The macOS/win32 SLIP-39 App

Perry Kundert

2022-02-02 22:22:00

Creating personal Ethereum, Bitcoin and other Cryptocurrency accounts is *urgently* needed, but is complex and fraught with potential for loss of funds.

All Crypto wallets start with a "Seed": a large, random number used to derive all of your 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 "Model T" 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 Cryptocurrency accounts. For the Ledger Nano and other hardware wallets supporting only BIP-39 Mnemonics, you can now use the SLIP-39 App to securely and reliably back up these BIP-39 phrases.

The macOS and win32 SLIP-39 App (download here – .dmg for macOS, .msi for Windows) 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 and computer-based wallets.

Later, if you (or your heirs!) need to recover **all** of your Cryptocurrency 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 derived from it 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 Back Up Your BIP-39 Phrase!

The SLIP-39 App helps you to break your BIP-39 recovery phrase into multiple "Groups" and "Cards", and recover it any time you need it. Any individual cards are **not** usable to access or recover the BIP-39 recovery phrase.

Even if you don't want to distributed the cards to multiple people, but just wish to more securely and reliably store your BIP-39 recover phrase, SLIP-39's Shamir's Secret Sharing System allows you to "break up" your BIP-39 recovery phrase into several pieces which you can store in different locations. If you lose some of them, you can still recover the BIP-39 recovery phrase!

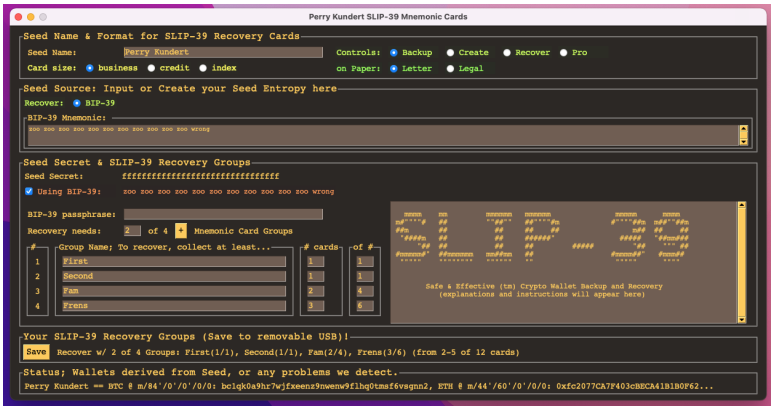

Figure 1: SLIP-39 App

1.2 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:

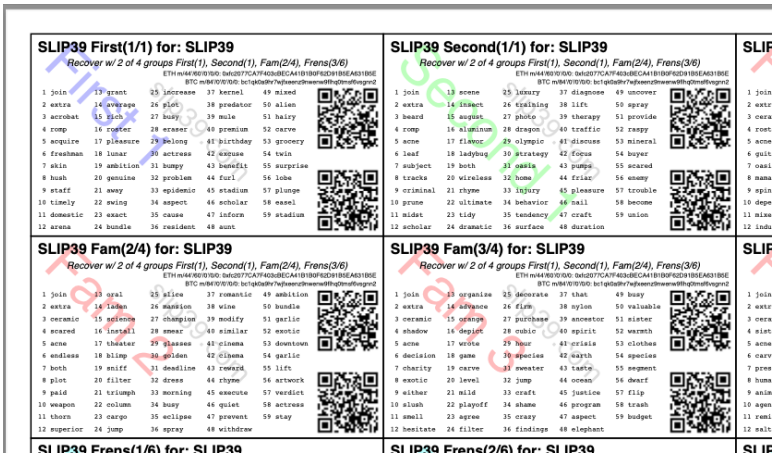

Figure 2: SLIP-39 Cards PDF

1.2.1 Why Not a BIP-39 Mnemonic Phrase?

If **everyone** you talk to is recommending that you just write down your 12- or 24-word phrase and store it somewhere, why not do this?

It is estimated that 20% of Bitcoin is already lost in the first 10 years of its existence, stored in wallet addresses that can never be accessed because the corresponding "Private Key" has been lost, or the passphrase forgotten.

The statistical chances of anyone successfully passing a Cryptocurrency wallet Private Key + passphrase or Seed to their heirs over a 50-year period is therefore very low. Since memory fades and "safe" storage places are lost, destroyed or forgotten, this risk actually increases exponentially over time.

I estimate the probability of successfully inheriting such a Paper Wallet + passphrase or BIP-39 Mnemonic protected Seed is probably less than 50%. Perhaps **much** less.

1.2.2 Why Not a BIP-38 Encrypted Wallet + Passphrase?

Have you ever forgotten a password to an online account?

Well, with a BIP-38 Encrypted Wallet + passphrase, there is *no password reset* option; there is no way to recover the passphrase.

If the Wallet is lost, there is of course no way to recover it, even if you have the passphrase.

This option is perhaps even less desirable than using a BIP-39 Mnemonic Seed phrase, because each and every Encrypted Wallet is exposed to this risk of loss.

1.3 Paper Wallets

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

1.3.1 Walking-Around Money

Money that doesn't *work* has low utility and hence low value. There are often situations where you want to transport money physically, perhaps to buy something somewhere where you have no access to a computer, or by mail. Paper Wallets allow this.

Figure 3: Paper Wallets

Losing this Paper Wallet usually results in the loss of the funds held in it. But, not if you generate it from your Seed!

Just pick a derivation path you aren't going to use for your own personal wallets (eg. ending in `..99'/0/0`), and generate some Paper Wallets (use each derivation path only once, of course). Fold them up so that the Private Key is not visible, laminate them and deposit funds into the wallet public address using the visible QR code.

The recipient can cut and unfold the Paper Wallet, exposing the private key and password hint, and can transfer the funds into their own wallet.

If the Paper Wallet is ever lost, you can recover the Private Key (it was derived from your Seed!), and transfer the Cryptocurrency back into one of your own wallets.

2 Recommended Vendors

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 Cryptocurrency Seed security and reliability that we consider it a necessity.

If you already have one of the less expensive Trezor wallets that only support BIP-39 backup, we also support those, using the same BIP-39 Seed Entropy backup via SLIP-39 as for the Ledger, and other traditional hardware wallets.

2.2 Ledger

The Ledger hardware wallets are also very popular – but they can be recovered only using BIP-39 Mnemonics. However, you can now use the SLIP-39 App to backup your BIP-39 Seed Entropy! Therefore, we now support the Ledger hardware wallets.

If you already have a BIP-39 Mnemonic, and would like back it up using SLIP-39 for more security and recovery reliability, you can use the Pro Controls to do so. Later, when you need to recover your BIP-39 Mnemonic, use the SLIP-39 App, select the Pro Controls, enter the SLIP-39 card Mnemonics, and click "Using BIP-39" to reveal your original BIP-39 Mnemonic phrase. Then, proceed with Ledger wallet recovery as normal, using the BIP-39 Mnemonic.

The Ledger Nano S Plus has a large screen, at a reasonable price point, and connects via USB-C.

The Ledger Nano X has a large screen and supports connectivity via Bluetooth, for much easier connectivity with mobile phone and laptop wallet software.

2.3 Netcoins.app

In Canada, one of the more highly regulatory-compliant Cryptocurrency exchanges is Netcoins.app (referral code: 5YO1MZ); 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.

2.4 Crypto.com

Use my referral link for Crypto.com (referral code: 2x4hk92dnf) 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.

2.5 Protecting your SLIP-39 Cards

Protect your printed SLIP-39 cards from water damage by laminating them in plastic or storing them in foil ziplock 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.