Ethereum SLIP-39 Account Generation

Perry Kundert

2021-12-20 10:55:00

Creating Ethereum, Bitcoin and other accounts is complex and fraught with potential for loss of funds.

A BIP-39 seed recovery phrase helps, but a **single** lapse in security dooms the account (and all derived accounts, in fact). If someone finds your recovery phrase (or you lose it), the accounts derived from that seed are *gone*.

The SLIP-39 standard allows you to split the seed between 1, 2, or more groups of several mnemonic recovery phrases. This is better, but creating such accounts is difficult; presently, only the Trezor supports these, and they can only be created "manually". Writing down 5 or more sets of 20 words is difficult, error-prone and time consuming.

The python-slip39 project (and the SLIP-39 macOS/win32 App) exists to assist in the safe creation and documentation of Ethereum HD Wallet seeds and derived accounts, with various SLIP-39 sharing parameters. It generates the new random wallet seed, and generates the expected standard Ethereum account(s) (at derivation path `m/44'/60'/0'/0/0` by default) and Bitcoin accounts (at Bech32 derivation path `m/84'/0'/0'/0/0` by default), with wallet address and QR code (compatible with Trezor derivations). It produces the required SLIP-39 phrases, and outputs a single PDF containing all the required printable cards to document the seed (and the specified derived accounts).

Output of BIP-38 or JSON encrypted Paper Wallets is supported, for import into standard software cryptocurrency wallets.

On an secure (ideally air-gapped) computer, new seeds can safely be generated and the PDF saved to a USB drive for printing (or directly printed without the file being saved to disk.). Presently, `slip39` can output example ETH, BTC, LTC, DOGE, BNB, CRO and XRP addresses derived from the seed, to *illustrate* what accounts are associated with the backed-up seed. Recovery of the seed to a Trezor "Model T" is simple, by entering the mnemonics right on the device.

We also support backup of existing insecure and unreliable BIP-39 recover phrases as SLIP-39 Mnemonic cards, for existing BIP-39 hardware wallets like the Ledger Nano! Recover from your existing BIP-39 Mnemonic, select "Using BIP-39", and generate a set of SLIP-39 Mnemonic cards. Later, use the SLIP-39 App to recover from your SLIP-39 Mnemonic cards, click "Using BIP-39" to get your BIP-39 Mnemonic back, and use it to recover your accounts to your Ledger (or other) hardware wallet.

Contents

1 Security with Availability

For both BIP-39 and SLIP-39, a 128- or 256-bit random "seed" is the source of an unlimited sequence of Ethereum and Bitcoin HD (Heirarchical Deterministic) derived 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. It must be *both* backed up securely, *and* be readily accessible.

Therefore, we must:

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

How can we address these conflicting requirements?

1.1 Shamir's Secret Sharing System (SSSS)

Satoshi Lab's (Trezor) SLIP-39 uses SSSS to distribute the ability to recover the key to 1 or more "groups". Collecting the mnemonics from the required number of groups allows recovery of the seed.

For BIP-39, the number of groups is always 1, and the number of mnemonics required for that group is always 1. This selection is both insecure (easy to accidentally disclose) and unreliable (easy to accidentally lose), but since most hardware wallets, **only** accept BIP-39 phrases, we also provide a way to *backup your BIP-39 phrase* using SLIP-39!

For SLIP-39, you specify a "group_threshold" of *how many* of your groups must be successfully collected, to recover the seed; this seed is (conceptually) split between 1 or more groups (though not in reality – each group's data *alone* gives away *no information* about the seed).

For example, you might have First, Second, Fam and Frens groups, and decide that any 2 groups can be combined to recover the seed. Each group has members with varying levels of trust and persistence, so have different number of Members, and differing numbers Required to recover that group's data:

Group	Required		Members	Description
First	1	/	1	Stored at home
Second	1	/	1	Stored in office safe
Fam	2	/	4	Distributed to family members
Frens	3	/	6	Distributed to friends and associates

The account owner might store their First and Second group data in their home and office safes. These are 1/1 groups (1 required, and only 1 member, so each of these are3 1-card groups.)

If the Seed needs to be recovered, collecting the First and Second cards from the home and office safe is sufficient to recover the Seed, and re-generate all of the HD Wallet accounts.

Only 2 Fam group member's cards must be collected to recover the Fam group's data. So, if the HD Wallet owner loses their home (and the one and only First group card) in a fire, they could get the one Second group card from the office safe, and also 2 cards from Fam group members, and recover the Seed and all of their wallets.

If catastrophe strikes and the wallet owner dies, and the heirs don't have access to either the First (at home) or Second (at the office) cards, they can collect 2 Fam cards and 3 Frens cards (at the funeral, for example), completing the Fam and Frens groups' data, and recover the Seed, and all derived HD Wallet accounts.

Since Frens are less likely to persist long term, we'll produce more (6) of these cards. Depending on how trustworthy the group is, adjust the Fren group's Required number higher (less trustworthy, more likely to know each-other, need to collect more to recover the group), or lower (more trustworthy, less likely to collude, need less to recover).

2 SLIP-39 Account Creation, Recovery and Address Generation

Generating a new SLIP-39 encoded Seed is easy, with results available as PDF and text. Any number of derived HD wallet account addresses can be generated from this Seed, and the Seed (and all derived HD wallets, for all cryptocurrencies) can be recovered by collecting the desired groups of recover card phrases. The default recovery groups are as described above.

2.1 Creating New SLIP-39 Recoverable Seeds

This is what the first page of the output SLIP-39 mnemonic cards PDF looks like:

Run the following to obtain a PDF file containing business cards with the default SLIP-39 groups for a new account Seed named "Personal"; insert a USB drive to collect the output, and run:

```
$ python3 -m pip install slip39        # Install slip39 in Python3
$ cd /Volumes/USBDRIVE/                # Change current directory to USB
$ python3 -m slip39 Personal           # Or just run "slip39 Personal"
2021-12-25 11:10:38 slip39           ETH m/44'/60'/0'/0/0    : 0xb44A2011A99596671d5952CdC22816089f142FB3
2021-12-25 11:10:38 slip39           Wrote SLIP-39-encoded wallet for 'Personal' to:\
  Personal-2021-12-22+15.45.36-0xb44A2011A99596671d5952CdC22816089f142FB3.pdf
```

The resultant PDF will be output into the designated file.

This PDF file contains business card sized SLIP-39 Mnemonic cards, and will print on a single page of 8-1/2"x11" paper or card stock, and the cards can be cut out (`--card index`, `credit`, `half` (page), `third` and `quarter` are also available, as well as 4x6 `photo` and custom `"(<h>,<w>),<margin>"`).

To get the data printed on the terminal as in this example (so you could write it down on cards instead), add a `-v` (to see it logged in a tabular format), or `--text` to have it printed to stdout in full lines (ie. for pipelining to other programs).

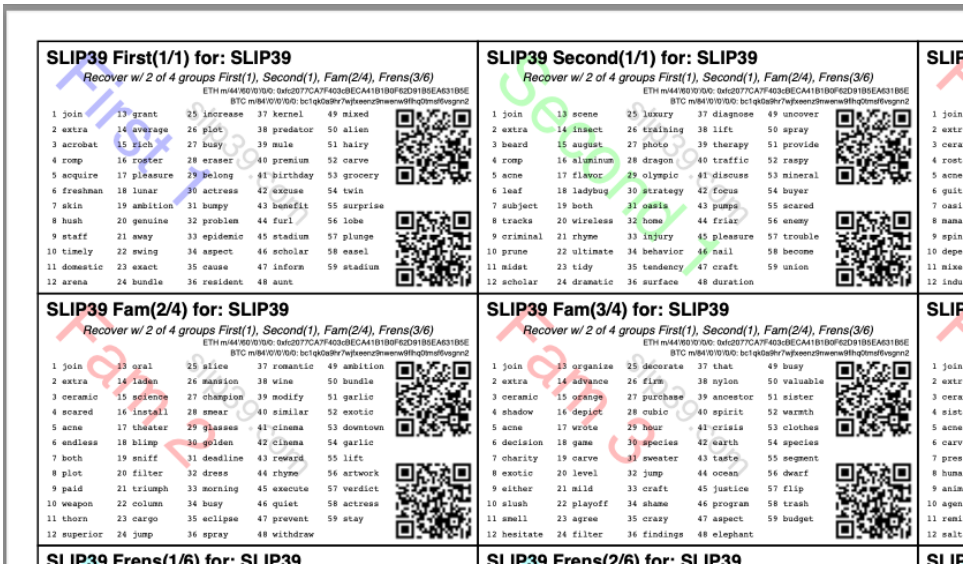


Figure 1: SLIP-39 Cards PDF (from `--secret ffff...`)

2.1.1 Paper Wallets

The Trezor hardware wallet natively supports the input of SLIP-39 Mnemonics. However, most software wallets do not (yet) support SLIP-39. So, how do we load the Crypto wallets produced from our Seed into software wallets such as the Metamask plugin or the Brave browser, for example?

