BitcoinScript Documentation

Release 0.1

fungibit

Sep 07, 2017

Contents:

Bitcoin Script Debugger and Interactive Shell

CHAPTER 1

What is the BitcoinScript library?

BitcoinScript is a python3 library which provides a clean OO class interface for accessing, creating, and manipulating Bitcoin scripts.

BitcoinScript also includes two powerful tools: a debugger and an interactive shell for bitcoin scripts.

BitcoinScript is **not** an alternative implementation of a bitcoin-script interpreter. It is built on top of the existing and well-known python-bitcoinlib library, which does all the heavly-lifting and takes care of the gory details.

CHAPTER 2

Main Features

Debugger

See the debugger section of the docs.

Interactive Shell

See the interactive shell section of the docs.

Class Interface

BitcoinScript provides a clean and intuitive interface to script entities.

The main features of OO interface:

- Specialized OutScript and InScript classes for each script type (P2PKH, P2SH, P2MULTISIG, etc.).
- Access script components as attributes.
  - *inscript.signature* (P2PKH), *outscript.pubkeys* (P2MULTISIG,), etc.
- Intuitive constructors.
  - *InScriptP2PKH.from_pubkey_and_signature(pubkey, sig)* –> creates an InScriptP2PKH object
- Recursive access of P2SH redeem scripts (the scripts embedded in the P2SH inscript), which are scripts as well.
  - *inscript_p2sh.redeem_script.type*, *inscript_p2sh.redeem_script.pubkeys*, etc.
- Easy to serialize script objects to raw binary form, and deserialize back to objects.
  - *script.raw.hex() –> '76a91492b8c3a56fac121ddcdffbc85b02fb9ef681038a88ac'*
- Easy to format script objects to human-readable form, and parse back to objects.

- *print(script) –> ‘OP_DUP OP_HASH160 92...8a OP_EQUALVERIFY OP_CHECKSIG’*

CHAPTER 3

Getting Started

Install using *pip*:

```
pip install bitcoinscript
```

Examples

For an easy start, see the code examples.

CHAPTER 4

Disclaimer

BitcoinScript *IS NOT* production-ready. It is new, and hasn't been tested in the wild.

For any task where mistakes can lose you money, please don't rely on BitcoinScript.

Although I put much effort into testing the code, there may still be bugs.

CHAPTER 5

More

Bug reports, suggestions and contributions are appreciated.

Issues are tracked on github.

- genindex
- modindex
- search