The macOS/win32 SLIP-39 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. SLIP-39 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 and win32 SLIP-39 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. Also, encrypted "Paper Wallets" can be output, to support software cryptocurrency wallets such as Metamask, Brave or various mobile phone wallets.

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

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, Bitcoin, etc. HD (Hierarchical Deterministic) 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:

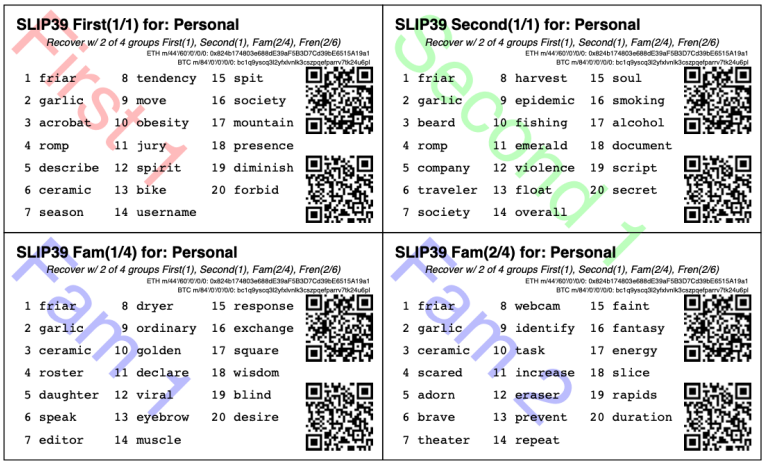

Figure 1: SLIP-39 Cards PDF

1.2 Paper Wallets

If desired, you can produce encrypted Paper Wallets, to support software crypto wallets (eg. Metamask, Brave or various mobile phone wallets):

2 Affiliate Links

To assist you in obtaining various SLIP-39 compatible components, we have established some relationship with reliable vendors.

2.1 Trezor

The Trezor Model T hardware wallet has built-in SLIP-39 generation and recovery capability. Enter the words on the SLIP-39 cards directly into the screen of the Trezor to recover your Cryptocurrency accounts.

We recommend the Trezor Model T for this reason. No other hardware wallet yet supports direct, on-screen SLIP-39 Seed recovery. This feature is, simply, so fundamentally important for Crypto Seed security and reliability that we consider it a necessity.

Figure 2: Paper Wallets

2.2 Netcoins.app

In Canada, one of the more highly regulatory-compliant Cryptocurrency exchanges is Netcoins.app; sign up with this referral link, and we both get some benefits.

They have higher than typical Interac e-transfer limits, which is very nice. However, they don't support a wide range of cryptocurrencies; presently, only BTC, ETH, XRP, LTC, BCH, USDC, and a few other lesser-known coins.

2.3 Crypto.com

Use my referral link for Crypto.com to sign up for Crypto.com and we both get $25 USD :)

The Crypto.com exchange has many more coins available, as well as a crypto-funded credit card that presently works in Canada.

2.4 Protecting your SLIP-39 Cards

Protect your printed SLIP-39 cards from water damage by laminating them in plastic or storing them in zip-loc bags before mailing them. Print the SLIP-39 cards and cut them out, and then lay them out with 1/2" margins (so you can cut them out after lamination and retain 1/4" borders), either with self-adhesive full-page laminating sheets - no machine required (or index-card size sheets), or with a heat-laminating machine in full-page pouches (or in index-card size pouches).

3 Privacy Policy

SLIP-39 does not save or store any data input to or output from the app. Any SLIP-39 Mnemonic card PDFs exported by the app are saved on your device in the location that you specify after clicking the 'Save' button.