QUESTIONÁRIO

SEGURO CRYPTO DIGITAL ASSET

YOU MUST READ THIS BEFORE SIGNING THIS FORM.

I declare on behalf of all insureds after inquiry, that the statements and particulars in this proposal and all supplemental materials provided along with or in conjunction with this attachment for the purposes of the insurer's evaluation and decision to issue this coverage are true and no material facts have been misstated or suppressed. I agree that this proposal form, any attachment, any information submitted therewith and any and all other information supplied or requested shall form the basis of any contract of insurance effected thereon. All written statements and materials furnished to the insurer in conjunction with this application are hereby incorporated by reference into this application and made part thereof. Signing this proposal does not bind the policyholder to complete this insurance.

QUESTIONARIO SEGURO DE ARMAZENAMENTO DE CRIPTOMEDAS
CRYPTO STORAGE PROPOSAL FORM

General Information

Name:

Address:

State/Country:

Date:

Registration:

Description:

General Questions

1. What are the specific risks that the insured wishes to transfer to insurers via a cryptocurrency policy? Hot, cold, etc?

2. What controls are in place at the insured level to assess and address financial crime (Anti-Money Laundering, Sanctions, Bribery & Corruption) risks? Have these controls been vetted by legal counsel and what is the opinion of any attorneys that have reviewed and approved such controls?

3. What internal resources, both technology and personnel, does the insured have in place to address and mitigate financial crime risk?

4. Has the insured conducted an independent risk assessment with respect to the financial crime risk(s) posed by their business and, if so, has the insured put in place appropriate controls and procedures to address and mitigate those risks?

5. How does the insured intend to market its services, with specific respect to any insurance that the company wishes to purchase?	
6. What is the business model for the operation to be insured? (cryptocurrency exchange / crypto currency custodian for third parties / cryptocurrency miner / investment fund / other - please be specific).	
7. When did the insured commence custody operations?	
8. Please separately provide a copy of the latest audited financial reports, the latest annual statement and year-to-date financials. Please confirm Y/N	
9. Please provide details of any financial services license held by the company.	
10. Please separately provide a Register of Directors (listing both former and current directors) and Senior Managers including the specific industry employment history for each senior member of management or board member. Please confirm Y/N	
11. Please confirm none of the above listed persons has ever been convicted of any crime.	
12. Please provide the addresses of all physical locations anticipated to provide storage solutions for crypto currencies.	

13. Has the company previously purchased any form of crypto currency insurance (hot / warm / cold)?

14. Has the insured suffered any loss instances from crypto currency risks (insured or otherwise)? If so please provide full details and amounts of each instance.

15. Precisely which crypto currencies is the insured requesting to insure? Please note this insurance does not provide cover for any crypto currencies that are:
not recorded on decentralized ledger; or
unencrypted.

16. What is the current number of each crypto currency under the care, custody and control of the insured? How has this developed over the past 3 years?

17. What policy limits are being requested?

18. Please confirm whether there is any counterparty risk to any 3rd party concerning the storage of private keys (e.g. crypto currency exchange or custodian)? This could be either:
(a) Providing secure custodial services to the insured's clients for their private keys; and/or
(b) Utilizing a third-party party to provide secure custodial services for the insured's own private keys and/or for the private keys of the insured's clients.
For each instance please provide copies of the contracts between the insured and the

third party establishing liability (or lack thereof) for the storage of crypto/digital assets.

19. If acting on behalf of third-party customers what is the estimated split between retail or institutional investors / clients?

20. If acting on behalf of third party customers how are the customers' assets are segregated from the insured's?

21. What is the current or anticipated allocation of crypto between cold and hot storage for your own crypto? For your customer's crypto?

22. What is the on-boarding process for new employees? What background checks are undertaken and by whom? How long must an employee work for the company before being given responsibility for any risk sensitive procedures / information?

Risk Specific Requirements/Questions/Considerations

23. In a separate document attached to this application, please provide your custody protocol/policies/procedures which describe in as much detail as possible the cradle to grave life cycle of all cryptocurrency private keys under the your control. If this process differs for different cryptocurrencies please detail each process separately. In addition to written record please also provide a flow diagram for each process. At a minimum this process should deal with, but is not limited to:

(a) The initial generation of private keys:

• How is this conducted?

• Where is this conducted?

• Who has the authority to create new private keys?

• Who provides the oversight for the above (i.e. four eyes process / dual control)?

• What is the maximum USD value you would transfer to the public address derived from a newly created private key?

(b) The creation of any multi-signature contracts for private keys:

• What is the minimum "m-of-n" required to perform a transaction for a multi-signature contract?

(c) The custody chain of private keys:

• Once created are the private keys encrypted in any way, if so by what process?

• On what physical media are the private keys stored?

