
Dear Sir/Madam,

Executive Summary

Binance welcomes the Sultanate of Oman Capital Markets Authority Consultation Paper - Virtual Asset Regulatory Framework. All regulatory frameworks should provide certainty and a safe space for innovation, and drive consumer trust, market order, clarity and impact. The framework needs to provide the foundations necessary to ensure financial stability and consumer protection, and to provide the confidence which users and providers need to innovate together.

The regulation of Virtual Assets (“VAs”) and Virtual Asset Service Providers (“VASPs”) should introduce robust governance and comprehensive systems and controls proportionate to the nature, scale and complexity of the risks inherent across the industry.

Particular consideration should be given to consumer protection, market integrity and financial stability solutions as the industry and technology continues to mature. Disproportionate regulation may inadvertently stifle innovation and growth, remove choice and competition, and potentially drive consumers to unregulated markets or operators. Achieving this balance is not easy.

Our detailed response is attached, however we highlight the following key points:

- We agree with the CMA that security ‘tokens’ should be within the scope of the proposed framework and excluded from ‘traditional’ securities legislation;
- As much as possible, new requirements for Virtual Assets should align with globally consistent terminology and definitions based on Global Standard-Setting Bodies and international best practices e.g. Financial Action Task Force (“FATF”);
- As the sector is still evolving, the cost of imposing a risk-based capital framework may be disproportionately high. As such, we would propose a simplified capital regime with necessary restrictions to limit the risks to the VASP;
- We agree that, subject to the principle of proportionality, a licensed local entity should have a local presence, including a registered address and accountable individual, in all scenarios;
• In general, we believe that more consideration is needed regarding specific expectations, or thresholds, concerning the operation of virtual asset holdings in “hot” and “cold” storage by regulators;
• We appreciate the CMA’s work to gain a better understanding of the appetite of reputable audit firms based in the Sultanate of Oman for onboarding clients from the virtual asset industry;
• We agree that virtual assets automatically created as a reward for the maintenance of a distributed ledger, or for the validation of transactions, should be excluded from the Issuers Regime;
• We believe VASPs should be primarily responsible for determining whether a virtual asset is admitted to trading;
• We agree that initially it may take time for the CMA to become familiar with the industry and entities seeking authorisation and, as such, a three month processing period following receipt of a completed application is reasonable; and
• In respect of implementation measures we would highlight the need for the CMA to consider adequate transitional measures to allow firms time to interpret, adapt and comply with final rules and guidance; and
• Depending on the relative complexity of the final regulatory framework, it may be appropriate to provide additional flexibility in the transitional arrangements to cater for larger, more complex or novel licensed entities

Please do not hesitate to contact us if you have any questions about our response or require any further information.

Yours faithfully,

Binance
Responses as submitted via e-mail.

Q1. Do you agree with the CMA's proposal to expressly prohibit the use of privacy coins and activity linked to such assets in the Sultanate of Oman?

We consider the protection of users and market integrity (including prevention of financial crime) to be of paramount importance in the regulation of virtual assets. This includes, amongst other matters, ensuring the appropriate regulation of virtual asset custodians and stringent mandatory anti-money laundering (AML)/counter-terrorist financing (CTF) requirements.

Prohibitions should be carefully considered against the outcome intended and, where possible, should be done in a way that does not create unintended consequences. Our working assumption is that the prohibition on the issuance and use of privacy coins by the CMA does not include scenarios where the transactions are public but the data in smart contracts is confidential, or through the use of VPNs or digital wallets, which by their nature provide a degree of privacy to the user.

Additionally, we highlight paragraph 174 of the FATF ‘Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers’ relating to the management and mitigation of anonymity-enhancing technology risks such as privacy coins. This is consistent with FATF’s guidance on ‘Virtual Asset Red Flag Indicators of Money Laundering and Terrorist Financing’ referenced at paragraph 304.

Q2. Do you agree with the CMA's proposal to bring security tokens within the scope of the proposed framework?

