SEGWIT

fikgol

<2018-10-28>

Outline

Defined

”Segregated Witness (abbreviated as SegWit) is an implemented protocol upgrade intended to provide protection from transaction malleability and increase block capacity. ”

Block size

Limited to 1,000,000 bytes (1MB) total size. Change this restriction as follows: Block weight is defined as Base

```
Block weight = size * 3 + Total size
```

The new rule block weight $<=$ 4,000,000

transcation format

- original transaction fromat

  `nVersion|txins|txouts|nLockTime`
- segwit-compatible transaction fromat:

  ```
  nVersion|marker|flag|txins|txouts
  | witness | nLockTime |
  ```
- Witness: witness data of the transaction. Each txin is associated with a witness field.
- transaction will have 2 IDs.
  - txid: remains unchanged.
  - wtxid: the double SHA256 of the new serialization format with witness data.

P2PKH(Pay-to-Witness-Public-Key-Hash)

- ScriptPubKey:

  `OP_DUP OP_HASH160 <Hash_PubKey>`
  `OP_EQUALVERIFY OP_CHECKSIG`
- scriptSig: <signature> <pubkey>

P2WPKH

- ScriptPubKey:

  `OP_DUP OP_HASH160 <Hash_PubKey>`
  `OP_EQUALVERIFY OP_CHECKSIG`
- scriptSig: <null>
- witness: <signature> <pubkey>

P2SH

(2-of-3 multisig)

- ScriptPubKey:

  ```
  OP_HASH160 <Hash160(redeemScript)> OP_EQUAL
  ```

- ScriptSig:

  ```
  + OP_0 <B sig> <A sig> <redeemScript>
  ```

- RedeemSig:

  ```
  <OP_2> <C pubkey> <B pubkey>
  <A pubkey> <OP_3> OP_CHECKMULTISIG
  ```

P2WSH

- ScriptPubKey:

  ```
  OP_HASH160 <Hash160(redeemScript)> OP_EQUAL
  ```

- ScriptSig: <null>
- RedeemSig:

  ```
  <OP_2> <C pubkey>
  <B pubkey> <A pubkey> <OP_3> OP_CHECKMULTISIG
  ```

- Witness:

  ```
  + OP_0 <B sig> <A sig> <redeemScript>
  ```