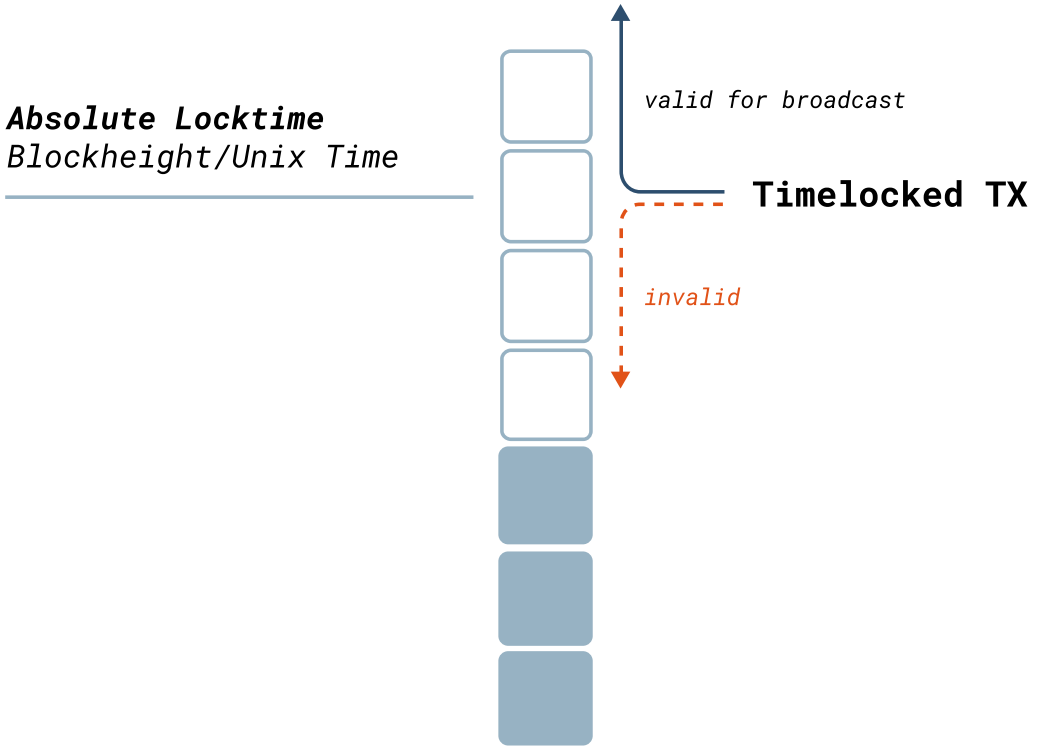
Absolute Transaction Timelocks



Imposed by timelocked TX	*Imposed by previous TX*
TX locktime field	**OP_CHECKLOCKTIMEVERIFY**

An absolute transaction timelock determines from which time on a transaction can be broadcast and mined on the Bitcoin network.

This type of timelock can either be created by the transaction signer(s), or the signers of the previous outputs:

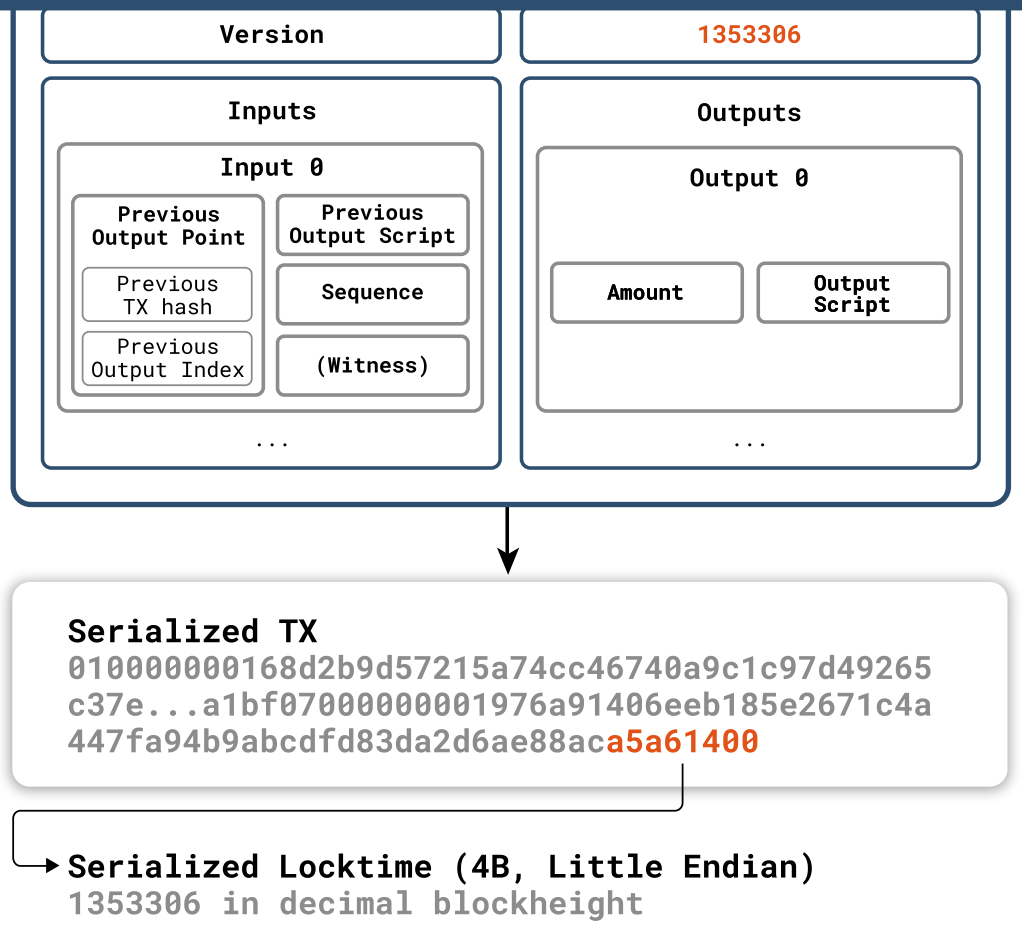
TX Locktime Field

- Describes the absolute time in unix time or blockheight, from when on the transaction is valid.
- Present from the beginning.

OP_CHECKLOCKTIMEVERIFY

- An output script operator, which describes what locktime the spending transaction must have.
- BIP-65 softfork activated in 2015

