OP_TXHASH[VERIFY]

a proposal for new tx introspection opcodes

OP_TX[HASH[VERIFY]]

a proposal for new tx introspection opcodes

Who am I?

- Steven Roose
- Bitcoin dev >10 years
- formerly Liquid team @ Blockstream
- rust-bitcoin
- Ark

History

- proposed by Russel O’Connor on bitcoin-dev
- ...
- formalized and implemented by myself
- awaiting feedback...

OP_CHECKTEMPLATEVERIFY

- think of pre-signed transactions
  - but take out the signatures
  - kinda
- “pre-determined transactions”
- super simple code

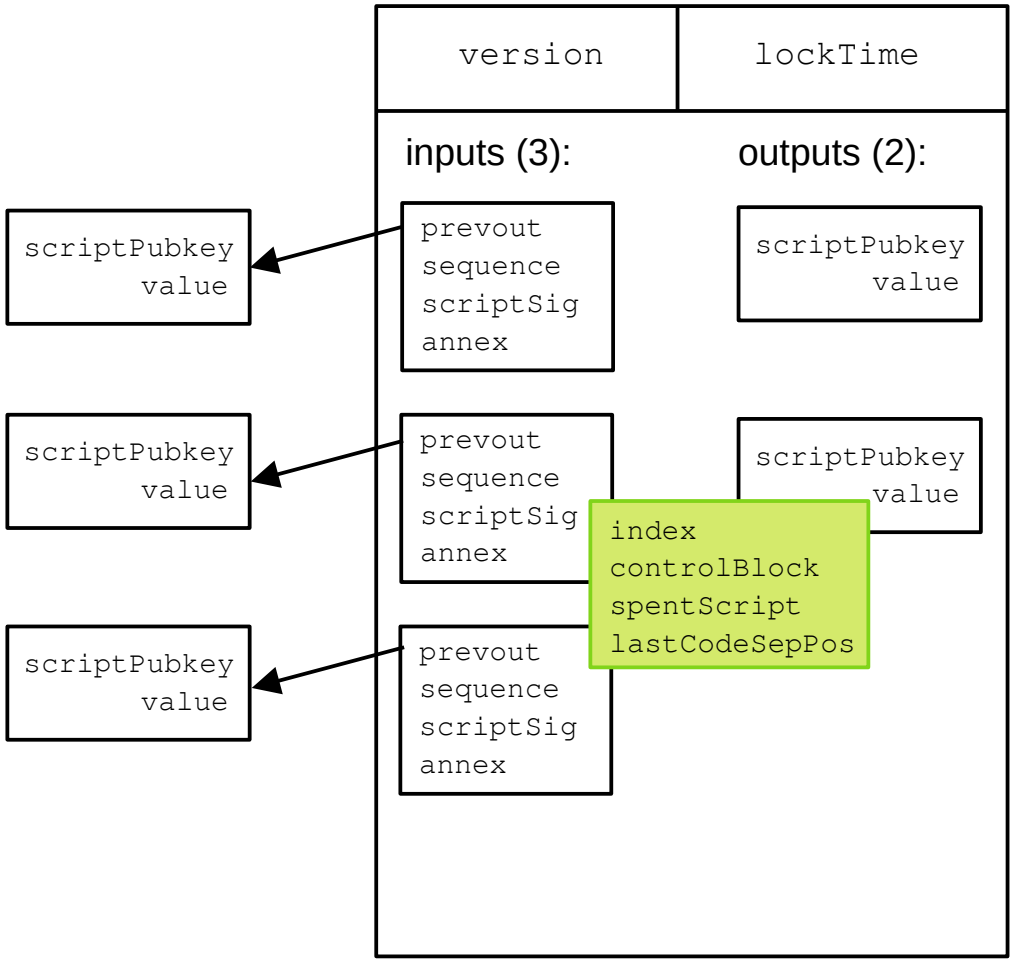
```
template<typename TxType>
uint256 GetDefaultCheckTemplateVerifyHashWithScript(const TxType& tx, const uint256& outputs_hash, const uint256& seq
                                const uint256& scriptSig_hash, const uint32_t input_index) {
    auto h = CHashWriter(SER_GETHASH, 0)
        << tx.nVersion
        << tx.nLockTime
        << scriptSig_hash
        << uint32_t(tx.vin.size())
        << sequences_hash
        << uint32_t(tx.vout.size())
        << outputs_hash
        << input_index;
    return h.GetSHA256();
}
```

TXHASH

- generalization of `OP_CHECKTEMPLATEVERIFY`
- "*TxFieldSelector*" to select parts of transaction
- two new opcodes
  - `OP_TXHASH`: push tx hash on stack (tapscript only)
  - `OP_CHECKTXHASHVERIFY`: compare tx hash with stack (tapscript, segwitv0, legacy)

- <txfs> TXHASH <txhash>
- <txhash|txfs> CHECKTXHASHVERIFY

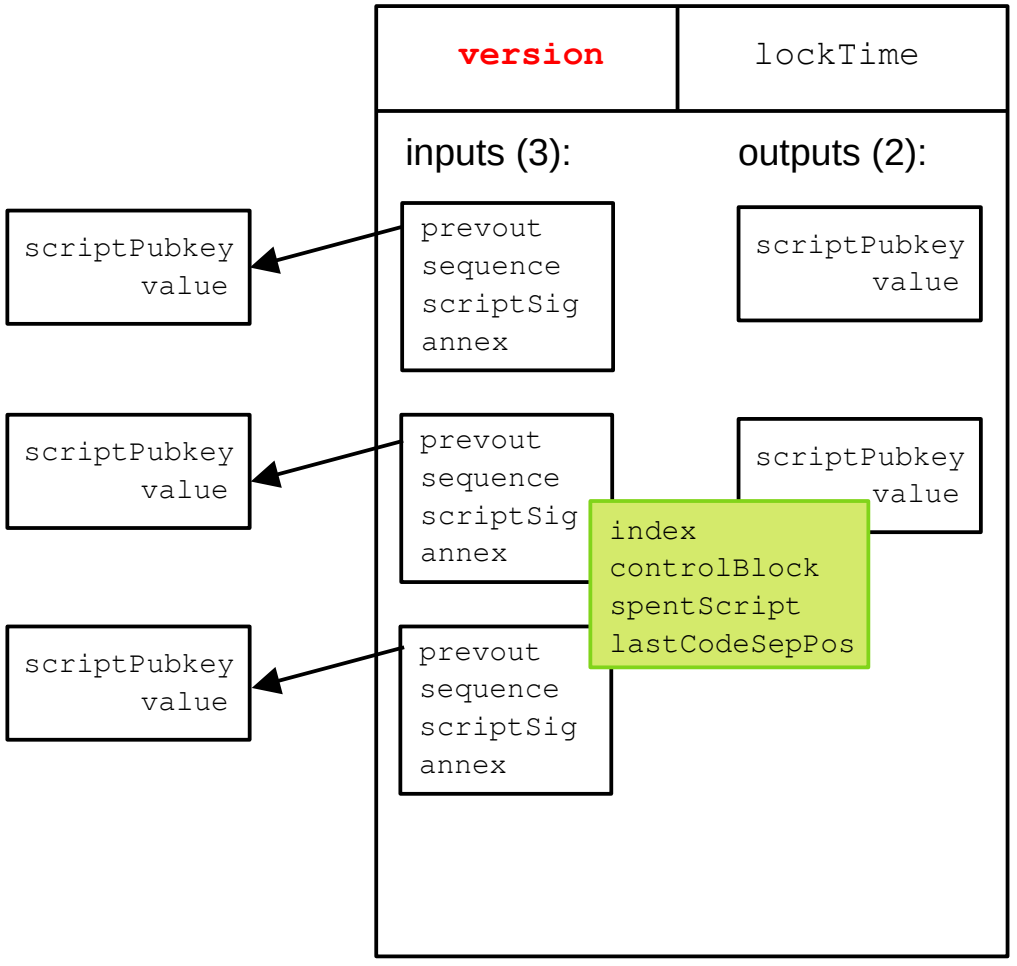
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

