```
BIP: 80
Title: Hierarchy for Non-Colored Voting Pool Deterministic Multisig Wallets
Author: Justus Ranvier <justus@opentransactions.org>
        Jimmy Song <jimmy@monetas.net>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0080
Status: Deferred
Type: Informational
Created: 2014-08-11
License: PD
```

Abstract

This BIP defines a logical hierarchy for non-colored voting pool deterministic multisig 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 and is based on BIP44.

Motivation

The hierarchy proposed in this paper allows the handling of multiple coins and multiple series from a single seed.

Path levels

We define the following 4 levels in BIP32 path:

```
m / purpose' / coin_type' / series' / 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 following the BIP43 recommendation to: the ASCII value of "80" with the most signifigant bit set to indicate hardened derivation (0x80000050). 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. The list of registered coin type constants should be obtained from BIP44.

Hardened derivation is used at this level.

Series

Series are used by voting pools in order to implement FIFO cold storage. By directing deposits into multiple series, the private keys for most of the deposits can be kept offline, and a limited portion can be brought online to process withdrawals.

Hardened derivation is used at this level.

Index

Public/private keypairs are numbered from index 0 in sequentially increasing manner. This number is used as child index in BIP32 derivation.

Public keys obtained at this level of the hierarchy are used to construct multisig deposit scripts, using a schema that is shared between the members as an out-of-band contract.

Public derivation is used at this level.

Compatible wallets

- btcwallet is the reference Bitcoin wallet for voting pools.

Copyright

Reference

- BIP32 - Hierarchical Deterministic Wallets
- BIP43 - Purpose Field for Deterministic Wallets
- BIP44 - Multi-Account Hierarchy for Deterministic Wallets