Transaction **Locktime Field**

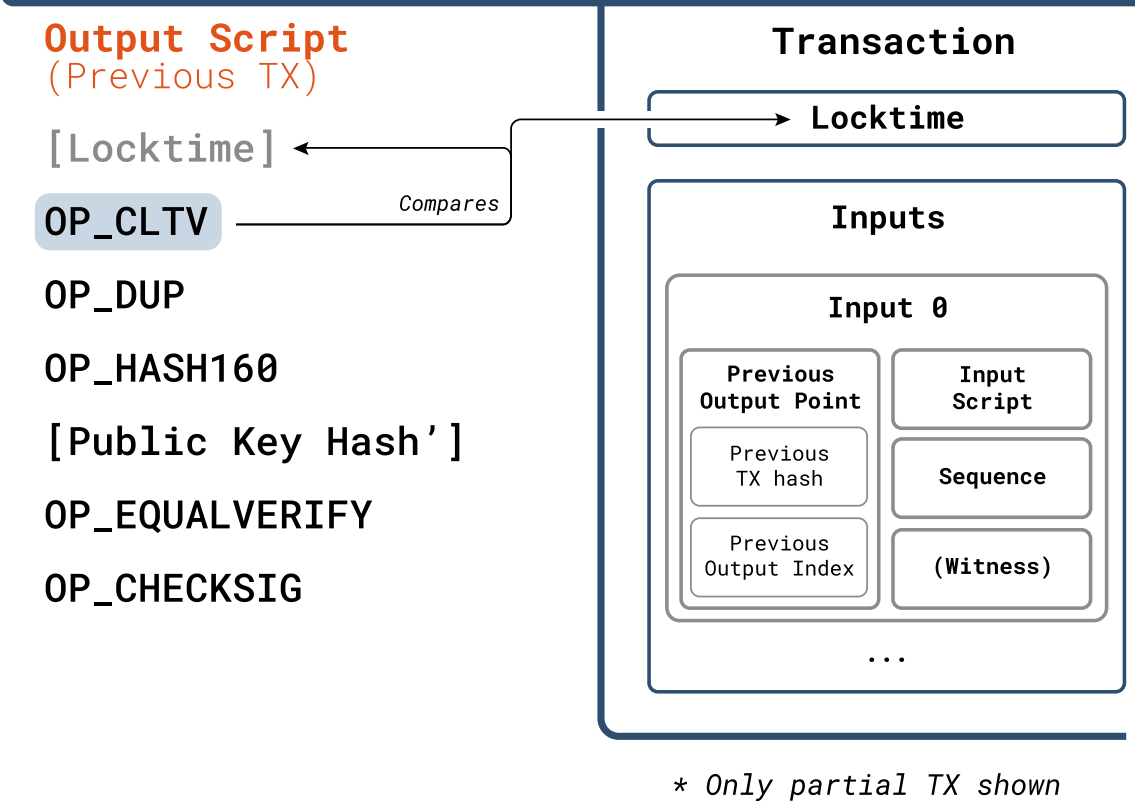


The locktime field is set and signed by the signer(s) of the transaction.

TX Locktime Field

- If locktime is set < 500million:
  - Locktime value is interpreted as blockheight.
- If locktime is set >= 500million:
  - Locktime value is interpreted as unix time.
- Encoded as 4Byte, little endian value

Check Locktime Verify



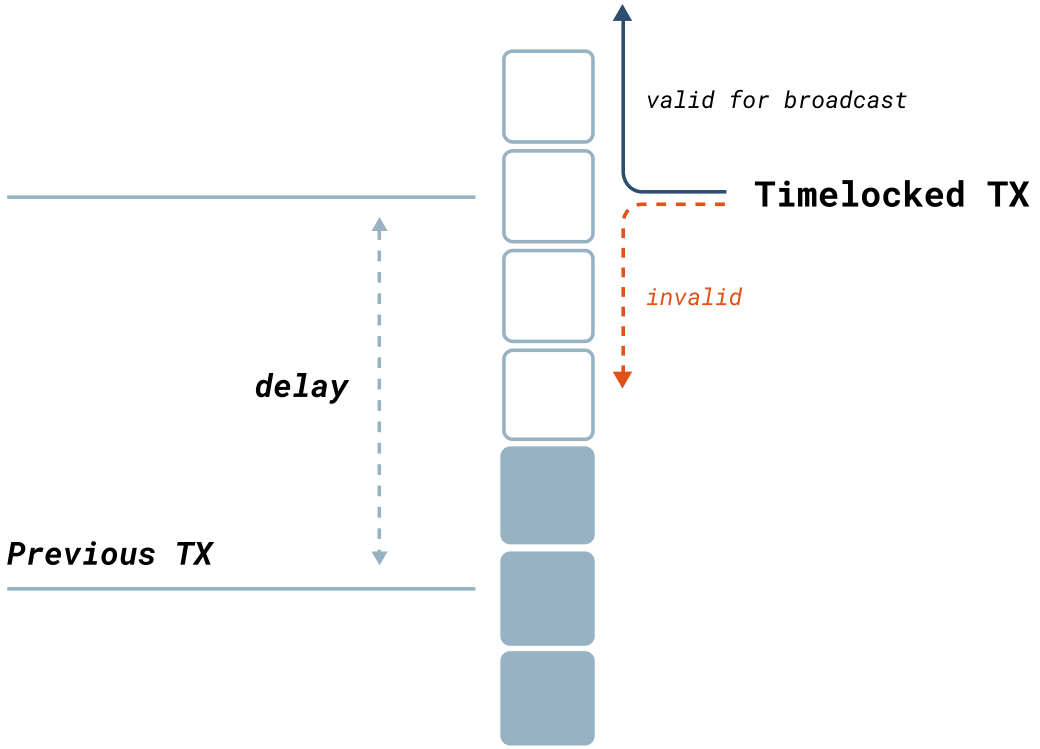
** Only partial TX shown*

Checklocktimeverify is a script operator which prevents a confirmed UXTO from being spent until locktime is expired.

OP_CHECKLOCKTIMEVERIFY

- Validates:
  - Spending TX Locktime >= top stack element
- Success: Continues without modifying stack
- Failure: Script verification fails

Relative Transaction Timelocks



Imposed by timelocked TX	*Imposed by previous TX*
TX sequence field	**OP_CHECKSEQUENCEVERIFY**

A relative transaction timelock determines the delay between confirmation of a UXTO and its spending.