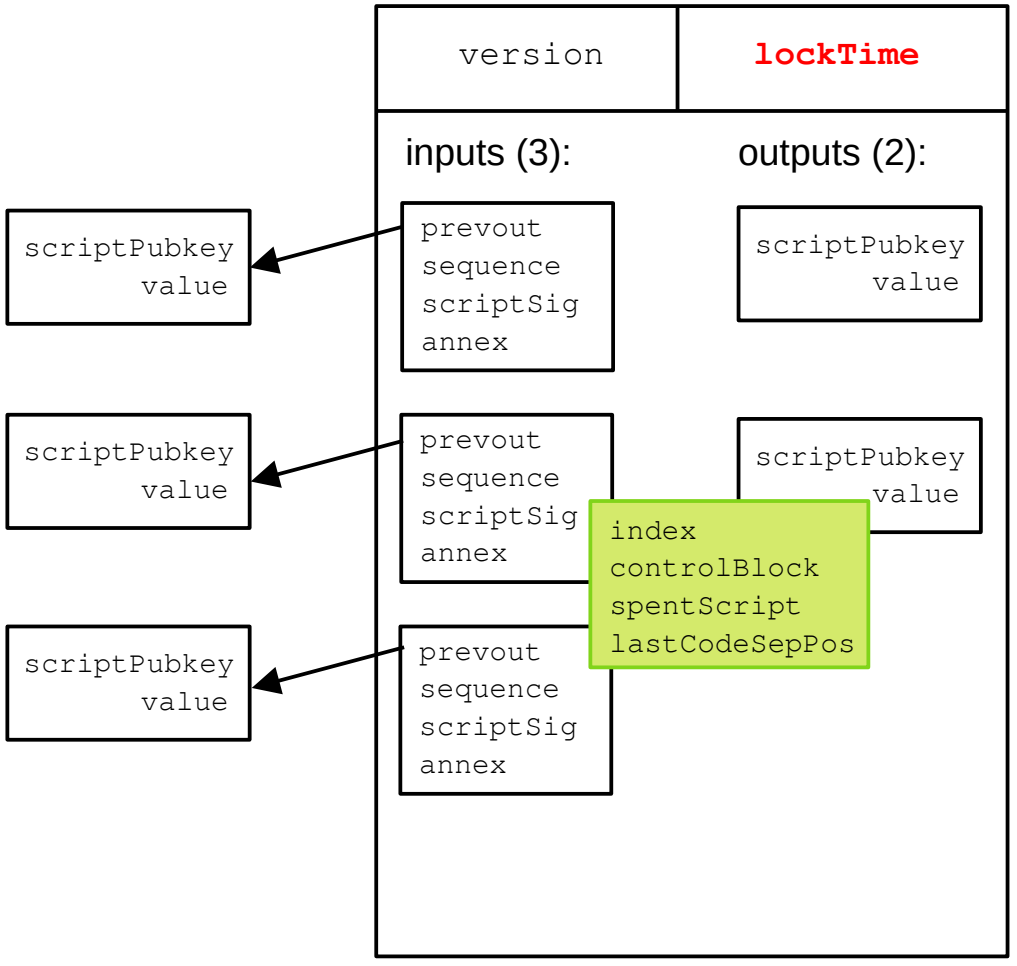
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

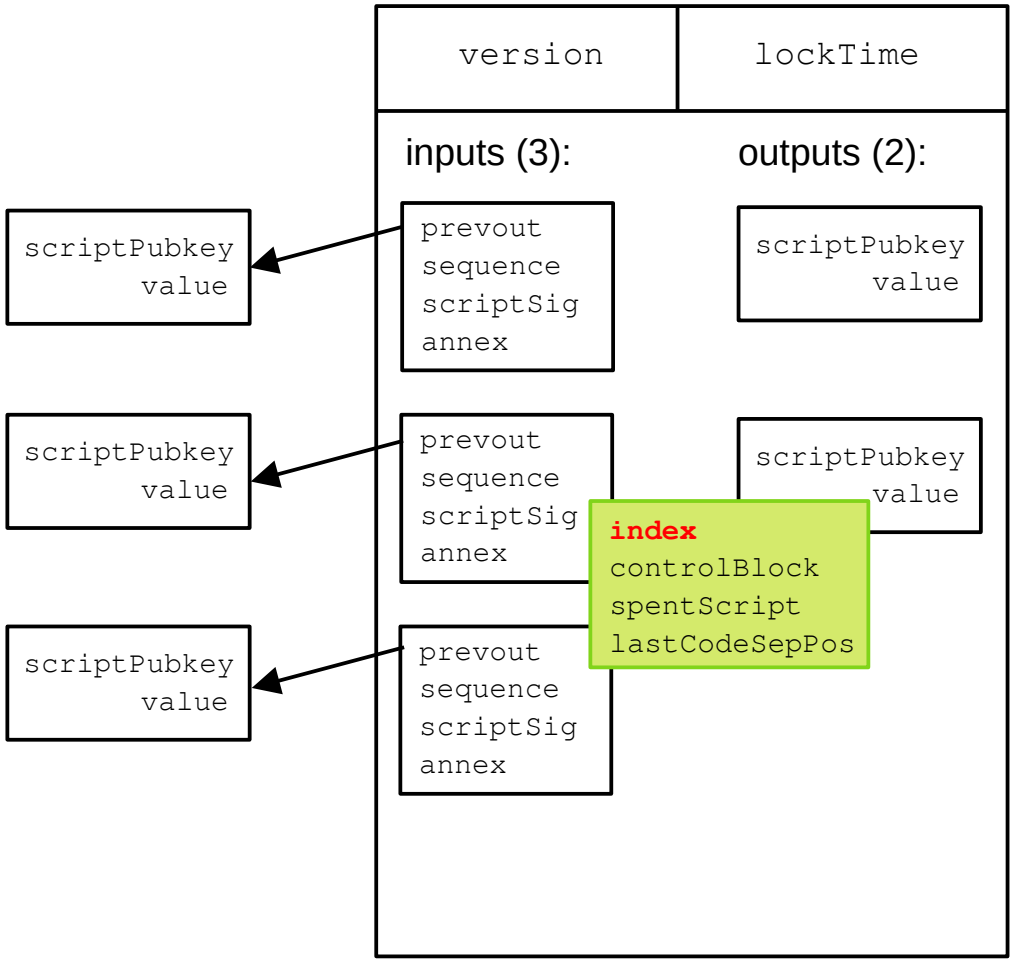
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