The `slip39.gui` (and the macOS/win32 SLIP-39.App) support output of standard BIP-38 encrypted wallets for Bitcoin-like cryptocurrencies such as BTC, LTC and DOGE. It also outputs encrypted Ethereum JSON wallets for ETH. Here is how to produce them (from a test secret Seed; exclude `--secret ffff...` for yours!):

```
slip39 -c ETH -c BTC -c DOGE -c LTC --secret ffffffffffffffffffffffffffffffff \
    --no-card --wallet password --wallet-hint 'bad:pass...' 2>&1
```

And what they look like:

To recover your real SLIP-39 Seed Entropy and print wallets, use the SLIP-39 App's "Recover" Controls, or to do so on the command-line, use `slip39-recover`:

```
    slip39-recovery -v \
--mnemonic "material leaf acrobat romp charity capital omit skunk change firm eclipse crush fancy best tracks flip grownup
      --mnemonic "material leaf beard romp disaster duke flame uncover group slice guest blue gums duckling total suitab
2>&1

2022-04-22 16:20:39 slip39.recovery  Recovered 128-bit SLIP-39 Seed Entropy with 2 (all) of 2 supplied mnemonics; Seed dec
2022-04-22 16:20:39 slip39.recovery  Recovered BIP-39 secret; To re-generate SLIP-39 wallet, send it to: python3 -m slip39
ffffffffffffffffffffffffffffffff
```

You can run this as a command-line pipeline. Here, we use some SLIP-39 Mnemonics that encode the `ffff...` Seed Entropy; note that the wallets match those output above:

Figure 2: Paper Wallets (from `--secret ffff...`)

```
    slip39-recovery \
--mnemonic "material leaf acrobat romp charity capital omit skunk change firm eclipse crush fancy best tracks flip grownup
        --mnemonic "material leaf beard romp disaster duke flame uncover group slice guest blue gums duckling total suitab
    | slip39 -c ETH -c BTC -c DOGE -c LTC --secret - \
        --no-card --wallet password --wallet-hint 'bad:pass...' \
2>&1
```

2.1.2 Supported Cryptocurrencies

While the SLIP-39 Seed is not cryptocurrency-specific (any wallet for any cryptocurrency can be derived from it), each type of cryptocurrency has its own standard derivation path (eg. `m/44'/3'/0'/0/0` for DOGE), and its own address representation (eg. Bech32 at `m/84'/0'/0'/0/0` for BTC eg. `bc1qcupw7k8enymvvsa7w35j5hq4ergtvus3zk8a8s`.

When you import your SLIP-39 Seed into a Trezor, you gain access to all derived HD cryptocurrency wallets supported directly by that hardware wallet, and **indirectly**, to any coin and/or blockchain network supported by any wallet software (eg. Metamask).

Crypto	Semantic	Path	Address	Support
ETH	Legacy	m/44'/60'/0'/0/0	0x...	
BNB	Legacy	m/44'/60'/0'/0/0	0x...	Beta
CRO	Bech32	m/44'/60'/0'/0/0	crc1...	Beta
BTC	Legacy	m/44'/ 0'/0'/0/0	1...	
	SegWit	m/44'/ 0'/0'/0/0	3...	
	Bech32	m/84'/ 0'/0'/0/0	bc1...	
LTC	Legacy	m/44'/ 2'/0'/0/0	L...	
	SegWit	m/44'/ 2'/0'/0/0	M...	
	Bech32	m/84'/ 2'/0'/0/0	ltc1...	
DOGE	Legacy	m/44'/ 3'/0'/0/0	D...	

1. ETH, BTC, LTC, DOGE

   These coins are natively supported both directly by the Trezor hardware wallet, and by most software wallets and "web3" platforms that interact with the Trezor, or can import the BIP-38 or Ethereum JSON Paper Wallets produced by `python-slip39`.

2. BNB on the Binance Smart Chain (BSC): binance.com

   The Binance Smart Chain uses standard Ethereum addresses; support for the BSC is added directly to the wallet software; here are the instructions for adding BSC support for the Trezor hardware wallet, using the Metamask software wallet. In `python-slip39`, BNB is simply an alias for ETH, since the wallet addresses and Ethereum JSON Paper Wallets are identical.

3. CRO on Cronos: crypto.com

   The Cronos chain (formerly known as the Crypto.org chain). It is the native chain of the crypto.com CRO coin.

   Cronos also uses Ethereum addresses on the `m/44'/60'/0'/0/0` derivation path, but represents them as Bech32 addresses with a "crc" prefix, eg. `crc19a6r74dvfxjyvjzf3pg9y3y5rhk6rds2c`. As with BNB, the wallet must support the Cronos blockchain; instructions exist for adding CRO support for the Trezor hardware wallet, using the Metamask software wallet.

2.2 The macOS/win32 `SLIP-39.app` GUI App

If you prefer a graphical user-interface, try the macOS/win32 SLIP-39.App. You can run it directly if you install Python 3.9+ from python.org/downloads or using homebrew `brew install python-tk@3.10`. Then, start the GUI in a variety of ways:

```
slip39-gui
python3 -m slip39.gui
```

Alternatively, download and install the macOS/win32 GUI App .zip, .pkg or .dmg installer from github.com/pjkundert/python-slip-39/releases.

2.3 The Python `slip39` CLI

From the command line, you can create SLIP-39 Seed Mnemonic card PDFs.

2.3.1 `slip39` Synopsis

The full command-line argument synopsis for `slip39` is:

```
slip39 --help 2>&1               | sed 's/^/: /' # (just for output formatting)

: usage: slip39 [-h] [-v] [-q] [-o OUTPUT] [-t THRESHOLD] [-g GROUP] [-f FORMAT]
:               [-c CRYPTOCURRENCY] [-p PATH] [-j JSON] [-w WALLET]
:               [--wallet-hint WALLET_HINT] [--wallet-format WALLET_FORMAT]
:               [-s SECRET] [--bits BITS] [--using-bip39]
:               [--passphrase PASSPHRASE] [-C CARD] [--no-card] [--paper PAPER]
:               [--cover] [--no-cover] [--text]
:               [names ...]
:
: Create and output SLIP-39 encoded Seeds and Paper Wallets to a PDF file.
:
: positional arguments:
:   names                 Account names to produce; if --secret Entropy is
:                         supplied, only one is allowed.
:
: optional arguments:
:   -h, --help            show this help message and exit
:   -v, --verbose         Display logging information.
:   -q, --quiet           Reduce logging output.
:   -o OUTPUT, --output OUTPUT
:                         Output PDF to file or '-' (stdout); formatting w/
:                         name, date, time, crypto, path, address allowed
:   -t THRESHOLD, --threshold THRESHOLD
:                         Number of groups required for recovery (default: half
:                         of groups, rounded up)
:   -g GROUP, --group GROUP
:                         A group name[[<require>/]<size>] (default: <size> = 1,
:                         <require> = half of <size>, rounded up, eg.
:                         'Frens(3/5)' ).
:   -f FORMAT, --format FORMAT
:                         Specify crypto address formats: legacy, segwit,
:                         bech32; default: ETH:legacy, BTC:bech32, LTC:bech32,
:                         DOGE:legacy, CRO:bech32, BNB:legacy, XRP:legacy
:   -c CRYPTOCURRENCY, --cryptocurrency CRYPTOCURRENCY
:                         A crypto name and optional derivation path (eg.
:                         '../<range>/<range>'); defaults: ETH:m/44'/60'/0'/0/0,
:                         BTC:m/84'/0'/0'/0/0, LTC:m/84'/2'/0'/0/0,
:                         DOGE:m/44'/3'/0'/0/0, CRO:m/44'/60'/0'/0/0,
:                         BNB:m/44'/60'/0'/0/0, XRP:m/44'/144'/0'/0/0
:   -p PATH, --path PATH  Modify all derivation paths by replacing the final
:                         segment(s) w/ the supplied range(s), eg. '.../1/-'
:                         means .../1/[0,...)
:   -j JSON, --json JSON  Save an encrypted JSON wallet for each Ethereum
:                         address w/ this password, '-' reads it from stdin
:                         (default: None)
:   -w WALLET, --wallet WALLET
:                         Produce paper wallets in output PDF; each wallet
:                         private key is encrypted this password
:   --wallet-hint WALLET_HINT
:                         Paper wallets password hint
:   --wallet-format WALLET_FORMAT
:                         Paper wallet size; half, third, quarter or
```

```
:                         '(<h>,<w>),<margin>' (default: quarter)
:   -s SECRET, --secret SECRET
:                         Use the supplied 128-, 256- or 512-bit hex value as
:                         the secret seed; '-' reads it from stdin (eg. output
:                         from slip39.recover)
:   --bits BITS           Ensure that the seed is of the specified bit length;
:                         128, 256, 512 supported.
:   --using-bip39         Generate Seed from secret Entropy using BIP-39
:                         generation algorithm (encode as BIP-39 Mnemonics,
:                         encrypted using --passphrase)
:   --passphrase PASSPHRASE
:                         Encrypt the master secret w/ this passphrase, '-'
:                         reads it from stdin (default: None/'')
:   -C CARD, --card CARD  Card size; business, credit, index, half, third,
:                         quarter, photo or '(<h>,<w>),<margin>' (default:
:                         business)
:   --no-card             Disable PDF SLIP-39 mnemonic card output
:   --paper PAPER         Paper size (default: Letter)
:   --cover               Produce PDF SLIP-39 cover page
:   --no-cover            Disable PDF SLIP-39 cover page
:   --text                Enable textual SLIP-39 mnemonic output to stdout
```

