How a cryptocurrency hardware wallet works

Outline

1. What is a Wallet?
2. What is a Hardware Wallet?
3. Ledger Nano S
4. Master Key Derivation
5. Summary

1. What is a Wallet?

A wallet is like a keychain, it keeps your private keys to allow you to sign transactions and spend Bitcoin. You are your own bank.

2. What is a Hardware Wallet?

A hardware wallet is a mini-computer, specifically designed to hold your private keys and sign transactions even when connected to an unsecure computer.

3. Ledger Nano S

Why would I want to buy this?

- STMicroelectronics ST31 Secure Element MCU[1]
- AIS-31 compliant true random number generator[2]
- Protection from physical attacks through Secure Element and plausible deniability
- Protection from remote attacks through transaction verification on the device's screen
- It's the safest way to store cryptocurrency

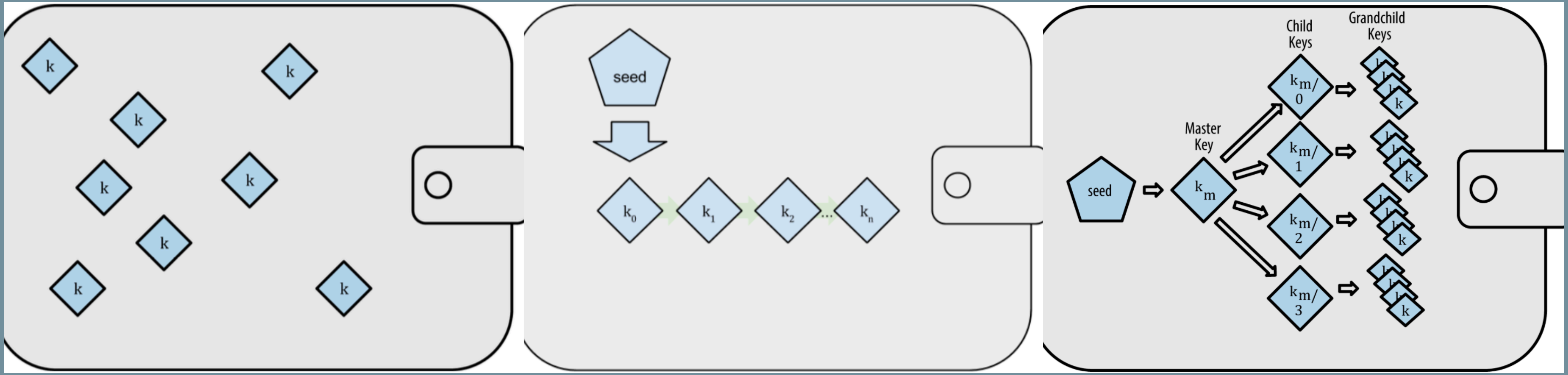
[1] https://media.readthedocs.org/pdf/ledger/latest/ledger.pdf page 27

[2] http://www.st.com/en/secure-mcus/st31h320.html, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS31pdf.pdf

4. Master Key Derivation

The three types of wallets:

- Random Wallet (hard to backup as addresses grow)
- Deterministic Wallet (easy to backup, no tree structure)
- Hierarchical Deterministic Wallet (easy to backup, tree structure)



4. Master Key Derivation

What are the benefits of HD wallets?

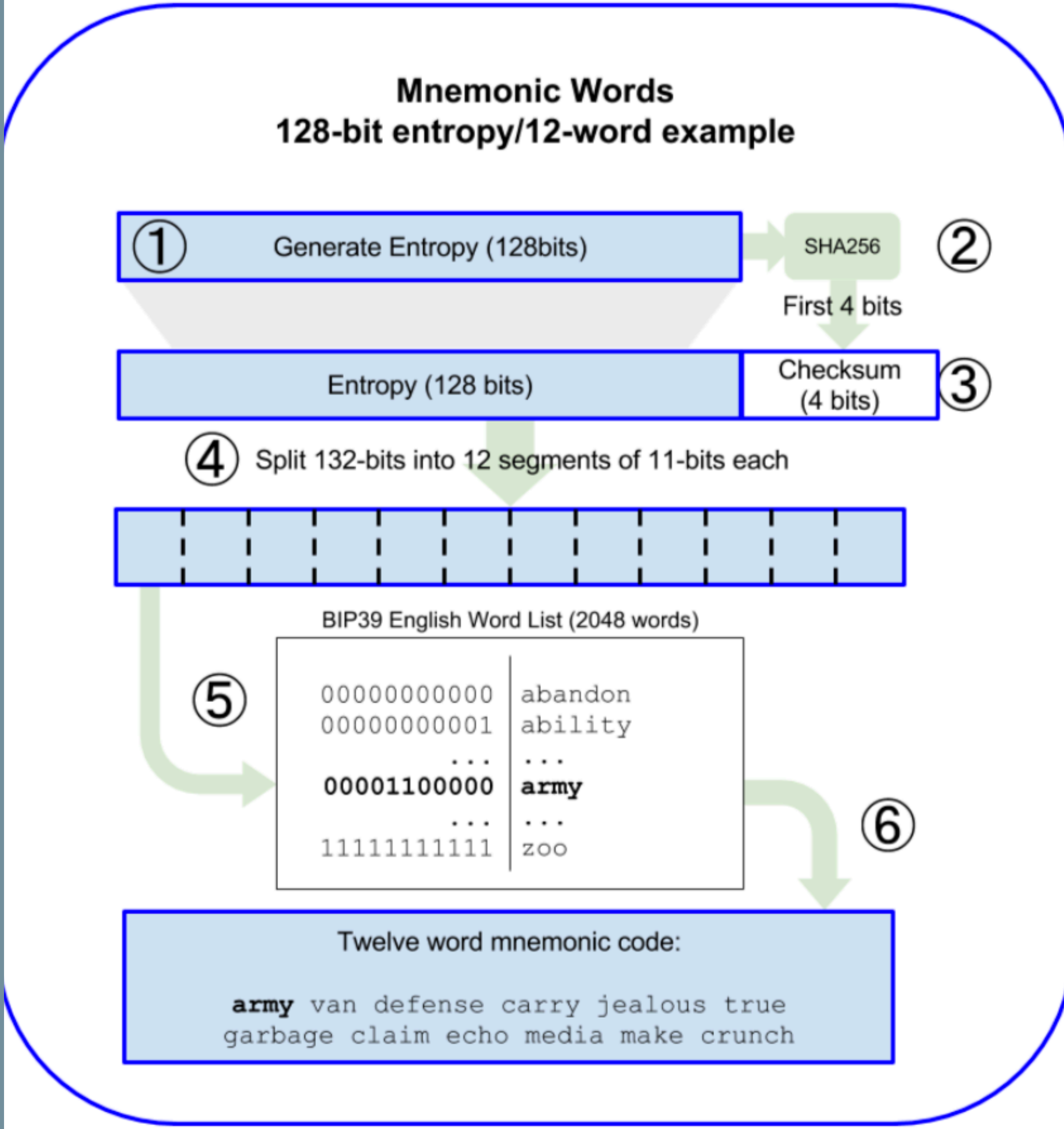
- Master public key allows insecure merchant webserver to generate BTC addresses for incoming payments without exposing the master private key[3]
- Different branches of keys can be used for different types of payments (one for customer payments, one for transaction change payments)
- Audits, per-office balances, etc.[4]

[3] https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki#unsecure-money-receiver-nmih0

[4] https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki#use-cases

4. Master Key Derivation (BIP39[5])

- Random number generator generates 128-256 bits of entropy
- Entropy (ENT) / 32 to get the bits of checksum required
- Concatenate entropy bits and checksum bits (checksum bits are taken from beginning of SHA256 of entropy bits)
- Devide into 11bit long strings
- Map those bits to words from one of the word lists[6] (2^11 = 2048 possible words)



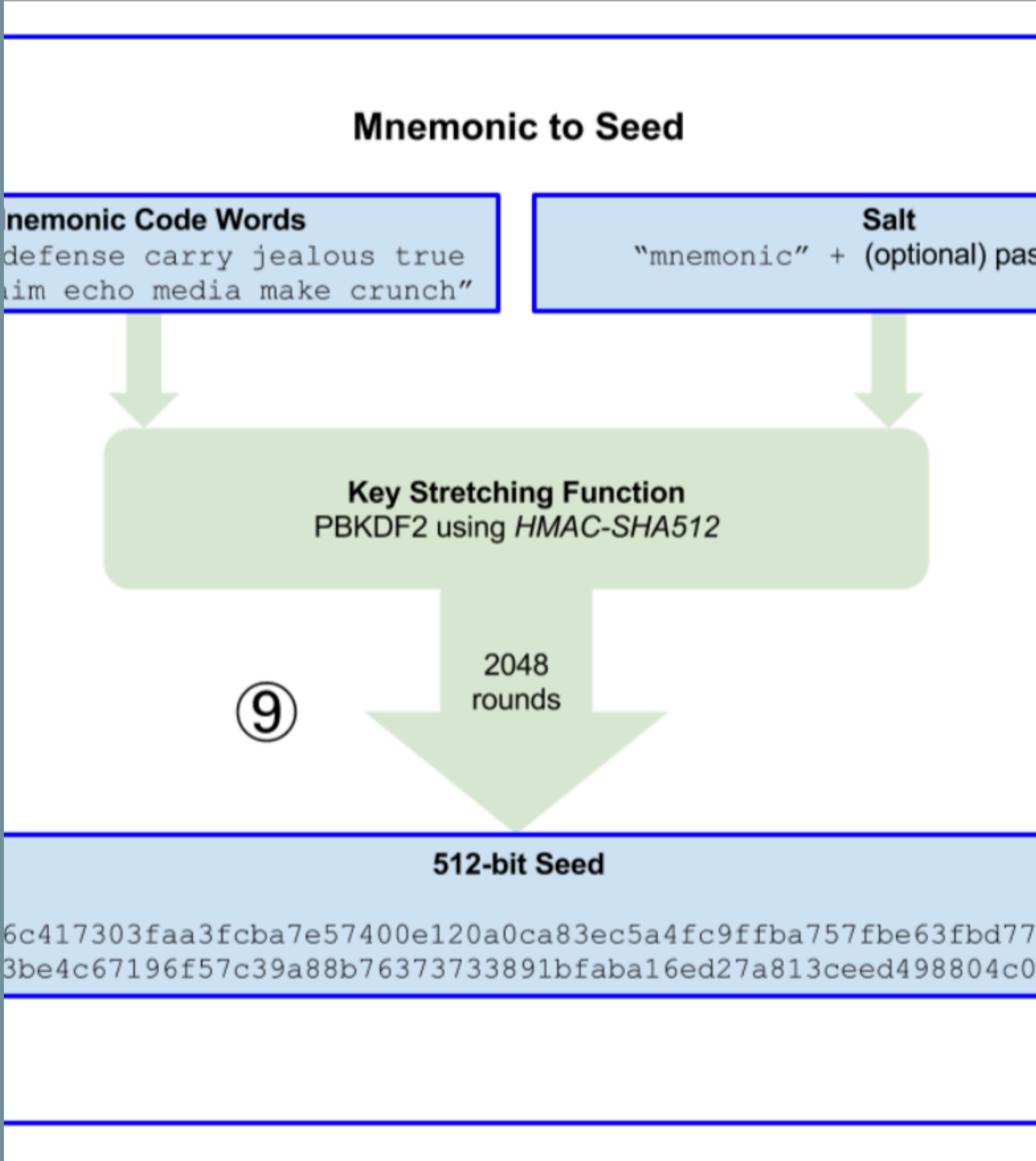
Mnemonic Words
128-bit entropy/12-word example
① Generate Entropy (128bits)
SHA256
②
First 4 bits
Entropy (128 bits)
Checksum (4 bits)
③
④ Split 132-bits into 12 segments of 11-bits each
BIP39 English Word List (2048 words)
⑤
00000000000 abandon
00000000001 ability
... ...
00001100000 army
... ...
11111111111 zoo
⑥
Twelve word mnemonic code:
army van defense carry jealous true garbage claim echo media make crunch

[5] https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

[6] https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt

4. Master Key Derivation

- Concatenate these words and use PBKDF2[7] with HMAC-SHA512 to produce a 512bit seed for your master private key
- Salt can be used as a "password" to provide plausible deniability. Keep one password for your checking and one for your savings account.


Mnemonic to Seed
nemonic Code Words
defense carry jealous true
im echo media make crunch"
Salt
"mnemonic" + (optional) pas
Key Stretching Function
PBKDF2 using HMAC-SHA512
2048
rounds
9
512-bit Seed
6c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fbd77
3be4c67196f57c39a88b76373733891bfaba16ed27a813ceed498804c0

[7] https://en.wikipedia.org/wiki/PBKDF2

5. Summary

- Do *NOT* loose your word wallet seed
- Hardware wallets are the safest way to store crypto assets (when used correctly[8])

[8] https://www.ledger.fr/2018/01/12/scam-second-hand-ledger-device/

Thank you 🙌