SLIP39 macOS App

Perry Kundert

2022-02-02 22:22:00

Creating Ethereum, Bitcoin and other accounts is complex and fraught with potential for loss of funds.

All Crypto wallets start with a "Seed": a large, random number that is used to generate all of the actual Bitcoin, Ethereum, etc. wallets.

The best practice for using these wallets is to load this "Seed" into a secure hardware device, like a Trezor hardware wallet.

Contents

1 Security with Availability

For both BIP-39 and SLIP-39, a 128-bit random "seed" is the source of an unlimited sequence of Ethereum HD Wallet accounts. Anyone who can obtain this seed gains control of all Ethereum, Bitcoin (and other) accounts derived from it, so it must be securely stored.

Losing this seed means that all of the HD Wallet accounts are permanently lost. Therefore, it must be backed up reliably, and be readily accessible.

Therefore, we must:

- Ensure that nobody untrustworthy can recover the seed, but
- Store the seed in many places with several (some perhaps untrustworthy) people.

How can we address these conflicting requirements?