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 **1**
1.1 SLIP-39 Mnemonic Recovery Cards 2

2 Affiliate Links **3**
2.1 Trezor 3

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:

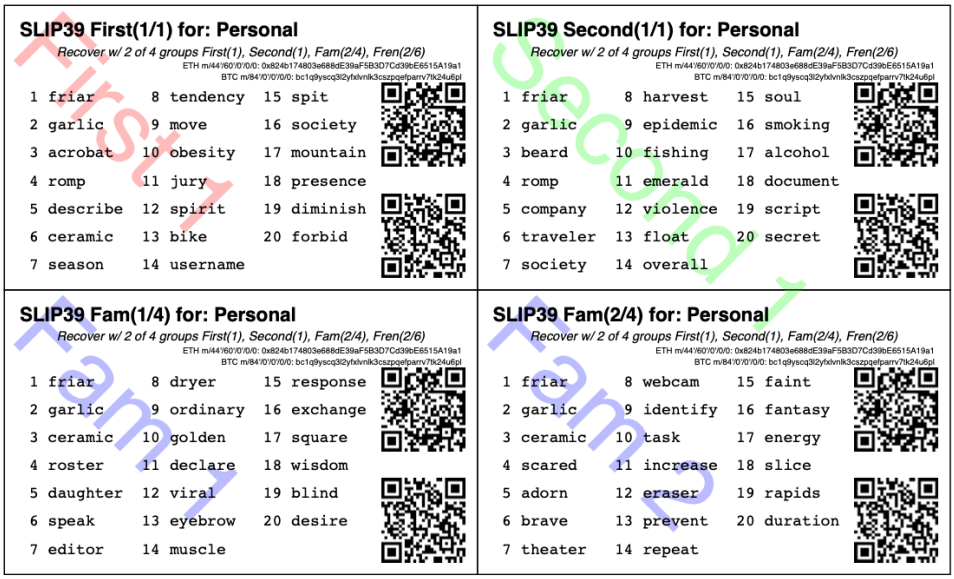
- Ensure that nobody untrustworthy can recover the seed, but
- Store the seed in many places with several (some perhaps untrustworthy) people.

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:



SLIP39 First(1/1) for: Personal

Recover w/ 2 of 4 groups First(1), Second(1), Fam(2/4), Fren(2/6)

ETH m/44'/60'/0'/0/0: 0x824b174803e688dE39aF5B3D7Cd39bE6515A19a1
BTC m/84'/0'/0'/0/0: bc1q9yscq3l2yfxlvnlk3cszpqefparrv7lk24u6pl

1 friar	8 tendency	15 spit
2 garlic	9 move	16 society
3 acrobat	10 obesity	17 mountain
4 romp	11 jury	18 presence
5 describe	12 spirit	19 diminish
6 ceramic	13 bike	20 forbid
7 season	14 username	

SLIP39 Second(1/1) for: Personal

Recover w/ 2 of 4 groups First(1), Second(1), Fam(2/4), Fren(2/6)

ETH m/44'/60'/0'/0/0: 0x824b174803e688dE39aF5B3D7Cd39bE6515A19a1
BTC m/84'/0'/0'/0/0: bc1q9yscq3l2yfxlvnlk3cszpqefparrv7lk24u6pl

1 friar	8 harvest	15 soul
2 garlic	9 epidemic	16 smoking
3 beard	10 fishing	17 alcohol
4 romp	11 emerald	18 document
5 company	12 violence	19 script
6 traveler	13 float	20 secret
7 society	14 overall	

SLIP39 Fam(1/4) for: Personal

Recover w/ 2 of 4 groups First(1), Second(1), Fam(2/4), Fren(2/6)

ETH m/44'/60'/0'/0/0: 0x824b174803e688dE39aF5B3D7Cd39bE6515A19a1
BTC m/84'/0'/0'/0/0: bc1q9yscq3l2yfxlvnlk3cszpqefparrv7lk24u6pl

1 friar	8 dryer	15 response
2 garlic	9 ordinary	16 exchange
3 ceramic	10 golden	17 square
4 roster	11 declare	18 wisdom
5 daughter	12 viral	19 blind
6 speak	13 eyebrow	20 desire
7 editor	14 muscle	

SLIP39 Fam(2/4) for: Personal

Recover w/ 2 of 4 groups First(1), Second(1), Fam(2/4), Fren(2/6)

ETH m/44'/60'/0'/0/0: 0x824b174803e688dE39aF5B3D7Cd39bE6515A19a1
BTC m/84'/0'/0'/0/0: bc1q9yscq3l2yfxlvnlk3cszpqefparrv7lk24u6pl

1 friar	8 webcam	15 faint
2 garlic	9 identify	16 fantasy
3 ceramic	10 task	17 energy
4 scared	11 increase	18 slice
5 adorn	12 eraser	19 rapids
6 brave	13 prevent	20 duration
7 theater	14 repeat	

Figure 1: SLIP39 Cards PDF

2 Affiliate Links

To assist you in obtaining various SLIP39 compatible components, we have established some relationship with reliable vendors.

2.1 Trezor

The Trezor Model T hardware wallet has built-in SLIP39 generation and recovery capability.