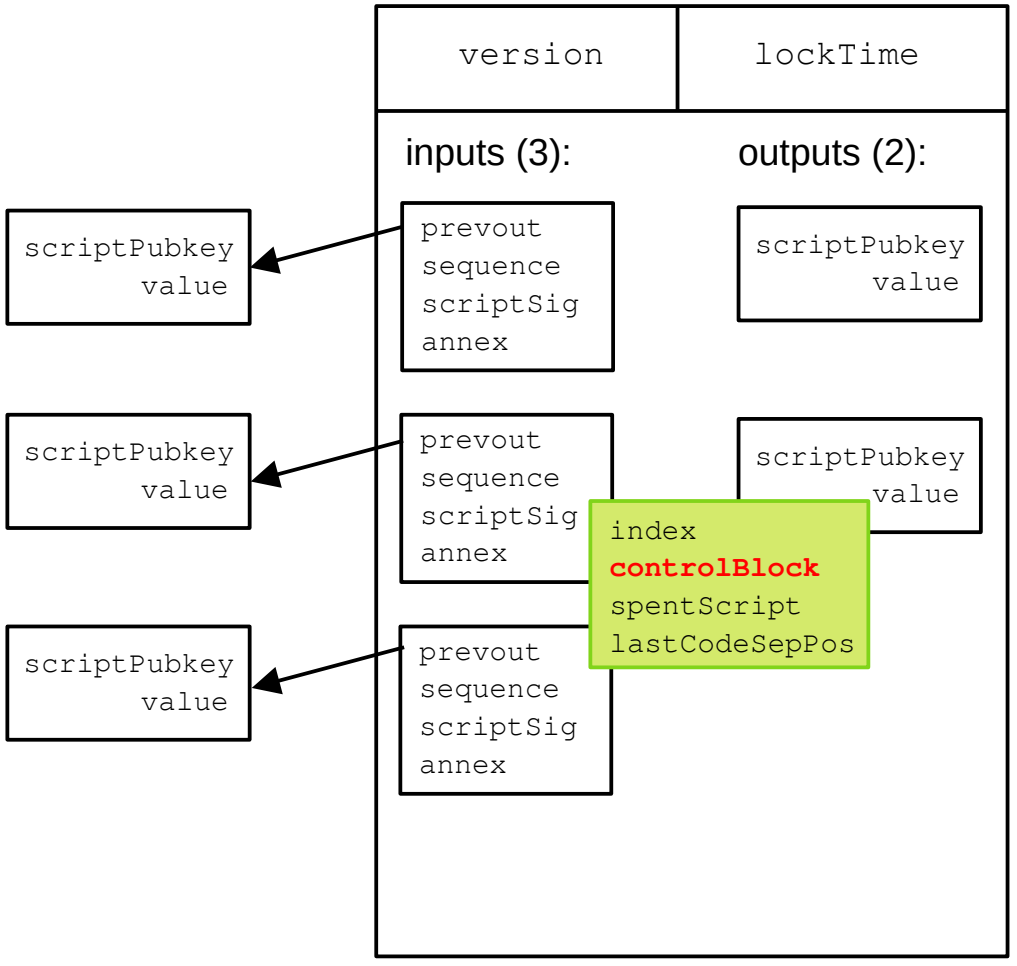
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

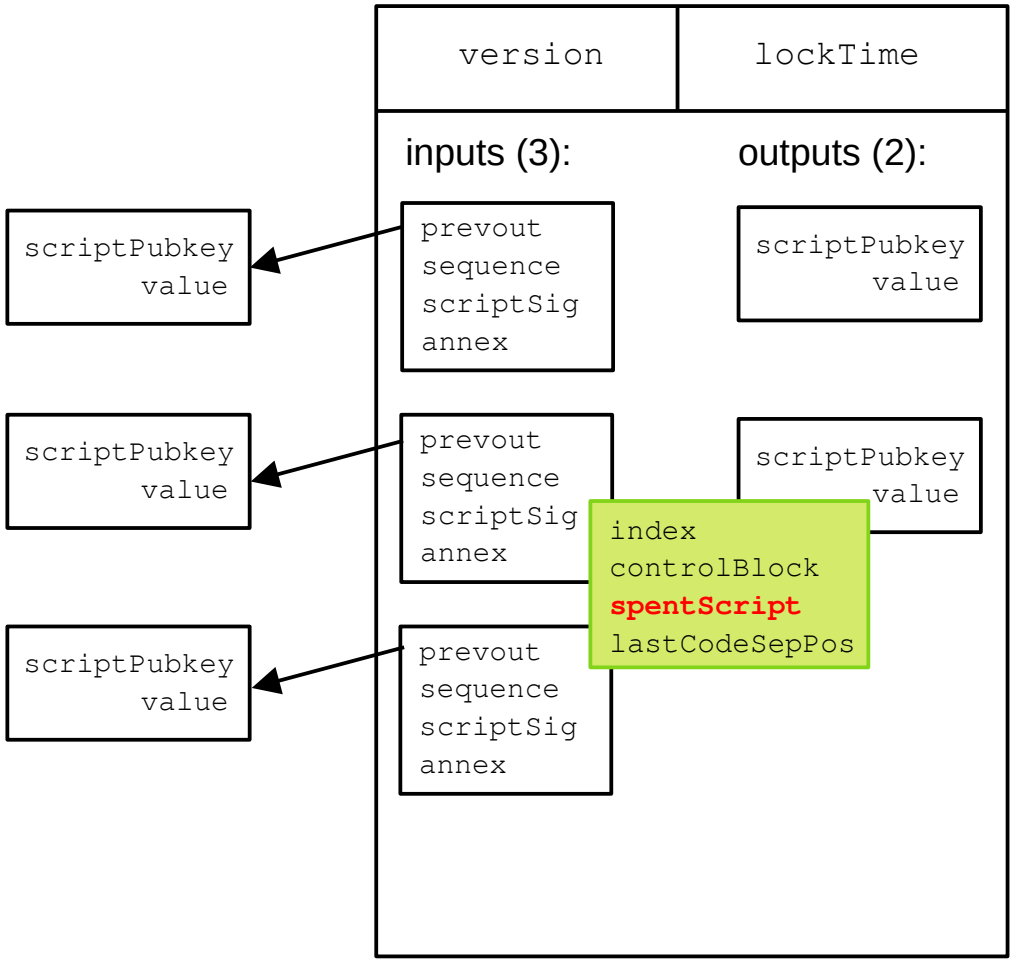
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