2.4 Recovery & Re-Creation

Later, if you need to recover the wallet seed, keep entering SLIP-39 mnemonics into `slip39-recovery` until the secret is recovered (invalid/duplicate mnemonics will be ignored):

```
$ python3 -m slip39.recovery   # (or just "slip39-recovery")
Enter 1st SLIP-39 mnemonic: ab c
Enter 2nd SLIP-39 mnemonic: veteran guilt acrobat romp burden campus purple webcam uncover ...
Enter 3rd SLIP-39 mnemonic: veteran guilt acrobat romp burden campus purple webcam uncover ...
Enter 4th SLIP-39 mnemonic: veteran guilt beard romp dragon island merit burden aluminum worthy ...
2021-12-25 11:03:33 slip39.recovery  Recovered SLIP-39 secret; Use:  python3 -m slip39 --secret ...
383597fd63547e7c9525575decd413f7
```

Finally, re-create the wallet seed, perhaps including an encrypted JSON Paper Wallet for import of some accounts into a software wallet (use `--json password` to output encrypted Ethereum JSON wallet files):

```
slip39 --secret 383597fd63547e7c9525575decd413f7 --wallet password --wallet-hint bad:pass... 2>&1
```

2.4.1 `slip39.recovery` Synopsis

```
slip39-recovery --help 2>&1               | sed 's/^/: /' # (just for output formatting)

: usage: slip39-recovery [-h] [-v] [-q] [-m MNEMONIC] [-e] [-b] [-u]
:                        [-p PASSPHRASE]
:
: Recover and output secret Seed from SLIP-39 or BIP-39 Mnemonics
:
: optional arguments:
:   -h, --help            show this help message and exit
:   -v, --verbose         Display logging information.
:   -q, --quiet           Reduce logging output.
:   -m MNEMONIC, --mnemonic MNEMONIC
:                         Supply another SLIP-39 (or a BIP-39) mnemonic phrase
:   -e, --entropy         Return the BIP-39 Mnemonic Seed Entropy instead of the
```

```
:                           generated Seed (default: False)
:   -b, --bip39             Recover Entropy and generate 512-bit secret Seed from
:                           BIP-39 Mnemonic + passphrase
:   -u, --using-bip39       Recover Entropy from SLIP-39, generate 512-bit secret
:                           Seed using BIP-39 Mnemonic + passphrase
:   -p PASSPHRASE, --passphrase PASSPHRASE
:                           Decrypt the SLIP-39 or BIP-39 master secret w/ this
:                           passphrase, '-' reads it from stdin (default: None/'')
:
: If you obtain a threshold number of SLIP-39 mnemonics, you can recover the original
: secret Seed Entropy, and then re-generate one or more wallets from it.
:
: Enter the mnemonics when prompted and/or via the command line with -m |--mnemonic "...".
:
: The secret Seed Entropy can then be used to generate a new SLIP-39 encoded wallet:
:
:     python3 -m slip39 --secret = "ab04...7f"
:
: SLIP-39 Mnemonics may be encrypted with a passphrase; this is *not* Ledger-compatible, so it rarely
: recommended!  Typically, on a Trezor "Model T", you recover using your SLIP-39 Mnemonics, and then
: use the "Hidden wallet" feature (passwords entered on the device) to produce alternative sets of
: accounts.
:
: BIP-39 Mnemonics can be backed up as SLIP-39 Mnemonics, in two ways:
:
: 1) The actual BIP-39 standard 512-bit Seed can be generated by supplying --passphrase, but only at
: the cost of 59-word SLIP-39 mnemonics.  This is because the *output* 512-bit BIP-39 Seed must be
: stored in SLIP-39 -- not the *input* 128-, 160-, 192-, 224-, or 256-bit entropy used to create the
: original BIP-39 mnemonic phrase.
:
: 2) The original BIP-39 12- or 24-word, 128- to 256-bit Seed Entropy can be recovered by supplying
: --entropy.  This modifies the BIP-39 recovery to return the original BIP-39 Mnemonic Entropy, before
: decryption and seed generation.  It has no effect for SLIP-39 recovery.
```

2.4.2 Pipelining `slip39.recovery | slip39 --secret -`

The tools can be used in a pipeline to avoid printing the secret. Here we generate some mnemonics, sorting them in reverse order so we need more than just the first couple to recover. Observe the Ethereum wallet address generated.

Then, we recover the master secret seed in hex with `slip39-recovery`, and finally send it to `slip39 --secret -` to re-generate the same wallet as we originally created.

```
( python3 -m slip39 --text --no-card \
   | ( sort -r  ; echo "...later..." 1>&2 ) \
   | python3 -m slip39.recovery \
   | python3 -m slip39 --secret - --no-card \
) 2>&1
```

```
2022-04-22 16:20:42 slip39.layout    ETH    m/44'/60'/0'/0/0    : 0xa9283386988639685B929DfA8acd3eA53CDEe97d
2022-04-22 16:20:42 slip39.layout    BTC    m/84'/0'/0'/0/0     : bc1quxcrrp72vlpyfwpvtl2kwd8k9mmdk5ce6mpn5f
...later...
2022-04-22 16:20:43 slip39.layout    ETH    m/44'/60'/0'/0/0    : 0xa9283386988639685B929DfA8acd3eA53CDEe97d
2022-04-22 16:20:43 slip39.layout    BTC    m/84'/0'/0'/0/0     : bc1quxcrrp72vlpyfwpvtl2kwd8k9mmdk5ce6mpn5f
```

2.5 Generation of Addresses

For systems that require a stream of groups of wallet Addresses (eg. for preparing invoices for clients, with a choice of cryptocurrency payment options), `slip-generator` can produce a stream of groups of addresses.

2.5.1 `slip39-generator` Synopsis

```
slip39-generator --help --version         | sed 's/^/: /' # (just for output formatting)

: usage: slip39-generator [-h] [-v] [-q] [-s SECRET] [-f FORMAT]
:                         [-c CRYPTOCURRENCY] [--path PATH] [-d DEVICE]
:                         [--baudrate BAUDRATE] [-e ENCRYPT] [--decrypt ENCRYPT]
:                         [--enumerated] [--no-enumerate] [--receive]
:                         [--corrupt CORRUPT]
:
: Generate public wallet address(es) from a secret seed
:
: optional arguments:
:   -h, --help            show this help message and exit
:   -v, --verbose         Display logging information.
:   -q, --quiet           Reduce logging output.
:   -s SECRET, --secret SECRET
:                         Use the supplied 128-, 256- or 512-bit hex value as
:                         the secret seed; '-' (default) reads it from stdin
:                         (eg. output from slip39.recover)
:   -f FORMAT, --format FORMAT
:                         Specify crypto address formats: legacy, segwit,
:                         bech32; default: ETH:legacy, BTC:bech32, LTC:bech32,
:                         DOGE:legacy, CRO:bech32, BNB:legacy, XRP:legacy
:   -c CRYPTOCURRENCY, --cryptocurrency CRYPTOCURRENCY
:                         A crypto name and optional derivation path (default:
:                         "ETH:{Account.path_default('ETH')}"), optionally w/
:                         ranges, eg: ETH:../0/-
:   --path PATH           Modify all derivation paths by replacing the final
:                         segment(s) w/ the supplied range(s), eg. '.../1/-'
:                         means .../1/[0,...)
:   -d DEVICE, --device DEVICE
:                         Use this serial device to transmit (or --receive)
:                         records
:   --baudrate BAUDRATE   Set the baud rate of the serial device (default:
:                         115200)
:   -e ENCRYPT, --encrypt ENCRYPT
:                         Secure the channel from errors and/or prying eyes with
:                         ChaCha20Poly1305 encryption w/ this password; '-'
:                         reads from stdin
:   --decrypt ENCRYPT
:   --enumerated          Include an enumeration in each record output (required
:                         for --encrypt)
:   --no-enumerate        Disable enumeration of output records
:   --receive             Receive a stream of slip.generator output
:   --corrupt CORRUPT     Corrupt a percentage of output symbols
:
: Once you have a secret seed (eg. from slip39.recovery), you can generate a sequence
: of HD wallet addresses from it.  Emits rows in the form:
:
:     <enumeration> [<address group(s)>]
:
: If the output is to be transmitted by an insecure channel (eg. a serial port), which may insert
: errors or allow leakage, it is recommended that the records be encrypted with a cryptographic
: function that includes a message authentication code.  We use ChaCha20Poly1305 with a password and a
: random nonce generated at program start time.  This nonce is incremented for each record output.
:
: Since the receiver requires the nonce to decrypt, and we do not want to separately transmit the
: nonce and supply it to the receiver, the first record emitted when --encrypt is specified is the
: random nonce, encrypted with the password, itself with a known nonce of all 0 bytes.  The plaintext
: data is random, while the nonce is not, but since this construction is only used once, it should be
: satisfactory.  This first nonce record is transmitted with an enumeration prefix of "nonce".
```

