Bitcoin Utilities Documentation

Release 0.2.5

Konstantinos Karasavvas

Mar 25, 2019

CONTENTS

1 Keys and Addresses module 3

2 Transactions module 9

3 Script module 13

4 Indices and tables 15

Python Module Index 17

Index 19

Contents:

CHAPTER

ONE

KEYS AND ADDRESSES MODULE

class keys.**Address**(*address=None*, *hash160=None*, *script=None*)

Represents a Bitcoin address

hash160

the hash160 string representation of the address; hash160 represents two consequtive hashes of the public key or the redeam script, first a SHA-256 and then an RIPEMD-160

Type str

from_address(*address*)

instantiates an object from address string encoding

from_hash160(*hash160_str*)

instantiates an object from a hash160 hex string

from_script(*redeem_script*)

instantiates an object from a redeem_script

to_address()

returns the address's string encoding

to_hash160()

returns the address's hash160 hex string representation

Raises

- TypeError – No parameters passed
- ValueError – If an invalid address or hash160 is provided.

classmethod from_address(*address*)

Creates and address object from an address string

classmethod from_hash160(*hash160*)

Creates and address object from a hash160 string

classmethod from_script(*script*)

Creates and address object from a Script object

to_address()

Returns as address string

Pseudocode:

network_prefix = (1 byte version number)
data = network_prefix + hash160_bytes
data_hash = SHA-256(SHA-256(hash160_bytes))

checksum = (first 4 bytes of data_hash)
address_bytes = Base58CheckEncode(data + checksum)

to_hash160()
Returns as hash160 hex string

class keys.**P2pkhAddress**(*address=None*, *hash160=None*)
Encapsulates a P2PKH address.

Check Address class for details

to_script_pub_key()
returns the scriptPubKey (P2PKH) that corresponds to this address

get_type()
returns the type of address

get_type()
Returns the type of address

to_script_pub_key()
Returns the scriptPubKey (P2PKH) that corresponds to this address

class keys.**P2shAddress**(*address=None*, *hash160=None*, *script=None*)
Encapsulates a P2SH address.

Check Address class for details

get_type()
returns the type of address

get_type()
Returns the type of address

class keys.**P2wpkhAddress**(*address=None*, *witness_hash=None*)
Encapsulates a P2WPKH address.

Check Address class for details

to_script_pub_key()
returns the scriptPubKey of a P2WPKH witness script

get_type()
returns the type of address

get_type()
Returns the type of address

to_script_pub_key()
Returns the scriptPubKey of a P2WPKH witness script

class keys.**P2wshAddress**(*address=None*, *witness_hash=None*, *script=None*)
Encapsulates a P2WSH address.

Check Address class for details

from_script(*witness_script*)
instantiates an object from a witness_script

get_type()
returns the type of address

get_type()
Returns the type of address

to_script_pub_key()
Returns the scriptPubKey of a P2WPKH witness script

class keys.**PrivateKey**(*wif=None*, *secret_exponent=None*)
Represents an ECDSA private key.

key
the raw key of 32 bytes

Type bytes

from_wif(*wif*)
creates an object from a WIF of WIFC format (string)

to_wif(*compressed=True*)
returns as WIFC (compressed) or WIF format (string)

to_bytes()
returns the key's raw bytes

sign_message(*message*, *compressed=True*)
signs the message's digest and returns the signature

sign_transaction(*tx*, *compressed=True*)
signs the transaction's digest and returns the signature

get_public_key()
returns the corresponding PublicKey object

classmethod from_wif(*wif*)
Creates key from WIFC or WIF format key

get_public_key()
Returns the corresponding PublicKey

sign_input(*tx*, *txin_index*, *script*, *sighash=1*)
Signs a transaction input with the private key

Bitcoin uses the normal DER format for transactions. Each input is signed separately (thus txin_index is required). The script of the input we wish to spend is required and replaces the transaction's script sig in order to calculate the correct transaction hash (which is what is actually signed!)

Returns a signature for that input

sign_message(*message*, *compressed=True*)
Signs the message with the private key (deterministically)

Bitcoin uses a compact format for message signatures (for tx sigs it uses normal DER format). The format has the normal r and s parameters that ECDSA signatures have but also includes a prefix which encodes extra information. Using the prefix the public key can be reconstructed when verifying the signature.

