SECURITY

overview

DESTOCX

1. DIGITAL ASSET SECURITY

The majority of our customers' digital assets (e.g., bitcoin) are held in our offline (i.e., air-gapped) vaulted storage system ("Cold Storage"). Only a small portion of digital assets are held in our online wallet ("Hot Wallet").

2. HOT WALLET

- ✓ Our Hot Wallet environment is hosted on OVH Datacenter. OVH has a proven track record for physical security and internal controls.
- ✓ Tiered access-controls are applied to our production environment to restrict access to employees based on role, following the principle of least-privilege.
- ✓ Administrative access to our production environment requires multi-factor authentication.

3. COLD STORAGE

- ✓ Our Cold Storage system provides two tiers of offline storage dubbed "cold" and "cryo" (short for "cryogenic") for improved security and redundancy.
- ✓ We use Multi-Signature technology ("Multi-Sig") to provide both security against attacks and tolerance for losing access to a key or facility, eliminating single points of failure.
- ✓ All Cold storage are stored in guarded, monitored and access-controlled facilities that are geographically distributed.
- ✓ Hardware is sourced from diverse manufacturers to guard against supply-chain risks.
- ✓ All fund transfers require the coordinated actions of multiple employees (i.e., all facilities are "no-lone zones").

4. INTERNAL CONTROLS

- ✓ Multiple signatories are required to transfer funds out of Cold

Storage.

- ✓ Our offices do not store or contain anything of value. All private keys are stored offsite in secure facilities (see Digital Asset Security above).
- ✓ All employees undergo criminal and credit background checks and are subject to ongoing background checks throughout their employment.
- ✓ All remote-access by employees uses public-key authentication – no passwords, one-time passwords (“OTPs”) or other phish able credentials are allowed.