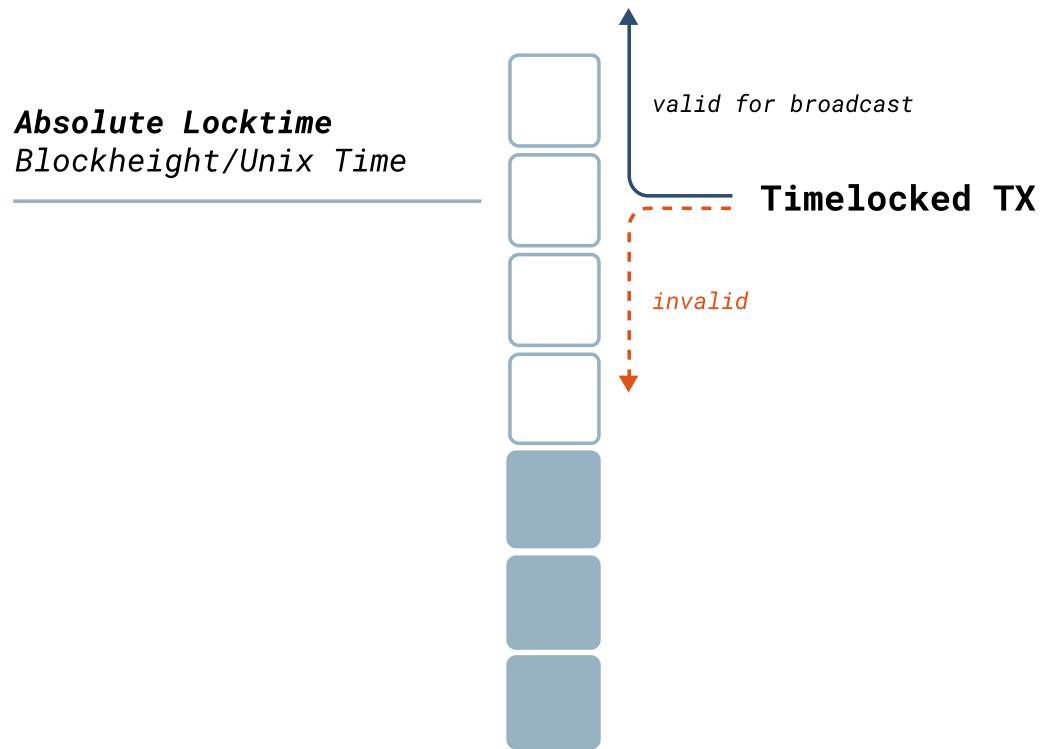


Absolute Transaction Timelocks



*Imposed
by timelocked TX*

TX locktime field

*Imposed
by previous TX*

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:

