Mar 30, 2023

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

By Online Submission

Dear Sir/Madam

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

Fireblocks appreciates the opportunity to provide comments on the Consultation Paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed by the Securities and Futures Commission ("**Consultation Paper**"). Fireblocks is committed to the mission of enabling businesses to easily and securely support virtual assets. As such, we welcome SFC's move to seek the crypto industry's views on the creation of a safe and trustworthy crypto ecosystem.

We set out, in this submission, our response to Question 6 of the Consultation Paper and our recommendations on certain topics addressed in the Guidelines for Virtual Asset Trading Platform Operators ("**VATP Guidelines**") that are not subject to consultation in the Consultation Paper.

About Fireblocks

Fireblocks Ltd is an Israeli company with various subsidiaries around the world (together, "**Fireblocks**"). Since 2019, Fireblocks has been providing institutional customers with an enterprise-grade platform that facilitates their self-custodial storage and transfer of virtual assets (the "**Platform**"). The Platform is provided to customers as a software-as-a-service offering.

The Platform enables customers to create secure environments known as "vaults" for the holding of virtual assets. Within these vaults, customers are able to designate "sub-vaults" to segregate their virtual asset holdings. These sub-vaults function as virtual asset wallets. Customers can also transfer virtual assets out of the vault to any specified location. The Platform allows customers to streamline the management of their virtual asset holdings with third-party exchanges, over-the-counter dealers, counterparties, and traditional "control" custodians by making these holdings visible to the customer and allowing their secure administration within a single software environment. There are currently more than 1,700 institutions using our Platform and Fireblocks is widely considered one of the most secure custodial solutions available.

To date, the Platform has obtained the following certification:

- SOCII Type2
- ISO 27001
- ISO 27017
- ISO 27018
- Cryptocurrency Security Standard (CCSS) Qualified Service Provider Level 3 certification by the Cryptocurrency Certification Consortium (C4)

Response to Question 6 of the Consultation Paper - 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?

Fireblocks believes that any institution engaging with digital assets – either for themselves or on behalf of customers – should keep up to date with the latest technical solutions with respect to private key generation, storage, and use:

1. **Private Key Generation**: Operators should employ technical solutions to ensure that the private key is not compromised at the point of generation, for example:
    - Generating private keys in a distributed manner, so that at no point is an entire single private key in the same place. This can be done through such threshold technologies as multi-signature (commonly known as "**multi-sig**") and multi-party computation ("**MPC**"), both of which are explained below in further detail.
    - Generating private keys in a secure environment (e.g. in an air-gapped device or in a hardware-level secure enclave within a cloud server) in a non-deterministic manner to ensure randomness.

2. **Private Key Storage**: Operators should adopt solutions and measures that minimise the risk of loss and unauthorised access to private keys. Specifically, private keys should be distributed across multiple locations (in the cloud and/or on-premises) so as to ensure security even if one location is compromised. In addition, each location in which private key material is contained should be adequately secured. The two most common ways to secure private key material are (i) Federal Information Processing Standards (FIPS) 140-2 compliant hardware security module (HSM) and (ii) Trusted Execution Environments (TEE) using hardware-level encryption (such as Intel software guard extension, Amazon AWS Nitro, ARM TrustZone and others). HSM is a physical device, separate from a computer, on which sensitive data can be stored, and that can only be accessed by authorized individuals. TEE is able to isolate sensitive data within a system, similar to HSM. However, compared to HSM, TEE offers additional benefits, such as its ability to support both cloud and on-premise deployment models and to protect larger categories of data (e.g. transaction authorisation policies). Each solution has its advantages and disadvantages, and the operator should have the flexibility to decide which solution best meets its operational and regulatory needs.

3. **Private Key Use**: Private keys are necessary to sign transactions for the transfer of virtual assets. Operators should use technologies that eliminate the 'single point of failure' risk with respect to the private keys, where a single private key is able to sign transactions. Today, the two most common technologies in the market that seek to eradicate the single point of failure risk are multi-sig and MPC:
    - Multi-sig is a signing process in which signatures from two or more users, each holding a piece of the private key, are needed to effect transactions. This means that no single person or private key is able to authorize transactions in relation to the associated virtual assets. For multi-sig, the entire signing process happens on the blockchain, meaning that information such as the number of signers and each signer's key information are visible on the blockchain.
    - With MPC, by comparison, the private key takes the form of at least three cryptographic key shares ("**MPC key share(s)**"). The data in relation to each MPC key share is encrypted and stored in different locations known as endpoints. Information is never shared between the endpoints, meaning that a bad actor who gains control over one of the endpoints will not have access to the data stored in another endpoint. When a signature on a blockchain transaction is requested, a quorum of at least three of the endpoints engage in a distributed signing process where each of the endpoints

individually validates the transaction. The MPC signing process happens outside of the blockchain. Only a single public key for all of the endpoints is exposed on the blockchain, meaning that data in relation to each MPC key share is not visible on any of the transactions recorded on the blockchain.

