



lokblok®

CASE STUDY 3

DIGITAL ASSET INHERITANCE

BACKGROUND

Clocr, a global digital asset platform sought a solution using split keys to enable designated guardians to help in the recovery of the private key to digital assets in the event of the owner's death. This meant that designated participants were responsible for securing shards of the key. This introduced a risk that they could lose part of the key (or it could be compromised through a hack). The existing solution meant that they were taking custodial responsibility for part of the key and could be subject to legal action requiring them to surrender their shard so that the main key could be reconstituted.

An important feature with a digital will is that private keys and seed phrases should never be included as part of the will as the latter document becomes public knowledge once probate is obtained from the relevant authority. It is crucial therefore that these details are not included as part of the will itself.

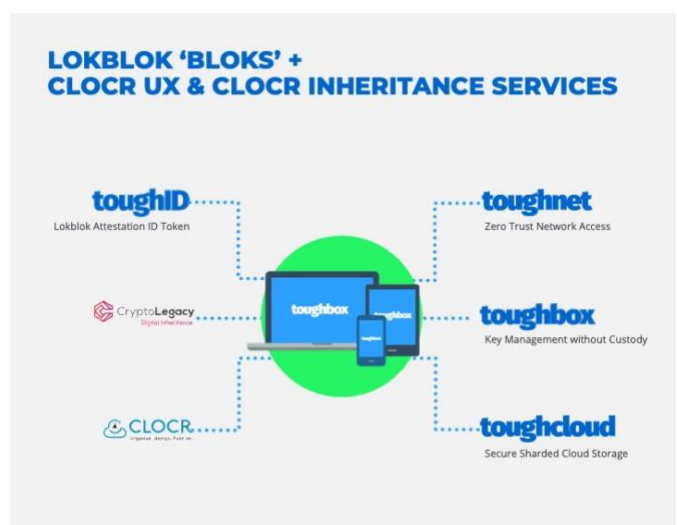
SOLUTION

CryptoLegacy Shielded by Lokblok, means that a unique method to provide key recovery can enable designated personal devices and/or people (or organisations) to act as recovery agents but not as custodians. This also reduces the security risk as they do not hold a shard of the key which can be used to reconstruct the key. Additionally, it means that the actual private keys (or seed phrases) are not held as part of any document set as part of a will. This means that when probate is granted to the executor of a will, the private keys/secrets are not made public.

The Lokblok Toughbox solution provided a more robust and secure means for secret recovery which could be extended to include private keys, seed phrases and other files. This was further extended to include encrypted, cloud-based, data storage with Lokblok's Toughcloud which allows custodial services to put in place additional data storage/retention policies.

BENEFITS

- Recovery agents do not hold any part of a key in custody
- A pool of recovery agents can be designated and the secret can be reconstituted with an agreed minimum threshold of participants. This means that not every recovery agent is required to participate in the recovery process
- Custody can be extended to cover not just private keys but also seed phrases, passwords, documents and files



- Data can be secured and distributed using cloud-based platforms and additional retention policies can be applied
- The will does not contain private keys or seed phrases