#Hashlock.

03/03/2023

Re: Token Mapping Consultation Paper Submission

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

The role of the government in the regulation of the crypto ecosystem should be to strike a balance between consumer protection and fostering innovation. The government should provide clear guidelines and standards for the issuance and trading of crypto assets, as well as ensure that intermediaries comply with existing laws and regulations. However, excessive regulation that stifles innovation should be avoided. Instead, the government should encourage self-regulation and industry best practices such as smart contract security auditing to ensure that the crypto ecosystem operates in a safe and secure manner. Ultimately, the goal should be to promote a healthy and thriving crypto ecosystem that benefits both consumers and the industry.

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

We believe that potential safeguards are alluded to in current industry best practices, and the best long term strategy for the government is to just further reinforce and support these best practices. The most common safeguard in the blockchain industry is smart contract auditing, by independent blockchain auditing firms. These audits ensure that scams, malicious code and functionality aren't built into the contracts, and also educates investors and the community about the asset within the report. It can also help to check the code to categorise tokens and systems for the purpose of token mapping. Making this a requirement to be listed on Australian exchanges and used by Australian businesses is a non-restrictive way of simply ensuring the code and token is safe and functions as promised. There is no feasible way to enforce the actual behaviour of project leaders, the least we can do at a bare minimum is ensure that the smart contract and functions are safe and audited.

Q3) Scams can be difficult for some consumers to identify. a) Are there solutions (e.g. disclosure, code auditing or other requirements) that could be applied to safeguard consumers that choose to use crypto assets? b) What policy or regulatory levers could be used to ensure crypto token exchanges do not offer scam tokens or more broadly, prevent consumers from being exposed to scams involving crypto assets?

A) Smart contract audits are a crucial tool in safeguarding consumers in the crypto space. These audits involve a comprehensive review of the code that underpins a particular token or asset to identify any vulnerabilities or weaknesses that could be exploited by bad actors.

B) By requiring smart contract audits for tokens and assets used in Australian exchanges and businesses, consumers can have greater confidence in the integrity of the assets they are investing in, and a true understanding of all possible functionality.

Smart contract audits can help to prevent scams by identifying any potential issues before they can be exploited. This can include issues such as code bugs, logical errors, and vulnerabilities in the underlying infrastructure. By catching these issues early, smart contract audits can help to prevent fraudulent activities and safeguard consumers' investments.

To ensure that smart contract audits are effective in preventing scams, they should be conducted by experienced and independent auditors with experience in the crypto space. Regulatory requirements for smart contract audits could help to ensure that consumers are protected and that bad actors are kept out of the market. By taking a proactive approach to preventing scams and promoting transparency, we can foster a more trustworthy and sustainable crypto ecosystem.

These audits will also be critical to improving the accuracy of token mapping, by categorising the functions of the smart contracts in the audit.

Q4) The concept of 'exclusive use or control' of public data is a key distinguishing feature between crypto tokens/crypto networks and other data records. a) How do you think the concepts could be used in a general definition of crypto token and crypto network for the purposes of future legislation? b) What are the benefits and disadvantages of adopting this approach to define crypto tokens and crypto networks?

a) Immutable, decentralised, public data is a key feature of the most widely used blockchains. This is what is being referenced when mentioning public data within a blockchain. Generally, this is derived from the nature of the primary smart contract supporting blockchain network, Ethereum. However, these aspects are not a universal general rule.

b) The Advantage is that this is generally a somewhat accurate description of most networks. The disadvantage is that this is likely a description that seems all inclusive and future proof but is not. Hashlock does believe this to be a core value of blockchain technology, however not all blockchain networks are built in such a way.

Q5) This paper sets out some reasons for why a bespoke 'crypto asset' taxonomy may have minimal regulatory value. a) What are additional supporting reasons or alternative views on the value of a bespoke taxonomy? b) What are your views on the creation of a standalone regulatory framework that relies on a bespoke taxonomy? c) 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?

A bespoke 'crypto asset' taxonomy would be inaccurate if you are categorising without looking at code and function. Blockchain assets are fundamental results of smart contracts or similar systems. They can have hidden functionality and future behaviours, and can be upgraded to change how they act. If you don't look at the code, the system will be gamed to produce tokens that gain a tax advantage whilst still being of another regulated category. In order to categorise effectively, the smart contracts need to be analysed and audited.

Q6) Some intermediated crypto assets are 'backed' by existing items, goods, or assets. These crypto assets can be broadly described as 'wrapped' real world assets. a) 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? b) 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 problem that arises here is that some tokens can transfer what they back or are backed by, and can also have misleading properties. Legislation needs to avoid being victim of manipulation by treating backed blockchain assets the same as the real world asset, if the code and smart contract itself is not analysed and reported on. Hashlock has clients that produce backed assets that dynamically change the asset they back, and this is extremely common within the industry.

