```
BIP: 384
Layer: Applications
Title: combo() Output Script Descriptors
Author: Pieter Wuille <pieter@wuille.net>
        Andrew Chow <andrew@achow101.com>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0384
Status: Draft
Type: Informational
Created: 2021-06-27
License: BSD-2-Clause
```

Abstract

This document specifies `combo()` output script descriptors. These take a key and produce P2PK, P2PKH, P2WPKH, and P2SH-P2WPKH output scripts if applicable to the key.

Copyright

Motivation

In order to make the transition from traditional key based wallets to descriptor based wallets easier, it is useful to be able to take a key and produce the scripts which have traditionally been produced by wallet software.

Specification

A new top level script expression is defined: `combo(KEY)`. This expression can only be used as a top level expression. It takes a single key expression as an argument and produces either 2 or 4 output scripts, depending on the key. A `combo()` expression always produces a P2PK and P2PKH script, the same as putting the key in both a `pk()` and a `pkh()` expression. If the key is/has a compressed public key, then P2WPKH and P2SH-P2WPKH scripts are also produced, the same as putting the key in both a `wpkh()` and `sh(wpkh())` expression.

Test Vectors

Valid descriptors followed by the scripts they produce. Descriptors involving derived child keys will have the 0th, and 1st scripts in additional sub-bullets.

- `combo(L4rK1yDtCWekvXuE6oXD9jCYfFNV2cWRpVuPLBcCU2z8TrisoyY1)`
  - `2103a34b99f22c790c4e36b2b3c2c35a36db06226e41c692fc82b8b56ac1c540c5bdac`
  - `76a9149a1c78a507689f6f54b847ad1cef1e614ee23f1e88ac`

  - 00149a1c78a507689f6f54b847ad1cef1e614ee23f1e
  - a91484ab21b1b2fd065d4504ff693d832434b6108d7b87
- combo(04a34b99f22c790c4e36b2b3c2c35a36db06226e41c692fc82b8b56ac1c540c5bd5b8dec5235a0fa8
  - 4104a34b99f22c790c4e36b2b3c2c35a36db06226e41c692fc82b8b56ac1c540c5bd5b8dec5235a0fa8
  - 76a914b5bd079c4d57cc7fc28ecf8213a6b791625b818388ac
- combo([01234567]xpub6ERApfZwUNrhLCkDtcHTcxd75RbzS1ed54G1LkBUHQVHQKqhMkhgbmJbZRkrgZw4kox
  - 2102d2b36900396c9282fa14628566582f206a5dd0bcc8d5e892611806cafb0301f0ac
  - 76a91431a507b815593dfc51ffc7245ae7e5aee304246e88ac
  - 001431a507b815593dfc51ffc7245ae7e5aee304246e
  - a9142aafb926eb247cb18240a7f4c07983ad1f37922687
- combo(xprvA2JDeKCSNNZky6uBCviVfJSKyQ1mDYahRjijr5idH2WwLsEd4Hsb2Tyh8RfQMuPh7f7RtyzTtdrbd
  - Child 0
    - 2102df12b7035bdac8e3bab862a3a83d06ea6b17b6753d52edecba9be46f5d09e076ac
    - 76a914f90e3178ca25f2c808dc76624032d352fdbdfaf288ac
    - 0014f90e3178ca25f2c808dc76624032d352fdbdfaf2
    - a91473e39884cb71ae4e5ac9739e9225026c99763e6687
  - Child 1
    - 21032869a233c9adff9a994e4966e5b821fd5bac066da6c3112488dc52383b4a98ecac
    - 76a914a8409d1b6dfb1ed2a3e8aa5e0ef2ff26b15b75b788ac
    - 0014a8409d1b6dfb1ed2a3e8aa5e0ef2ff26b15b75b7
    - a91473e39884cb71ae4e5ac9739e9225026c99763e6687

Invalid descriptors

- combo() in sh : sh(combo(03a34b99f22c790c4e36b2b3c2c35a36db06226e41c692fc82b8b56ac1c540c5b
- combo() in wsh : wsh(combo(03a34b99f22c790c4e36b2b3c2c35a36db06226e41c692fc82b8b56ac1c540c
- Script in combo(): combo(pkh(03a34b99f22c790c4e36b2b3c2c35a36db06226e41c692fc82b8b56ac1c54

Backwards Compatibility

combo() descriptors use the format and general operation specified in 380. As this is a wholly new descriptor, it is not compatible with any implementation. However the scripts produced are standard scripts so existing software are likely to be familiar with them.

Reference Implementation

combo() descriptors have been implemented in Bitcoin Core since version 0.17.