RAKKAR DIGITAL (HONG KONG) LIMITED
17/F, Leighton Centre, 77
Leighton Road, Causeway Bay,
Hong Kong

Securities and Futures Commission
54/F, One Island East,
18 Westlands Road, Quarry Bay
Hong Kong

Re: Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators licensed by the Securities and Futures Commission

Dear Sir/Madam,

I am writing on behalf of Rakkar Digital (Hong Kong) Limited hereafter Rakkar Digital or Rakkar, a licensed Trust and Company Services Provider with the registration number TC008755, to express our opinions on the consultation paper.

Company Background

Rakkar Digital is a Singapore-headquartered digital assets custodian powered by Fireblocks, the market leader on digital assets custody solution, utilizing MPC-CMP technology to protect private keys. We aim to be a leader in digital assets and blockchain-based financial services specialized in custody services in Hong Kong and ASEAN region.

Rakkar is a qualified custodian that offers digital asset custody products and services for businesses, corporates, and institutions. The platform provides a one stop service to allow clients to securely store and manage digital assets with the choice to store their cryptographic private keys in a warm or cold environment through the products Rakkar Warm and Rakkar Cold.

The Rakkar platform allows customers to make transactions through a customizable policy engine. The product utilizes MPC-CMP technology to protect customers' private keys. The platform has two engagement channels which are the web application and the mobile application, with the latter containing the authentication of approvals and transactions. In addition, the platform also performs KYC/CDD and AML/CFT screening on onboarding and monitors their transactions through on-chain analytics tools (Know Your Transaction).

General Opinion on the new license scheme

We are pleased to see that SFC is opening the digital assets market to the wider public where more residents in HK can explore and use regulated digital assets services legally. In the last five years, we have seen many residents choose to use offshore VASP services and they are typically unprotected under Hong Kong's authority. This would damage the reputation of Hong Kong as a global financial hub where the residents are targets of frauds.

RAKKAR DIGITAL (HONG KONG) LIMITED
17/F, Leighton Centre, 77
Leighton Road, Causeway Bay,
Hong Kong

Regarding the investor protection measures, we would like to raise our concern about the custody of the customer's digital assets. We understood that the use of "wholly owned subsidiary of the licensee" as the custodian is a long-lasting condition since the establishment of the licensing regime, however, it is no longer the best solution to protect customers' funds. After the FTX and Celsius Network incidents, people in the digital assets industry are losing patience and confidence in centralized exchanges who utilize the customers' funds to trade while holding them in custody. This is an obvious conflict of interest where the liquidity provider, i.e., the centralized exchange, always has an interest in using the customer's funds to make profits. They may structure their products as "staking" and "earning" so that customers' funds are locked as liabilities for them and then they can use the funds for proprietary interests. If the custodian belongs to the Trading Operator, the chance of a conflict of interest and insider fraud would be much bigger. Moreover, if the trading operator and custodian go bankrupt together, it will take a long time for the customers to take the funds back even though there is a trust relationship between the exchange and custodian. The customers will suffer a massive loss from the incident because they cannot liquidate their positions as soon as possible. It will cause a systemic blow to the financial market.

We recommend SFC to consider modifying the definition of "associated entity" to allow third-party custodian service providers. To preserve the stability of the financial market, we agree that the associated entity should be licensed as TCSP (Trust or Company Service Provider) and incorporated in Hong Kong. With the use of third-party custodians in Hong Kong, customers will be able to receive funds within days not months. This would also lower the chance of conflict of interest or collusion among directors between exchange and custodian. Also, to tackle the concentration risk, such as cybersecurity and crime risk is concentrated into one wholly owned subsidiary, we also recommend SFC consider allowing the licensee to appoint additional custodians to diversify the risks. This concentration risk is much reflected in the high premium requested by insurers.

Response to Question 1

We agree with the direction to open the market to retail investors with robust investor protection measures. Retail investors are the foundation of market liquidity. If Hong Kong is aiming to be the Asian digital assets hub, we believe that it is necessary to allow retailers to trade in regulated markets. Also, as we mentioned, we have seen people using offshore VASP services. The outflux of liquidity is not healthy for Hong Kong to grow in the digital assets space.

Another driver in the market is the Small and Medium-sized Enterprises (SMEs) who might not be qualified as accredited investors under the current scheme. We believe that SMEs are the enabler for the Hong Kong community to adopt digital assets by accepting cryptocurrency as a payment instrument or alternative cash management mechanism. By allowing

cryptocurrency as payment instrument, HK businesses can have a better outreach to the global market and expose themselves to a new asset class to risk diversification. It will also help SMEs to tackle the ever-increasing interest rate by investing into digital assets with a better volatility and return.