Yes, as per our response to Q3 we agree with the CMA that security ‘tokens’ should be within the scope of the proposed framework and excluded from ‘traditional’ securities legislation.

Q3. Do you agree with the CMA's proposal to adopt the FATF’s broad definition of VAs and VASPs?

Yes, as much as possible, new requirements for Virtual Assets should align with globally consistent terminology and definitions based on Global Standard-Setting Bodies and international best practices e.g. Financial Action Task Force (“FATF”).

For the avoidance of doubt the following comments relate to scope and virtual asset activities for consideration:

Virtual Assets, including stablecoins. This approach is consistent with FATF’s Updated Guidance, which notes that a “Virtual Asset that is exchangeable for another asset, such as a stablecoin that is exchangeable for a fiat currency or a Virtual Asset at a stable rate” will be a Virtual Asset providing it is considered to have “inherent value to be traded or transferred and used for payment”, rather than just being a record of ownership of something else.

The virtual asset regulatory framework should consider explicitly excluding the following activities:

Traditional securities, investments and e-money/payments activities;
Central Bank Digital Currencies;
Decentralised Finance (DeFi), unless the issuance to the public has been deemed by a competent authority to be centralised;
Non-Fungible tokens (NFTs), as they are not fungible (consistent with FATF); and
Other virtual assets used to buy a service, or access a Distributed Ledger Technology (DLT) platform, and are only accepted by the issuer of that token (closed loop systems), being technically impossible to transfer directly to other holders.

Additionally, the CMA may wish to give consideration to the following activities that are synonymous with virtual assets and may not be explicitly covered in existing CMA regimes:

- Fan Tokens (Fan Tokens are utility tokens, issued by the Applicant and traded on its platform; the Club/Brand. Fan Tokens may grant their holders various exclusive benefits, including participating in the decision-making and invitations to fan events);
- Mining Pools: Pools allow users to access a mining pool and use their computational power to help validate blocks and earn rewards; and
- Retail crowdfunding: digital asset/virtual currency launch platforms to assist blockchain projects in raising funds.

**VASPs:**

We agree with the approach to use the FATF activities or operations to define the scope of a VASP. We highlight the following activities for the Sultanate of Oman and the CMA to consider as part of a wider virtual asset regulatory framework:

- Virtual Asset Stored Value Facility Services or Card Payments;
- Virtual Asset Payments and Remittance Services (with a permission to settle merchants in virtual assets or Fiat);
- DeFi activities (e.g. staking); and
- Banking Facilities within the Sultanate of Oman to facilitate a VASP’s client money account and business banking arrangements.

The overall aim of the high-level regulatory obligations on VASPs, and the detailed requirements that underpin them, is that a VASP’s policies and practices should be risk-based and must be appropriate and proportionate to the nature, scale and complexity of the risks inherent in the business model and the activities of the firm.

As such, careful consideration should be given to whether DeFi and NFTs should be considered as VASPs or virtual assets at this time until governments and market participants can better assess their characteristics and develop suitable regulatory approaches to them.

**Q4. Do you agree with the CMA’s intention to impose minimum capital requirements and require VASPs to retain an additional risk-based capital buffer based on identified risks?**

As the sector is still evolving, the cost of imposing a risk-based capital framework may be disproportionately high. As such, we would propose a simplified capital regime with necessary restrictions to limit the risks to the VASP.
Q5. Do you have any suggestions on the minimum capital requirements to be maintained for VASPs?

Some suggestions based on approaches in other jurisdictions² include:

- Base capital – Higher than $1 million or 50% of annual operating expenses of the VASP;
- Solvency – To hold at all times, liquid assets* which are valued at higher than 50% of annual operating expenses, or an amount assessed by the VASP issuer to be needed to achieve recovery or an orderly wind-down; and
- Business restrictions – A VASP issuer is not allowed to undertake other activities that introduce additional risks to itself. This includes investing in and extending loans to other companies, lending or staking of virtual assets, and trading of virtual assets. This is to ringfence and mitigate risks to the VASP in lieu of a comprehensive risk-based capital regime. Such activities can still be conducted from other related entities (e.g. sister company in which the VASP does not have a stake).