Prefix values:

27 - 0x1B = first key with even y
28 - 0x1C = first key with odd y
29 - 0x1D = second key with even y
30 - 0x1E = second key with odd y

If key is compressed add 4 (31 - 0x1F, 32 - 0x20, 33 - 0x21, 34 - 0x22 respectively)

Returns a Bitcoin compact signature in Base64

to_bytes()
Returns key's bytes

to_wif(*compressed=True*)
Returns key in WIFC or WIF string

Pseudocode:

network_prefix = (1 byte version number)
data = network_prefix + (32 bytes number) [+ 0x01 if compressed]
data_hash = SHA-256(SHA-256(data))
checksum = (first 4 bytes of data_hash)
wif = Base58CheckEncode(data + checksum)

class keys.**PublicKey**(*hex_str*)
Represents an ECDSA public key.

key
the raw public key of 64 bytes (x, y coordinates of the ECDSA curve)

Type bytes

from_hex(*hex_str*)
creates an object from a hex string in SEC format

from_message_signature(*signature*)
NO-OP!

verify_message(*address*, *signature*, *message*)
Class method that constructs the public key, confirms the address and verifies the signature

to_hex(*compressed=True*)
returns the key as hex string (in SEC format - compressed by default)

to_bytes()
returns the key's raw bytes

to_hash160()
returns the hash160 hex string of the public key

get_address(*compressed=True)*)
returns the corresponding P2pkhAddress object

get_segwit_address()
returns the corresponding P2wpkhAddress object

classmethod from_hex(*hex_str*)
Creates a public key from a hex string (SEC format)

get_address(*compressed=True*)
Returns the corresponding P2PKH Address (default compressed)

get_segwit_address()
Returns the corresponding P2WPKH address

Only compressed is allowed. It is otherwise identical to normal P2PKH address.

to_bytes()
Returns key's bytes

to_hash160(*compressed=True*)
Returns the RIPEMD(SHA256( )) of the public key in hex

to_hex(*compressed=True*)
Returns public key as a hex string (SEC format - compressed by default)

verify(*signature*, *message*)
Verifies a that the message was signed with this public key's corresponding private key.

classmethod verify_message(*address*, *signature*, *message*)
Creates a public key from a message signature and verifies message

Bitcoin uses a compact format for message signatures (for tx sigs it uses normal DER format). The format has the normal r and s parameters that ECDSA signatures have but also includes a prefix which encodes extra information. Using the prefix the public key can be reconstructed from the signature.

Prefix values:

27 - 0x1B = first key with even y
28 - 0x1C = first key with odd y
29 - 0x1D = second key with even y
30 - 0x1E = second key with odd y

If key is compressed add 4 (31 - 0x1F, 32 - 0x20, 33 - 0x21, 34 - 0x22 respectively)

Raises `ValueError` – If signature is invalid

class keys.**SegwitAddress**(*address=None*, *witness_hash=None*, *script=None*)
Represents a Bitcoin segwit address

Note that currently the python bech32 reference implementation is used (by Pieter Wuille).

witness_hash
the hash string representation of either the address; it can be either a public key hash (P2WPKH) or the hash of the script (P2WSH)

Type str

from_address(*address*)
instantiates an object from address string encoding

from_hash(*hash_str*)
instantiates an object from a hash hex string

from_script(*witness_script*)
instantiates an object from a witness_script

to_address()
returns the address's string encoding (Bech32)

to_hash()
returns the address's hash hex string representation

Raises

- `TypeError` – No parameters passed
- `ValueError` – If an invalid address or hash is provided.

classmethod from_address(*address*)
Creates and address object from an address string

classmethod from_hash(*witness_hash*)
Creates and address object from a hash string

classmethod from_script(*script*)
Creates and address object from a Script object

to_address()
Returns as address string

Uses a segwit's python reference implementation for now. (TODO)

to_hash()
Returns as hash hex string

CHAPTER

TWO

TRANSACTIONS MODULE

class transactions.**Locktime**(*value*)

Helps setting up appropriate locktime.

value

The value of the block height or the 512 seconds increments

Type int

for_transaction()

Serializes the locktime as required in a transaction

Raises ValueError – if the value is not within range of 2 bytes.

for_transaction()

Creates a timelock as expected from Transaction

class transactions.**Sequence**(*seq_type*, *value=None*, *is_type_block=True*)

Helps setting up appropriate sequence. Used to provide the sequence to transaction inputs and to scripts.

value

The value of the block height or the 512 seconds increments

Type int

seq_type

Specifies the type of sequence (TYPE_RELATIVE_SEQUNCE | TYPE_ABSOLUTE_SEQUENCE | TYPE_REPLACE_BY_FEE

Type int

is_type_block

If type is TYPE_RELATIVE_SEQUENCE then this specifies its type (block height or 512 secs increments)