This type of timelock can be created by the transaction input signer(s), or the signers of the previous output(s):

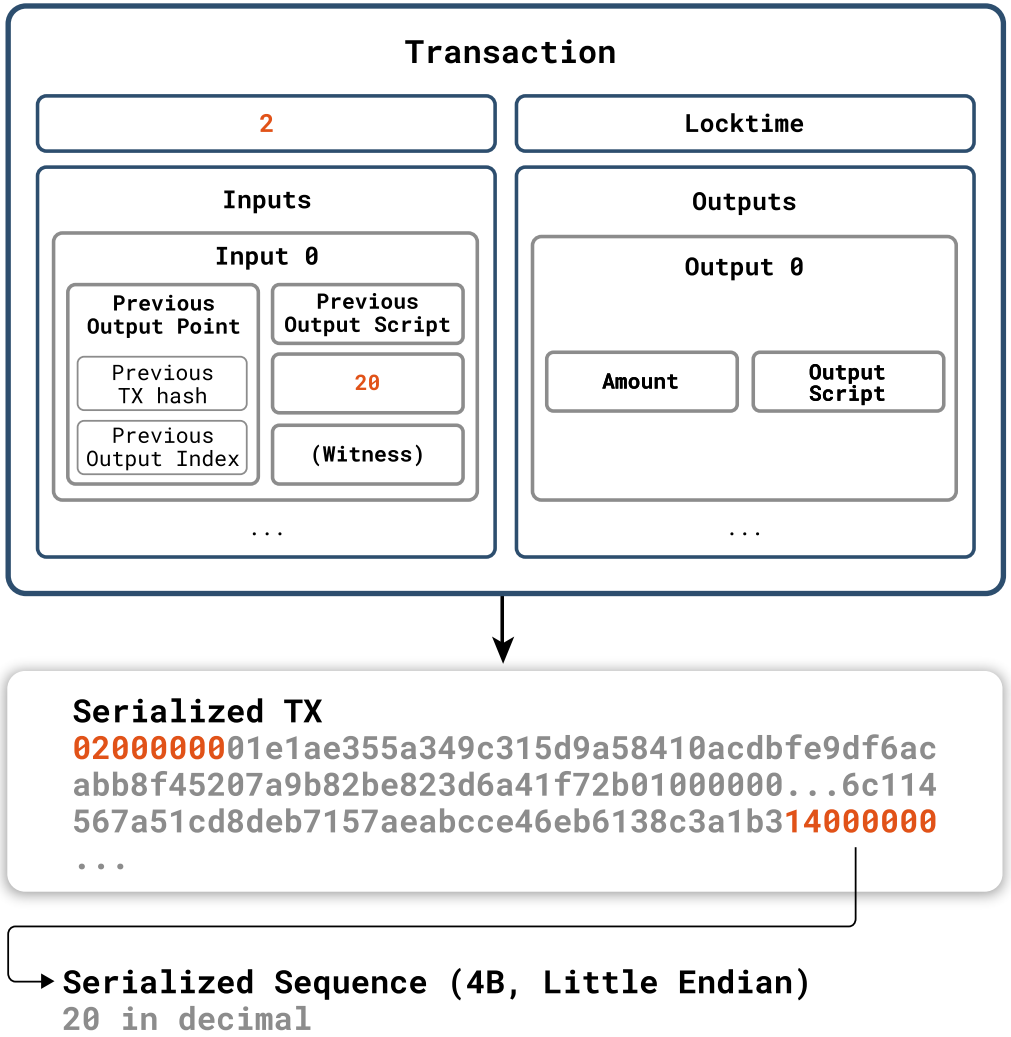
TX Input Sequence Field

- Describes the relative delay time in unix time or blocks, from which on a timelocked transaction is valid.
- BIP-68 softfork activated in 2016

OP_CHECKSEQUENCEVERIFY

- An output script operator, which describes what relative locktime the spending transaction input must have.
- BIP-112 softfork activated in 2016

