Fireblocks

27 May 2022

Director - Crypto Policy Unit
Financial System Division
The Treasury
Langton Crescent
PARKES ACT 2600

By Email: crypto@treasury.gov.au

Dear Sir/Madam

Submission on Crypto asset secondary service providers: Licensing and custody requirements - Consultation Paper

Fireblocks appreciates the opportunity to provide comments on Treasury's 21 March 2022 Consultation Paper - Crypto asset secondary service providers: Licensing and custody requirements ("**Consultation Paper**").

Fireblocks is committed to the mission of enabling businesses to easily and securely support crypto assets. As such, we welcome Treasury's move to seek the crypto industry's views on the creation of a safe and trustworthy crypto ecosystem for consumers, specifically in the area of custody.

This submission:

- Introduces Fireblocks' business and provides information on how our technology enables our customers to securely store and transfer their crypto assets.
- Provides generalized comments as well as high level responses to some of the questions raised in the Consultation Paper, specifically Questions 11 and 20.

About Fireblocks

Fireblocks Ltd is an Israeli company with various subsidiaries around the world (together, "**Fireblocks**"). Fireblocks provides an enterprise-grade SOC 2 Type II certified platform to facilitate the self-custodial storage and transfer of crypto assets by financial institutions (the "**Platform**"). The Platform is provided to customers as a software-as-a-service offering.

The Fireblocks Platform enables customers to create secure environments known as "vaults" for the holding of crypto assets. Within these vaults, a customer is able to designate "sub-vaults" to segregate their crypto asset holdings. These sub-vaults function as crypto asset wallets. The customer can also transfer crypto assets out of the vault to any specified location. The Platform allows customers to streamline the management of their crypto 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 1,200 institutions using our Platform and Fireblocks is widely considered as one of the most secure institutional solutions available in the market.

Fireblocks' approach to security addresses the three primary attack vectors that hackers and other malicious actors (e.g. rogue employees) frequently exploit:

- **Credentials and authentication** - Hackers may impersonate users within an organisation and use their login credentials and authentication to compromise the organisation's wallets or exchange accounts. Once a hacker is able to login to such wallets and accounts, they can issue and authorise fraudulent transactions. The most common method used to protect against the compromise of user credentials is two-factor authentication, but that method is not foolproof. For example, two-factor authentication via SMS is susceptible to SIM swaps and in extreme cases, hackers are able to deploy attacks that can defeat one-time password generators.

- **Deposit addresses** - Deposit addresses are long alphanumeric strings that designate the public address of a wallet. Hackers can, through the deployment of malware, cause the sender of crypto assets to send such assets to the hacker's deposit address instead of the intended recipient's deposit address. Common methods used for securing deposit addresses include test transfers, whitelisting, and using hardware wallets. These methods may not be operationally viable or foolproof. For example, whitelisting cannot stop human error and test transfers are usually time-consuming.

- **Private keys** - Hackers may attempt to compromise a victim's wallet in order to access the victim's private keys, which control the funds the victim has stored on the blockchain.

Fireblocks mitigates these attack vectors by deploying a multi-layer defense solution:

- **MPC + multi-server** - Fireblocks relies on a cryptographic technology called multi-party computation, or MPC. MPC works by requiring multiple parties to solve a problem that requires the input of secret information from each party in a decentralized way, without any party ever sharing the secret information with the other parties. With MPC, the private key takes the form of at least 3 cryptographic key shares. Each key share is encrypted and stored in different locations. The customer maintains control over one key share while the other key shares cannot be accessed by anyone (including Fireblocks and the customer). When the customer triggers a request, each of the key shares engages in a distributed and independent signing process to validate the transaction. The private key thus is never gathered as a whole, neither during the first creation of the wallet nor during the actual signature. Fireblocks further offers customers multiple cloud and on-premise options for storage of the key shares to ensure an extra layer of security even if one location is compromised. MPC technology, in combination with Fireblocks' multi-server approach, mitigates the risk of a hacker taking control of an entire private key in order to compromise a wallet.

