CASE STUDY 1

PROVIDING SEGREGATION OF DUTIES FOR DIGITAL ASSET CUSTODY

BACKGROUND

A US client, receiving and sending cryptocurrency and issuing ERC20 tokens, required a secure Treasury Management function that ensured that funds were held securely and not at risk from external or internal theft or fraud.

The existing solution was to use multiple wallets, along with a multisig approval process. This was realized as inadequate as:

- Risk of internal participants leaving and retaining their knowledge about their wallet's key.
- A Bitcoin multisig wallet is easily identified – thereby increasing vulnerability.
- Required all parties to participate simultaneously in signing process and this led to delay in completing signing of transactions.
- Range of crypto assets trade was limited to only those where the protocol was multisig compatible.

SOLUTION

Hokan shielded by Lokblok, provides a robust, secure, private key management service using Threshold Signature Scheme (TSS), to significantly improve the security of digital assets. Using TSS means that not all signatories are required to co-sign a transaction (instead an N of M solution has been implemented, whereby at least N signatories of the M total signatories can be used).

BENEFITS

- Segregation of Duties has been enhanced by permitting a designated subset of approved signatories to agree to a transaction being signed asynchronously, i.e., not all participants need to sign at the same time. This is much more flexible.
- Speed of transaction review, approval and signing significantly reduced.
- Security is obfuscated by it no longer being possible to identify that the funds are managed via Multisig.
- The range of protected assets has been extended beyond just native Bitcoin (not all blockchains provided multisig capability). This means that the organization can now offer a custodial capability dealing in multiple cryptocurrencies and tokens, including NFT's.
- Easily demonstrable to auditors that effective and robust segregation of duties now in place.
- Solution allowed as many wallets as desired by client to be used for segregation, thereby further reducing the risk through improved security as a master wallet was not needed.