Transaction Input **Sequence Field**

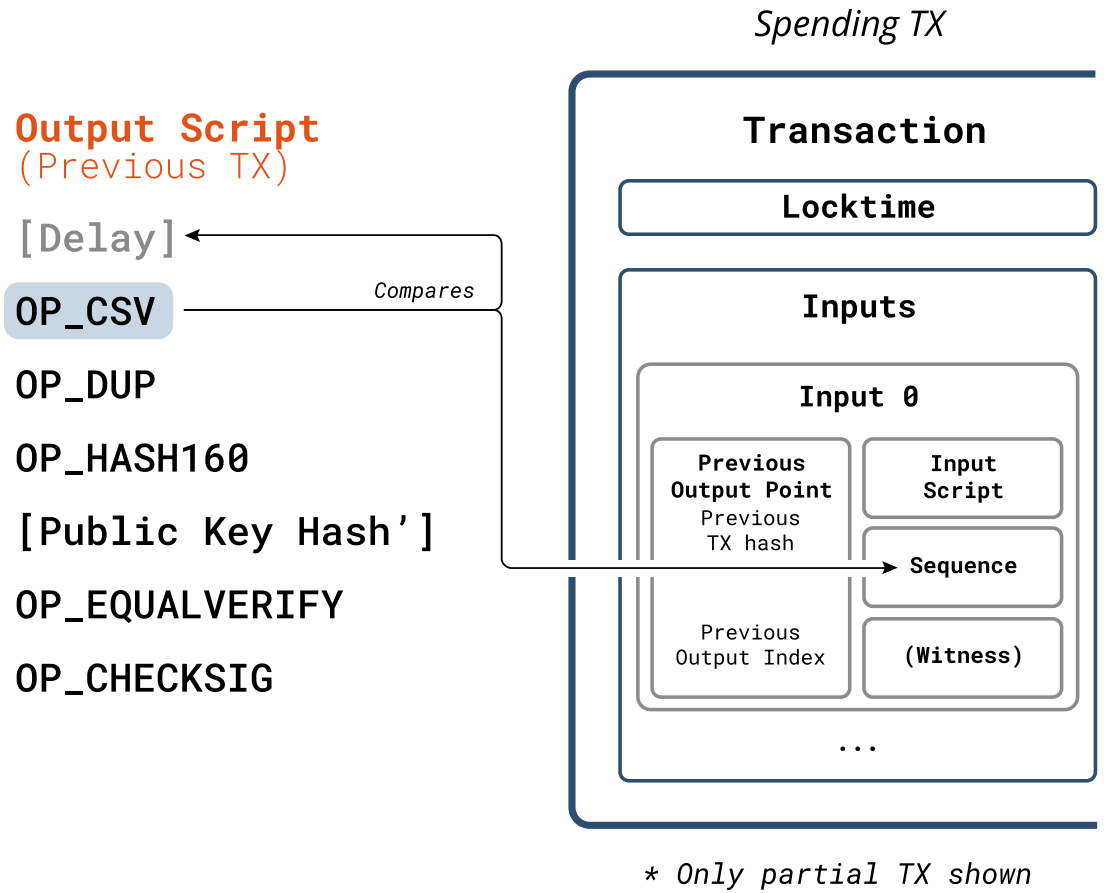


The input sequence field is set and endorsed by the signer(s) of the transaction input.

TX Input Sequence Field

- For sequence field to be interpreted as relative timelock:
  - TX version must be >= 2
- Timelock encoded in 16 least signficant bits of sequence field.
  - For delay in multiples of 512 seconds, typeflag bit (1 << 22) in sequence field must be activated.
  - Otherwise, delay interpreted as blocks (e.g. 0x00000014 = 20 block delay)

Check Sequence Verify



Checksequenceverify is a script operator which prevents a confirmed UXTO from being spent until the delay since its confirmation has passed.

OP_CHECKSEQUENCEVERIFY

- Validates:
  - Spending TX Input Sequence Delay >= top stack element
- Script [Delay] Encoding:
  - 3 Bytes Little Endian (not 4 Bytes)
  - Same typeflag bit (1 << 22) function as in sequence field.
  - Relative timelock encoded in 16 least signficant bits.

Median time past

- Synchronizing time in a distributed system :(
- No way to reach consensus on timetsamp in block header
- BIP 113 activated together with relative timelock BIPs
  - MTP = Median of last 11 block timestamps
  - Used to evaluate timelocks (lags approx. 1 hour)
  - Consensus rule: Timestamp > MTP $\Rightarrow$ MTP increases monotonically

Timelocks resources

- BitMex Research blog post