*Liquid assets is the sum of –
(a) cash and cash equivalents;
(b) debentures of the Government;
(c) negotiable certificates of deposit; and
(d) money market funds.

Q6. What are your thoughts on the CMA's proposal to require active participation of key personnel in Oman?

We agree that a licensed local entity should have a local presence, including a registered address and accountable individual, in all scenarios. This should allow for “double hatting” of certain positions where there wouldn't be any conflict of interest, and the amount of time required to discharge relevant duties is in proportion to the responsibilities of the position. Also, outsourcing or contracting of certain functions to third parties (after they pass through a selection process that includes a thorough due diligence) where the VASP remains ultimately accountable.

We would highlight that the CMA may wish to distinguish between a ‘branch’ and ‘subsidiary’ of a VASP when determining its risk-based approach to authorisation and supervision.

For example, whether the VASP can serve the Sultanate of Oman’s customers from an entity incorporated outside the Sultanate ‘branch’, or through a Sultanate of Oman-incorporated entity ‘subsidiary’.

Proportionate risk-based authorisation and supervision, including where a VASP meets equivalent standards to that of the virtual asset regulatory framework in the Sultanate of Oman, should enable ‘branch’ authorisation.

Q7. Should VASPs be required to hold only a low percentage of VAs in hot wallets? If so, how should this percentage be calculated?

We agree the percentage should not be predefined. In general, we believe that more

consideration is needed regarding specific expectations, or thresholds, concerning the operation of virtual asset holdings in “hot” and “cold” storage by regulators. A badly implemented cold solution is far more insecure than a strong hot solution so we would not assume cold is always 'better'.

We would suggest that the proportion and mix of virtual assets in hot and cold wallets is dependent on the VASP’s business model and should be managed in line with, for example, its liquidity risk management policy and processes to ensure good operational resilience. This proportion and mix should be managed operationally and not mandated by CMA. For example, mandating a small upper limit on the overall volume of virtual assets that are able to be stored in a VASP’s hot wallet (e.g. 10 percent) could (i) impact the speed at which customer withdrawals can take place; (ii) compromise security systems of the VASP as it will require more sweeping from the cold to the hot wallet.

We also suggest looking at Lloyds markets’ or insurers’ methods of rating a custodian’s security overall and have custodians or ‘ratings’ agencies independently provide this score to clients and regulators (i.e. A+ etc). We also agree that the CMA should consider other virtual asset related matters such as ring-fencing from other group entities, bankruptcy protection (of custodian and any 3rd-party providers), 3rd party-audits, contingency and resilience solutions (i.e. identification of other custodians that can hold the client’s assets or hold backup / recovery keys / shards) when the primary encounters a negative event.

Q8. Do you agree with the CMA’s approach to the outsourcing of safekeeping of VAs?

Yes, which we assume applies to both external and intra-group outsourcing equally.

Other points relating to the provision of custody of virtual assets to consider includes:

- Restrictions on signatory arrangements that allow a sole party or signatory from being able to completely authorise the movement, transfer or withdrawal of virtual assets or client money held under custody on behalf of clients, in favour of multi-signature approaches.
- VASPs should also have the ability to immediately halt all further transactions with regard to the virtual assets and client money.

Q9. Do you agree with the CMA’s approach of requiring an audit of safeguarded assets to supplement a required financial statement audit by an independent audit firm?

Yes, VASPs should have independent third party verification or checks carried out to verify that the amount and value of virtual assets and client money (e.g., fiat) held on custody on behalf of clients is correct and matches what the virtual asset Custodian is supposed to hold.

We appreciate the CMA’s work to gain a better understanding of the appetite of reputable audit firms based in the Sultanate of Oman for onboarding clients from the virtual asset industry. A VASP should be able to exercise due skill, care and diligence in the selection and appointment of the auditors to perform an audit of the financial statements of the VASP, and should have regard to their experience and track record auditing virtual asset-related business and their capability in acting as auditors of the VASP.