2.5.2 Producing Addresses

Addresses can be produced in plaintext or encrypted, and output to stdout or to a serial port.

```
    slip39-generator --secret ffffffffffffffffffffffffffffffff --path '../-3' 2>&1

2022-04-22 16:20:44 slip39.generator It is recommended to not use '-s|--secret <hex>'; specify '-' to read from input
    0: [["ETH", "m/44'/60'/0'/0/0", "0x824b174803e688dE39aF5B3D7Cd39bE6515A19a1"], ["BTC", "m/84'/0'/0'/0/0", "bc1q9yscq3l
    1: [["ETH", "m/44'/60'/0'/0/1", "0x8D342083549C635C0494d3c77567860ee7456963"], ["BTC", "m/84'/0'/0'/0/1", "bc1qnec684y
    2: [["ETH", "m/44'/60'/0'/0/2", "0x52787E24965E1aBd691df77827A3CfA90f0166AA"], ["BTC", "m/84'/0'/0'/0/2", "bc1q2snj0zc
    3: [["ETH", "m/44'/60'/0'/0/3", "0xc2442382Ae70c77d6B6840EC6637dB2422E1D44e"], ["BTC", "m/84'/0'/0'/0/3", "bc1qxwekjd4
```

To produce accounts from a BIP-39 or SLIP-39 seed, recover it using slip39-recovery.

Here's an example of recovering a test BIP-39 seed; note that it yields the well-known ETH `0xfc20...1B5E` and BTC `bc1qk0...gnn2` accounts associated with this test Mnemonic:

```
    ( slip39-recovery --bip39 --mnemonic 'zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo wrong' \
        | slip39-generator --secret - --path '../-3' ) 2>&1

0: [["ETH", "m/44'/60'/0'/0/0", "0xfc2077CA7F403cBECA41B1B0F62D91B5EA631B5E"], ["BTC", "m/84'/0'/0'/0/0", "bc1qk0a9hr7wjfx
1: [["ETH", "m/44'/60'/0'/0/1", "0xd1a7451beB6FE0326b4B78e3909310880B781d66"], ["BTC", "m/84'/0'/0'/0/1", "bc1qkd33yck74lg
2: [["ETH", "m/44'/60'/0'/0/2", "0x578270B5E5B53336baC354756b763b309eCA90Ef"], ["BTC", "m/84'/0'/0'/0/2", "bc1qvr7e5aytd0h
3: [["ETH", "m/44'/60'/0'/0/3", "0x909f59835A5a120EafE1c60742485b7ff0e305da"], ["BTC", "m/84'/0'/0'/0/3", "bc1q6t9vhestkcf
```

We can encrypt the output, to secure the sequence (and due to integrated MACs, ensures no errors occur over an insecure channel like a serial cable):

```
    ( slip39-recovery --bip39 --mnemonic 'zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo wrong' \
        | slip39-generator --secret - --path '../-3' --encrypt 'password' ) 2>&1



nonce: 5b80cb186b92dddbbb5b3e433b5a45240b34e916cdcd02bd0da3ef8f
    0: fa93612e0648f725e63128a447c3a02a95409f7049ffc2374252b21603b92ba5593001045266086ac8a3cabca1153bf168ebd46222e584d4c78
    1: 8042d2ed4e1bb384af96eeb5f547cc7e99096acd0ed8e36735c0896807b6ac8ad0d363b9a05df9aecfe9ad489edbc845b49ccd3c3ce9a1d5290
    2: 4fa4dbd7709c79f11a015d2ad31a85295f127432a47333f75ffe326d16b80b46a4a99abc949046b4fa4ee2ca5d7b9b38fea748e2be90f412b0b
    3: e4c27477fbafab3e7bfc5b01d8da2b14385488ac6f8a752c545ec598da27ab7966c31bf28093cc1a4d773d4289b2db648204512ffe300f8e3b3
```

On the receiving computer, we can decrypt and recover the stream of accounts from the wallet seed; any rows with errors are ignored:

```
    ( slip39-recovery --bip39 --mnemonic 'zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo wrong' \
        | slip39-generator --secret - --path '../-3' --encrypt 'password' \
        | slip39-generator --receive --decrypt 'password' ) 2>&1

0: [["ETH", "m/44'/60'/0'/0/0", "0xfc2077CA7F403cBECA41B1B0F62D91B5EA631B5E"], ["BTC", "m/84'/0'/0'/0/0", "bc1qk0a9hr7wjfx
1: [["ETH", "m/44'/60'/0'/0/1", "0xd1a7451beB6FE0326b4B78e3909310880B781d66"], ["BTC", "m/84'/0'/0'/0/1", "bc1qkd33yck74lg
2: [["ETH", "m/44'/60'/0'/0/2", "0x578270B5E5B53336baC354756b763b309eCA90Ef"], ["BTC", "m/84'/0'/0'/0/2", "bc1qvr7e5aytd0h
3: [["ETH", "m/44'/60'/0'/0/3", "0x909f59835A5a120EafE1c60742485b7ff0e305da"], ["BTC", "m/84'/0'/0'/0/3", "bc1q6t9vhestkcf
```

2.6 The `slip39` module API

Provide SLIP-39 Mnemonic set creation from a 128-bit master secret, and recovery of the secret from a subset of the provided Mnemonic set.

2.6.1 `slip39.create`

Creates a set of SLIP-39 groups and their mnemonics.

Key	Description
name	Who/what the account is for
group_threshold	How many groups' data is required to recover the account(s)
groups	Each group's description, as {"<group>":(<required>, <members>), ...}
master_secret	128-bit secret (default: from secrets.token_bytes)
passphrase	An optional additional passphrase required to recover secret (default: "")
using_bip39	Produce wallet Seed from master_secret Entropy using BIP-39 generation
iteration_exponent	For encrypted secret, exponentially increase PBKDF2 rounds (default: 1)
cryptopaths	A number of crypto names, and their derivation paths]
strength	Desired master_secret strength, in bits (default: 128)

Outputs a `slip39.Details` namedtuple containing:

Key	Description
name	(same)
group_threshold	(same)
groups	Like groups, w/ <members> = ["<mnemonics>", ...]
accounts	Resultant list of groups of accounts

This is immediately usable to pass to `slip39.output`.

```
import codecs
import random

#
# NOTE:
#
# We turn off randomness here during SLIP-39 generation to get deterministic phrases;
# during normal operation, secure entropy is used during mnemonic generation, yielding
# random phrases, even when the same seed is used multiple times.
#
import shamir_mnemonic
shamir_mnemonic.shamir.RANDOM_BYTES = lambda n: b'\00' * n

import slip39

cryptopaths         = [("ETH","m/44'/60'/0'/0/-2"), ("BTC","m/44'/0'/0'/0/-2")]
master_secret       = b'\xFF' * 16
passphrase          = b""
create_details      = slip39.create(
    "Test", 2, { "Mine": (1,1), "Fam": (2,3) },
    master_secret=master_secret, passphrase=passphrase, cryptopaths=cryptopaths )
[
    [
        f"{g_name}({g_of}/{len(g_mnems)}) #{g_n+1}:" if l_n == 0 else ""
    ] + words
    for g_name,(g_of,g_mnems) in create_details.groups.items()
    for g_n,mnem in enumerate( g_mnems )
    for l_n,(line,words) in enumerate(slip39.organize_mnemonic(
            mnem, label=f"{g_name}({g_of}/{len(g_mnems)}) #{g_n+1}:" ))
]
```

0	1	2	3
Mine(1/1) #1:	1 academic	8 safari	15 standard
	2 acid	9 drug	16 angry
	3 acrobat	10 browser	17 similar
	4 easy	11 trash	18 aspect
	5 change	12 fridge	19 smug
	6 injury	13 busy	20 violence
	7 painting	14 finger	
Fam(2/3) #1:	1 academic	8 prevent	15 dwarf
	2 acid	9 mouse	16 dream
	3 beard	10 daughter	17 flavor
	4 echo	11 ancient	18 oral
	5 crystal	12 fortune	19 chest
	6 machine	13 ruin	20 marathon
	7 bolt	14 warmth	
Fam(2/3) #2:	1 academic	8 prune	15 briefing
	2 acid	9 pickup	16 often
	3 beard	10 device	17 escape
	4 email	11 device	18 sprinkle
	5 dive	12 peanut	19 segment
	6 warn	13 enemy	20 devote
	7 ranked	14 graduate	
Fam(2/3) #3:	1 academic	8 dining	15 intimate
	2 acid	9 invasion	16 satoshi
	3 beard	10 bumpy	17 hobo
	4 entrance	11 identify	18 ounce
	5 alarm	12 anxiety	19 both
	6 health	13 august	20 award
	7 discuss	14 sunlight	

Add the resultant HD Wallet addresses:

```
[
    [ account.path, account.address ]
    for group in create_details.accounts
    for account in group
]
```

0	1
m/44'/60'/0'/0/0	0x824b174803e688dE39aF5B3D7Cd39bE6515A19a1
m/44'/0'/0'/0/0	bc1qm5ua96hx30snwrwsfnv97q96h53l86ded7wmjl
m/44'/60'/0'/0/1	0x8D342083549C635C0494d3c77567860ee7456963
m/44'/0'/0'/0/1	bc1qwz6v9z49z8mk5ughj7r78hjsp45jsxgzh29lnh
m/44'/60'/0'/0/2	0x52787E24965E1aBd691df77827A3CfA90f0166AA
m/44'/0'/0'/0/2	bc1q690m430qu29auyefarwfrvfumncunvyw6v53n9

2.6.2 `slip39.produce_pdf`

Key	Description
name	(same as `slip39.create`)
group_threshold	(same as `slip39.create`)
groups	Like groups, w/ <members> = ["<mnemonics>", ...]
accounts	Resultant { "path": Account, ... }
card_format	'index', '(<h>,<w>),<margin>', ...
paper_format	'Letter', ...