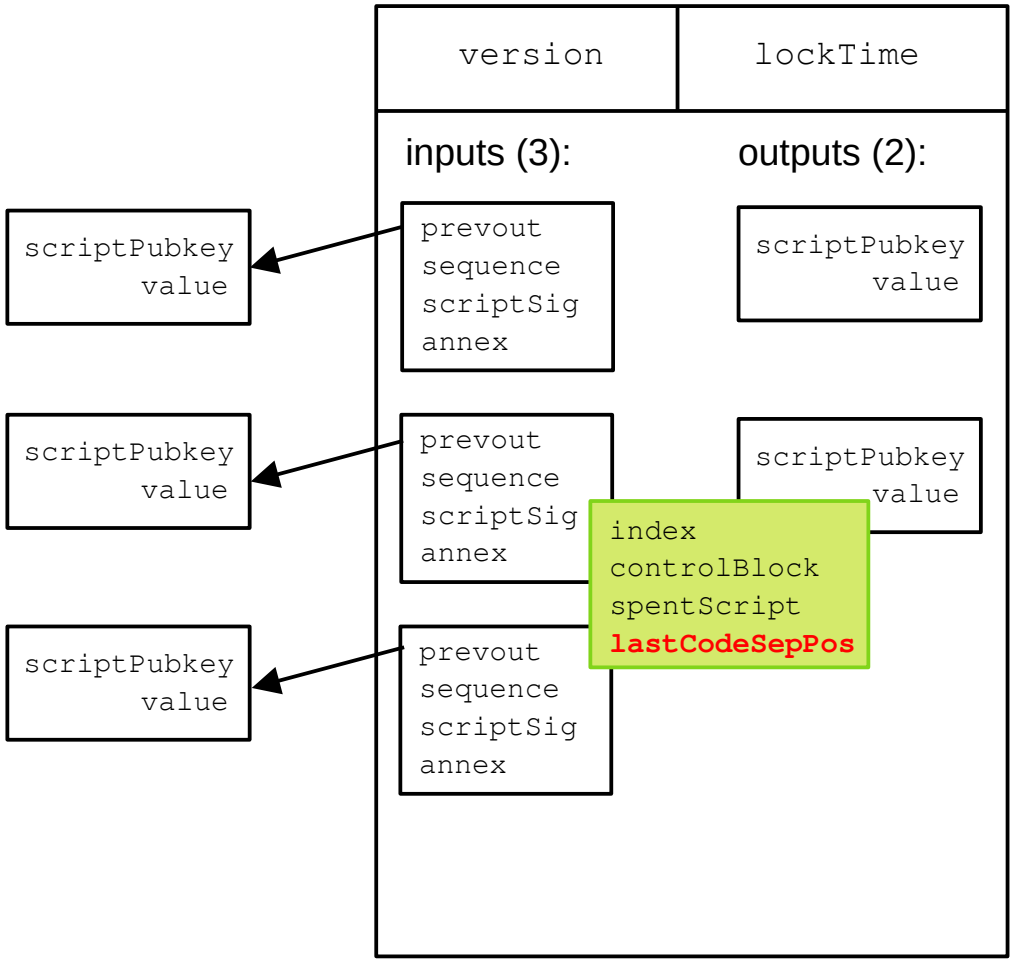
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

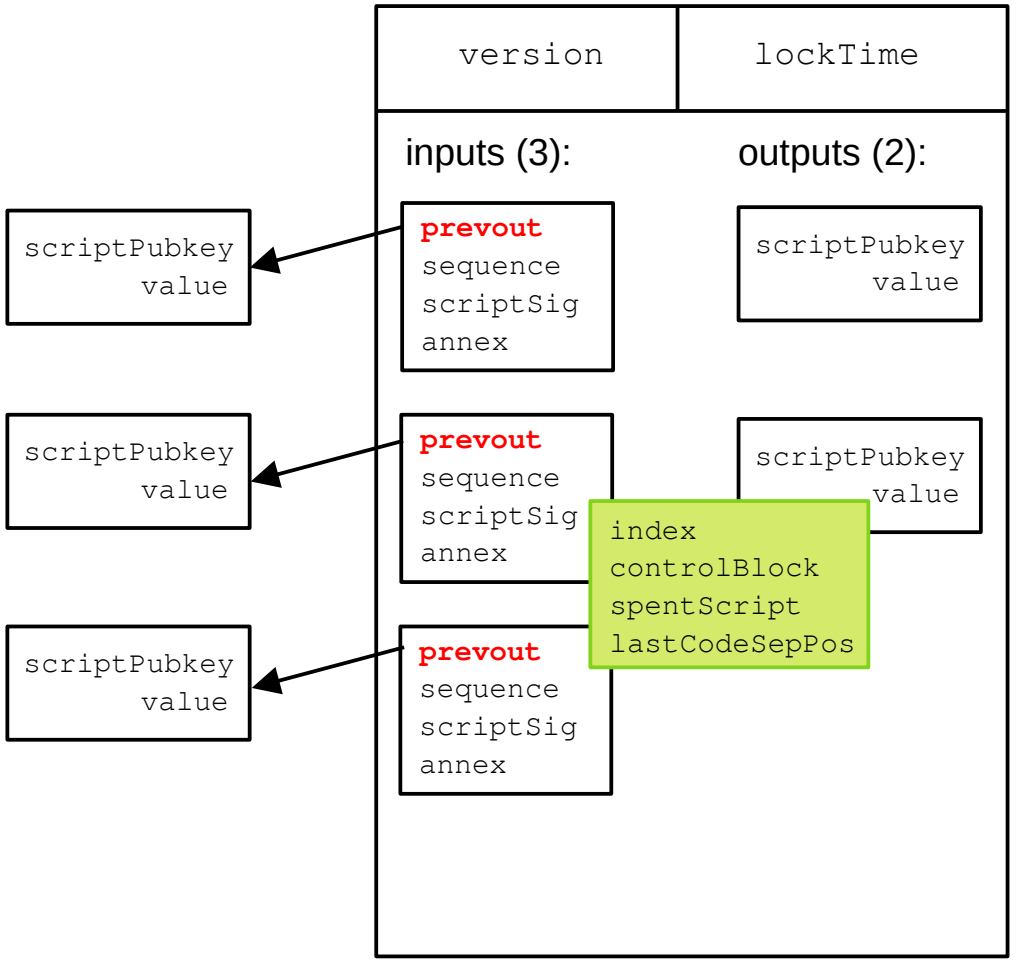
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

