Fireblocks

28 February 2025

Response to CONSULTATION PAPER 381

Updates to INFO 225: Digital assets: Financial products and services

A1Q1 Are there any topics or guidance that have not been included in the draft updated INFO 225 that you think should be? Please provide details.

- On principle, our feedback is that regulatory clarity, financial stability, and consumer protection in markets for digital assets is best achieved through dedicated regulatory frameworks.

- Such frameworks, be they primary legislation such as the EU's Markets in Crypto-assets Regulation (MiCA), or guidelines, such as the Hong Kong Securities and Futures Commission's (SFC) Guidelines for Virtual Assets Trading Platform Operators, or crypto-specific provisions added to existing legislation, such as those currently under consultation in by the US Securities and Exchanges Commission (SEC), have, in our view, two very important commonalities. Firstly, they define digital assets as separate from financial instruments. Secondly, they set up dedicated licensing regimes for digital asset custodial intermediary services.

- In the absence of these, we believe certain types of digital assets and digital asset services may remain unregulated, as they do not clearly fit in existing financial services legislation.

- A case in point, Example 9 under the draft information sheet to INFO 225 states that meme coins are " unlikely to be a security or any other type of financial product". This is a consumer protection risk, to which EU consumers, for example, would not be exposed under MiCA.

- Overall, three main risks stem from the absence of dedicated digital assets rules:
    - Consumer choice: Regulatory uncertainty disincentivises the development of home-grown digital asset products and services, limiting the ability of Australian

consumers to access a competitive marketplace, and the Australian economy to attract capital and talent. When crypto-assets are regulated as financial instruments, regulatory disputes and uncertainty is a well recorded experience from other markets, most notably the US.

- Consumer protection: In the absence of a sustainable home-grown digital assets economy, Australian consumers will be either incentivised to access digital assets off-shore, without any consumer protection in place, or to access those unregulated digital assets product and services proliferating domestically.

- Cybersecurity: All transactions with a blockchain-based token have commonalities in operational resilience requirements, be they with stablecoins, tokenized equities, meme coins, or Bitcoin, for example in the context of custody. Therefore intermediaries involved with all these types of tokens need to be subject to the same operational resilience and cybersecurity requirements.

A1Q3 Do you agree that the good practice guidance in INFO 225 directed to responsible entities is applicable to providers of custodial and depository services that provide custody of digital assets that are financial products? Are there any good practices that you would like added (e.g. on staking services)? Please provide details.

- We believe that good practices in cybersecurity ought to be applicable to providers of custodial and depository services for any digital assets, regardless of whether they are financial products or not.

- We believe that absence of such a clear cybersecurity posture creates vulnerabilities for the entire market for digital assets – weak links in a chain – which can be exploited as the ability to transact between different types of tokens and blockchains grows.

- We firmly believe that good practices in cybersecurity should require licensed entities to demonstrate an end-to-end zero trust security architecture, where no one component (e.g.

private key management or wallet temperature) is, in itself, to deliver sufficient protection. We expand on this view below.

- On staking: we agree that staking-as-a-service providers which take custody of client assets are most importantly regulated for the operational risk they effectively take away from consumers and non-custodial staking-as-a-service technologies.

A2Q1 Do you have comments on any of the proposed worked examples? Please give details, including whether you consider the product discussed may/may not be a financial product.

- Without wishing to comment on the specific proposed examples, we have the following observations which apply to all, in addition to comments made under A1Q1.

- Firstly, we would encourage regulatory reform which clearly delineates between digital asset issuers and digital asset service providers. Within digital asset issuers, it ought to be differentiated between those that are legal entities and those that are fully decentralised networks. It is impractical that the latter are subjected to regulation. International experience shows that impractical rules drive consumers and investors off-shore, but it does not deter them.

- Further, it is very common in markets for digital assets that issuers are located in third-countries. There has to be clarity on how service providers are to interact with such issuers, particularly when there is a domestic demand for their tokens.