Type bool

for_input_sequence()

Serializes the relative sequence as required in a transaction

for_script()

Returns the appropriate integer for a script; e.g. for relative timelocks

Raises ValueError – if the value is not within range of 2 bytes.

for_input_sequence()

Creates a relative timelock sequence value as expected from TxInput sequence attribute

for_script()
Creates a relative/absolute timelock sequence value as expected in scripts

class transactions.**Transaction**(*inputs=[]*, *outputs=[]*, *locktime=b'x00x00x00x00'*, *version=b'x02x00x00x00'*)
Represents a Bitcoin transaction

inputs
A list of all the transaction inputs

Type list (*TxInput*)

outputs
A list of all the transaction outputs

Type list (*TxOutput*)

locktime
The transaction's locktime parameter

Type bytes

version
The transaction version

Type bytes

stream()
Converts Transaction to bytes

serialize()
Converts Transaction to hex string

get_txid()
Calculates txid and returns it

copy()
creates a copy of the object (classmethod)

get_transaction_digest(*txin_index*, *script*, *sighash*)
returns the transaction input's digest that is to be signed according to sighash

classmethod copy(*tx*)
Deep copy of Transaction

get_transaction_digest(*txin_index*, *script*, *sighash=1*)
Returns the transaction's digest for signing.

SIGHASH types (see constants.py):
SIGHASH_ALL - signs all inputs and outputs (default)
SIGHASH_NONE - signs all of the inputs
SIGHASH_SINGLE - signs all inputs but only txin_index output
SIGHASH_ANYONECANPAY (only combined with one of the above)
- with ALL - signs all outputs but only txin_index input
- with NONE - signs only the txin_index input
- with SINGLE - signs txin_index input and output

txin_index
The index of the input that we wish to sign

Type int

script
The scriptPubKey of the UTXO that we want to spend
Type list (string)

sighash
The type of the signature hash to be created
Type int

get_txid()
Hashes the serialized tx to get a unique id

serialize()
Converts to hex string

stream()
Converts to bytes

class transactions.**TxInput**(*txid*, *txout_index*, *script_sig=<bitcoinutils.script.Script object>*, *sequence=b'xffxffxffxff'*)
Represents a transaction input.

A transaction input requires a transaction id of a UTXO and the index of that UTXO.

txid
the transaction id as a hex string (little-endian as displayed by tools)

Type str

txout_index
the index of the UTXO that we want to spend

Type int

script_sig
the op code and data of the script as string

Type list (strings)

sequence
the input sequence (for timelocks, RBF, etc.)

Type bytes

stream()
converts TxInput to bytes

copy()
creates a copy of the object (classmethod)

classmethod copy(*txin*)
Deep copy of TxInput

stream()
Converts to bytes

class transactions.**TxOutput**(*amount*, *script_pubkey*)
Represents a transaction output

amount
the value we want to send to this output (in BTC)

Type float

script_pubkey
the script that will lock this amount

Type list (string)

stream()
converts TxInput to bytes

copy()
creates a copy of the object (classmethod)

classmethod copy(*txout*)
Deep copy of TxOutput

stream()
Converts to bytes

CHAPTER

THREE

SCRIPT MODULE

class script.**Script**(*script*)

Represents any script in Bitcoin

A Script contains just a list of OP_CODES and also knows how to serialize into bytes

script

the list with all the script OP_CODES and data

Type list

to_bytes()

returns a serialized byte version of the script

Raises ValueError – If string data is too large or integer is negative

to_bytes()

Converts the script to bytes

If an OP code the appropriate byte is included according to: https://en.bitcoin.it/wiki/Script If not consider it data (signature, public key, public key hash, etc.) and and include with appropriate OP_PUSHDATA OP code plus length

to_hex()

Converts the script to hexadecimal

to_p2sh_script_pub_key()

Converts script to p2sh scriptPubKey (locking script)

Calculates the hash160 (via the address) of the script and uses it to construct a P2SH script.

to_p2wsh_script_pub_key()

Converts script to p2wsh scriptPubKey (locking script)

Calculates the sha256 of the script and uses it to construct a P2WSH script.

