Key sharding

Key sharding involves cryptographically splitting a private key or recovery phrase into several pieces. These pieces can be shared among several parties and/or locations. A threshold, or all, pieces are recombined to recover the private key or recovery phrase. Recombined private keys can be used in the same way as single key scheme. Recombined recovery phrases can be used to restore wallets. This gives a similar experience to true multisig.

A not so widely adopted standard for key sharding exists called SLIP-0039 by Satoshi Labs. SLIP-0039 splits up a 12, 18, or 24 word recovery phrase into multiple (up to 16) 20 or 33 word recovery word shares. These shares can be combined to restore the original recovery phrase which is then used to restore the wallet.

{image}

Pros

- **Lower fees –** Sharding gives a similar security model to multi-key distributed setups with lower fees as only one signature is committed on-chain.
- **More private - Only one signature is recorded on-chain concealing the identity of other parties if used in a multi-party setup.
- **Theft resistant -** High resistance to loss from theft as pieces can be distributed.
- **Destruction resistant** – Using thresholds and distributed pieces this prevents having a single key that if destroyed all your bitcoin is lost.

Cons

- **Single point of failure** – When creating and combining pieces the private key exists on a single device making it susceptible to theft through malware.
- **No key invalidation -**
- **No standard -**
- **Poor auditability -**

https://github.com/satoshilabs/slips/blob/master/slip-0039.md

https://iancoleman.io/shamir/

https://iancoleman.io/shamir39/

https://trezor.io/shamir/

https://docs.keys.casa/wealth-security-protocol/rejected-key-schemes/key-sharding-shamirs-secret-sharing