Learn About Cryptocurrency: Homework

Perry Kundert

2022-04-09 12:17:00

Getting set up to convert between Fiat CAD$ and Cryptocurrencies requires some . . . plumbing.

This "homework" helps you establish the Cryptocurrency "Exchange" account(s) you need to get Fiat CAD$ into and out of Cryptocurrency. (PDF version)

Contents

1 Establish A Cryptocurrency Exchange Account

Just like you need a Stock "Trading" account to use CAD$ to buy and sell stocks, you need an Cryptocurrency "Exchange" account to use CAD$ to buy and sell Cryptocurrencies.

1.1 Netcoins.app

Of the dozen or so bigger Canadian Cryptocurrency Exchanges, Netcoins.app is presently one of the smoothest, most reliable experiences we've had.

It is a registered Canadian "Money Services Business". As such, it must comply with banking "KYC" (Know Your Client) regulations. You'll need:

1. Proof of Identity. A passport or driver's license will do.

2. Proof of Residency. A recent utility bill or bank statement, with your current address.

When you sign up for your Netcoins.app account, they'll walk you through the steps to upload this information.

1.1.1 Get Some Cryptocurrency

In order to do the full round-trip from CAD$, to Crypto, to your Personal Wallet, you'll need to get some Cryptocurrency. The big ones, ETH or BTC, are probably worth buying some of. These will also be easy to withdraw to your Personal Wallet. Some of the others like XRP may require more work to get out to your personal wallet.

1.1.2 Referral Fee

When you set up your Netcoins.app account (referral code: 5YO1MZ), fund it and buy a bit of Cryptocurrency, we get a referral fee. This is why we can reduce the cost of Part 2 of the course.

1.2 Security

If you do not properly secure your accounts (*particularly* your main email account!), then you *will lose your funds* held in an exchange account!

1.2.1 Password Managers

Do not re-use passwords, or parts of passwords between accounts. Yes, I realize that this is impossible, and that literally *everybody* does this...

You **cannot** remember passwords sufficient to secure even a small number of accounts. *Do Not Try – You Will Fail.* Don't beat yourself up; nobody has successfully done this (contrary to the nagging admonitions of every corporate "security" advisor). Use a password manager that works across all platforms (eg. phone, tablet and computer) that you use.

1.2.2 2FA (Two-Factor Authentication)

Secure your most critical accounts with 2FA (Two-Factor Authentication) token using an Authenticator app on your mobile device (eg. Twilio Authy). I recommend **at least** your primary email account, and ideally every cryptocurrency exchange account.

If an account must be accessed by multiple individuals, this is *no problem* – install the Authenticator app on several devices, and when you turn on 2FA on the account, have all the devices available so that you can import the Authenticator "token" QR code on each device. They will all produce the same sequence of numbers, and any device can be used to log into the account.

Once the QR code is unavailable, you will not be able to configure more identical "tokens", and will have to disable and re-enable 2FA, and re-configure each Authenticator from the new QR code.

2 Print SLIP-39 Cards

Get the SLIP-39 App for your Mac or Windows PC, generate a "Seed" and print your "Mnemonic" recovery cards.

Once you install and open the SLIP-39 App on your computer, if you already have a 24-word BIP-39 Mnemonic phrase, you can type them into the "BIP-39 Mnemonic" box and pretty much just hit the "Save" button.