Layout and produce a PDF containing all the SLIP-39 details on cards for the crypto accounts, on the paper_format provided. Returns the paper (orientation,format) used, the FPDF, and passes through the supplied cryptocurrency accounts derived.

```
(paper_format,orientation),pdf,accounts = slip39.produce_pdf( *create_details )
pdf_binary = pdf.output()
[
```

```
    [ "Orientation:",orientation ],
    [ "Paper:",paper_format ],
    [ "PDF Pages:",pdf.pages_count ],
    [ "PDF Size:",len( pdf_binary )],
]
```

0	1
Orientation:	landscape
Paper:	Letter
PDF Pages:	1
PDF Size:	13031

2.6.3 `slip39.write_pdfs`

Key	Description
names	A sequence of Seed names, or a dict of { name: <details> } (from slip39.create)
master_secret	A Seed secret (only appropriate if exactly one name supplied)
passphrase	A SLIP-39 passphrase (not Trezor compatible; use "hidden wallet" phrase on device instead)
group	A dict of {"<group>":(<required>, <members>), ...}
group_threshold	How many groups are required to recover the Seed
cryptocurrency	A sequence of ["<crypto>", "<crypto>:<derivation>", ...] w/ optional ranges
edit	Derivation range(s) for each cryptocurrency, eg. "../0-4/-9" is 9 accounts first 5 change addresses
card_format	Card size (eg. "credit"); False specifies no SLIP-39 cards (ie. only BIP-39 or JSON paper wallets)
paper_format	Paper size (eg. "letter")
filename	A filename; may contain "...{name}..." formatting, for name, date, time, crypto path and address
filepath	A file path, if PDF output to file is desired; empty implies current dir.
printer	A printer name (or True for default), if output to printer is desired
json_pwd	If password supplied, encrypted Ethereum JSON wallet files will be saved, and produced into PDF
text	If True, outputs SLIP-39 phrases to stdout
wallet_pwd	If password supplied, produces encrypted BIP-38 or JSON Paper Wallets to PDF (preferred vs. json_pwd)
wallet_pwd_hint	An optional passphrase hint, printed on paper wallet
wallet_format	Paper wallet size, (eg. "third"); the default is 1/3 letter size

For each of the names provided, produces a separate PDF containing all the SLIP-39 details and optionally encrypted BIP-38 paper wallets and Ethereum JSON wallets for the specified cryptocurrency accounts derived from the seed, and writes the PDF and JSON wallets to the specified file name(s).

```
slip39.write_pdfs( ... )
```

2.6.4 `slip39.recover`

Takes a number of SLIP-39 mnemonics, and if sufficient `group_threshold` groups' mnemonics are present (and the options `passphrase` is supplied), the `master_secret` is recovered. This can be used with `slip39.accounts` to directly obtain any `Account` data.

Note that the SLIP-39 passphrase is **not** checked; entering a different passphrase for the same set of mnemonics will recover a **different** wallet! This is by design; it allows the holder of the SLIP-39 mnemonic phrases to recover a "decoy" wallet by supplying a specific passphrase, while protecting the "primary" wallet.

Therefore, it is **essential** to remember any non-default (non-empty) passphrase used, separately and securely. Take great care in deciding if you wish to use a passphrase with your SLIP-39 wallet!

Key	Description
mnemonics	["<mnemonics>", ...]
passphrase	Optional passphrase to decrypt secret Seed Entropy
using_bip39	Use BIP-39 Seed generation from recover Entropy

```
# Recover with the wrong password (on purpose, as a decoy wallet w/ a small amount)
recoverydecoy       = slip39.recover(
    create_details.groups['Mine'][1][:] + create_details.groups['Fam'][1][:2],
    passphrase=b"wrong!"
)
recoverydecoy_hex   = codecs.encode( recoverydecoy, 'hex_codec' ).decode( 'ascii' )

# But, recovering w/ correct passphrase yields our original Seed Entropy
recoveryvalid       = slip39.recover(
    create_details.groups['Mine'][1][:] + create_details.groups['Fam'][1][:2],
    passphrase=passphrase
)
recoveryvalid_hex   = codecs.encode( recoveryvalid, 'hex_codec' ).decode( 'ascii' )

[
  [ f"{len(recoverydecoy)*8}-bit secret (decoy):", f"{recoverydecoy_hex}" ],
  [ f"{len(recoveryvalid)*8}-bit secret recovered:", f"{recoveryvalid_hex}" ]
]
```

0	1
128-bit secret (decoy):	2e522cea2b566840495c220cf79c756e
128-bit secret recovered:	ffffffffffffffffffffffffffffffff

2.6.5 `slip39.recover_bip39`

Generate the 512-bit Seed from a BIP-39 Mnemonic + passphrase. Or, return the original 128- to 256-bit Seed Entropy, if `as_entropy` is specified.

Key	Description
mnemonic	"<mnemonic>"
passphrase	Optional passphrase to decrypt secret Seed Entropy
as_entropy	Return the BIP-39 Seed Entropy, not the generated Seed

2.6.6 `slip39.produce_bip39`

Produce a BIP-39 Mnemonic from the supplied 128- to 256-bit Seed Entropy.

Key	Description
entropy	The `bytes` of Seed Entropy
strength	Or, the number of bits of Entropy to produce (Default: 128)
language	Default is "english"

3 Conversion from BIP-39 to SLIP-39

If we already have a BIP-39 wallet, it would certainly be nice to be able to create nice, safe SLIP-39 mnemonics for it, and discard the unsafe BIP-39 mnemonics we have lying around, just waiting to be accidentally discovered and the account compromised!

Fortunately, **we can** do this! It takes a bit of practice to become comfortable with the process, but once you do – you can confidently discard your original insecure and unreliable BIP-39 Mnemonic backups.

3.1 BIP-39 vs. SLIP-39 Incompatibility

Unfortunately, it is **not possible** to cleanly convert a BIP-39 generated wallet Seed into a SLIP-39 wallet. Both BIP-39 and SLIP-39 preserve the original 128- to 256-bit Seed

Entropy (random) bits, but these bits are used **very differently** – and incompatibly – to generate the resultant wallet Seed.

The least desirable method is to preserve the 512-bit **output** of the BIP-39 mnemonic phrase as a set of 512-bit (59-word) SLIP-39 Mnemonics. But first, lets review how BIP-39 works.

3.1.1 BIP-39 Entropy to Mnemonic

BIP-39 uses a single set of 12, 15, 18, 21 or 24 BIP-39 words to carefully preserve a specific 128 to 256 bits of initial Seed Entropy. Here's a 128-bit (12-word) example using some fixed "entropy" `0xFFFF..FFFF`. You'll note that, from the BIP-39 Mnemonic, we can either recover the original 128-bit Seed Entropy, **or** we can generate the resultant 512-bit Seed w/ the correct passphrase:

```
from mnemonic import Mnemonic
bip39_english       = Mnemonic("english")
entropy             = b'\xFF' * 16
entropy_hex = codecs.encode( entropy, 'hex_codec' ).decode( 'ascii' )
entropy_mnemonic    = bip39_english.to_mnemonic( entropy )

recovered = slip39.recover_bip39( entropy_mnemonic, as_entropy=True )
recovered_hex = codecs.encode( recovered, 'hex_codec' ).decode( 'ascii' )

recovered_seed = slip39.recover_bip39( entropy_mnemonic, passphrase=passphrase )
recovered_seed_hex = codecs.encode( recovered_seed, 'hex_codec' ).decode( 'ascii' )

[
 [ "Original Entropy", entropy_hex ],
 [ "BIP-39 Mnemonic", entropy_mnemonic ],
 [ "Recovered Entropy", recovered_hex ],
 [ "Recovered Seed", f"{recovered_seed_hex:.50}..." ],
]
```

0	1
Original Entropy	ffffffffffffffffffffffffffffffff
BIP-39 Mnemonic	zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo wrong
Recovered Entropy	ffffffffffffffffffffffffffffffff
Recovered Seed	b6a6d8921942dd9806607ebc2750416b289adea669198769f2...