4. **Cold Storage**: Cold storage solutions have historically been perceived by some as more secure than hot storage solutions. This is because the storage of private keys in an online environment, as with a hot storage solution, causes the private keys to be vulnerable to bad actors on the internet. On the other hand, if the full private keys are not exposed online, the risk of compromise is diminished (at least as to remote actors). However cold storage solutions also have risks. As such, Fireblocks recommends the following in relation to cold storage solutions:
    - Neither the private key nor device securing the private key should come online after the completion of device setup and installation. Cold storage devices that have to be connected to a computer for the signing of transactions, even for a brief period, may run the risk of exposing the private key to compromise.
    - Fully air-gapped optical solutions are generally preferable to solutions where the transaction is moved between the online computer and offline computer through a disk-on-key storage device that can be compromised.
    - The private key that is contained in a single cold storage device should not be able to sign transactions on its own, as the cold storage device then becomes a single point of failure. Operators should employ cold storage solutions that are compatible with (i) technologies that, as mentioned in section 3 above, seek to eradicate the single point of failure risk, and (ii) internal controls and other technology that ensure that only authorised transactions proceed to signing.

Recommendations on Certain Topics in the VATP Guidelines

Fireblocks agrees with the general requirement in Para 10.9 of the Guidelines for Virtual Asset Trading Platform Operators ("**Guidelines**") that operators should keep "wallet storage technology up-to-date and in line with international best practices or standards". The technology around signing approaches and private key management is rapidly evolving. It is important that regulation does not mandate one type of technology, because institutions should retain flexibility to utilise the technology that is most appropriate for their business, as long as they are able to meet the SFC's requirements around security.

In the spirit of keeping the Guidelines applicable to new technology whilst adhering to the SFC's desire to maintain a safe crypto economy, Fireblocks proposes the following changes to the VATP guidelines:

1. Paragraph 10.8(a) of the VATP Guidelines:

    Current wording: "*The generated seeds and private keys must be sufficiently resistant to speculation or collusion... Where practicable, seeds and private keys should be generated offline and kept in a secure environment, such as a Hardware Storage Module (HSM), with appropriate certification for the lifetime of the seeds or private keys.*"

    Proposed re-wording: "*The generated seeds and private keys must be sufficiently resistant to speculation or collusion… Where practicable, seeds and private keys should be generated offline and kept in a secure environment, such as a Hardware Storage Module (HSM)* ***or using Trusted Execution Environments (TEE) using hardware-level encryption****, with appropriate certification for the lifetime of the seeds or private keys.*"

2. Paragraph 10.8(e) of the VATP Guidelines:

    Current wording: "*Seeds and private keys are stored in Hong Kong.*"

Proposed re-wording: "***<u>If distributed threshold signing technology such as MPC or multi-sig is employed, the following must be stored in Hong Kong: (i) in the case of MPC, at least one MPC key share; and (ii) in the case of multi-sig, the majority quorum of private keys required to generate a blockchain signature. In addition, backups of</u>*** *seeds or private keys are stored in Hong Kong.*"

Fireblocks also proposes that the SFC includes the following technical requirements, controls and procedures in the VATP guidelines:

1. Signing approaches that minimise the 'single point of failure' risk should be adopted.

2. Operators should deploy technological solutions to ensure that only successfully authorised transactions, in accordance with the operators' corporate governance, legal, and compliance obligations, proceed to signing.

3. Where cold storage solutions are used, operators should ensure that a single entire private key is never stored on a cold storage device. Operators should have the flexibility to use cold storage solutions that are compatible with MPC, where at least one MPC key share is stored offline in an air-gapped device.

****

We look forward to further discussions with the SFC on the points raised in this submission. Please do not hesitate to reach out to

Yours faithfully,