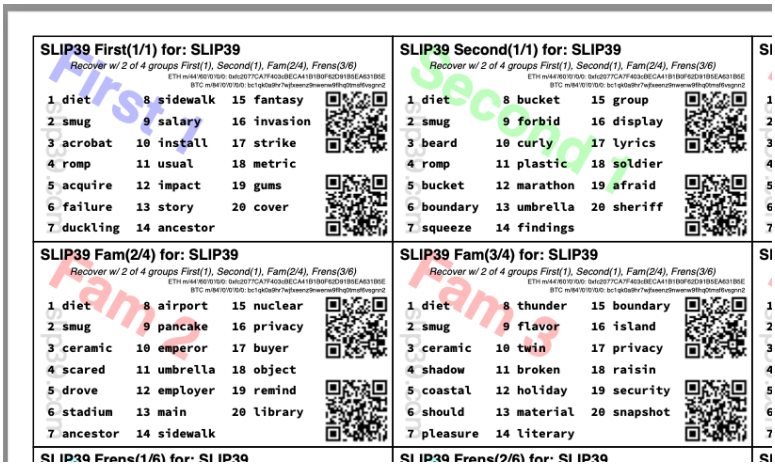

Figure 1: SLIP-39 Cards PDF

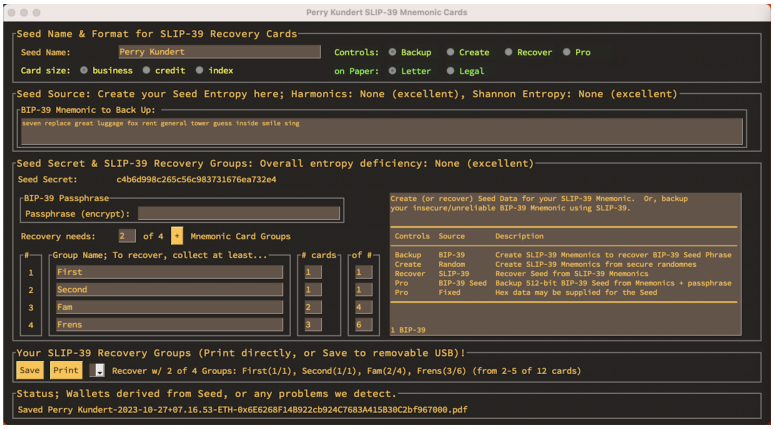

Figure 2: SLIP-39 App: Back-up Existing BIP-39 Mnemonic

If you need to create a brand-new account "Seed", select "Create", and click "256-bit" in Seed Source for a secure random seed (if you don't care about the details of how your Cryptocurrency account master "Seed" is created), and hit the "Save" button.

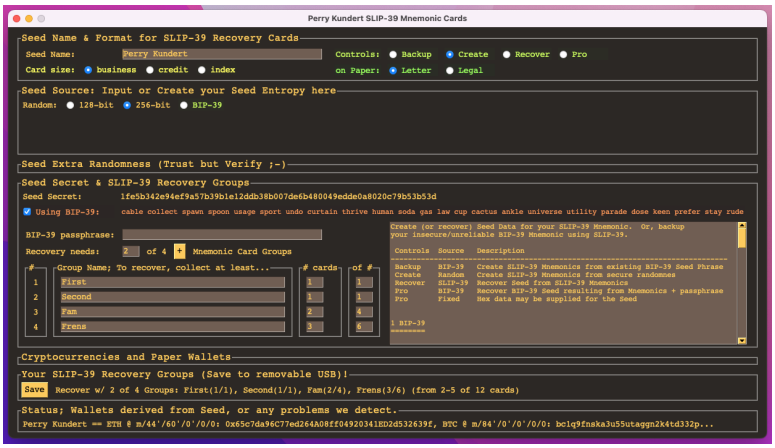

Figure 3: SLIP-39 App: Create New BIP-39 Mnemonic

I would recommend you save it to a USB stick (instead of your computer's hard drive), print it from there, and then securely erase the USB stick. Do *not* "delete" the file! It will be trivially recoverable (either from the USB stick or your computer's Trash)! Just throw the USB stick in the fireplace. No, seriously. I'm not joking.

Unfortunately, we probably **won't** be able to help you generate, print and laminate your SLIP-39 Seed Mmemonic Cards on the day of the course, if you take Part 2: Lets Do This! It just takes too long to do this for everyone.

In order to fund your account with crypto ("withdraw" it from Netcoins.app into your personal account) on the day of the course, you must **at least** have generated your SLIP-39 Seed Mnemonic Card PDF, and saved it to your PC (or USB stick).

3 Get a Hardware Wallet (optional)

We don't recommend using "Software" wallets, like the browser-based Metamask or Brave wallets, or the various mobile phone or computer wallets. It is just *too easy* to be hacked, and lose your funds; extreme care must be taken at all times, and it is virtually inevitable that you will have a momentary lapse of security, and your Cryptocurrency investment will just *vanish*.

3.1 The Trezor Safe 3

The Trezor Safe 3 is the one of the Hardware Wallet we recommend, because it supports direct recovery of all of your Cryptocurrency wallets from SLIP-39 "Seed" Mnemonic Cards – without the need to recover and use a BIP-39 Mnemonic. It also, of course, supports recovery from standard BIP-39 Mnemonics.

3.2 The Ledger "Nano X"

The Ledger "Nano X" is an excellent hardware wallet that supports BIP-39 Mnemonic recovery, but doesn't directly support SLIP-39 Mnemonics; you must recover and use your BIP-39 Mnemonic

Figure 4: Trezor Safe 3 Hardware Wallet

phrase with these, which is handled easily using the SLIP-39 App or `https://iancoleman.io/slip39/`.

These are smaller, but still have a clear screen and support most cryptocurrencies (support for new ones is added quickly).