Each word is one of a corpus of 2048 words; therefore, each word encodes 11 bits (2048 = `2**11) of entropy. So, we provided 128 bits, but 12*11` = 132. So where does the extra 4 bits of data come from?

It comes from the first few bits of a SHA256 hash of the entropy, which is added to the end of the supplied 128 bits, to reach the required 132 bits: 132 / 11 == 12 words.

This last 4 bits (up to 8 bits, for a 256-bit 24-word BIP-39) is checked, when validating the BIP-39 mnemonic. Therefore, making up a random BIP-39 mnemonic will succeed only 1 / 16 times on average, due to an incorrect checksum 4-bit (16 == 2**4) . Lets check:

```
def random_words( n, count=100 ):
    for _ in range( count ):
        yield ' '.join( random.choice( bip39_english.wordlist ) for _ in range( n ))

successes           = sum(
    bip39_english.check( m )
```

```
    for i,m in enumerate( random_words( 12, 10000 ))) / 100

[
  [ "Valid random 12-word mnemonics:", f"{successes}%" ],
  [ "Or, about: ", f"1 / {100/successes:.3}" ],
]
```

0	1
Valid random 12-word mnemonics:	6.09%
Or, about:	1 / 16.4

Sure enough, about 1/16 random 12-word phrases are valid BIP-39 mnemonics. OK, we've got the contents of the BIP-39 phrase dialed in. How is it used to generate accounts?

3.1.2 BIP-39 Mnemonic to Seed

Unfortunately, BIP-39 does **not** use the carefully preserved 128-bit entropy to generate the wallet! Nope, it is stretched to a 512-bit seed using PBKDF2 HMAC SHA512. The normalized **text** (*not the Entropy bytes*) of the 12-word mnemonic is then used (with a salt of "mnemonic" plus an optional passphrase, "" by default), to obtain the 512-bit seed:

```
seed                = bip39_english.to_seed( entropy_mnemonic )
seed_hex            = codecs.encode( seed, 'hex_codec' ).decode( 'ascii' )
[
 [ f"{len(seed)*8}-bit seed:", f"{seed_hex:.50}..." ]
]
```

0	1
512-bit seed:	b6a6d8921942dd9806607ebc2750416b289adea669198769f2...

3.1.3 BIP-39 Seed to Address

Finally, this 512-bit seed is used to derive HD wallet(s). The HD Wallet key derivation process consumes whatever seed entropy is provided (512 bits in the case of BIP-39), and uses HMAC SHA512 with a prefix of b"Bitcoin seed" to stretch the supplied seed entropy to 64 bytes (512 bits). Then, the HD Wallet **path** segments are iterated through, permuting the first 32 bytes of this material as the key with the second 32 bytes of material as the chain node, until finally the 32-byte (256-bit) Ethereum account private key is produced. We then use this private key to compute the rest of the Ethereum account details, such as its public address.

```
path                = "m/44'/60'/0'/0/0"
bip39_eth_hd        = slip39.account( seed, 'ETH', path )
[
 [ f"{len(bip39_eth_hd.key)*4}-bit derived key path:", f"{path}" ],
 [ "Produces private key: ", f"{bip39_eth_hd.key}" ],
 [ "Yields Ethereum address:", f"{bip39_eth_hd.address}" ],
]
```

0	1
256-bit derived key path:	m/44'/60'/0'/0/0
Produces private key:	7af65ba4dd53f23495dcb04995e96f47c243217fc279f10795871b725cd009ae
Yields Ethereum address:	0xfc2077CA7F403cBECA41B1B0F62D91B5EA631B5E

Thus, we see that while the 12-word BIP-39 mnemonic careful preserves the original 128-bit entropy, this data is not directly used to derive the wallet private key and address.

Also, since an irreversible hash is used to derive the Seed from the Mnemonic, we can't reverse the process on the seed to arrive back at the BIP-39 mnemonic phrase.

3.1.4 SLIP-39 Entropy to Mnemonic

Just like BIP-39 carefully preserves the original 128-bit Seed Entropy bytes in a single 12-word mnemonic phrase, SLIP-39 preserves the original 128- or 256-bit Seed Entropy in a *set* of 20- or 33-word Mnemonic phrases.

```
name,thrs,grps,acct = slip39.create(
    "Test", 2, { "Mine": (1,1), "Fam": (2,3) }, entropy )
[
 [ f"{g_name}({g_of}/{len(g_mnems)}) #{g_n+1}:" if l_n == 0 else "" ] + words
 for g_name,(g_of,g_mnems) in grps.items()
 for g_n,mnem in enumerate( g_mnems )
 for l_n,(line,words) in enumerate(slip39.organize_mnemonic(
         mnem, rows=7, cols=3, label=f"{g_name}({g_of}/{len(g_mnems)}) #{g_n+1}:" ))
]
```

0	1	2	3
Mine(1/1) #1:	1 academic	8 safari	15 standard
	2 acid	9 drug	16 angry
	3 acrobat	10 browser	17 similar
	4 easy	11 trash	18 aspect
	5 change	12 fridge	19 smug
	6 injury	13 busy	20 violence
	7 painting	14 finger	
Fam(2/3) #1:	1 academic	8 prevent	15 dwarf
	2 acid	9 mouse	16 dream
	3 beard	10 daughter	17 flavor
	4 echo	11 ancient	18 oral
	5 crystal	12 fortune	19 chest
	6 machine	13 ruin	20 marathon
	7 bolt	14 warmth	
Fam(2/3) #2:	1 academic	8 prune	15 briefing
	2 acid	9 pickup	16 often
	3 beard	10 device	17 escape
	4 email	11 device	18 sprinkle
	5 dive	12 peanut	19 segment
	6 warn	13 enemy	20 devote
	7 ranked	14 graduate	
Fam(2/3) #3:	1 academic	8 dining	15 intimate
	2 acid	9 invasion	16 satoshi
	3 beard	10 bumpy	17 hobo
	4 entrance	11 identify	18 ounce
	5 alarm	12 anxiety	19 both
	6 health	13 august	20 award
	7 discuss	14 sunlight	

Since there is some randomness used in the SLIP-39 mnemonics generation process, we would get a **different** set of words each time for the fixed "entropy" `0xFFFF..FF` used in this example (if we hadn't manually disabled entropy for `shamir_mnemonic`, above), but we will **always** derive the same Ethereum account `0x824b..19a1` at the specified HD Wallet derivation path.

```
[
 [ "Crypto", "HD Wallet Path:", "Ethereum Address:" ]
] + [
 [ account.crypto, account.path, account.address ]
```

```
 for group in create_details.accounts
 for account in group
]
```

0	1	2
Crypto	HD Wallet Path:	Ethereum Address:
ETH	m/44’/60’/0’/0/0	0x824b174803e688dE39aF5B3D7Cd39bE6515A19a1
BTC	m/44’/0’/0’/0/0	bc1qm5ua96hx30snwrwsfnv97q96h53l86ded7wmjl
ETH	m/44’/60’/0’/0/1	0x8D342083549C635C0494d3c77567860ee7456963
BTC	m/44’/0’/0’/0/1	bc1qwz6v9z49z8mk5ughj7r78hjsp45jsxgzh29lnh
ETH	m/44’/60’/0’/0/2	0x52787E24965E1aBd691df77827A3CfA90f0166AA
BTC	m/44’/0’/0’/0/2	bc1q690m430qu29auyefarwfrvfumncunvyw6v53n9

3.1.5 SLIP-39 Mnemonic to Seed

Lets prove that we can actually recover the **original** Seed Entropy from the SLIP-39 recovery Mnemonics; in this case, we’ve specified a SLIP-39 group_threshold of 2 groups, so we’ll use 1 Mnemonic from Mine, and 2 from the Fam group:

```
_,mnem_mine         = grps[’Mine’]
_,mnem_fam          = grps[’Fam’]
recseed             = slip39.recover( mnem_mine + mnem_fam[:2] )
recseed_hex         = codecs.encode( recseed, ’hex_codec’ ).decode( ’ascii’ )
[
 [ f"{len(recseed)*8}-bit Seed:", f"{recseed_hex}" ]
]
```

0	1
128-bit Seed:	ffffffffffffffffffffffffffffffff

3.1.6 SLIP-39 Seed to Address

And we’ll use the same style of code as for the BIP-39 example above, to derive the Ethereum address **directly** from this recovered 128-bit seed:

```
slip39_eth_hd       = slip39.account( recseed, ’ETH’, path )
[
 [ f"{len(slip39_eth_hd.key)*4}-bit derived key path:", f"{path}" ],
 [ "Produces private key: ", f"{slip39_eth_hd.key}" ],
 [ "Yields Ethereum address:", f"{slip39_eth_hd.address}" ],
]
```

0	1
256-bit derived key path:	m/44’/60’/0’/0/0
Produces private key:	6a2ec39aab88ec0937b79c8af6aaf2fd3c909e9a56c3ddd32ab5354a06a21a2b
Yields Ethereum address:	0x824b174803e688dE39aF5B3D7Cd39bE6515A19a1

And we see that we obtain the same Ethereum address `0x824b..1a2b` as we originally got from `slip39.create` above. However, this is **not the same** Ethereum wallet address obtained from BIP-39 with exactly the same `0xFFFF...FF` Seed Entropy, which was `0xfc20..1B5E`!