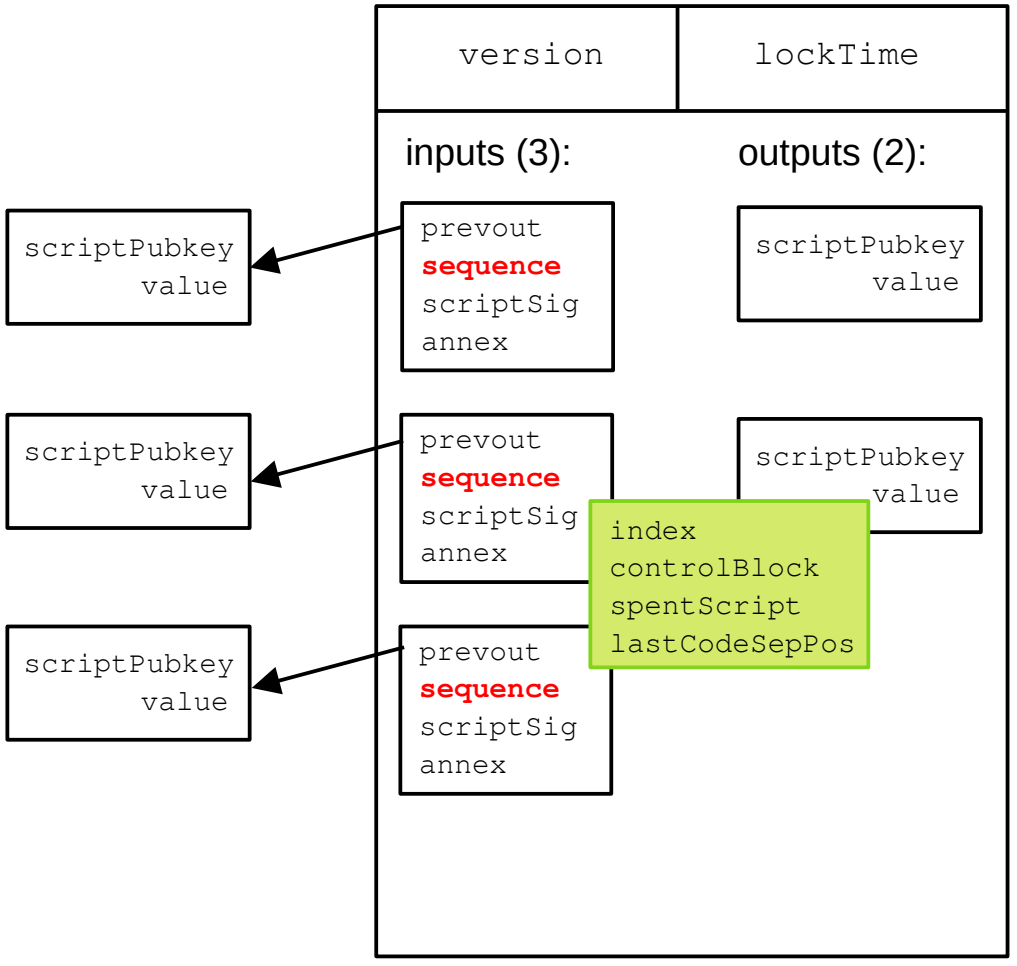
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

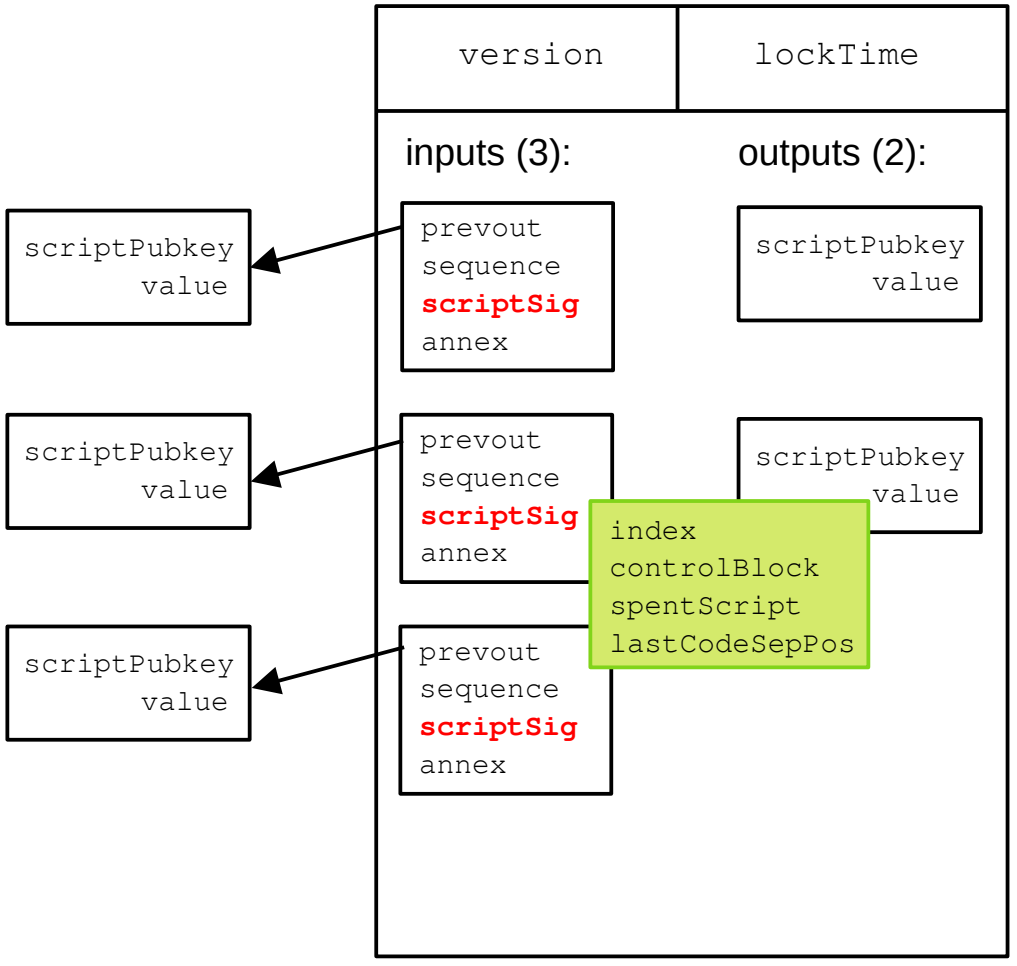
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