Response to Question 2

In general, we agree with the directions of the general and specific token admission criteria. To add better transparency to the token admission criteria, we would recommend including an additional requirement for external audits.

For example, a secure smart contract audit to uncover security vulnerabilities should be performed before a token is accepted for listing. The current market practice is to employ two independent smart contract auditors to review the source code before genesis (the first block of transaction, i.e., the token is started to be issued). This is to provide additional transparency and assurance to investors that they are investing in a digital asset which is cyber-resilient. We have seen many major security incidents in Web 3.0 were related to the vulnerabilities of smart contracts.

Another type of external audit could be a KYC audit for the investors of the token during the first sale. This was one of the serious issues of the unregulated ICO during the past years. Investors should be able to understand the background of the investors previously invested in the ICO projects to avoid scam exit risk. The source of funds and investor identities should be vetted before admission. This measure should be applied to small cap, newfound ICO projects in which the background is unknown. However, this requirement should be exempted for a large-cap ICO project since the effort of audit is disproportionate to the return from listing it.

Response to Question 3

Echoing the recommendation in our general opinion section, appointing a third-party custodian service provider should be the most feasible solution for the purpose of investor protection. SFC should establish measures to ensure that individual investors, who are always the last to respond to market turbulence, can receive the funds from the custodian within days after the collapse or closure of the trading operator.

Another consideration is the adoption of "proof of reserve" reports as a general requirement for licensees. There is a market trend where proof of reserve will be published by centralized exchange periodically. While there are many criticisms from the public on the transparency and impartiality of the reports, we believe this is the right direction for the market to explore because the digital assets market is all about trust and transparency. What we believe is missing an attestation of the liability held by the trading platform operators by an independent entity, such as a custodian. As the asset under custody is easy to verify, by

crawling data from the blockchain, it may be difficult to determine the amount of liability because some of the transactions might be off chain. We believe that a custodian has a bigger role here to verify the liabilities held by the exchange and issue an independent proof of reserve report, together with proof of assets and liabilities with an independent audit firm. This enhances trust and attracts more confidence from the public.

Response to Question 4

While we agree that having third-party insurance coverage and funds setting aside would help protect the investors, we would like to insist that the difficulty of getting insurance from global insurers is because of the concentration risk of our current market practice. Most of the crypto market players are liquidity providers and custodian providers at the same time. Therefore, there is a higher chance of crypto exchanges going into trouble and jeopardizing clients' funds. Assuming an insurer can provide a maximum of 100 million USD coverage for a crypto player, regardless of their holding, if the crypto player is doing self-custody or appointing her sister company to hold the funds in trust. The maximum coverage would always be 100 million USD, which is not significant to a crypto exchange. However, if the crypto exchange appoints five crypto custodians which have 100 million USD coverage each, it would be able to access 500 million USD coverage immediately. This amount would be quite significant to ensure the operations are protected. The same analogy can apply to custodians as well. If a custodian is serving only the principal from the holding group, the maximum coverage would be low because the chance of failure or a claim coming through would be high. However, if the custodian is serving multiple crypto players with different profiles and market segments, the chance of the worst-case scenario would be much lower. The insurer would be able to insure more coverage, up to 2 – 3 times. In short, an exchange pairing with her own sister custodian would be a less favorable situation for insurers while multiple exchanges partnering with multiple custodians (m-m relationship) would be preferred.

Response to Question 5

As a general practice, it would be better to segregate the funds set aside from the house account, preferably escorted by a third party/trustee. This is to avoid fraudulent management taking the funds out to cover the loss in trading. If this arrangement is not feasible economically, the licensee must set aside the funds and report the segregated fund amount to the regulator periodically. Moreover, an independent auditor should be appointed to review the arrangement to ensure proper internal controls are implemented to avoid collusion.

We would also recommend the regulator adopt the approach from the self-regulated market where the market participants created a SAFU fund to cover the loss in case there is an incident. We believe that the regulator can be of a pivotal role in leading the establishment of the fund with the licensee and regional investors to co-insure the market for stability. The

fund should be established to protect investors from global infrastructure issues such as a security compromise of a blockchain network or bailing out a market participant who is systemically important.

Response to Question 6

Hot wallet infrastructure is always a topic of discussion because of its bad history. Due to the intrinsic nature of hot wallets, private keys are always connected to the internet in a way to facilitate frequent transaction signing. With the ease of setup, many exchanges are using hot wallets as their core infrastructures to accept funds while moving most of them to cold wallets for storage.

