OST
Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

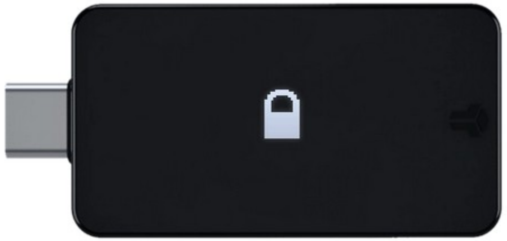
Seeds and Wallets

Thomas Bocek

29.10.2023

Introduction to Cryptocurrency Wallets

- What Are Cryptocurrency Wallets?
  - Digital tools to store, send, and receive digital currencies
  - Analog to ~bank accounts
- Key Functions of a Wallet
  - Storage of Private and Public Keys
    - Sign transactions
  - Interaction with blockchain
    - Balance checking and transaction history
- Types of Wallets
  - Hardware Wallets, Software Wallets, Paper Wallets



- Hardware Wallets
  - Trezor, Ledger, BitBox – specialized hardware
- Software Wallets
  - Metamask, THORWallet
- Paper Wallet
  - Physical document with mnemonic words

	SW wallet	HW wallet	Paper wallet
Hot wallet	x	x	
Cold wallet		x	x

Introduction to Cryptocurrency Wallets

- Importance of wallet security
  - Keeping assets safe from unauthorized access and cyber theft
  - Importance of backup and recovery methods
- Convenience and accessibility
  - Ease of use, mobile and desktop access
  - Importance for widespread adoption of cryptocurrencies
- Cryptocurrency wallets vs traditional banking
  - User-controlled security vs. bank-managed security

Introduction to HD Wallets

- Hierarchical Deterministic (HD) Wallets
  - Most cryptocurrency wallet are HD wallets
  - Based on the BIP32/BIP44 protocol
  - Allows creation of derived keys from a **single** master seed
- Key Features
  - Generation of multiple cryptocurrency addresses from a single seed
  - Simplifies management and backup
  - Each transaction could use a unique address for enhanced privacy
- Understanding BIP32/BIP44
  - BIP32 (Bitcoin Improvement Proposal 32) introduces the concept of hierarchical deterministic wallets
  - BIP44 builds on BIP32, adding a structure for multiple coin types and accounts
- Mechanism of HD Wallets
  - Based on a single seed (typically based on a BIP39 mnemonic phrase)
  - Seed leads to the generation of a master private key

Introduction to HD Wallets

- Benefits of HD Wallets
  - **Efficient Backup**: Single seed backup is sufficient for multiple addresses and keys
  - **Easy Organization**: Easy management of funds across various addresses/accounts
    - e.g., THORWallet, one seed, many accounts, BTC, ETH, …
- Disadvantages
  - User Experience → most wallets ask you to write down the seed phrase
    - Unexperienced user: what is this? Is this important?

- BIP39 mnemonic phrase
  - Seed phrase: series of words from a defined list
  - Essential for wallet backup and restoration
    - If lost, your cryptos are lost
- Seed Phrase Composition
  - Typically a sequence of 12 or 24 words
  - Encoding of 128bit or 256bit
- Let’s see how it works:

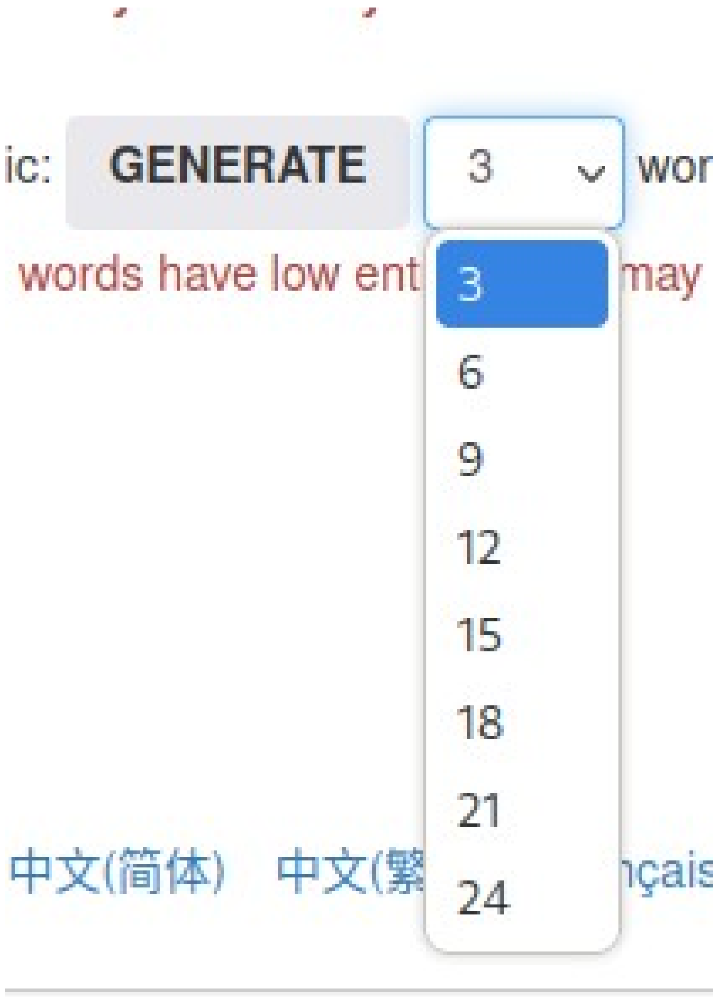
BIP39

- Generate a random number 128 bit or 256
  - Lets use 128bit for simplicity
  - Create random hex number (128bit)
    - `hex=$(hexdump -vn16 -e'4/4 "%08X" 1 "\n"' /dev/urandom)`
    - `padded_hex=$(printf "%032s" "$hex" | tr ' ' '0')`
  - Convert to binary
    - `padded_hex_bin=$(echo ${padded_hex} | (echo "obase=2; ibase=16;" && cat) | bc)`
    - `padded_hash_bin=$(echo ${hash_hex} | (echo "obase=2; ibase=16;" && cat) | BC_LINE_LENGTH=0 bc)`
  - Word list has 2048 entries = 11bit
  - 12 words x 11 bit = 132bit, 4 bit wasted?
    - 4bit used as checksum – append first 4 bit of sha256(rand number)
  - 24 words x 11 bit = 264bit, 8 bit checksum
    - `hash_hex=$(echo "$padded_hex" | xxd -r -p | openssl dgst -sha256 -binary | xxd -p | tr -d '\n' | tr '[:lower:]' '[:upper:]')`
    - `echo ${padded_hex_bin}${padded_hash_bin:0:4}`

-
```
110100111110111111010111110001101110
101011110011100100001010010111011101
000001010000001101110001110111000000
000001100101000111111111
```
- Take first 11 bit, lookup word
  - `11111100011` → 2019 → **wisdom**
- Take second 11 bit, lookup word
  - `11100101101` → 1837 → **tortoise**
- …
- Take the last 11 bit, lookup word
  - `00111111111` → 511 → **divert**
- Wrong words = checksum won’t match

BIP39

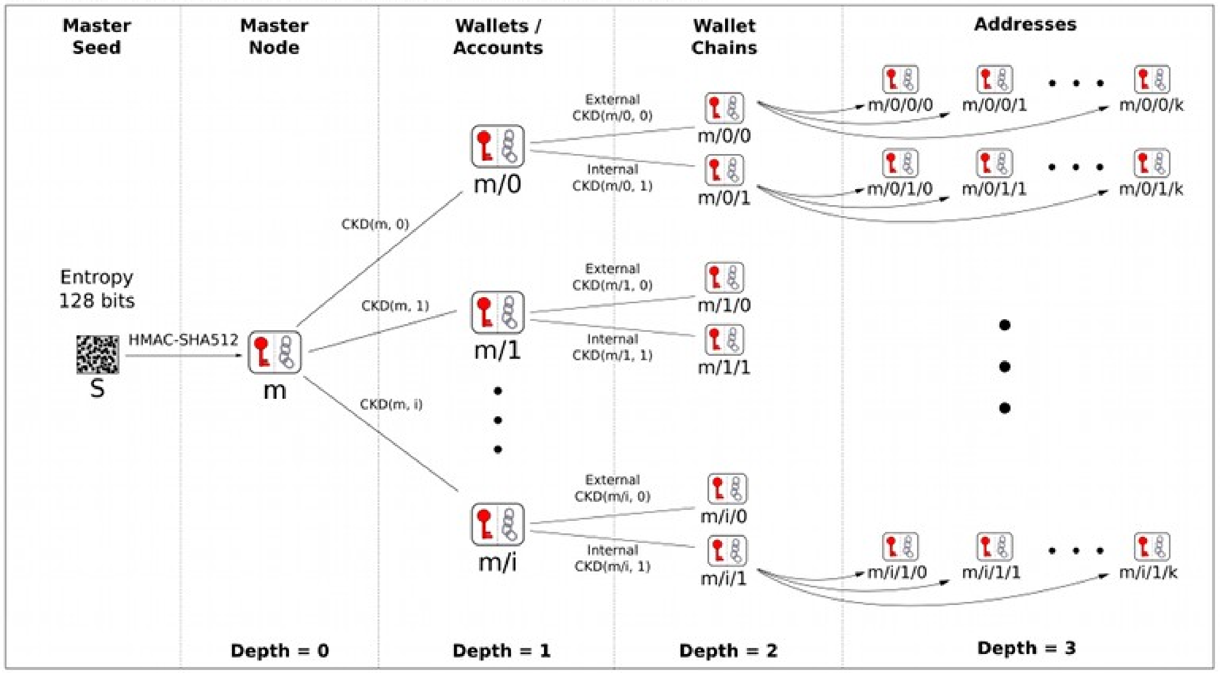
- 256 bit, same, but 8bit checksum
  - Mnemonic Code Converter [link]
- Seed extension
  - 13th/25th word
- From mnemonic to seed
  - PBKDF2 function with mnemonic sentence as password, string "mnemonic" + passphrase as salt
  - Seed = PBKDF2(“wisdom tortoise relief”, “mnemonicyourpassphrase”, 2048, ...)
- Seed can be used for BIP-32



BIP32/BIP44

- BIP 32

BIP 32 - Hierarchical Deterministic Wallets



Child Key Derivation Function ~ $\mathrm{CKD}(x,n) = \text{HMAC-SHA512}(x_{\text{Chain}}, x_{\text{PubKey}} \,||\, n)$

- BIP 44
  - m / purpose' / coin_type' / account' / change / address_index
    - Purpose → 44
    - Coin type
      - Bitcoin: m/44'/0'/2'/0/1
      - Ethereum: m/44'/60'/2'/0/1
    - Account → Account 2
    - Change (Bitcoin specific – resp. UTXO)
    - Address_index → Index 1
  - Hardened vs. non-hardened
    - Hardened: hash(parent private key + index)
    - Non: hash(parent public key + index)
    - Security implications: leaking derived private keys
      - But: if someone has access to a non-hardened public key, they can generate all subsequent non-hardened public keys in the same branch.

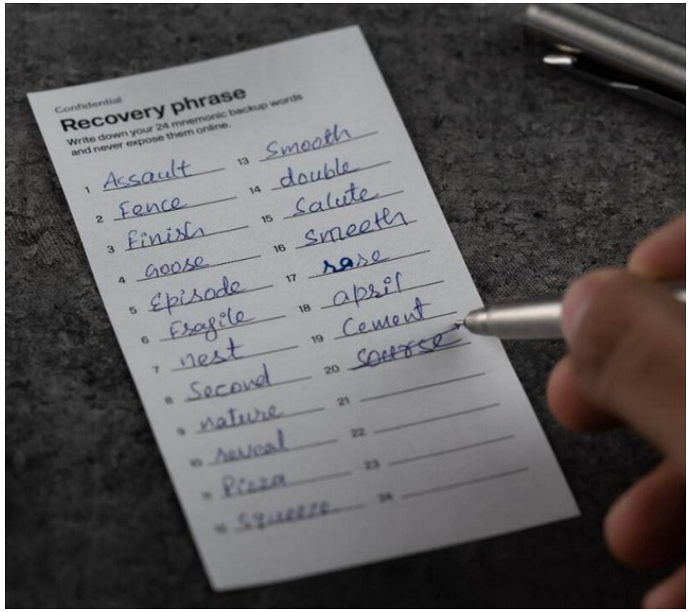
ECC

- $K = k \times G$
  - Private Key (k)
  - Base Point (G)
  - Public Key (K)
  - "×" is scalar multiplication on the elliptic curve
- Key derivation
  - $x \times K = x \times (k \times G)$
  - k is based on seed
  - x based on
    - hash(parent private key + index)
    - hash(parent public key + index)

- HD Wallets are the backbone of DeFi
- Be aware:
  - Single Point of Failure: The seed phrase represents a single point of failure; its compromise can lead to the loss of all associated assets
  - User Responsibility: In DeFi, users are solely responsible for their seed phrases. There's no central authority to appeal to for recovery if the seed is lost or stolen
  - Awareness: Educating users about the importance of securing their seed phrase and the mechanics of HD wallets is crucial in the DeFi space.
  - Best Practices: Promoting security best practices and the responsible use of DeFi services.

Best Practices Mnemonic

- When showing Metamask, I actually showed how **not** to do it
  - **Write It Down**: always write down the seed phrase, avoid digital storage unless it's encrypted. In addition



Confidential

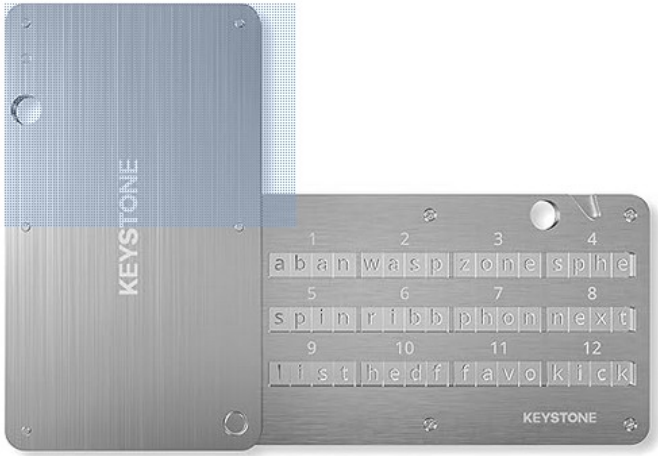
Recovery phrase

Write down your 24 mnemonic backup words and never expose them online.

1 Assault
2 Fence
3 Finish
4 Goose
5 Episode
6 Fragile
7 nest
8 Second
9 nature
10 sewcal
11 Pizza
12 Squeeze
13 Smooth
14 double
15 Salute
16 smeeth
17 rase
18 apsil
19 Cement
20 soucse
21
22
23
24

https://www.cypherock.com/blogs/post-seedless-wallets

- **Use Metal Backups**: For added durability against physical damage, store the seed phrase on a metal plate.
- **Maintain Multiple Backups**: prevent loss due to accidents or natural disasters
- **Educate Yourself Continuously**



1 aban 2 wasp 3 zone 4 sphe
5 spin 6 ribb 7 phon 8 next
9 list 10 hedf 11 favo 12 kick

https://www.amazon.com.au/Keystone-Mnemonic-Compatible-Hardware-Coldcard/dp/B09DKP6GMW?th=1