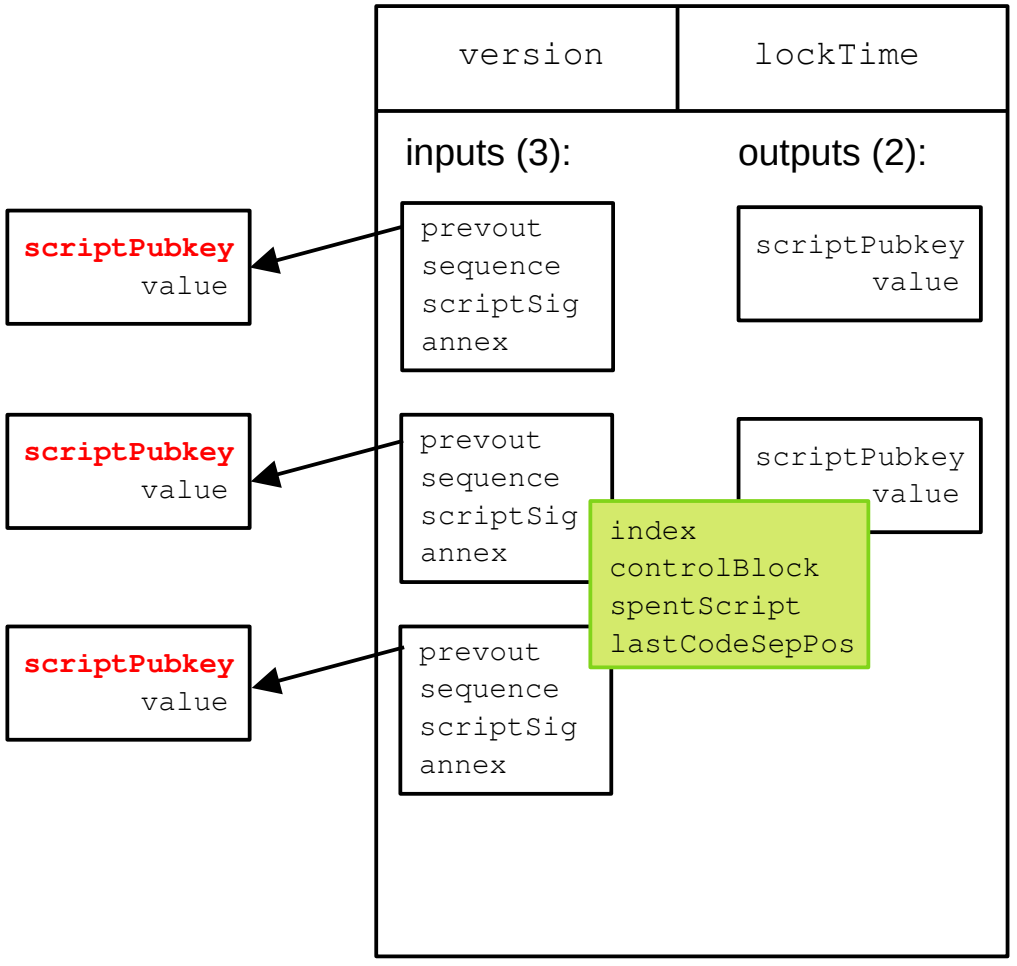
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

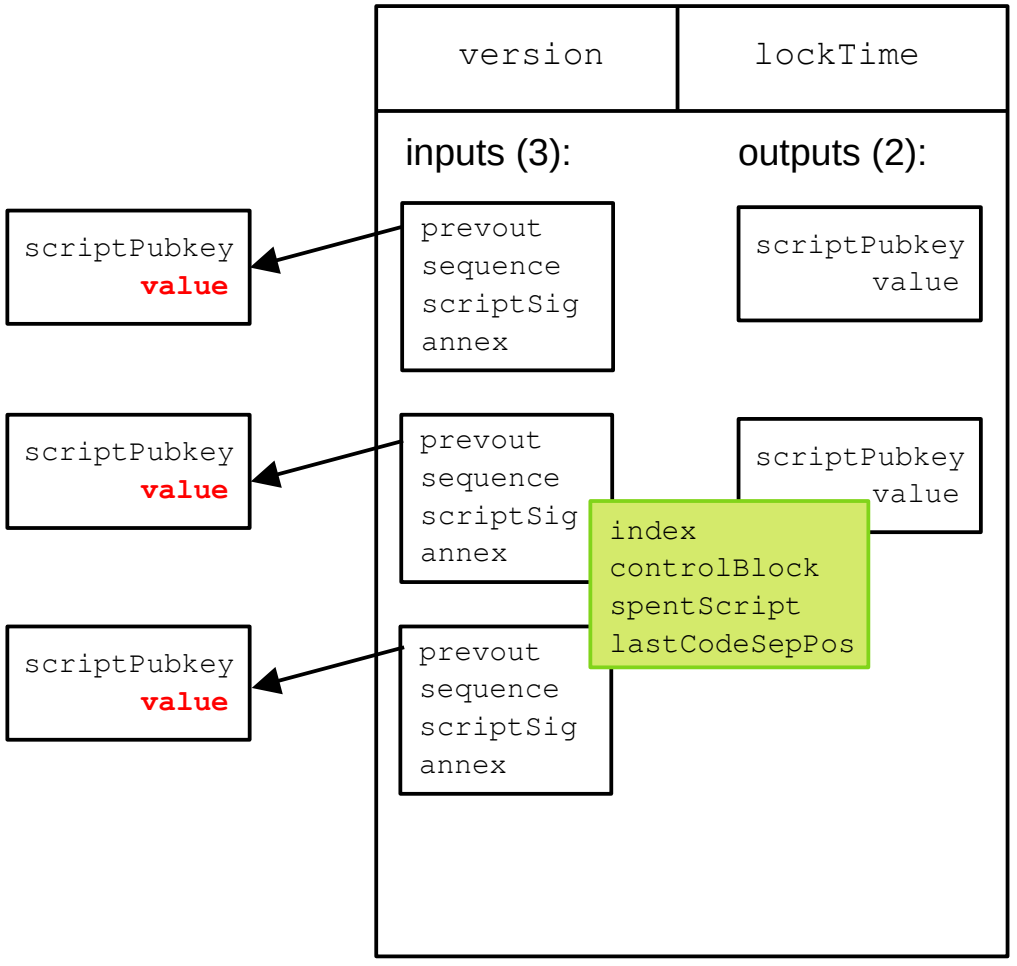
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

