```
BIP: 81
Title: Hierarchy for 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-0081
Status: Deferred
Type: Informational
Created: 2014-08-11
License: PD
```

Abstract

This BIP defines a logical hierarchy for colored coin 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 color definitions from a single seed.

Path levels

We define the following 8 levels in BIP32 path:

```
m / purpose' / series' / (5 color definition levels) / 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 "81" with the most signifigant bit set to indicate hardened derivation (0x80000051). It indicates that the subtree of this node is used according to this specification.

Hardened derivation is used at this level.

Color Definition

Index values which can be applied to a BIP32 node are limited to 4 bytes (32 bits).

Since this is not sufficient to identify color definitions without a risk of collision, multiple levels are used.

Color definitions are first shortened to 20 bytes using the Bitcoin hash160 function.

The resulting 20 bytes are split into five groups in little endian format, and where each group is used as the seed for the five levels of color definition levels

Public derivation is used at these levels, even when the index exceeds 2ˆ31.

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
- BIP80 - Hierarchy for Non-Colored Voting Pool Deterministic Multisig Wallets