Suitably qualified independent audit rights should be exercised in a proportionate and
risk-based way necessary for the regulator to gain the assurance required for the proper performance of their functions, whilst enabling the provider to protect the security and integrity of the service provided for the benefit of consumers and market integrity. Accepted practice is that audits would take place annually, unless otherwise agreed.

Q10. Do you believe that proof of reserves techniques can be effective in ensuring customer assets are appropriately segregated from a VASP’s reserves?

Yes, we would highlight the Merkle Tree/zk-SNARK method for proof of reserves proposed by Vitalik Buterin and implemented in the Binance Proof of Reserves (POR) system\(^3\) as one solution intended to safeguard client assets in the way described. The POR solution is new and innovative but is particularly well aligned with the virtual ethos of transparency and trustlessness. It also illustrates how new technology and innovation from the virtual asset industry can evolve from a proof-of-concept to something that can potentially help consumers and industry, including in the traditional securities markets.

Q11. Do you have views on the key elements of the proposed authorisation requirements for the VASP regime?

A VASP wishing to provide specific virtual asset services must first be authorised or registered by the relevant authorities.

Minimum standards may include:

- Business model: a VASP should evidence that its business model is suitable for the regulated activities that it wishes to undertake;
- Effective supervision: a VASP must demonstrate that it is capable of being supervised effectively;
- The location of offices: e.g. if a VASP is a body corporate where its head offices are located (and its registered office, if it has one);
- Appropriate resources: the firm must have the right people with the required level of competence and independence, financial resources and systems to deliver the products or service; and
- Suitability: a VASP must be fit and proper and give regard to e.g. connections with other persons/firms, relations with regulators, objectives of the regulators, competence of those who manage the business and the way in which they manage the business.

The factors, including any reporting requirements, should consider the type of financial services a VASP wants to provide, the nature and size of its customer base, and whether the VASP intends a phased approach or “soft” launch as part of its business plan.

**Stablecoins:** We understand that the CMA will exempt issuers already licensed by the Central Bank of Oman to issue electronic money under the National Payment Systems Law from needing to obtain a licence under the CMA Issuers Regime if they are issuing fiat backed stablecoins only. We would ask that this is reciprocated where those with CMA Issuer Regime licences for stablecoins are exempt from the need to also obtain a licence from the Central Bank of Oman under the National Payment Systems Law to issue fiat backed stablecoins only.

---

\(^3\) [https://www.binance.com/en/blog/ecosystem/binances-proofofreserves-system-upgraded-to-include-24-tokens-169046415632926329]
Q12. Do you agree with the VA types that have been proposed as in or out of scope of the Issuers Regime?

Yes, we are supportive of the proposals and have elaborated in previous questions e.g. Q3.

In particular, we agree that virtual assets automatically created as a reward for the maintenance of a distributed ledger or for the validation of transactions should be excluded from the Issuers Regime. Specifically, mining, validating, staking and node infrastructure is integral to the operation of the technology infrastructure and such “validation and governance activities” should be excluded where such software developers and non-custodial service providers do not maintain control over users’ funds and do not engage in any decision making regarding individual transactions.

Where ‘free’ or ‘airdropped’ tokens are involved we would suggest that VASPs could perform an internal risk assessment and take responsibility for dealing with related scams, disputes and claims and educating users in this regard to mitigate risk. Similar consideration should apply to the marketing and promotion of free tokens so that any regulatory requirements applied are proportionate to the potential benefits and harms to innovation, markets and consumers.

The CMA may also wish to give consideration to whether VASPs and their activities involving virtual assets meet the “by way of business” test and therefore require authorisation. Factors may include:

- the degree of continuity;
- the existence of a commercial element;
- the scale of the activity;
- the proportion which the activity bears to other activities carried on by the same person but which are not regulated; and
- the nature of the particular regulated activity that is carried on.