- **Intel SGX (software guard extension)** - Fireblocks uses Intel SGX, a hardware-level enclave, to isolate and protect all code or data pertaining to each key share. With Intel SGX, even if a hacker gains control of the server/device containing a key share, the hacker will not be able to access the key share's data.

- **Policy engine** - As part of the transaction validation process, the policy engine enables customers to set up specific approval policies for every crypto asset transaction. For example, the customer can set a rule in which crypto asset transfers above a certain quantum require the approval of two team leads within the customer's organisation. Fireblocks secures the policy engine inside an SGX enclave and distributes the policy verification across several MPC servers. This ensures that hackers and even insiders (e.g. IT administrators) are unable to modify the implemented roles or the logic of the policy engine.

- **Secure Transfer Environment** - The Platform uses the latest breakthroughs in secure enclave technology and data-in-motion encryption to provide an encrypted environment for the querying of the recipient's deposit address. This encrypted environment is protected within a secure enclave on both the sending wallet and receiving wallet. The Fireblocks solution allows for: (a) full mitigation of man-in-the-middle attacks on both the network and host levels; (b) proofing the address at the source, and full authentication of the recipient; (c) guaranteed fail-close system if an attack is detected on either end; and (d) automatic rotation of deposit addresses on every transfer to preserve pseudo-anonymity.

Responses to Consultation Questions

1. **General Comments.**

As noted above, the Platform facilitates the self-custodial storage of crypto assets by institutions. Fireblocks does not hold crypto assets or safeguard private keys for its customers. Customers instead use the Platform technology as infrastructure that enables them to:

- Manage the storage and transfer of their own holdings of crypto assets;
- Utilise crypto asset services from third parties with whom they have independently established account holder and/or counterparty relationships; and
- Support the provisions of the same or similar services to their own customers.

Accordingly, crypto assets in the vault are at all times held by and controlled by the Fireblocks customer. The transfer of crypto assets is initiated by the customer and always registered as occurring on the relevant blockchain (i.e., never on a ledger maintained by Fireblocks on the Platform on behalf of its customers).

As such, Fireblocks should not be regulated as a crypto asset secondary service provider ("CASSPr"). We believe this conclusion is consistent with the generally accepted principle that technology service providers that do not have control of, or exercise possession over, customer crypto assets are not intended to be included in the definition of a CASSPr.

2. **Question 11: Are the proposed obligations appropriate? Are there any others that ought to apply?**

We broadly agree that CASSPrs should be subject to certain minimum obligations in line with Treasury's proposal. To help further flesh out these obligations, we would like to highlight some risks that our customers consider when evaluating sub-custodians:

- **Data offshoring** - Does the organisation need to send transaction and customer records to a sub custodian located overseas, and do the laws applicable to the sub custodian provide adequate protection over these records? If the organisation is a financial institution, considerations around compliance with banking secrecy obligations are especially crucial.

- **Counterparty risk** - Does the sub custodian have sufficient financial resources in relation to the assets that it holds under custody? Is the sub custodian suitably insured? Unfortunately, the balance sheets of today's largest crypto-native sub custodians still pale in comparison to those of traditional financial institutions.

- **Regulatory and compliance risk** - Is the sub custodian bound by sufficiently robust laws in relation to the prevention of financial fraud, money laundering and terrorist financing? Does the sub custodian possess regulatory clarity in relation to its status to operate as a qualified custodian? A change in the regulatory status or compliance standards of the sub custodian can materially impact the operations and standing of a financial institution.

- **Technological risk** - What kind of technology does the sub custodian utilise? Does the sub custodian's technology offer the operational flexibility that is needed when an organisation grows? What assurance does the organisation have that the sub custodian's technology remains future-proof, bearing in mind the constant emergence of new blockchains and use cases for crypto assets.

