## Abstract

This BIP defines a logical hierarchy for deterministic wallets based on an algorithm described in BIP-0032 (BIP32 from now on) and purpose scheme described in BIP-0043 (BIP43 from now on).

This BIP is a particular application of BIP43.

## Motivation

The hierarchy proposed in this paper is quite comprehensive. It allows the handling of multiple coins, multiple accounts, external and internal chains per account and millions of addresses per chain.

## Path levels

We define the following 5 levels in BIP32 path:

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

Apostrophe in the path indicates that BIP32 hardened derivation is used.

Each level has a special meaning, described in the chapters below.

### Purpose

Purpose is a constant set to 44' (or 0x8000002C) following the BIP43 recommendation. It indicates that the subtree of this node is used according to this specification.

Hardened derivation is used at this level.

### Coin type

One master node (seed) can be used for unlimited number of independent cryptocoins such as Bitcoin, Litecoin or Namecoin. However, sharing the same space for various cryptocoins has some disadvantages.

This level creates a separate subtree for every cryptocoin, avoiding reusing addresses across cryptocoins and improving privacy issues.

Coin type is a constant, set for each cryptocoin. Cryptocoin developers may ask for registering unused number for their project.

The list of already allocated coin types is in the chapter "Registered coin types" below.

Hardened derivation is used at this level.

### Account

This level splits the key space into independent user identities, so the wallet never mixes the coins across different accounts.

Users can use these accounts to organize the funds in the same fashion as bank accounts; for donation purposes (where all addresses are considered public), for saving purposes, for common expenses etc.

Accounts are numbered from index 0 in sequentially increasing manner. This number is used as child index in BIP32 derivation.

Hardened derivation is used at this level.

Software should prevent a creation of an account if a previous account does not have a transaction history (meaning none of its addresses have been used before).

Software needs to discover all used accounts after importing the seed from an external source. Such an algorithm is described in "Account discovery" chapter.

### Change

Constant 0 is used for external chain and constant 1 for internal chain (also known as change addresses). External chain is used for addresses that are meant to be visible outside of the wallet (e.g. for receiving payments). Internal chain is used for addresses which are not meant to be visible outside of the wallet and is used for return transaction change.

Public derivation is used at this level.

### Index

Addresses are numbered from index 0 in sequentially increasing manner. This number is used as child index in BIP32 derivation.

Public derivation is used at this level.

## Account discovery

When the master seed is imported from an external source the software should start to discover the accounts in the following manner:

1. derive the first account's node (index = 0)
2. derive the external chain node of this account
3. scan addresses of the external chain; respect the gap limit described below
4. if no transactions are found on the external chain, stop discovery
5. if there are some transactions, increase the account index and go to step 1

This algorithm is successful because software should disallow creation of new accounts if previous one has no transaction history, as described in chapter "Account" above.

Please note that the algorithm works with the transaction history, not account balances, so you can have an account with 0 total coins and the algorithm will still continue with discovery.

### Address gap limit

Address gap limit is currently set to 20. If the software hits 20 unused addresses in a row, it expects there are no used addresses beyond this point and stops searching the address chain. We scan just the external chains, because internal chains receive only coins that come from the associated external chains.

Wallet software should warn when the user is trying to exceed the gap limit on an external chain by generating a new address.

## Registered coin types

These are the default registered coin types for usage in level 2 of BIP44 described in chapter "Coin type" above.

All these constants are used as hardened derivation.

| index | hexa | coin |
|---|---|---|
| 0 | 0x80000000 | Bitcoin |
| 1 | 0x80000001 | Bitcoin Testnet |

This BIP is not a central directory for the registered coin types, please visit SatoshiLabs that maintains the full list:

SLIP-0044 : Registered coin types for BIP-0044

To register a new coin type, an existing wallet that implements the standard is required and a pull request to the above file should be created.

## Examples

| coin | account | chain | address | path |
|---|---|---|---|---|
| Bitcoin | first | external | first | m / 44' / 0' / 0' / 0 / 0 |
| Bitcoin | first | external | second | m / 44' / 0' / 0' / 0 / 1 |
| Bitcoin | first | change | first | m / 44' / 0' / 0' / 1 / 0 |
| Bitcoin | first | change | second | m / 44' / 0' / 0' / 1 / 1 |
| Bitcoin | second | external | first | m / 44' / 0' / 1' / 0 / 0 |
| Bitcoin | second | external | second | m / 44' / 0' / 1' / 0 / 1 |
| Bitcoin | second | change | first | m / 44' / 0' / 1' / 1 / 0 |
| Bitcoin | second | change | second | m / 44' / 0' / 1' / 1 / 1 |
| Bitcoin Testnet | first | external | first | m / 44' / 1' / 0' / 0 / 0 |
| Bitcoin Testnet | first | external | second | m / 44' / 1' / 0' / 0 / 1 |
| Bitcoin Testnet | first | change | first | m / 44' / 1' / 0' / 1 / 0 |
| Bitcoin Testnet | first | change | second | m / 44' / 1' / 0' / 1 / 1 |
| Bitcoin Testnet | second | external | first | m / 44' / 1' / 1' / 0 / 0 |
| Bitcoin Testnet | second | external | second | m / 44' / 1' / 1' / 0 / 1 |
| Bitcoin Testnet | second | change | first | m / 44' / 1' / 1' / 1 / 0 |
| Bitcoin Testnet | second | change | second | m / 44' / 1' / 1' / 1 / 1 |