This is due to the fact that BIP-39 does not use the recovered Seed Entropy to produce the seed like SLIP-39 does, but applies additional one-way hashing of the Mnemonic to produce a 512-bit Seed.

3.2 BIP-39 vs SLIP-39 Key Derivation Summary

At no time in BIP-39 account derivation is the original 128-bit Seed Entropy used (directly) in the derivation of the wallet key. This differs from SLIP-39, which directly uses the 128-bit Seed Entropy recovered from the SLIP-39 Shamir's Secret Sharing System recovery process to generate each HD Wallet account's private key.

Furthermore, there is no point in the BIP-39 Seed Entropy to account generation where we **could** introduce a known 128-bit seed and produce a known Ethereum wallet from it, other than as the very beginning.

Therefore, our BIP-39 Backup via SLIP-39 strategy must focus on backing up the original 128- to 256-bit Seed Entropy.

3.3 BIP-39 Backup via SLIP-39

Here are the two available methods for backing up insecure and unreliable BIP-39 Mnemonic phrases, using SLIP-39.

The first "Emergency Recovery" method allows you to recover your BIP-39 generated wallets **without the passphrase**, but does not support recovery using hardware wallets; you must output "Paper Wallets" and use them to recover the Cryptocurrency funds.

The second "Best Recovery: Using BIP-39" allows us to recover the accounts to *any* standard BIP-39 hardware wallet! However, the SLIP-39 Mnemonics are **not** compatible with standard SLIP-39 wallets like the Trezor "Model T" – you have to use the recovered BIP-39 Mnemonic phrase to recover the hardware wallet.

3.3.1 Emergency Recovery: Using Recovered Paper Wallets

There is one approach which can preserve an original BIP-39 generated wallet addresses, using SLIP-39 mnemonics.

It is clumsy, as it preserves the BIP-39 **output** 512-bit stretched seed, and the resultant 59-word SLIP-39 mnemonics cannot be used (at present) with the Trezor hardware wallet. They can, however, be used to recover the HD wallet private keys without access to the original BIP-39 Mnemonic phrase *or passphrase* – you could generate and distribute a set of more secure SLIP-39 Mnemonic phrases, instead of trying to secure the original BIP-39 mnemonic – without abandoning your BIP-39 wallets.

We'll use `slip39.recovery --bip39 ...` to recover the 512-bit stretched seed from BIP-39:

```
( python3 -m slip39.recovery --bip39 -v \
    --mnemonic "zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo wrong"
) 2>&1
```

```
2022-04-22 16:20:53 slip39.recovery  Recovered 512-bit BIP-39 secret from english mnemonic
2022-04-22 16:20:53 slip39.recovery  Recovered BIP-39 secret; To re-generate SLIP-39 wallet, send it to: python3 -m slip39
b6a6d8921942dd9806607ebc2750416b289adea669198769f2e15ed926c3aa92bf88ece232317b4ea463e84b0fcd3b53577812ee449ccc448eb45e6f54
```

Then we can generate a 59-word SLIP-39 mnemonic set from the 512-bit secret:

```
( python3 -m slip39.recovery --bip39 \
    --mnemonic "zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo wrong" \
  | python3 -m slip39 --secret - --no-card -v
) 2>&1 | tail -20

2022-04-22 16:20:54 slip39                7 living    19 bumpy     31 memory    43 scandal   55 obesity
2022-04-22 16:20:54 slip39                8 screw     20 oven      32 piece     44 teammate  56 grasp
2022-04-22 16:20:54 slip39                9 luck      21 grant     33 evil      45 brother   57 theory
2022-04-22 16:20:54 slip39               10 guilt     22 modern    34 dismiss   46 fishing   58 station
2022-04-22 16:20:54 slip39               11 marathon  23 boundary  35 critical  47 alien     59 pistol
2022-04-22 16:20:54 slip39               12 medal     24 plains    36 script    48 maximum
2022-04-22 16:20:54 slip39          6th   1 submit    13 erode     25 stilt     37 credit    49 civil
2022-04-22 16:20:54 slip39                2 acid      14 staff     26 platform  38 fact      50 ordinary
2022-04-22 16:20:54 slip39                3 decision  15 formal    27 spelling  39 chemical  51 device
2022-04-22 16:20:54 slip39                4 spider    16 rich      28 humidity  40 game      52 predator
2022-04-22 16:20:54 slip39                5 acquire   17 step      29 believe   41 swimming  53 picture
2022-04-22 16:20:54 slip39                6 adequate  18 human     30 aircraft  42 mouse     54 river
2022-04-22 16:20:54 slip39                7 scroll    19 soul      31 secret    43 makeup    55 intimate
2022-04-22 16:20:54 slip39                8 source    20 fatigue   32 frost     44 scholar   56 sympathy
2022-04-22 16:20:54 slip39                9 stilt     21 yield     33 drove     45 document  57 negative
2022-04-22 16:20:54 slip39               10 endorse   22 axle      34 pajamas   46 dictate   58 beyond
2022-04-22 16:20:54 slip39               11 crowd     23 warn      35 exotic    47 funding   59 dilemma
2022-04-22 16:20:54 slip39               12 rich      24 task      36 chew      48 laden
2022-04-22 16:20:54 slip39.layout    ETH    m/44'/60'/0'/0/0    : 0xfc2077CA7F403cBECA41B1B0F62D91B5EA631B5E
2022-04-22 16:20:54 slip39.layout    BTC    m/84'/0'/0'/0/0     : bc1qk0a9hr7wjfxeenz9nwenw9flhq0tmsf6vsgnn2
```

This `0xfc20..1B5E` address is the same Ethereum address as is recovered on a Trezor using this BIP-39 mnemonic phrase. Thus, we can generate "Paper Wallets" for the desired Cryptocurrency accounts, and recover the funds.

So, this does the job:

- Uses our original BIP-39 Mnemonic
- Does not require remembering the BIP-39 passphrase
- Preserves all of the original wallets

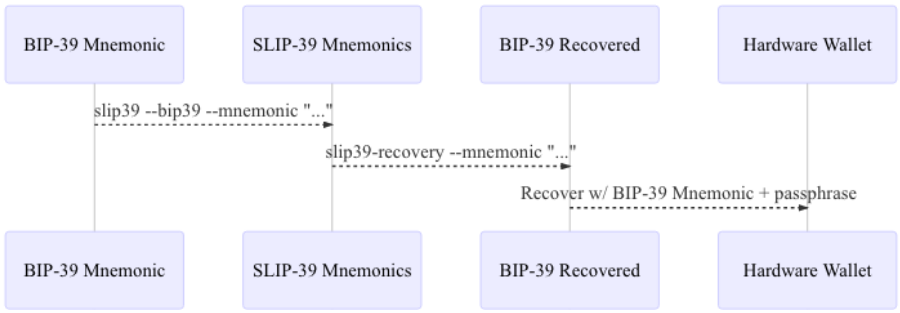
But:

- The 59-word SLIP-39 Mnemonics cannot (yet) be imported into the Trezor "Model T"
- The original BIP-39 Mnemonic phrase cannot be recovered, for any hardware wallet
- Must use the SLIP-39 App to generate "Paper Wallets", to recover the funds

So, this is a good "emergency backup" solution; you or your heirs would be able to recover the funds with a very high level of security and reliability.

3.3.2 Best Recovery: Using Recovered BIP-39 Mnemonic Phrase

The best solution is to use SLIP-39 to back up the original BIP-39 Seed Entropy, and then later recover that Seed Entropy and re-generate the BIP-39 Mnemonic phrase:



First, observe that we can recover the 128-bit Seed Entropy from the BIP-39 Mnemonic phrase (not the 512-bit generated Seed): 3

```
( python3 -m slip39.recovery --bip39 --entropy -v \
    --mnemonic "zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo wrong"
) 2>&1
```

```
2022-04-22 16:20:55 slip39.recovery  Recovered 128-bit BIP-39 secret from english mnemonic
2022-04-22 16:20:55 slip39.recovery  Recovered BIP-39 secret; To re-generate SLIP-39 wallet, send it to: python3 -m slip39
ffffffffffffffffffffffffffffffff
```