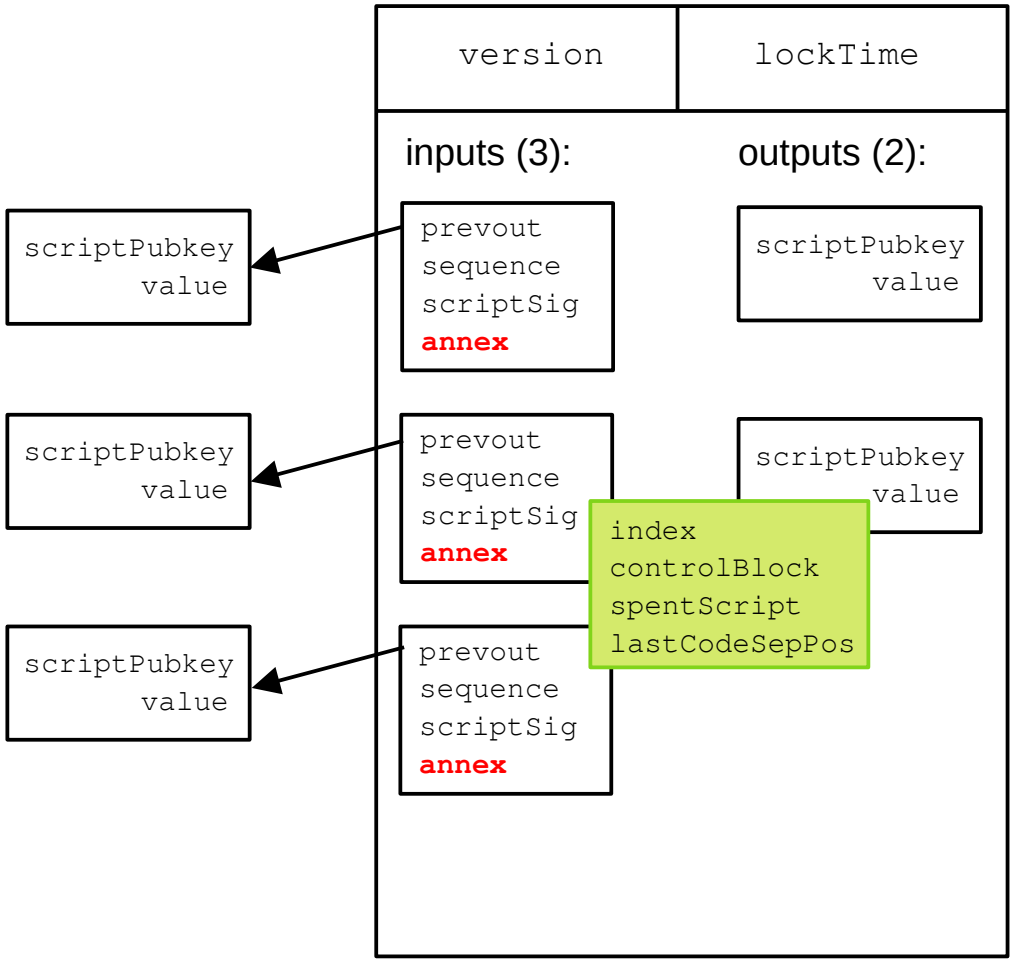
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

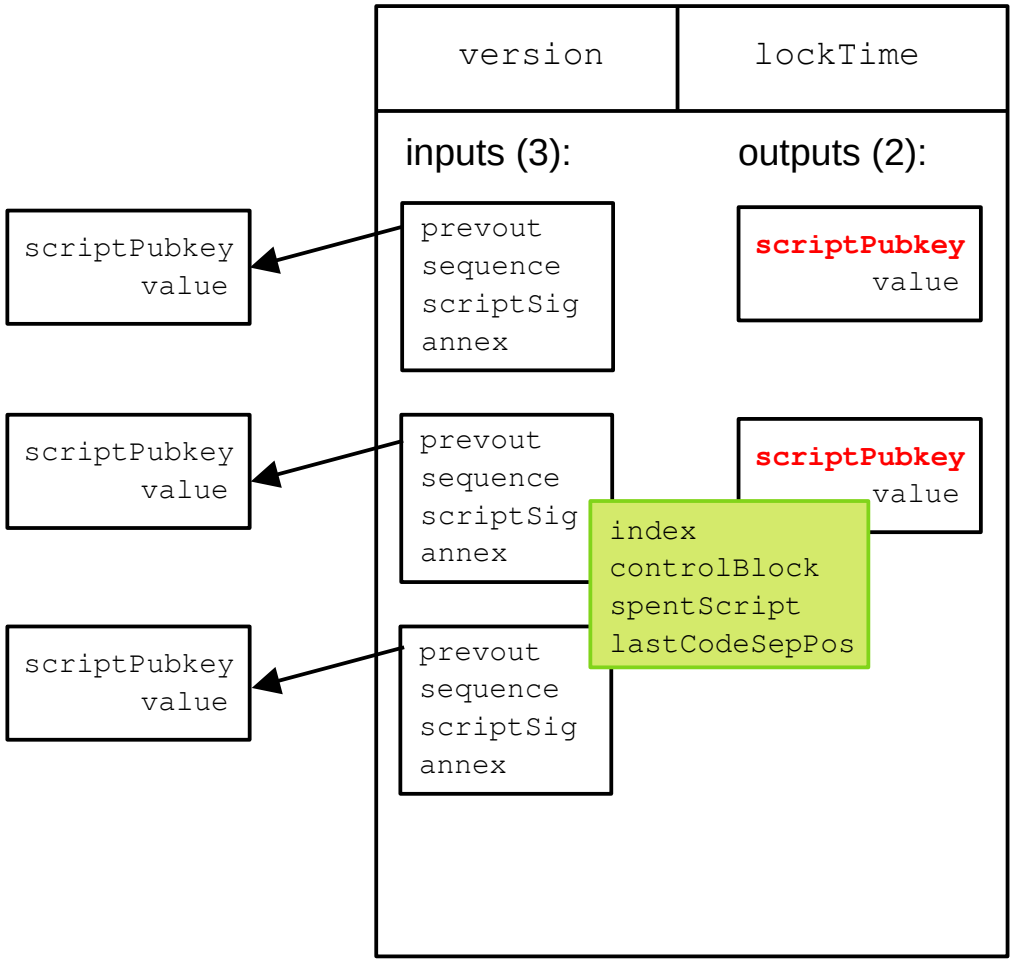
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

