30 March 2023

Thank you again for the opportunity to comment on the Virtual Asset Trading Platform (VATP) Consultation Paper dated 20 Feb 23. Our comments are along similar lines to those we made following earlier consultation initiatives by the SFC. They focus on aspects of the proposed licensing regime that are relevant to Custody, especially as they relate to institutional clients.

Comments

General

We support the SFC's proposed licensing of the Virtual Asset industry as we believe it will provide greater security for holders of virtual assets, will help to improve the overall standards of the industry and thereby raise legitimacy which in the long term will benefit the industry and assist in its acceptance by traditional financial institutions and investors. Launching a licensing regime that compares favourably with other jurisdictions, would provide Hong Kong the opportunity to wrest back its former position as a hub for the virtual asset industry.

Scope of licensing

As observed in prior communications, we believe strongly that all providers of custody services should be licensed, not just those owned by VATPs. We believe licensing only VATP-provided custody and requiring VATPs to use their in-house custody provider risks some undesired and negative implications for the market and does not eliminate the risk of mishandling of clients' assets by the VATPs:

- It forces those looking for a licensed provider to use a service provider whose focus is on other activities and - as is noted in a footnote in the paper itself - custody is offered only as "an ancillary activity to their trading services"
- It ironically puts professional custodians, offering top-class custody, at a significant competitive disadvantage for the sole reason that their primary business focus is on the provision of top-class custody services
- It significantly limits clients' choice of custodians
- It could make the VATP unprofitable as it has to set up and maintain its own custody
- It puts Hong Kong at a potential disadvantage to other jurisdictions such as Dubai (VARA), Abu Dhabi (ADGM), Singapore, Bahamas, EU, UK, to name but a few, which either already include professional custody in their licensing regimes or plan to do so in the near future

We therefore contend that all custody providers should be regulated equally in order to maximise asset safety, extend best practice, provide a level competitive playing field and enhance the attractiveness of the Hong Kong market. If that is not possible under current regulatory scope then we propose that VATPs should be able, or preferably required, to use an independent custodian satisfying minimum criteria.

Full separation of VATP and Custody activity

Recent events have shown the risks involved in allowing exchanges or VATPs to maintain influence over the custody of assets. Although the draft regulations state that custody should be provided by a separate legal entity to the VATP entity, the fact is that the custody-providing company is likely to be an affiliate of the VATP and fall under the same controlling management and staff. To prevent any risk of improper influence over, or misuse of, client assets we propose that custody for VATPs should be provided by an entity which is entirely independent of the VATP itself to achieve a complete separation from the company operating the trades or at a minimum that the custody entity should not be a subsidiary of the VATP.

Insurance / Set-aside funds
We refer to the 3 specific questions posed by the SFC and respond as below:

1. *Do you have any comments on the proposal to allow a combination of third-party insurance and funds set aside by the licensed platform operator or a corporation within its same group of companies? Do you propose other options?*

   We continue to see problems with the proposals as described, not least the extent of coverage implied (either by insurance or set-aside funds) and the difficulty of implementing it in a commercially viable manner.

   Instead of setting a ratio of asset value to insurance/funds cover, we propose that every custodian should decide what level of coverage they believe is best suited to their business model and the levels of coverage expected by their clients. Within the custody industry for traditional assets, custodians are free to hold whatever insurance cover they see as commercially necessary (balancing cost v cover) and clients assess the selected coverage as part of the overall evaluation of a custodian Client expectations of cover vary tremendously and are partly based on their evaluation of the risks involved and the extent to which their custodian manages these risks. The actual levels of cover in the traditional asset space are much lower than those initially envisaged by the SFC - normally a tiny fraction of a percent.

2. *Do you have any suggestions as to how funds should be set aside by the licensed platform operators (for instance, under house account of the licensed platform operator or under an escrow arrangement)? Please explain in detail the proposed arrangement and how it may provide the same level of comfort as third-party insurance.*

   We do not have any suggestions regarding this topic.