• If using any form of digital storage how is the risk protected against malware infiltration (for reference please see: https://arxiv.org/pdf/1804.08714.pdf)

• How is dual control established for the generation, custody and subsequent storage for private keys?

(d) The cold storage of private keys:

• What are the physical addresses of the secure facilities for storing private keys?

• If multi-signature type contracts are utilized please confirm different secure facilities are utilized for storing each of the

• If the physical address for the storage of private keys differs from the physical address at which the private keys were

• Are tamper proof bags / boxes used for the protection of the media on which private keys are stored?

• If tamper proof bags / boxes are used are one time numbered seals used for each bag / box?

• What is the security rating of the vault or safe the private keys are stored in?

• What alarm and CCTV systems are in place, who is responsible for monitoring these?

• Are any guards utilized (armed other otherwise). Does the number differ during working hours and closed periods?

• What notice period is required for the insured to access the cold storage facility?

(e) Retrieval of private keys:

• Under what circumstances would a private key be retrieved from cold storage?

• How frequently is this anticipated to occur?

• What is the retrieval process for accessing private keys? How is dual control maintained for this process?

• Will transactions out of cold storage only ever return crypto currency to the public address from which it was received?

• If a transaction out of cold storage is for less than 100% of the crypto currency contained in the public address derived from the private key to be used where will the remaining balance will be deposited?

(f) What redundancy or backup methods are employed for the storage of private keys?

(g) How often are backups audited and tested to ensure they are fit for purpose?

(h) How is the safe and secure disposal of any materials used to generate, record or store private keys ensured?

(i) Is an auditable log retained for each of the processes detailed above?

(j) Would the insured be prepared to undergo a 3rd party risk survey prior to the inception of the policy and at their own expense (to be funded by insurers in the event of a firm order)?

Risk Management Principles and Considerations

24. Designated Premises and Secure Areas

(a) Designated Premises must be named and addressed unambiguously and specified by reference to GPS coordinates.

(b) Secure Areas must be certified as secure against intrusion or damage due to natural events or malicious events. Please confirm ☐ Yes ☐ No

25. Hardware

(a) Hardware must have high-specification equipment recently purchased from reputable suppliers. Please confirm. ☐ Yes ☐ No

(b) Hardware must not permit access by external media, such as flash drives, CD-ROMs, etc. Please confirm. ☐ Yes ☐ No

(c) Hardware used for the generation, storage, retrieval, reconstruction and retirement of Cryptocurrency Private Keys must be initiated with up-to-date versions of a standard operating system software (for example, Linux, Windows, Apple OS) prior being placed in the Secure Area. Please confirm. ☐ Yes ☐ No

(d) Hardware must not be used for any purpose other than for the generation, storage, retrieval, reconstruction and retirement of Cryptocurrency Private Keys. For example, it must not be used to host other applications, games, entertainment or business software (such as word processing applications), etc. Please confirm. ☐ Yes ☐ No

26. Software and Algorithms

(a) Encryption and Cryptocurrency Private Key infrastructure algorithms must use random number generator algorithms from software libraries that are compliance with the FIPS (Federal Information Processing Standard) 140-2 Standard (Security Requirements for Cryptographic Modules) and any subsequently adopted successors to this standard. Please confirm. ☐ Yes ☐ No

(b) Each Cryptocurrency Private Key and its associated Cryptocurrency Address must be generated on a computer that has no access via fixed or wireless means to any network, whether public or private, and has never had such access. Please confirm. ☐ Yes ☐ No

(c) Each Cryptocurrency Private Key must be copied and encrypted immediately upon generation, with all unencrypted versions immediately wiped from all hardware and software. Please confirm ☐ Yes ☐ No

(d) Where Cryptocurrency Private Keys are to be sharded (divided), each encrypted copy of the Cryptocurrency Private Key must then be sharded into not less than [five] parts, with not less than a ratio of [three] of [five] parts required in order to reconstruct the relevant Cryptocurrency Private Key. Each part relating to one copy of the Cryptocurrency Private Key must be held in separate Secure Areas (with no identical parts relating to separate copies of the same encrypted Cryptocurrency Private Key held in the same Secure Area) and under the control of separate Designated Custodians or separate groups of Designated Custodians. Please confirm

☐ Yes ☐ No

(e) Where Cryptocurrency Multi-Signature Addresses are to be utilized each Cryptocurrency Multi-Signature Address must be comprised of alphanumeric characters that is mathematically derived from [three] Cryptocurrency Addresses and requires no less than [two] of the [three] Cryptocurrency Private Keys relating to the Cryptocurrency Addresses from which it was derived to authorize any transaction associated with it. Please confirm ☐ Yes ☐ No