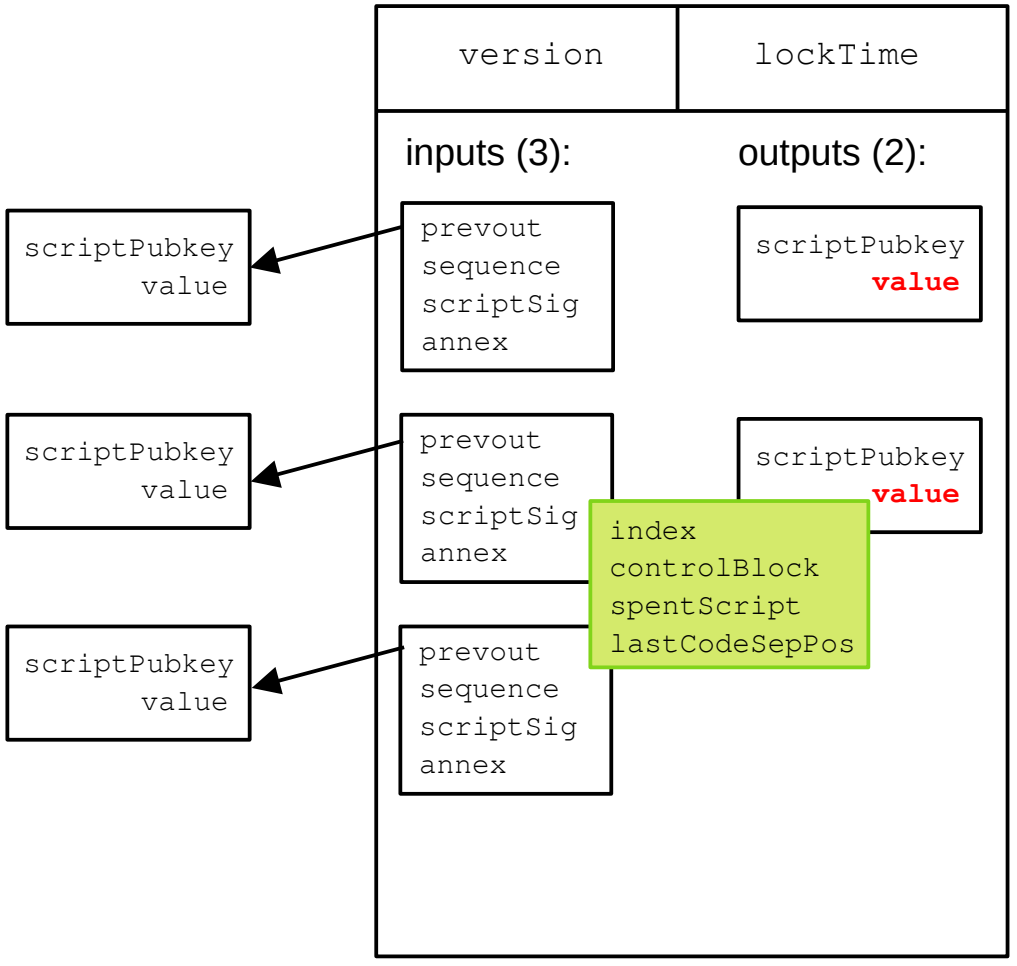
TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

TxFieldSelector




```
global:
1. version
2. locktime
3. current input index
4. current input control block
5. current input spent script
6. current script last OP_CODESEP
7. (unused)
8. CONTROL

inputs:
1. prevouts
2. sequences
3. scriptSigs
4. prevout scriptPubkeys
5. prevout values
6. taproot annexes
outputs:
7. scriptPubkeys
8. values
```

in/output selection

- commit number of in/outputs
- special cases: “none” / “all” / “current”
- *leading*: “first N” (up to 7936)
- *individual*: “pick N” (up to 32)
  - *absolute* indices (up to 16384)
  - *relative* indices to current input (-8191 to +8192)

Compatible with CTV

- default, empty *TxFieldSelector*
  - `TEMPLATE` ~== CTV
- other special case
  - `ALL (0x00)` ~== “`SIGHASH_ALL`”

SIGHASH_EVERYTHING

- TXHASH is basically a sighash
  - <sig> TXHASH <pubkey> CHECKSIGFROMSTACK
  - ALL ~== SIGHASH_ALL
  - TEMPLATE ~== SIGHASH_ANYPREVOUT (APO)
  - SIGHASH_GROUP
- CONTROL bit commits the *TxFieldSelector* itself

Stacking

- the “*individual*” selection supports stacking
- first input commits all outputs
  - other inputs commit previous input
- provide sigs for many relative indices
  - *absolute* indices works
  - *relative* indices probably works better

Caching!!!

- no quadratic hashing!
- cache all variable-sized fields at tx level
  - once-per-tx hashing of them (cfr. sighash)
- clear bounds on per-invocation hashing
- 25 validation budget cost

Status

- specification written: BIP 346
  - reference implementation and ~vectors
  - NEEDS REVIEW
- implementation in Bitcoin Core (& Inquisition)
  - NEEDS REVIEW
- implementation in rust-bitcoin
  - kinda also needs review, but nvm

OP_TX?

- use the same TxFieldSelector
- OP_TX pushes selected fields to the stack
- CONTROL bit means separate <> together
- <txfs> TX <field1|field2|field3>
- <txfs> TX <field1> <field2> <field3>

Native new sighash?

- `<signature|txfs>`