Q13. Do you agree that initial coin offerings should be subject to a registration regime?

Yes, Binance already has a comprehensive listings process in place with the appropriate expertise and resources to manage the listings process. Taking into consideration the unique nature of virtual assets, their significant trading volumes and global accessibility it is important to establish a regulatory framework that allows VASPs to swiftly manage the listing and delisting of these assets.

VASPs should be primarily responsible for determining whether a virtual asset is admitted to trading. It is also important to ensure appropriate regulatory oversight of the admission process to trading virtual assets on exchanges and this could be achieved in different ways e.g.:

- Self-certification: Under this route, prior to admitting a new virtual asset to trading the exchange would self-certify to the relevant competent regulator that the virtual asset it intends to list is a virtual asset within the relevant definition, and that the virtual asset has met the VASP’s requirements for listing. The regulator would then have an opportunity to stay the listing within a prescribed time period. This approach may involve the regulator reviewing, or approving, the companies listing and delisting policy to provide the necessary assurance required for self-certification;
- Review and approval: Under this route, an exchange may instead request the relevant
regulator review and approve a particular virtual asset for admission to trading rather than the exchange undertaking a self-certification process.

Regulators could also publish a list of all virtual assets submitted to it under either route. The publication of such a list would provide certainty to the industry regarding which virtual asset products are deemed to be regulated. This would be of particular assistance to new or developing exchanges and would provide users with additional comfort that the virtual assets they are buying or selling are regulated products.

Operationally we would identify the following additional points for the CMA to consider:

- what information should be submitted by a virtual asset issuer for admission to trading e.g. “whitepaper”, bearing in mind that whitepaper content requirements should be aligned as much as possible across jurisdictions;
- the level of due diligence to be undertaken by the VASP in respect of key risks such as the background of the issuer of the virtual asset, product roadmap, tokenomics, finances, code design and infrastructure security;
- acceptable processes for the orderly delisting of a virtual asset; and
- regulatory resilience when virtual asset markets operate 24/7/365, requiring a reconceptualisation of regulatory oversight. Traditional regulatory bodies will need to consider the demands of such market activity, which extends beyond conventional working hours and often intensifies during weekends and public holidays.

Additionally, the CMA may wish to make a distinction between the policy and procedures involved in listing a new virtual asset, as part of an ICO listing, and the listing of mature virtual assets that have been successfully traded in other jurisdictions.

Q14. Do you agree with the CMA’s proposal that ongoing issuances should be subject to a more comprehensive licensing regulatory framework?

We agree with the proposal on the assumption that VASPs, in addition to virtual asset issuers, whether subject to one-off or post-issuance obligations, are authorised and supervised directly by the CMA.

In the context of the virtual asset issuer responsibilities proposed to be performed directly by the CMA, we highlight our options and thoughts in respect of virtual asset listing at Q13, specifically that “VASPs should be primarily responsible for determining whether a virtual asset is admitted to trading.”

We would suggest the overall aim of the high-level regulatory obligations on VASPs, and the detailed requirements that underpin them, is that a VASP’s policies and practices should be risk-based and must be appropriate and proportionate to the nature, scale and complexity of the risks inherent in the business model and the activities of the firm.

As the regulatory environment matures we would highlight the following additional areas for the CMA and the Sultanate of Oman to consider:

- Territoriality: Cross-border cooperation and coordination is important given the borderless, global nature of digital and financial markets. It should be clear how any rules/requirements apply to the regulated firm’s operations, its employees and its
customers. This may avoid competing claims involving different country regulators by clearly defining home and host state powers in the case of cross border provision of services;

- **VASP tokens**: We disagree that VASPs should be prohibited from listing or trading virtual assets in which they, or their affiliates, have a material interest. As long as there is sufficient governance in place to mitigate conflicts of interest, including appropriate disclosure, transparency and separation of market makers away from the exchange, it should be allowed;