Q7) It can be difficult to identify the arrangements that constitute an intermediated token system. a) Should crypto asset service providers be required to ensure their users are able to access information that allows them to identify arrangements underpinning crypto tokens? How might this be achieved? b) What are some other initiatives that crypto asset service providers could take to promote good consumer outcomes?

In the blockchain industry, the current way community transparency, security and trust is achieved is via smart contract auditing, these audits produce human-readable reports about the tokens functionality, system, behaviour, and risk. We believe that by making these audits required for assets traded on Australian exchanges, we can increase consumer protection without having to legislate against innovation.

Q8) 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. a) Are there any kinds of intermediated crypto assets that ought to be specifically defined as financial products? Why? b) Are there any kinds of crypto asset services that ought to be specifically defined as financial products? Why?

In general, the vast majority of crypto assets are not suitable to be classified as financial products. This classification alone would make new innovations far less likely to succeed. Whilst some unique crypto assets do fit the criteria, it would be far more suitable to place them in a category of their own, as the blockchain is still an emerging and evolving technology.

Q9) 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?

The only way to reliably evaluate blockchain systems is via code analysis, that assesses the actual foundations of that system. Otherwise, whitepapers, founders and legal teams will manipulate wording to hide the nature of their system and how it is built.

Q10) 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?

If a crypto asset is seen to have a sole purpose of backing a real-world asset, there should still be consideration that it may not be an actual representation of that asset financially, especially when it has other technological use cases within its own or other smart contracts.

Q11) 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?

If a crypto asset is marketed for short term financial gain purposes, then yes it should not be advertised in a traditional way that can mislead investors. However, Hashlock believes that the core technology and use cases of new blockchain protocols should be marketed and not limited in any way.

Q12) Smart contracts are commonly developed as 'free open-source software'. They are often published and republished by entities other than their original authors. a) What are the regulatory and policy levers available to encourage the development of smart contracts that comply with existing regulatory frameworks? b) What are the regulatory and policy levers available to ensure smart contract applications comply with existing regulatory frameworks?

Smart contracts are generally developed using templated, community audited foundations. These usually come from a company that intends them to be used in this way. The leading creator of such foundational contracts is OpenZeppelin. This actually makes contracts more secure, as they have audited, security focused foundations. In our experience as an auditing firm, the remaining code is typically developed from scratch in a genuine way. When we are auditing, we often do research to ensure the code is original and legitimate, and to better understand existing attack vectors.

Q13) Some smart contract applications assist users to connect to smart contracts that implement a pawn-broker style of collateralised lending (i.e. only recourse in the event of default is the collateral). a) What are the key risk differences between smart-contract and conventional pawn-broker lending? b) 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) The key risk differences between smart-contract and conventional pawn-broker lending lie in the transparency and immutability of the transactions. In smart contract-based lending, the terms of the contract are coded into the blockchain and are therefore immutable, meaning that they cannot be changed once the contract is executed. This provides greater transparency and reduces the risk of fraud or manipulation. Additionally, smart contract-based lending can be more accessible to a wider range of borrowers and lenders, as it removes the need for intermediaries such as banks or pawnshops.

   On the other hand, conventional pawn-broker lending can have higher fees and interest rates, as well as a lack of transparency in the process. There is also a greater risk of fraud or mismanagement, as the process relies on human intermediaries who may not always act in the best interest of the borrower or lender.

b) Currently, there is limited quantifiable data on the consumer outcomes in conventional pawn-broker lending compared with user outcomes for comparable services provided through smart contract applications. However, there is potential for smart contract-based lending to provide better outcomes for borrowers and lenders due to the transparency and immutability of the transactions. This could lead to more efficient lending markets and lower costs for borrowers.

It is important to note, however, that the outcomes for users of smart contract-based lending will ultimately depend on the quality and security of the smart contracts and the level of due diligence conducted by both borrowers and lenders. As with any financial transaction, there is always a level of risk involved and it is important for users to thoroughly understand the terms of the contract and the risks involved before participating in any lending activity.

Q14) Some smart contract applications assist users to connect to automated market makers (AMM). a) What are the key differences in risk between using an AMM and using the services of a crypto asset exchange? b) Is there quantifiable data on consumer outcomes in trading on conventional crypto asset exchanges compared with user outcomes in trading on AMMs?

The key difference in risk between using an AMM and using the services of a crypto asset exchange is that AMMs rely on automated algorithms to match buyers and sellers, whereas exchanges rely on manual order matching. This means that the risks of trading on an AMM may be different than trading on an exchange, as AMMs may be more susceptible to price manipulation and other forms of market manipulation. There is limited quantifiable data on consumer outcomes in trading on conventional crypto asset exchanges compared with user outcomes in trading on AMMs.