- **Operational risk** - Is the sub custodian able to support the organisation's need to deal with its crypto assets on a 24/7 basis and at short notice? With the volatility of the crypto market, organisations may need the ability to be able to buy or sell their crypto assets at short notice at any time of the day.

The risks highlighted above may also affect an organisation's risk profile in relation to its insurers and consequently, insurance premiums.

The many considerations to be made on sub custody tend to result in our customers (mainly established financial institutions) deciding to deploy a direct custody model where they custody their own crypto assets instead of engaging a sub custodian. Direct custody enables financial institutions to leverage their own balance sheets and retain tighter control around third party risks.

3. **Question 20: Are there any additional obligations that need to be imposed in relation to the custody of crypto assets that are not identified above?**

We note that the Consultation Paper has identified the safeguarding of private keys as the only security concern for crypto asset custody. As we have highlighted above, the private key is but one of the possible attack vectors. We propose that the minimum standards for the safe custody of crypto assets by CASSPrs be expanded to include expectations around:

- Mitigating the risk of a compromise of account and wallet login credentials and authentication, whether by external hackers or rogue employees; and
- Mitigating the risk of compromise of deposit addresses.

****

We look forward to further discussions with Treasury on the points raised in this submission and generally on the broader crypto economy. Please do not hesitate to reach out to John McCarthy [redacted] and Stephen Richardson [redacted].

Yours faithfully,

John McCarthy
General Counsel

Fireblocks

5 July 2022

Director - Crypto Policy Unit
Financial System Division
The Treasury of the Australian Government
Langton Crescent
PARKES ACT 2600

By Email: Crypto@treasury.gov.au, Ben.Jordan@treasury.gov.au

To whom it may concern:

Fireblocks thanks Treasury for taking the time to speak with us about our custody solution and our 27 May 2022 response to Treasury's 21 March 2022 Consultation Paper - Crypto asset secondary service providers: Licensing and custody requirements. As we mentioned during our 14 June 2022 meeting, we have been preparing a proposal for the operational and technical requirements that should be imposed on a custodian of crypto assets. This proposal is now ready and we have appended it to this letter.

Please do not hesitate to reach out to John McCarthy [redacted] and Stephen Richardson [redacted] should you require additional information or clarification on any of the matters raised in our proposal. We look forward to Treasury's next steps on this.

Sincerely,

John McCarthy
General Counsel

Proposed Operational Requirements for Crypto Custodians

Crypto assets differ significantly from traditional financial instruments. Securing them properly requires appropriate operational standards that account for, among other things, the anonymity and immutability of blockchain transfers, the bearer nature of the assets, the importance of public and private keys, the ability to acquire assets through usage opportunities (e.g. staking) and distribution mechanisms (e.g. forks and airdrops).

Fireblocks recommends that a crypto asset custodian should, at the minimum, maintain operational standards to ensure:

- Private key security
- Secure transfers
- Segregation of customer assets
- Business continuity
- Security best practices

Details on each of these categories are set forth below.

1. Private Key Security

Private keys are necessary for the "signing" of blockchain transactions that move crypto assets from one address to another. Given this critical function, private keys must be securely generated, stored, and used. In order to protect private keys, crypto asset custodians should ensure the following:

a. Secure Generation of Private keys

Crypto asset custodians should take steps to ensure that the private key is not compromised at the point of generation by, for example:

- Ensuring that the private keys are generated in a distributed manner, so that at no point is a single private key present. 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).

b. Secure Cloud and On-Premise Storage of Private Keys

Crypto asset custodians should adopt solutions and measures that minimize the risk of loss and unauthorized access of the 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, in each location where a private key material is contained, it 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) hardware-level secure enclave technology (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. Hardware-level secure enclaves isolate sensitive data within a system. Each has its advantages, although compared to HSM, hardware-level secure enclaves offer certain key benefits:

- A bad actor that gains possession over the HSM can use the private key material stored on the HSM to sign transactions. Whereas, with secure enclaves, even if a hacker gains control of the server/device containing the private key, the hacker will not be able to access the private key material.
- HSMs have a fairly limited logic. The request to sign a transaction is validated against an external access token that a server or computer stores. A bad actor that compromises that server or computer can obtain the authorisation token and force the HSM to sign transactions. On the other hand, secure enclaves are able to protect cryptographic algorithms such as MPC and zero-knowledge proofs.
- While HSMs can protect the codes and data in relation to a private key, they are unable to protect policies (e.g. transaction authorisation policies, as described below) or transaction workflow logics. Custodians using HSMs therefore implement such policies and logics in user-mode, making it easy for bad actors to modify such policies and logics to circumvent transaction authorisation controls. On the other hand, secure enclave technology is able to isolate and protect policies, whitelisting databases, and workflow logics.
- HSMs are operationally burdensome since they require certain employees to be physically present where the HSM is located; whereas secure enclaves are operationally elastic and have a high degree of scalability across public clouds and on-premise deployments.

c. Zero Online Connection for Any Cold Storage Solutions

Cold storage solutions are perceived to be more secure than hot storage solutions. This is because the storage of private keys in an online environment, which is the case for a hot storage solution, causes the private keys to be vulnerable to bad actors. On the other hand, if the full private keys are not exposed online, the risk of compromise is diminished. However, not all cold storage solutions stay offline all the time. For example, some cold storage devices may have to be connected to a computer (that will have internet connectivity) in order to sign transactions. This brief moment of connection to the computer may run the risk of exposing the private key to compromise.

For security, crypto asset custodians should therefore ensure that they employ cold storage solutions in which neither the private key nor the device securing the private key is required to come online at any stage after the completion of the initial device setup and installation.

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.[1]

d. Transaction signing that minimizes 'single point of failure' risk

Crypto asset custodians should avoid the use of a single private key to sign transactions.

Today, the two most common technologies in the market that seek to eradicate the single point of failure risk are multi-signature (commonly known as "**multi-sig**") and multi-party computation ("**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 private key is able to authorize transactions in relation to the associated crypto assets.

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 that manages to gain control over one of the endpoints will not be able to access 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.

It is possible that newer and more secure signing approaches may be developed in the future. A crypto asset custodian needs to carefully consider the risks and benefits associated with each signing approach. It is important that regulation does not mandate any one type of signing approach so as to provide crypto asset custodians with the flexibility to utilize the technology that is most appropriate for their business.

In any event, the theoretical protocol should be reviewed by third parties, and one or more third-party "white box" security code reviews should be implemented on the solutions.

2. Secure Transfers

Even without access to the private key, crypto assets can be maliciously stolen through unauthorized transactions. For example, an organization's internal personnel (e.g. employees or

[1] Attackers have developed dozens of methods for using USB devices to compromise computers, and others are likely to proliferate. See, e.g., https://www.bleepingcomputer.com/news/security/heres-a-list-of-29-different-types-of-usb-attacks/.

contractors) may collude to steal the organization's crypto assets. Or a hacker may deploy malware to send an organization's crypto assets to the hacker's deposit address instead of the intended recipient. The danger of unauthorized transactions is compounded by the fact that transactions conducted over most blockchains are immutable, making them difficult or impossible to reverse, even if the recipient of the crypto assets can be identified.

In order to mitigate the risk of unauthorized transactions, a crypto asset custodian needs robust and secure systems and practices for the validation, review, and execution of transactions, including the following:

a. Transaction Authorisation Policy

The custodian should ensure that only successfully authorized transactions proceed to signing by implementing a transaction authorisation policy (**TAP**). TAPs should be:

- Customisable, to accommodate corporate governance, legal, and compliance requirements and changes in organizational structures.

- Secured against compromise from external and internal bad actors (e.g. through encryption technology or storage in a hardware-level secure enclave within a cloud server).