- **Multiple Activities**: We believe that in-scope regulated entities considered to be “vertically integrated” or “agglomerated” should be expected to follow rules relevant to those regulated activities – not just those relevant to operating a VASP. Where multiple activities subject to regulation (such as custody or a broker dealer) coexist within a VASP, they should be supported by robust governance, effective risk procedures and adequate internal and external control mechanisms. However, legal separation of activities of VASPs undertaking a variety of services similar to traditional financial services may not be necessary to achieve segregation of risks in practice. This is partly because the inherent characteristics of VASPs, and the underlying technology used, may require a different approach to regulating them compared to traditional financial entities;

- **Scams**: The CMA should consider appropriate mitigation measures to manage the risk of consumers being subject to scams e.g. providing information and support to help consumers spot scam warning signs and cloned or unauthorised firms;

- **Retail/professional clients**: Appropriate levels of access and protection should be considered when designing any regulatory framework. For example, the knowledge, skills and expertise of the client;

- **Passporting**: Where there is equivalence in standards we would encourage implementing a “passporting” concept through which a VASP in one jurisdiction may be able to offer certain services in another jurisdiction, including the making available of funds in a certain jurisdiction that may be domiciled in another;

- **Global liquidity pools**: Given the important role of liquidity in maintaining market stability and efficiency, licensed VASPs should be permitted to retain their global liquidity pools, rather than being required to segregate orders by jurisdiction. Order routing via a global order book is permitted in a number of jurisdictions. In many jurisdictions there are no specific regulatory prohibitions against using a global order book. The overall business model and settlement risk, foreign exchange risk, AML, KYC and counterparty risk in any such transactions should be evaluated;

- **Peer-to-peer transactions**: Customers should be afforded the opportunity to buy and sell virtual assets on a peer to peer (“P2P”) basis in order to ensure customers are able to freely transact with one another. P2P trading in virtual assets should remain subject to full KYC checks and compliance with FATF Travel Rule compliance;

- **Authorised persons / responsible officers**: Depending on the nature, scale and complexity of its business, it may be appropriate for a VASP to have separate Compliance, Risk, Internal Audit or Financial Crime functions;

- **Waivers/modifications from rules/licences for firms**: The CMA should consider waivers and modifications to enable flexible application of their rules and licensing requirements given the innovative nature of virtual and blockchain based businesses. A waiver means a VASP would not have to comply with a rule. A modification would allow a VASP to comply with a rule amended to fit their circumstances; and

- **Decentralised Finance (DeFi)**: It will be important for the CMA to consider the appropriate way to address the regulation of DeFi.
Q15. Do you agree with the proposed high-level minimum capital requirement for VA issuers in the context of encouraging innovation and enhancing consumer protection?

Yes, we are supportive of the proposals and have elaborated in previous questions e.g. Q4 & Q5 in the context of VASPs. In the context of issuers of ICOs the CMA may wish to apply a similar approach proportionate to the nature, scale and complexity of the risks inherent in the business model and the activities of the firm.

Q16. Should the proposed amount of minimum capital required be based solely on the issuer’s financial projections and business?

Given that the sector is still in its early phase of development we are supportive of a simplified capital regime and have elaborated in previous questions e.g. Q4, Q5 & Q15 in the context of a VASP.

Q17. Do you agree with the proposed ‘risk-based’ buffer for issuers who are more systematically important as an appropriate measure to mitigate against reputational or systemic risk?

Yes, we are supportive of a risk-based approach and the CMA’s intent to ensure that such requirements remain flexible enough to allow reserves to be held in a way that would cater for the business model and the activities of the VASPs and virtual assets.

Q18. Should the CMA determine the amount of reserves required for issuers under the proposed ‘risk-based’ buffer using a prescribed amount?

Given that the sector is still in its early phase of development we are supportive of a simplified capital regime and have elaborated in previous questions e.g. Q4, Q5 & Q15 in the context of a VASP.

Q19. Do you agree with the proposal to introduce additional audit requirements for issuers, including audits for smart contracts utilised in the process of issuing?