Now we generate SLIP-39 Mnemonics to recover the 128-bit Seed Entropy. Note that these are 20-word Mnemonics. However, these are **NOT** the wallets we expected! These are the well-known native SLIP-39 wallets from the `0xFFFF...FF` Seed Entropy; not the well-known native BIP-39 wallets from that Seed Entropy, which generate the Ethereum wallet address `0xfc20..1B5E`! Why not?
3

```
( python3 -m slip39.recovery --bip39 --entropy \
    --mnemonic "zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo wrong" \
  | python3 -m slip39 --secret - --no-card -v
) 2>&1 | tail -20
```

```
2022-04-22 16:20:56 slip39                4 skin      11 duckling  18 phantom
2022-04-22 16:20:56 slip39                5 daughter  12 failure   19 kernel
2022-04-22 16:20:56 slip39                6 timely    13 meaning   20 aircraft
2022-04-22 16:20:56 slip39                7 goat      14 shrimp
2022-04-22 16:20:56 slip39           5th  1 daughter   8 beard     15 best
2022-04-22 16:20:56 slip39                2 discuss    9 explain   16 necklace
2022-04-22 16:20:56 slip39                3 decision  10 magazine  17 slow
2022-04-22 16:20:56 slip39                4 snake     11 painting  18 flip
2022-04-22 16:20:56 slip39                5 avoid     12 element   19 impact
2022-04-22 16:20:56 slip39                6 cricket   13 grief     20 losing
2022-04-22 16:20:56 slip39                7 prune     14 picture
2022-04-22 16:20:56 slip39           6th  1 daughter   8 woman     15 smart
2022-04-22 16:20:56 slip39                2 discuss    9 trip      16 jewelry
2022-04-22 16:20:56 slip39                3 decision  10 plan      17 crazy
2022-04-22 16:20:56 slip39                4 spider    11 penalty   18 round
2022-04-22 16:20:56 slip39                5 damage    12 numerous  19 seafood
2022-04-22 16:20:56 slip39                6 deliver   13 mouse     20 yoga
2022-04-22 16:20:56 slip39                7 stadium   14 traveler
2022-04-22 16:20:56 slip39.layout    ETH    m/44'/60'/0'/0/0    : 0x824b174803e688dE39aF5B3D7Cd39bE6515A19a1
2022-04-22 16:20:56 slip39.layout    BTC    m/84'/0'/0'/0/0     : bc1q9yscq3l2yfxlvnlk3cszpqefparrv7tk24u6pl
```

Because we must tell `slip39` to that we're using the BIP-39 Mnemonic and Seed generation process to derived the wallet addresses from the Seed Entropy (not the SLIP-39 standard). So, we add the `-using-bip39` option:
3

```
( python3 -m slip39.recovery --bip39 --entropy \
    --mnemonic "zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo zoo wrong" \
  | python3 -m slip39 --secret - --no-card -v --using-bip39
) 2>&1 | tail -20

2022-04-22 16:20:56 slip39                4 skin      11 dictate   18 install
2022-04-22 16:20:56 slip39                5 agree     12 injury    19 valid
2022-04-22 16:20:56 slip39                6 tricycle  13 seafood   20 aquatic
2022-04-22 16:20:56 slip39                7 hospital  14 veteran
2022-04-22 16:20:56 slip39           5th  1 activity   8 warn      15 pacific
2022-04-22 16:20:56 slip39                2 provide    9 woman     16 document
2022-04-22 16:20:56 slip39                3 decision  10 training  17 coding
2022-04-22 16:20:56 slip39                4 snake     11 album     18 hunting
2022-04-22 16:20:56 slip39                5 brave     12 daisy     19 prisoner
2022-04-22 16:20:56 slip39                6 aide      13 freshman  20 expect
2022-04-22 16:20:56 slip39                7 spray     14 sister
2022-04-22 16:20:56 slip39           6th  1 activity   8 finger    15 glasses
2022-04-22 16:20:56 slip39                2 provide    9 counter   16 upstairs
2022-04-22 16:20:56 slip39                3 decision  10 editor    17 flash
2022-04-22 16:20:56 slip39                4 spider    11 western   18 relate
2022-04-22 16:20:56 slip39                5 acne      12 upstairs  19 evidence
2022-04-22 16:20:56 slip39                6 focus     13 endless   20 tactics
2022-04-22 16:20:56 slip39                7 golden    14 drove
2022-04-22 16:20:56 slip39.layout    ETH    m/44'/60'/0'/0/0    : 0xfc2077CA7F403cBECA41B1B0F62D91B5EA631B5E
2022-04-22 16:20:56 slip39.layout    BTC    m/84'/0'/0'/0/0     : bc1qk0a9hr7wjfxeenz9nwenw9flhq0tmsf6vsgnn2
```

And, there we have it – we've recovered exactly the same Ethereum and Bitcoin wallets as would a native BIP-39 hardware wallet like a Ledger Nano.

1. On the GUI: Select "Using BIP-39"

   In the SLIP-39 App, change Controls to "Recovery". In "Seed Source", select "BIP-39", and in "Seed & SLIP-39 Recover Groups", select "Using BIP-39".

   This will

4 Building & Installing

The `python-slip39` project is tested under both homebrew:

```
$ brew install python-tk@3.9
```

and using the official python.org/downloads installer.

Either of these methods will get you a `python3` executable running version 3.9+, usable for running the `slip39` module, and the `slip39.gui` GUI.

4.1 The `slip39` Module

To build the wheel and install `slip39` manually:

```
$ git clone git@github.com:pjkundert/python-slip39.git
$ make -C python-slip39 install
```

To install from Pypi, including the optional requirements to run the PySimpleGUI/tkinter GUI, support serial I/O, and to support creating encrypted BIP-38 and Ethereum JSON Paper Wallets:

```
$ python3 -m pip install slip39[gui,paper,serial]
```

4.2 The slip39 GUI

To install from Pypi, including the optional requirements to run the PySimpleGUI/tkinter GUI:

```
$ python3 -m pip install slip39[gui]
```

Then, there are several ways to run the GUI:

```
$ python3 -m slip39.gui     # Execute the python slip39.gui module main method
$ slip39-gui                # Run the main function provided by the slip39.gui module
```

4.2.1 The macOS/win32 SLIP-39.app GUI

You can build the native macOS and win32 SLIP-39.app App.

This requires the official python.org/downloads installer; the homebrew python-tk@3.9 will not work for building the native app using either PyInstaller. (The py2app approach doesn't work in either version of Python).

```
$ git clone git@github.com:pjkundert/python-slip39.git
$ make -C python-slip39 app
```

4.2.2 The Windows 10 SLIP-39 GUI

Install Python from https://python.org/downloads, and the Microsoft C++ Build Tools via the Visual Studio Installer (required for installing some slip39 package dependencies).

To run the GUI, just install slip39 package from Pypi using pip, including the gui and wallet options. Building the Windows SLIP-39 executable GUI application requires the dev option.

```
PS C:\Users\IEUser> pip install slip39[gui,wallet,dev]
```

To work with the python-slip39 Git repo on Github, you'll also need to install Git from git-scm.com. Once installed, run "Git bash", and

```
$ ssh-keygen.exe -t ed25519
```

to create an id_ed25519.pub SSH identity, and import it into your Git Settings SSH keys. Then,

```
$ mkdir src
$ cd src
$ git clone git@github.com:pjkundert/python-slip39.git
```

1. Code Signing

   The MMC (Microsoft Management Console) is used to store your code-signing certificates. See stackoverflow.com for how to enable its Certificate management.

5 Dependencies

Internally, python-slip39 project uses Trezor's python-shamir-mnemonic to encode the seed data to SLIP-39 phrases, python-hdwallet to convert seeds to ETH, BTC, LTC and DOGE wallets, and the Ethereum project's eth-account to produce encrypted JSON wallets for specified Ethereum accounts.

5.1 The `python-shamir-mnemonic` API

To use it directly, obtain , and install it, or run `python3 -m pip install shamir-mnemonic`.

```
$ shamir create custom --group-threshold 2 --group 1 1 --group 1 1 --group 2 5 --group 3 6
Using master secret: 87e39270d1d1976e9ade9cc15a084c62
Group 1 of 4 - 1 of 1 shares required:
merit aluminum acrobat romp capacity leader gray dining thank rhyme escape genre havoc furl breathe class pitch location r
Group 2 of 4 - 1 of 1 shares required:
merit aluminum beard romp briefing email member flavor disaster exercise cinema subject perfect facility genius bike inclu
Group 3 of 4 - 2 of 5 shares required:
merit aluminum ceramic roster already cinema knit cultural agency intimate result ivory makeup lobe jerky theory garlic en
merit aluminum ceramic scared beam findings expand broken smear cleanup enlarge coding says destroy agency emperor hairy d
merit aluminum ceramic shadow cover smith idle vintage mixture source dish squeeze stay wireless likely privacy impulse to
merit aluminum ceramic sister duke relate elite ruler focus leader skin machine mild envelope wrote amazing justice mornin
merit aluminum ceramic smug buyer taxi amazing marathon treat clinic rainbow destroy unusual keyboard thumb story literary
Group 4 of 4 - 3 of 6 shares required:
merit aluminum decision round bishop wrote belong anatomy spew hour index fishing lecture disease cage thank fantasy extra
merit aluminum decision scatter carpet spine ruin location forward priest cage security careful emerald screw adult jerky
merit aluminum decision shaft arcade infant argue elevator imply obesity oral venture afraid slice raisin born nervous uni
merit aluminum decision skin already fused tactics skunk work floral very gesture organize puny hunting voice python trial
merit aluminum decision snake cage premium aide wealthy viral chemical pharmacy smoking inform work cubic ancestor clay ge
merit aluminum decision spider boundary lunar staff inside junior tendency sharp editor trouble legal visual tricycle auct
```