3.2.1 Just Saving? You Don't Need One.

If you don't plan on "spending" your Cryptocurrency any time soon, you do **not** need a Hardware Wallet.

The *safest* form of Cryptocurrency wallet is your "Paper Wallet": your SLIP-39 "Mnemonic" cards, which you will print off and store in a couple of secure places, and give to friends and family.

When you print off your SLIP-39 cards with the SLIP-39 App, we include a couple of QR codes for the Cryptocurrencies you plan on investing in (eg. BTC, or ETH for any of the Ethereum-compatible Cryptocurrencies).

Once you've gained confidence that you *can* recover all your Cryptocurrency wallets to your Hardware Wallet whenever you need to spend or redeem them, then you can confidently buy Cryptocurrencies on an exchange and "Withdraw" them into your secure, offline "Paper Wallet" accounts.

3.3 Use SLIP-39 Cards to "Recover wallet"

Now that you've printed your SLIP-39 Mnemonic recovery cards, you'll use them to import your Cryptocurrency account "Seed" into your Trezor, using "Recover wallet" on the device. Plug in your new Trezor Safe 3, start the Trezor Suite App, and start the setup process. You want to select "Recover wallet":

3.4 Trezor "Hidden wallet"

Once you recover your wallets to the Trezor, set an PIN and select the Cryptocurrencies you want to create wallets for, you'll reach an important decision point. Do you want to have separate sub-accounts for your Cryptocurrency wallet? Some ideas:

Password	Purpose...	
<default>:	Business	Decoy
Hidden 1:	Personal	Personal
Hidden 2:	Savings	Savings
Hidden 3:		Child

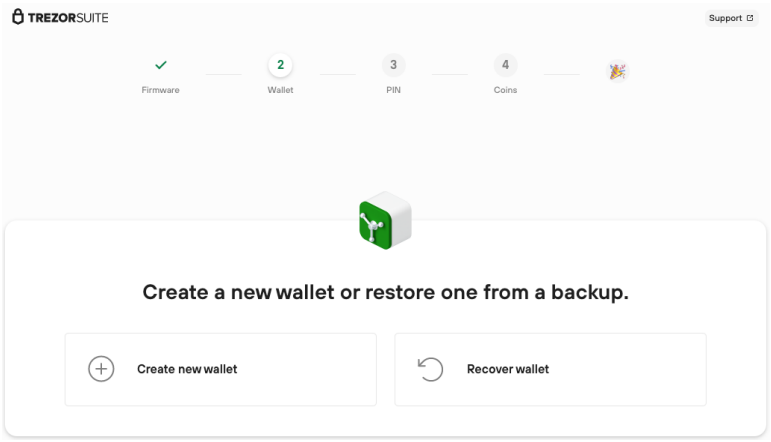

Figure 5: Recover Wallets from SLIP-39 Cards

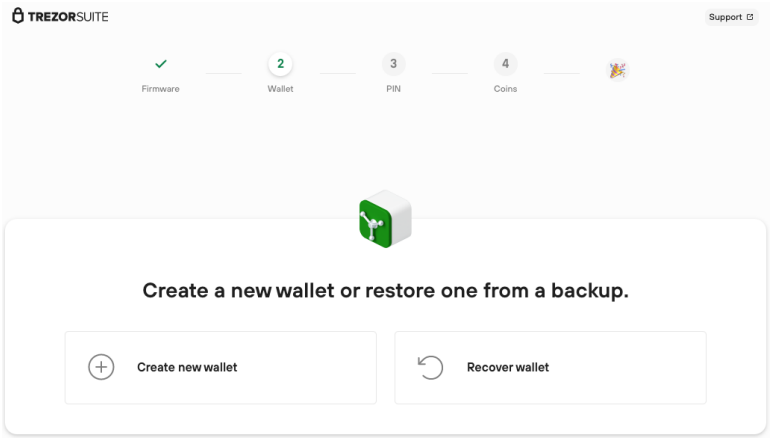

Figure 6: Hidden wallets

If you **do** specify "Hidden wallet" sub-accounts for your Seed, these are:

- Specific to Trezor; you'll need another Trezor hardware wallet to access them
  - The crypto underlying the hidden wallets is simple and open-source
  - It'll eventually be added to the SLIP-39 App
- A Sub-account is **lost** if you forget its password!
  - Don't make them too crazy, and make sure your family knows them.
  - Write hints for your heirs somewhere, such as on the SLIP-39 cards
- Put something in the <default> "Standard wallet" as a "decoy"
  - To satisfy an attacker who gets into your Trezor, or forces you to access your account.