(f) Secure processes for generation, copying, encryption and (if relevant) sharding of Cryptocurrency Private Keys; storage of encrypted Cryptocurrency Private Keys; retrieval and (if relevant) reconstruction of Cryptocurrency Private Keys (in the case where they are lost or intended to be used) and destruction of Cryptocurrency Private Keys (in the event that they are compromised or to be retired) must be defined. Please confirm ☐ Yes ☐ No

(g) The use of a Cryptocurrency Private Key to sign a transaction (following its retrieval and (if relevant) reconstruction from a Secure Area) relating to a Cryptocurrency Multi-Signature Address must be governed by a Cryptocurrency Multi-Signature Contract. Each Cryptocurrency Multi-Signature Contract must be programmed in computer code to implement a natural language contract, a template version of which must be notified by the Insured to the Lead Insurer for review prior to the inception of the policy. Each Cryptocurrency Multi-Signature Contract relating to the relevant Cryptocurrency Multi-Signature Address notified to the Lead Insurer in accordance with the policy must be uploaded to the relevant Cryptocurrency Protocol immediately following generation of such Cryptocurrency Multi-Signature Address. Please confirm ☐ Yes ☐ No

27. Processes

(a) Documentation setting out all interactions between system elements, devices, application software and Designated Custodians must be presented in the form of comprehensive Message Sequence Charts (MSCs) (International Telecommunications Union Standard Z.120 approved 2011-02-13). Please confirm ☐ Yes ☐ No

(b) Designated Custodians must include (i) persons who, in the normal course of their employment or agency have access to the physical media on which Insured Interests are stored and

(ii) person who are employees of the Insured and have knowledge of, or access to, an Insured Interest at any stage following generation until retirement of such Insured Interest. Designated Custodians must be specified by reference to either: (i) a record of pre-determined persons identified by name and role or (ii) a defined class of persons in respect of which it is possible to identify each constituent member of such class (in which case, a record of all persons identified as Designated Custodian by name and role must be maintained by the Insured at all times and made available to the Insurers upon request). Records must be maintained identifying any subsets of roles of Designated Custodians and listing powers, obligations, workflows and interactions of each such role. Any changes to the descriptions of Designated Custodian roles or updates to the list Designated Custodians must be communicated to the Insurer within 15 days of the changes being made. Please confirm Designated Custodians at time of

(c) Records must be maintained identifying any actions that require approval from more than one Designated Custodian or independent stakeholder, specifying the precise nature of these requirements. Please confirm ☐ Yes ☐ No

(d) Operational compliance with the documentation described above must be subjected to ongoing monitoring (for example, an independent audit or assessment) not less than once per quarter. Evidence of such compliance monitoring must be made available to the Insurers upon request. Please Confirm ☐ Yes ☐ No

28. Testing

(a) All systems must be tested independently by an independent third party "red-team" tasked with penetrating the system (pen- testing) and retrieving valuable information such as Cryptocurrency Private Keys. Such testing is to be undertaken at least annually.

(b) Documentation setting out test plans and reporting on the results of tests undertaken according to such plans must be made available to the Insurers upon request.

(c) Cryptographic hardware and software systems should be tested by a Cryptographic and Security Testing laboratory accredited by the US/Canada National Voluntary Laboratory Accreditation Program. Please confirm ☐ Yes ☐ No

(d) The results of testing must certify that all systems are at least at Level 3 in the 4 level classification system of the FIPS 140- 2 standard (Security Requirements for Cryptographic Modules) and any subsequently adopted successor standards. Please confirm

☐ Yes ☐ No

29. Risk Assessment

(a) The Insurer may require that your Risk Management Protocols (or equivalent) be subjected to a risk assessment undertaken by a third party acceptable to the Insurer with a view to identify all potential risks, points of attack and any possibilities for collusive attacks must be undertaken prior to the inception of the policy. (j) Would the insured be prepared to undergo a 3rd party risk survey prior to the inception of the policy and at their own expense (to be funded by insurers in the event of a firm order)? Please confirm ☐ Yes ☐ No

(b) In the event the Insurer requires an independent risk assessment to be conducted, a report detailing the outcome of the risk assessment along with plans for risk preclusion and mitigation must be presented to the Insurers prior to the inception of the policy.

30. Collusion Awareness

(a) Assuming the Risk Management Protocol process is followed to the letter, and assuming an imperfect knowledge of the technical security architecture for any one employee, what the minimum number of employees that need to collude in order to perpetrate a theft?

(b) Assuming the Risk Management Protocol process is partially circumnavigated by an employee or employees with perfect knowledge of the technical security architecture, what is the minimum number of employees that need to collude in order to perpetrate a theft?

Required documentation:

- Latest audited report
- Latest annual statement
- Year-to-date statement
- AML/KYC Manual
- Complete application/submission for your financial license, or equivalent
- Service provider agreements/contracts for the following, to the extent applicable:

1. Any form of crypto custody
2. AML/KYC
3. Regulatory Compliance

Name of Applicant's authorized representative and title

Date