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 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. SLIP39 Mnemonic cards contain the recovery words, which are typed directly into the Trezor device to recover the Seed, and all of its accounts.

The macOS SLIP39 app helps you generate Mnemonic cards and back up this seed, securely and reliably, by distributing Mnemonic cards for the seed to partners, family and friends.

Later, if you (or your heirs!) need to recover the accounts, they can collect a sufficient threshold of the cards and regain access to the account.

Contents

1 Security with Availability

For both BIP-39 and SLIP-39, a 128-bit or 256-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?

1.1 SLIP-39 Mnemonic Recovery Cards

We don't recommend writing down one BIP-39 12-word or 24-word Mnemonic phrase, and hoping that **you** can find it, but that nobody else **ever** finds it!

Instead, generate a number of SLIP-39 Mnemonic cards, which can be collected to recover the Seed:

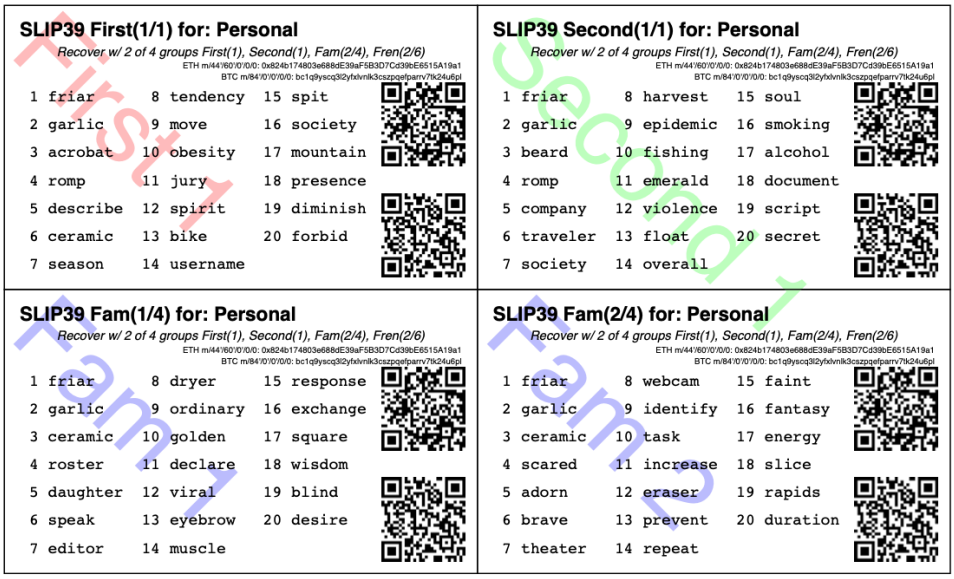

Figure 1: SLIP39 Cards PDF