Vault Description (Part 1)

The Bitcoin Vault is composed of the following elements:
- 5 Seeds
- Passphrase
- Wallet Descriptor
- Offline Signing Device

The 5 Signing Keys form the highly-confidential part of the Bitcoin Vault. They are the combination of each Seed and the Passphrase.

The Signing Keys serve to sign outgoing transactions from the Vault. They must ALWAYS remain disconnected from the internet and NEVER be shared with anyone else than the owner and the heirs.

For each Signing Key exists an associated Public Key.

The 5 Public Keys form the semi-public part of the Bitcoin Vault, also known as the Wallet Descriptor.

The Wallet Descriptor, once loaded in a Wallet Management Interface, allows the vault to interact with the Bitcoin network, and receive information on the vault, such as the previous transactions and the total balance.

Whereas the Public Keys are meant to be loaded into an internet-connected device in order to interact with the network, the Signing Keys must ALWAYS remain disconnected from the internet and kept secure.

The Offline Signing Device allows the owner and the heirs to sign outgoing transactions from the vault, while keeping the Signing Keys offline and disconnected from the internet.

To do so the Signing Device receives an unsigned transaction from the Wallet Interface via QR code, signs it offline with the Signing Keys loaded temporarily in the device, and then returns it to the interface via QR code so that it can be broadcast.

For an outgoing transaction to be valid, it needs 3 signatures from the 5 Signing Keys.

The 5 Seeds are stored in 5 different locations:
- Location 1
- Location 2
- Location 3
- Location 4
- Location 5

Each Guardian is in charge of securing and protecting one of the Seeds.

Each Seed combined with the Passphrase forms one of the Signing Keys. For example, Seed 1 combined with the Passphrase forms the Signing Key 1.

The Passphrase is secured and protected by the heirs and the owner.

WARNING:

Sharing highly-confidential information like the Seeds and Passphrase on the Internet or with third parties will undermine the safe's security, and put the funds at risk.

Take the time to fully understand how the Bitcoin vault works before attempting to make any transactions with it, to ensure its security.