- Secondly, given this view on issuers, we recognize that most rules in digital assets, particularly linked to consumer protection, fall to service providers. We are concerned that the provided examples do not clearly make this delimitation, which risks that the market becomes fundamentally unclear on how to allocate responsibility.

- On the contrary some examples, for instance Example 13 (“Company M offers a non-custodial digital asset wallet service and issues their own proprietary stablecoin token on a public

blockchain"), activities which may or may not be bundled together in the market are presented as a single offering.

- We would encourage a consideration of the fact that digital assets markets, like digital finance markets before them, often unbundle activities previously bundled together. Therefore dedicated activity-based regulation is a must if Australia's regime is to have both certainty and ability to not create loopholes.

A2Q2 Are there any additional examples you would like to see included? Please give details of the suggested example(s), and why you consider the digital asset discussed may/may not be a financial product.

- We would encourage development of examples of a digital assets custody function as integrated with (i) exchanges and brokerages (ii) asset management and (iii) banking . We would strongly propose the objective of these examples would be to confirm that all these types of business can integrate a custody function and that the custody function needs to have a cybersecurity architecture specific to the nature of digital assets.

A3Q1 Do you think it would be helpful to include an example of a wrapped token and/or a 'stablecoin' in INFO 225? If so, do you have any suggestions on the features of the potential examples in paragraphs 20-21?

- We did note that among the provided examples, none deals with the case of a Company A issuing a non-yield-bearing stablecoin backed by a foreign currency, or backed by the AUD. We believe these would be very important additional examples to develop.

- We would indeed encourage ASIC to provide guidance on the treatment of this market. As implied in A3Q2, we would encourage this guidance to differentiate between the issuers of such a stablecoins, and the service providers which typically offer consumer access to them.

- In sum, we would encourage the development of at least four additional examples - USD-backed global stablecoins, AUD-backed stablecoins, as well as fiat-to-stablecoin and stablecoin-to-token exchanges and brokerages.

B2Q1 Do you agree that the same regulatory obligations should apply to digital assets and traditional financial products of the same category (e.g. securities, derivatives)? Please explain your response and provide specific examples.

- We agree that the same rules should apply to financial products and tokenized financial products. For example, should a firm offer Money Market Funds and tokenized Money Market Funds, that firm should be subject to the same prudential, market integrity and consumer protection requirements.

- However, we emphasize that the cybersecurity reality of a MMF and a tokenized MMF are fundamentally different, particularly in the context of custody. As the risk is different, the rules should be different too.

B2Q3 Do you agree that the approach proposed for custodial and depository services is appropriate for holding custody of digital assets? Do you agree that extending the omnibus client accounts is appropriate for digital assets that are financial products? Please explain, providing examples, if relevant.

- Most important for this submission is our stance on the proposed approach for custodial and depository services:

- We agree with the statement that “the entity responsible for custody has specialist expertise and infrastructure relating to digital asset custody” and we note that it is our experience that third-party technology providers are essential for the development and delivery of such expertise.

- We would seek to clarify that the requirement for client digital assets to be “segregated on the blockchain” does not preclude exchanges from trading from omnibus accounts. This practice is as common in digital assets as it is in financial instruments, and it ensures efficiencies, privacy, and cost-effectiveness as centralised intermediaries manage client assets.

- We appreciate the focus on private key management and avoidance of a single point of failure, which MPC technology delivers effectively.

- We would encourage ASIC to develop good practices, and ability for their evaluation, which treat digital asset cyber security as an end-to-end system. This could include:

    - Secure key storage through reliance on advanced cryptographic technology
    - Requirement for risk-based transaction authorization policies
    - Requirements for robust transaction processing safeguards such as transaction simulation, address white-listing, and reliance on confidential computing for transaction processing.
    - The aim of end-to-end cybersecurity good practices ought to be to ensure that multiple layers of key custody security are in place, and these layers act as effective checkpoints before a transaction is executed.

- We agree it would be good practice for licensed entities to independently verify to an appropriate standard, as determined by industry practice. This would give Australia the ability to always be at the forefront of digital asset cybersecurity.