3. *Do you have any suggestions for technical solutions which could effectively mitigate risks associated with the custody of client virtual assets, particularly in hot storage?*

   A professional custodian will normally have significant levels of defence against hacking or cybersecurity attacks as well as more conventional theft or internal fraud threats. These safeguards are normally tested and assessed (eg by means of SOC2 certification) by an expert external party to confirm not only that the procedures are in place but also that they are actively complied with.

   Please see below a summary of some of the safeguards employed by the industry.

   Key Generation / Management
   Securing the key generation or key management process is essential to safeguarding the hot wallets. When generating the wallet, the entropy sources determine the randomness of the random bit generation output. NIST SP 800-90b compliant entropy sources should be highly recommended for such use cases. Custodian should be managing its wallets using an HSM or MPC protocol to eliminate the risk of human error and insider threats. Selection of HSM or MPC protocol should reference from the Cryptographic Module Validation Program established by NIST to ensure the compliance level to FIPS 140-2 of any shortlisted solution.
   Secure Coding / Secure SDLC
   Due to the nature of digital assets, Secure Software Development Lifecycle (SSDLC) is essential to safeguarding digital assets. Custodians should ensure security requirements are embedded into the SDLC. DevSecOps approaches should be considered whenever possible in order to implement adequate security measures and enforce segregation of duties for the software development, testing and release functions.
   Vulnerability Assessment / Penetration Testing
   Regular vulnerability assessment and penetration testing should be performed on both infrastructure and application of the custody solution. Custodians should engage CREST

Approved service providers to conduct independent penetration testing. Vulnerability assessments should be performed with a risk based approach, referencing industry standards such as CVE and CVSS.

Data-at-rest Protection

Sensitive or secret data at rest should be encrypted by strong encryption algorithms approved by industry standards. Access to such data should be governed by a comprehensive access control process, according to the least privilege principle and need-to-know basis. Authentication methods such as Just-in-time access and Multi-factor Authentication should be encouraged.

Data-in-transit Protection

Data-in-transit should be encrypted by strong encryption algorithms approved by industry standards to mitigate the risk of Man-in-the-middle attack. Secured communication protocols such as TLS/mTLS are to be considered for data-in-transit protection.

Segregation of Duties

Strict segregation of Duties should be enforced in sensitive operations like wallet generation, access to production data, and key management. Maker-checker mechanisms should be established across teams, business units or departments to ensure process integrity.

Human Resources Security

Staff that might access, process or manage cryptographic key materials (such as key operators, software engineers, and infrastructure engineers) should undergo a background check and a reference check prior to their employment.

Outsourcing Risk Management

Utilisation of third party services is very common in modernised technology-driven environments, the custodians should establish a sound vendor management process which allows continuous monitoring of the availability, security, confidentiality and integrity of their service providers.

Certifications and Attestations

A custodian should invite external inspection of its internal control regularly, the inspection should be performed by reputable external auditors with relevant expertise. Obtaining industry standard certification / attestation campaigns such as SOC2 and ISO27000 series should be encouraged. In addition, CCSS Certification by CryptoCurrency Certification Consortium provides a comprehensive view on security controls that are relevant to a digital assets custody solution (for both hot and cold wallets).

Hot wallet v cold wallet holding ratio

We refer to the requirement in the draft regulations to hold 98% of client assets in cold wallets.

The way in which assets are held depends in large part on the nature of a client's business and their assessment of the risks involved. Typically, "buy and hold" clients, for whom rapid access is not a major consideration, hold all or most of their assets in cold wallets for greater security. Active traders of virtual assets, however, normally hold a proportion of their assets in hot wallets to facilitate easy and rapid trading. The proportion can vary from time to time, depending on market conditions and trading strategies.

For every client this is an individual decision which they then instruct to their custodian. As a custodian we can advise clients on the pros and cons of each approach but, since we act solely as agent, we are not in a position to dictate how a client should hold their assets. We therefore recommend that this decision be left with the asset owner and it be communicated in writing to their custodian.

External assessment

It is stated in the paper that external assessments will be required (1) at the time of application to cover the effectiveness of the proposed controls etc and (2) on the issuing of in-principle approval covering implementation and effectiveness of the actual adoption . This makes sense for a new company which has not yet started up its business but for an established, already operational company we suggest that only the assessment focusing on the actual implementation of controls etc would be required.