Currently, the market is developing a new solution to address the hot wallet issue, which is called "off-exchange" settlement. The essence of off-exchange settlement is to segregate the fund away from the exchange while maintaining the liquidity in the exchange. The fund will be stored in the custodian system and access to the custody is maintained by the custodian and the exchange, via holding signing keys. Once the customer has deposited funds to the custodian wallet, the fund is locked by the custodian and confirmed by the exchange. The exchange will create trading credit on their platform based on how much the fund is locked in custody. The customers can then trade freely on the exchange platform. Once a trade is matched on the exchange, the settlement will be solely handled by the custodian on-chain or together with the exchange depending on the location of funds. This off-exchange settlement solution offers better security and flexibility for customers to trade without considering the reliability of the exchange platform. It also eliminates the need for hot wallets to hold customers' funds. We strongly recommend the regulator to investigate this solution and support its adoption.

If the use of hot wallets is inevitable, due to the economical constraints or technical limitation such as lack of support, we recommend the exchange to adopt multi-party computation (MPC) instead of just hardware security module together with multisig wallets. Multi-party computation allows users to communicate their private data without disclosing it. This helps achieve the zero-knowledge computation where the private key of the wallet has never been constructed or disclosed.

Response to Question 7

In general, we welcome virtual assets derivatives in the sense that they give more liquidity and risk transfer mechanisms for customers in the market. However, since the market risk and liquidity risk for most digital assets are new and unknown to most retailers. We recommend only vanilla contracts such as perpetual contracts for customers to lock their prices or options without margin. Any margin trading for retailers should be avoided since it will become a preach to retailers to speculate without much capital. This causes a lot of stress in the market.

While the market is still growing, we shall not prohibit the development of the derivative market. Accredited investors should be allowed to expose themselves to a bigger risk and trade with more advanced derivatives.

Response to Question 8

As per our previous opinion on the custody of digital assets, we believe the VASP T&C should be amended when incorporated into the VATP guideline to allow third-party custodians to be appointed by the licensees so that the operational risk or the custody risk could be diversified among the custodians and exchanges.

Response to Question 9

The major debate on AML/CFT compliance for regulated businesses is the implementation of the travel rule mechanism. While the industry welcomes the legislation of travel rule compliance requirements for licensees to follow, it is still a headache for licensees to implement since there are many different standards in the industry for data transfer. Once the mechanism is not compatible with the counterparty, the transaction will be rejected or not initiated. Otherwise, licensees must integrate all viable solutions in the market so they can send or receive funds around the world. This impacts the profitability of the business and introduces a lot of tractions to the businesses to operate normally. We strongly urge the regulator to standardize the Travel Rule technical standard for the HK market and take the lead to simplify the complexity of travel rule implementation. A Travel Rule data schema should be openly established so that all travel rule solution providers can adopt it.

Response to Question 10

We welcome the disciplinary ruling guideline. However, due to the intrinsic nature of digital assets, they are more prone to cyberattacks. Therefore, we believe that licensees should take a bigger responsibility to enhance the security and reliability of the information systems that provide trading services to the customers. Apart from MIC and RO, who are subject to compliance and conduct risks, we recommend the regulator investigate the responsibility of the person in charge of information technology and security. While we believe that technical personnel should not bear too many liabilities for any incident, the lack of governance regarding technology and security risk could be a major misconduct for the board and the senior management. We urge the regulator to include responsibility for the board and the senior management on technology and security risks in the disciplinary factors. The appointment of MIC for information technology and security will be a good initiative for better governance.

Conclusion

RAKKAR DIGITAL (HONG KONG) LIMITED
17/F, Leighton Centre, 77
Leighton Road, Causeway Bay,
Hong Kong

We are grateful to witness the development of the regulatory framework for the digital assets industry. While the first initiative is to govern and regulate virtual assets trading platforms, we strongly encourage the regulator to explore the possibilities to regulate virtual assets custodian providers. Authorities among ASEAN countries, including Singapore and Thailand, have already legislated, or are going to legislate regulatory regimes to govern virtual assets custodian business and repair the public confidence in the market after the recent turmoil. As a custodian in the Hong Kong crypto community, we are happy to participate in the discussion with the regulators directly to enhance the trust and transparency of the market.

Your Faithfully,

Rakkar Digital (Hong Kong) Limited
Licensed Trust and Company Services Provider (TCSP) (License No. TC008755)
E:
T: