

Week 20 11.28

11.28 HD Wallet

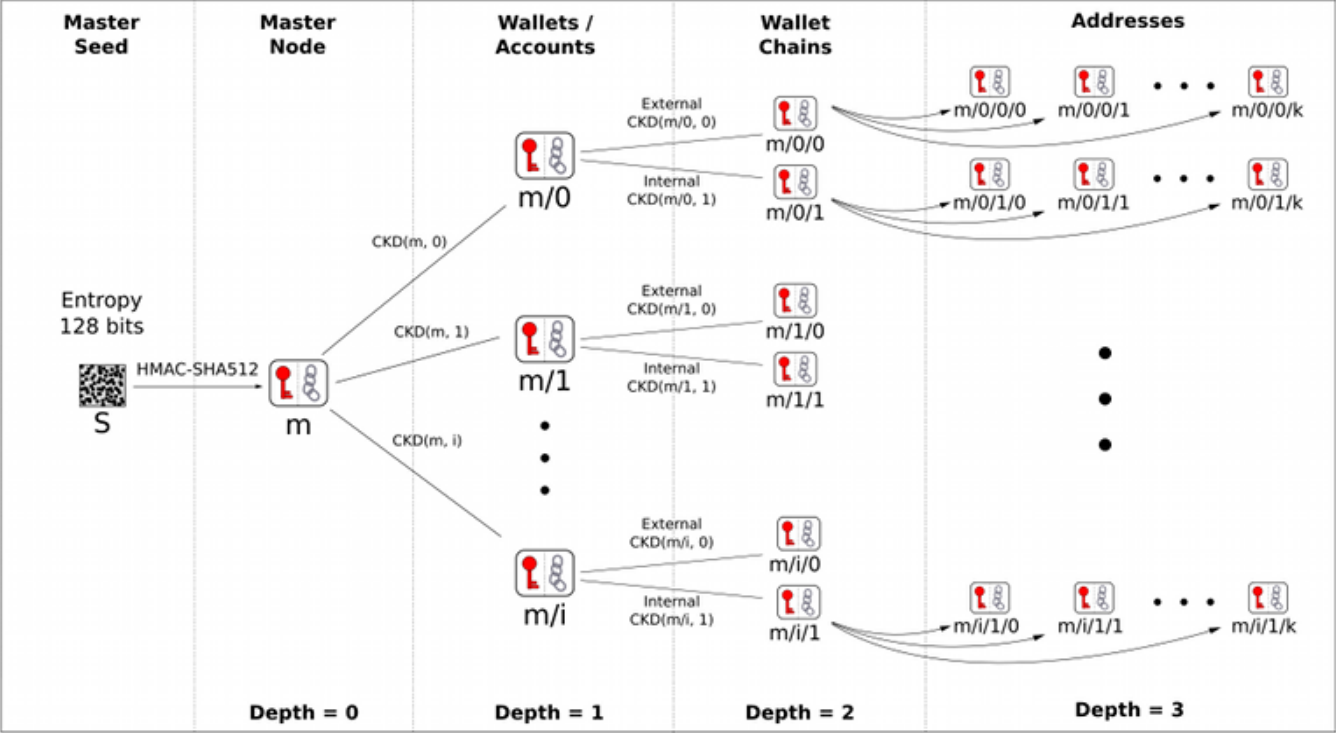
BIP-32 HD Wallet / Hierarchical Deterministic BIP-44

m / purpose' / coin_type' / account' / change / address_index

coin_type coin_type 0 60 Conflux 503

HD Wallet BIP-32 Master Seed 128bit 512bit

BIP 32 - Hierarchical Deterministic Wallets



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

11.29 HD Wallet

HD HD Master Seed “ ” fluent, meta

```
DK = PBKDF2(PRF, Password, Salt, c, dkLen)
```

5 BIP39

• PRF

BIP-39

HMAC-SHA512

• Password

PBKDF2

BIP-39

Master Seed

utf-8

• Salt

mnemonic

123456

mnemonic

+

mnemonic123456

• c

BIP-39

2048.

• dkLen

BIP-39

512

HD Wallet

Master Seed

HD

Master Seed

11.30

BIP-39

• 2048

12

nurse silk fiber machine jelly reduce coffee language fox forum cause team

204nurse12121001011110012(12*11=)132bit132128

1. ENT bit E128<=ENT<=256os.urandompython

2. ENT256ENT/32ENT=1284

3. 3/32*ENT

12.1 Keystore

KeystoreKeystore

```
{  "version": 3,  "id": "db029583- f1bd- 41cc- aeb5- b2ed5b33227b",  "address": "1cad0b19bb29d4674531d6f115237e16afce377c",  "crypto": {    "cipher text": "3198706577b0880234ecbb5233012a8ca0495bf2cfa2e45121b4f09434187aba",  }
```

```

    "cipherparams": {"iv": "a9a1f9565fd9831e669e8a9a0ec68818"},
    "cipher": "aes-128-ctr",
    "kdf": "scrypt",
    "kdfparams": {
      "dklen": 32,
      "salt": "3ce2d51bed702f2f31545be66fa73d1467d24686059776430df9508407b74231",
      "n": 8192,
      "r": 8,
      "p": 1,
    },
    "mac": "cf73832f328f3d5d1e0ec7b0f9c220facf951e8bba86c9f26e706d2df1e34890",
  },
}

```

[ciphertext](#)
[cipher](#)
[cipherparams](#)
[kdf](#)
[kdfparams](#)

[keystore](#)

[SDK](#)
[Keystore](#)
[Keystore](#)

12.2

[random](#)
[pyrandom.random](#)
[java.util.random](#)
[wintermute](#)

[SDK](#)
[/dev/urandom](#)
[/dev/random](#)

[Linux](#)

[SDK](#)

```

extra_key_bytes = text_if_str(to_bytes, extra_entropy)
key_bytes = keccak(os.urandom(32) + extra_key_bytes)

```

[/dev/urandom](#)
[urandom](#)
[u](#)
[/dev/random](#)
[/dev/urandom](#)
[/dev/urandom](#)
[/dev/random](#)

```

with open("/dev/random", 'rb') as f:
    print(f.read(32).hex())

```

Revision #10

Created 28 November 2022 03:28:23 by Darwin

Updated 2 December 2022 03:59:03 by Darwin