CHAPTER

FOUR

INDICES AND TABLES

- genindex
- modindex
- search

PYTHON MODULE INDEX

k

keys, 3

s

script, 13

t

transactions, 9

INDEX

A

Address (class in keys), 3
amount (transactions.TxOutput attribute), 11

C

copy() (transactions.Transaction class method), 10
copy() (transactions.Transaction method), 10
copy() (transactions.TxInput class method), 11
copy() (transactions.TxInput method), 11
copy() (transactions.TxOutput class method), 12
copy() (transactions.TxOutput method), 12

F

for_input_sequence() (transactions.Sequence method), 9
for_script() (transactions.Sequence method), 9
for_transaction() (transactions.Locktime method), 9
from_address() (keys.Address class method), 3
from_address() (keys.Address method), 3
from_address() (keys.SegwitAddress class method), 8
from_address() (keys.SegwitAddress method), 7
from_hash() (keys.SegwitAddress class method), 8
from_hash() (keys.SegwitAddress method), 7
from_hash160() (keys.Address class method), 3
from_hash160() (keys.Address method), 3
from_hex() (keys.PublicKey class method), 6
from_hex() (keys.PublicKey method), 6
from_message_signature() (keys.PublicKey method), 6
from_script() (keys.Address class method), 3
from_script() (keys.Address method), 3
from_script() (keys.P2wshAddress method), 4
from_script() (keys.SegwitAddress class method), 8
from_script() (keys.SegwitAddress method), 7
from_wif() (keys.PrivateKey class method), 5
from_wif() (keys.PrivateKey method), 5

G

get_address() (keys.PublicKey method), 6
get_public_key() (keys.PrivateKey method), 5
get_segwit_address() (keys.PublicKey method), 6
get_transaction_digest() (transactions.Transaction method), 10
get_txid() (transactions.Transaction method), 10, 11
get_type() (keys.P2pkhAddress method), 4
get_type() (keys.P2shAddress method), 4
get_type() (keys.P2wpkhAddress method), 4
get_type() (keys.P2wshAddress method), 4

H

hash160 (keys.Address attribute), 3

I

inputs (transactions.Transaction attribute), 10
is_type_block (transactions.Sequence attribute), 9

K

key (keys.PrivateKey attribute), 5
key (keys.PublicKey attribute), 6
keys (module), 3

L

Locktime (class in transactions), 9
locktime (transactions.Transaction attribute), 10

O

outputs (transactions.Transaction attribute), 10

P

P2pkhAddress (class in keys), 4
P2shAddress (class in keys), 4
P2wpkhAddress (class in keys), 4
P2wshAddress (class in keys), 4
PrivateKey (class in keys), 5
PublicKey (class in keys), 6

S

Script (class in script), 13
script (module), 13
script (script.Script attribute), 13
script (transactions.Transaction attribute), 11
script_pubkey (transactions.TxOutput attribute), 11
script_sig (transactions.TxInput attribute), 11
SegwitAddress (class in keys), 7
seq_type (transactions.Sequence attribute), 9

Sequence (class in transactions), 9
sequence (transactions.TxInput attribute), 11
serialize() (transactions.Transaction method), 10, 11
sighash (transactions.Transaction attribute), 11
sign_input() (keys.PrivateKey method), 5
sign_message() (keys.PrivateKey method), 5
sign_transaction() (keys.PrivateKey method), 5
stream() (transactions.Transaction method), 10, 11
stream() (transactions.TxInput method), 11
stream() (transactions.TxOutput method), 12

T

to_address() (keys.Address method), 3
to_address() (keys.SegwitAddress method), 7, 8
to_bytes() (keys.PrivateKey method), 5, 6
to_bytes() (keys.PublicKey method), 6
to_bytes() (script.Script method), 13
to_hash() (keys.SegwitAddress method), 7, 8
to_hash160() (keys.Address method), 3, 4
to_hash160() (keys.PublicKey method), 6, 7
to_hex() (keys.PublicKey method), 6, 7
to_hex() (script.Script method), 13
to_p2sh_script_pub_key() (script.Script method), 13
to_p2wsh_script_pub_key() (script.Script method), 13
to_script_pub_key() (keys.P2pkhAddress method), 4
to_script_pub_key() (keys.P2wpkhAddress method), 4
to_script_pub_key() (keys.P2wshAddress method), 5
to_wif() (keys.PrivateKey method), 5, 6
Transaction (class in transactions), 10
transactions (module), 9
txid (transactions.TxInput attribute), 11
txin_index (transactions.Transaction attribute), 10
TxInput (class in transactions), 11
txout_index (transactions.TxInput attribute), 11
TxOutput (class in transactions), 11

V

value (transactions.Locktime attribute), 9
value (transactions.Sequence attribute), 9
verify() (keys.PublicKey method), 7
verify_message() (keys.PublicKey class method), 7
verify_message() (keys.PublicKey method), 6
version (transactions.Transaction attribute), 10

W

witness_hash (keys.SegwitAddress attribute), 7