain networks due to restrictions imposed by other regulators.

4. User base of real-world assets by type: The network’s existing user base and adoption rate could also be important to assess its potential demand for real-world assets. While

transactions in real-world assets such as stablecoins will have a large retail base, it is more likely that securities such as bonds will be dominated by institutional or wholesale counterparts. This might reflect in the networks where these assets will be hosted.

5. Transparency: The network's level of transparency and auditability is essential to enable adequate oversight and monitoring to prevent fraud and other illegal activities. The auditability requirements might be also higher depending on the underlying financial product.

In summary, a thorough assessment of a public crypto network's security, performance, compliance, user base, and transparency would be vital in determining its suitability to host wrapped real-world assets.

Q10. Response

Intermediated crypto assets are relatively new and can involve complex arrangements. Therefore, there may be a need for limits, restrictions or frictions on the investment by consumers in relation to any arrangements that are not covered already by the financial services framework. This can protect consumers from potential fraud or abuse, ensure market stability, and prevent systemic risks to the broader financial system.

The specifics of these limits, restrictions or frictions would need to be carefully assessed on a case by case basis, balancing innovation and consumer protection.

Q11. Response

We believe that there needs to be a separation between analysis applied to public network tokens and public smart contract applications.

Implementing regulatory frameworks that address the marketing and promotion of products within the crypto ecosystem regarding public networks (e.g. Ethereum, Bitcoin) should be developed in a nuanced way before a suitable solution applies for Australia. It should consider the balance between "public good" vs "private interest" in the development of public networks. Given public networks serve primarily a technically functional objective (e.g. transferability, platform for deployment of smart contracts, ecosystem security), they should be regarded differently to applications or protocols developed to fulfil primarily financial functions e.g. DeFi contracts.

If this distinction is carefully considered, this will help protect consumers from fraudulent activities and ensure that investors are provided with accurate and transparent information regarding the risks of investing in either one type of ecosystem or the other.

The implementation of these frameworks should follow the principles of transparency, accountability, and proportionality. Regulators should be transparent about their objectives, the scope of their powers, and the criteria used in analysis and decision-making.

The regulatory framework should also ensure that marketing promoters are held accountable for their actions in cases where a promotion is misleading or bluntly fraudulent (e.g. a "DeFi" protocol that is effectively "intermediated" by a set of owners).

Equally, in such cases consumers should be provided with access to dispute resolution mechanisms.

The implementation of regulatory frameworks can be achieved through various measures such as licensing requirements, disclosure obligations and restrictions on advertising and promotions depending on the kind of primary functions of ecosystems.

In conclusion, implementing regulatory frameworks that address the marketing and promotion of products within the crypto ecosystem requires nuance and clear distinction between public good networks (e.g. Bitcoin, Ethereum) and clear financial applications. It can help protect consumers, promote transparency and accountability, and ensure that investors are provided with accurate information. The implementation of these frameworks should follow the principles of transparency, accountability, and proportionality.

Q12a. Response

There are several regulatory and policy levers available to encourage the development of smart contracts that comply with existing regulatory frameworks. These include:

1. Education and outreach: Ensuring that developers and bootstrapping teams are aware of the regulatory frameworks and requirements that apply to smart contracts can lead to the development of compliant contracts. Use of sandbox approaches ensures that startup teams can approach regulatory bodies to validate assumptions before scaling their applications.

2. Incentives: Innovation agencies can work alongside regulators to offer incentives for developer teams who create smart contracts that comply with existing regulations. For example, they may provide funding, mentoring and recognition to teams developing compliant contracts. This “promotion by example” helps build trust in teams making an extra effort to map regulatory requirements with innovation.

3. Risk benchmarks: Regulators can work with the industry counterparties such as auditing firms to conduct risk analyses and promote ratings that reflect an understanding of the risks associated with smart contracts protocols. Therefore doing a gap analysis and promoting the development of publicly compliant contracts via innovation funds.

4. Collaboration: Collaboration between regulators and developers can lead to the development of more effective regulatory frameworks that support the development of compliant smart contracts while also supporting innovations in financial services.

5. Enforcement: Once the ecosystem develops and good standards are clearly recognised for financial products, regulators could use enforcement actions as a means to encourage compliance with regulatory frameworks either through the intermediated crypto services providers or foundation teams developing software.

Overall, a combination of education, incentives, risk analysis, collaboration, and enforcement can encourage the development of smart contracts that comply with existing regulatory frameworks.

Q12b. Response

There are different regulatory and policy levers that can be used to ensure smart contract applications comply with existing regulatory frameworks. These include:

1. Legal frameworks: Governments can enhance existing legal frameworks that determine which principles and functions should be catered by smart contracts for the types of financial products developed. These frameworks should take into account existing laws and regulations concerning contracts, property rights, and data privacy.

