```
BIP: 43
Layer: Applications
Title: Purpose Field for Deterministic Wallets
Author: Marek Palatinus <slush@satoshilabs.com>
        Pavol Rusnak <stick@satoshilabs.com>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0043
Status: Final
Type: Informational
Created: 2014-04-24
```

Abstract

This BIP introduces a "Purpose Field" for use in deterministic wallets based on algorithm described in BIP-0032 (BIP32 from now on).

Motivation

Although Hierarchical Deterministic Wallet structure as described by BIP32 is an important step in user experience and security of the cryptocoin wallets, the BIP32 specification offers implementors too many degrees of freedom. Multiple implementations may claim they are BIP32 compatible, but in fact they can produce wallets with different logical structures making them non-interoperable. This situation unfortunately renders "BIP32 compatible" statement rather useless.

Purpose

We propose the first level of BIP32 tree structure to be used as "purpose". This purpose determines the further structure beneath this node.

`m / purpose' / *`

Apostrophe indicates that BIP32 hardened derivation is used.

We encourage different schemes to apply for assigning a separate BIP number and use the same number for purpose field, so addresses won't be generated from overlapping BIP32 spaces.

Purpose codes from 10001 to 19999 are reserved for SLIPs.

Example: Scheme described in BIP44 should use 44' (or 0x8000002C) as purpose.

Note that m / 0' / * is already taken by BIP32 (default account), which preceded this BIP.

Not all wallets may want to support the full range of features and possibilities described in these BIPs. Instead of choosing arbitrary subset of defined features and calling themselves BIPxx compatible, we suggest that software which needs only a limited structure should describe such structure in another BIP and use different "purpose" value.

Node serialization

Because this scheme can be used to generate nodes for more cryptocurrencies at once, or even something totally unrelated to cryptocurrencies, there's no point in using a special version magic described in section "Serialization format" of BIP32. We suggest to use always 0x0488B21E for public and 0x0488ADE4 for private nodes (leading to prefixes "xpub" and "xprv" respectively).

Reference

- BIP32 - Hierarchical Deterministic Wallets