We are supportive of high IT security standards designed to safeguard VASP platforms and users. We utilise commonly accepted international standards (e.g. externally audited and certified ISO27000, SOC2 Type/II) relevant to the provision of IT services, including in our approach to business resilience, data and cyber security and customer information protection.

We highlight our response at Q13 relating to the listing of virtual assets and the level of due diligence currently undertaken by Binance in respect of key risks such as the background of the issuer of the virtual asset, product roadmap, tokenomics, finances, smart contract/code design and infrastructure security

Q20. Do you think the benefits of these additional audit requirements outweigh the potential challenges for issuers?

Yes. However, suitably qualified independent audit rights should be exercised in a proportionate and risk-based way necessary for the regulator to gain the assurance required for the proper performance of their functions, whilst enabling the provider to protect the security and integrity of the service provided for the benefit of consumers and market integrity.
Q21. Do you agree that periodic financial reporting and disclosure of material events should be mandatory for issuers?

Yes, we agree that VASPs should be subject to reporting and notification requirements, for example:

- Material changes in nature of business carried on and types of services provided;
- Material changes in business plan;
- Material changes in share capital or shareholding structure; and
- Material breaches of existing laws which the VASP is subject to.

Q22. Do you think ongoing reporting and compliance obligations will increase transparency and accountability in the VAs market?

Data reporting can raise numerous complexities and requires collaboration with industry to ensure that confidentiality, integrity and availability can be achieved on a consistent basis and in a format that is sustainable by industry and purposeful to regulators.

Consistency in areas such as a single supervisory contact point, language, standardised forms, data breakdown, reporting frequency, deadlines and coordination of activity between regulators should all be considered. We would encourage greater regulatory harmonisation and coordination in this area.

Existing transparency reporting requirements (such as EU MIFID) will be very costly for virtual asset firms due to the sheer volume of trades and traders, potentially impacting the trading systems performance. These costs can be particularly prohibitive for new entrants, thereby limiting market competition and stifling innovation.

Q23. Do you agree with the CMA’s approach to setting a 3-month processing standard for VASPs and issuer licensing applications?

We agree that initially it may take time for the CMA to become familiar with the industry and entities seeking authorisation and, as such, a three month processing period following receipt of a completed application is reasonable.

In support of an efficient authorisation process we would encourage the CMA to:

- take into consideration any authorisations already held in other equivalent jurisdictions for the same or similar activities being sought from the CMA; and
- that the CMA is clear on what information and standard it requires to assess an application for authorisation, and in what format the information is required.

Q24. Do you agree that for registered issuers, the CMA should meet a shorter processing standard of 1-month?

We believe that the authorisation process should be risk-based, proportionate and efficient based on the authorisation being sought and the entity applying. In some cases it may be appropriate for registered issuers’ applications to take longer than one month.

To support the entry of VASPs and virtual assets into the Sultanate of Oman, the CMA may wish
to consider a sandbox for firms and authorisations to test innovative propositions in the market with real consumers. This would allow the CMA to understand and trial these innovative business models before issuing a full financial permission to allow operations to scale.

**Q25. Do you agree with the CMA’s approach to dealing with firms already operating in the VA space in the Sultanate of Oman as they transition into the new VA regulatory framework?**

Yes, and we agree that there will be a need for the regulators to consider transitional arrangements as new and existing firms adapt to the new virtual asset regulatory framework.

**Q26. Do you have any comments on the length of the transitional period for eligible firms?**

In respect of implementation measures we would highlight the need for the CMA to consider:

- adequate time and opportunity for industry to engage on any binding guidance;
- adequate transitional measures to allow firms time to interpret, adapt and comply with final rules and guidance; and
- consistency with respect to how global standard setting bodies approach the regulation and oversight of virtual asset activities.

Depending on the relative complexity of the final regulatory framework it may be appropriate to provide additional flexibility in the transitional arrangements to cater for larger, more complex or novel licensed entities seeking to comply with the new virtual asset regulatory framework.