2. Standards and certification: Standards and certification can be leveraged to ensure that smart contracts meet certain quality, regulatory compliance and security criteria. This can be done by industry organisations, governments, independent firms or accreditation bodies.

3. Auditing and testing: Smart contracts can be audited and tested to ensure that they are operating as intended and are free from bugs or security vulnerabilities. Depending on the financial products developed and the outreach in terms of financial stability, these requirements could be more or less stringent.

4. Regulatory oversight: Regulatory authorities can oversee or appoint parties that oversee and report back the use of smart contracts to ensure compliance with existing laws and regulations. This can include monitoring for fraud, misrepresentation, or non-compliance with consumer protection laws. It is important to consider here the upgradability of these ecosystems and therefore how oversight will be applied across opensource contracts.

5. Incentives for self-regulation: The industry can adopt self-regulatory frameworks that establish guidelines for the development and use of smart contracts. These frameworks can be enforced by industry bodies, and can complement existing legal and regulatory frameworks. However, self-regulation on its own will not suffice.

Q13a. Response

There are several key risk differences between smart-contract and conventional pawn-broker lending:

1. Transparency: Smart contracts are transparent and tamper-proof, which provides more transparency for both the lender and borrower. In conventional pawn-broker lending, there is often a lack of transparency regarding the terms and conditions of the loan and the valuation of the collateral. Whereas in a smart contract, risk parameters are pre-defined and collateral valuation is determined by oracles that are constantly feeding the contracts with the real time price of the collateral pledged.

2. Automation: In most smart contracts both lending and collateral liquidation is entirely automated and eliminates the need for intermediaries on both origination and debt recovery. This can reduce costs and improve efficiency of the system. In conventional

pawn-broker lending, intermediaries such as pawn shops can add additional fees and costs to the loan.

3. Security: In smart contracts the collateral is secured through the use of cryptography and blockchain technology in “vaults'' or “asset pools”. Whereas in pawn-broker lending, the physical collateral such as jewellery or other valuable items can be lost, stolen or damaged. Of course, the security of collateral in vaults and pools is only as secure as the smart contract practices that allowed their development.

4. Dispute resolution: smart contract lending does not provide a dispute resolution system through the courts but the transparency in the public blockchain and oracles network provide a mechanism for assessing misappropriation of collateral. In conventional pawn-broker lending, the resolution of disputes is often done through informal negotiations or through the court system.

Overall, smart contract lending provides more transparency, security, efficiency, and reliability than conventional pawn-broker lending. However, when it comes to dispute resolutions, few jurisdictions provide a framework to protect consumers of smart contract protocol errors.

Q13b. Response

Unfortunately, I do not have access to any quantifiable comparative analysis on consumer outcomes in conventional pawn-broker lending versus user outcomes for analogous services provided through smart contract applications. However it is a valuable research topic.

Q14a. Response

There are several key differences in risk between using an AMM and using the services of a crypto asset exchange, including:

1. Counterparty risk: When using a crypto asset exchange, there is a risk that the exchange may become insolvent or provide fraudulent financial information e.g. FTX resulting in the loss of user funds should the exchange offer custodial wallets. On the other hand, AMMs do not offer custodial wallets and do not rely on a central entity holding or trading user assets, which reduces the counterparty risk.

2. Liquidity risk: AMMs derive their liquidity from the users (aka Liquidity providers) who deposit tokens into the liquidity pools. If there are not enough participants in the pool or if the pool size is too small, there may be liquidity and slippage risks for traders. Liquidity providers on their end may suffer impermanent losses if imbalances in the pool are significant and deviate from the underlying offchain asset prices e.g. Stablecoins within Curve. In contrast, centralised exchanges specialise in sourcing liquidity from multiple sources, including other exchanges. While this can guarantee greater liquidity, it can also lead to market manipulation and front running.

3. Pricing risk: AMMs use an algorithm to determine the price of assets in the liquidity pool, which may differ from the market price on a centralised exchange. The AMM algorithms are for their part oblivious to the pricing of the assets offchain. Therefore users who trade with an AMM may face asset price risks, but they can also benefit from these price differences through arbitraging opportunities.

4. Smart contract risk: AMMs are heavily reliant on smart contracts, which are immutable and cannot be changed once deployed. If there were issues or vulnerabilities in the smart contract, there may be significant financial losses for traders and liquidity providers.

Overall, the risk profile of using an AMM is different from that of using a centralised exchange. In the crypto ecosystem, these two services are mostly complimentary to enable capital efficiency. Centralised exchanges may even use AMMs to source some of their liquidity.

Q14b. Response

Yes, there are many resources available on this topic. This may require analysing trading volume, liquidity, transaction fees, slippage, price impact, and other metrics across different exchanges and AMMs.

It is also important to consider the incentive mechanisms and risks associated with using AMMs, including their unique features such as liquidity pools, automated pricing algorithms, and potential impermanent loss.