- Authorizations should be validated through multi-factor authenticators (including biometric and/or hardware tokens), and securely recorded for later audit.

b. Secure Transfer Environment

The custodian should deploy a secure environment for the querying of recipient deposit addresses and transfer of crypto assets in order to mitigate man-in-the-middle attacks and recipient deposit address spoofing. Any such environment should be protected from external and internal attacks through hardware-level protection. Acceptable options include:

- Data-in-motion encryption technology.

- Multi-user approved whitelisting of withdrawal addresses.

3. Segregation of Customer Assets

A crypto asset custodian needs to be able to segregate each customer's crypto asset holdings from the holdings of other customers (and from any crypto assets the custodian may hold on its own behalf).

Segregation is necessary to protect each customer's holdings from creditors of other customers and/or the custodian itself. Crypto assets should be segregated on the blockchain, meaning that

the crypto asset custodian needs to be able to maintain unique public and private keys for each customer's crypto assets.

Blockchain segregation – as opposed to commingling all holdings (whether belonging to customers or the crypto asset custodian) and relying on internal records to document each party's holdings – provides customers with an added layer of assurance that their crypto assets are secure because:

- Blockchain segregation makes it clear that the holdings belong to customers and cannot be used by the crypto asset custodian to conduct business operations.

- Internal records may not be fully accurate and up-to-date, especially where there is a high frequency of transactions undertaken by multiple customers at the same time.

- If the crypto asset custodian becomes insolvent, the segregation of customer holdings serves to ringfence such holdings from the creditors of the crypto asset custodian, allowing customers to withdraw their assets without having to undergo lengthy legal tussles with the creditors.

4. Business Continuity Plan

Operational disruptions, if not addressed promptly, compromise the ability of a crypto asset custodian to meet its obligations to its customers. Given the volatility of the crypto market and the ability to trade crypto assets on a 24/7 basis, severe disruptions in the crypto asset custodian's operations may result in significant financial damages for its customers. Crypto asset custodians should therefore strive to achieve high levels of service availability (e.g., 99.9% of the time, which is a generally accepted industry standard).

Custodians should also maintain an effective business continuity plan ("**BCP**") to minimize the impact of operational disruptions on the crypto asset custodian's ability to continually deliver its services. Most BCP practices for traditional financial institutions would also apply to crypto asset custodians. Among other things, a minimally adequate BCP for a traditional financial institution should: identify critical business services and functions and establish service recovery time objectives for these services; identify critical third party dependencies and impose obligations on those third parties to ensure their own robust BCPs; and continually review, improve, test, and audit the BCP.

Crypto asset custodians should be subject to additional BCP requirements due to the unique nature of their services. In particular, a crypto asset custodian should have a comprehensive plan that guides the process around private key reconstruction and crypto asset retrieval without any dependency on the custodian's service/technology providers (including in the event of a disaster giving rise to the need for recovery). The back-up recovery package should be generated in a secure manner and stored, with appropriate encryption, in an offline, air-gapped manner and with access given only to authorized individuals during pre-defined circumstances and with all requisite

controls (technical and otherwise) and reporting in place. It is important that only the customer has access to the back-up recovery package.

5. Security Best Practices

Crypto asset custodians should maintain certain minimum cybersecurity practices and controls, including the following:

- Governance, Risk & Compliance (GRC) program, to manage crypto & cyber risks, enable the custodian to reliably achieve objectives, address uncertainty, and act with integrity.

- Independent verification for their custodial solution in accordance with international standards such as ISO/IEC 27001:2005 (Information Security Management), ISO/IEC 27017:2015 (Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services), ISO/IEC 27018:2019 (Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors), and Service Organization Control (SOC) 2 Type 2.

- Security Operations Center, for the custodian to identify and respond to cybersecurity risks in a timely manner.

- Vulnerability and Patch Management Program including regular penetration tests, or authorized attacks performed on a computer system to evaluate its security and uncover vulnerabilities. The custodial solution provider should adapt offensive security methodology and use a combination of methods by internal and external actors to ensure a high degree of accuracy in its evaluation of its systems.

- User awareness program, to educate and test employees to help protect the custodial solution provider from phishing and other social-engineering attacks.