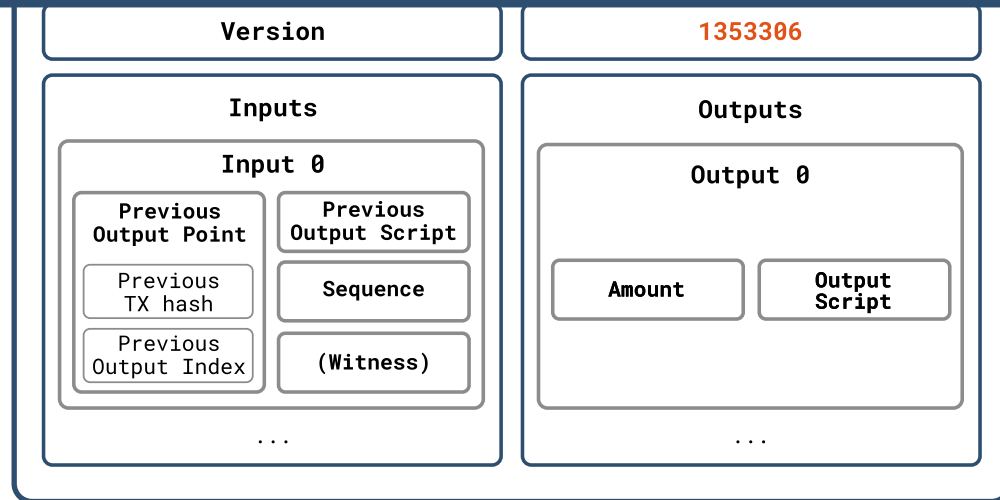
TX Locktime Field

- 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



Serialized TX

01000000168d2b9d57215a74cc46740a9c1c97d49265
c37e...a1bf07000000001976a91406eeb185e2671c4a
447fa94b9abcdfd83da2d6ae88aca5a61400

→ Serialized Locktime (4B, Little Endian)
1353306 in decimal blockheight

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

Output Script
(Previous TX)

[Locktime]

OP_CLTV

Compares

OP_DUP

OP_HASH160

[Public Key Hash']

OP_EQUALVERIFY

OP_CHECKSIG

Transaction

Locktime

Inputs

Input 0

Previous
Output Point

Previous
TX hash

Previous
Output Index

Input
Script

Sequence

(Witness)

...

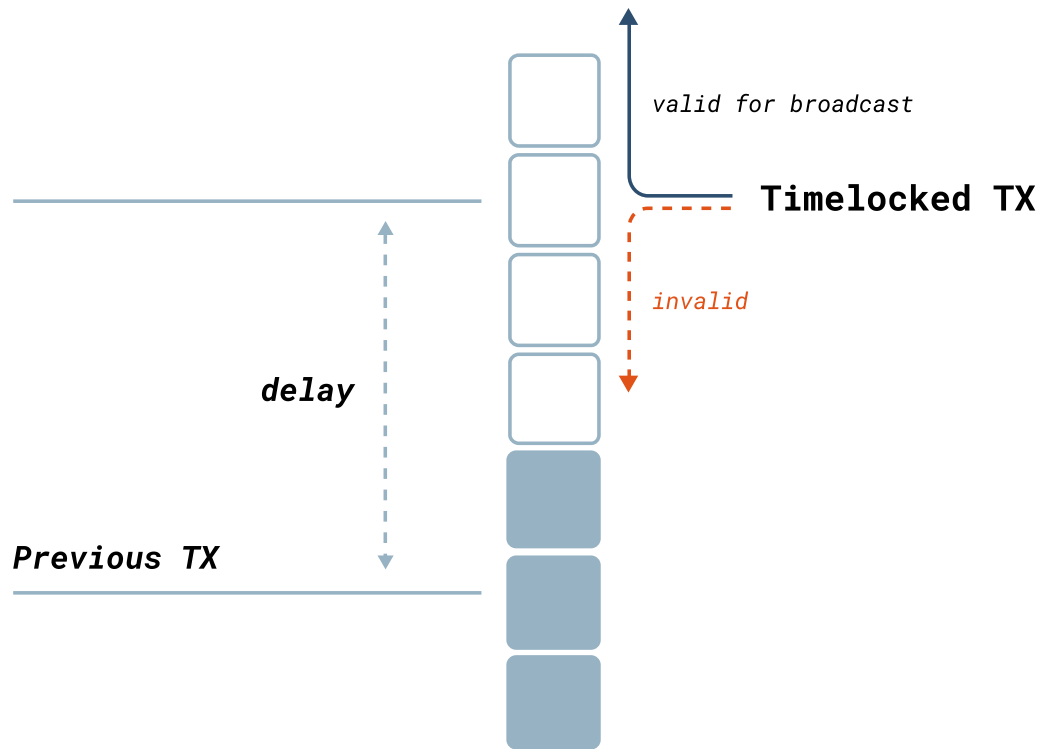
* Only partial TX shown

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

OP_CHECKLOCKTIMEVERIFY

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

Relative Transaction Timelocks



Imposed
by timelocked TX
TX sequence field

Imposed
by previous TX
OP_CHECKSEQUENCEVERIFY

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

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

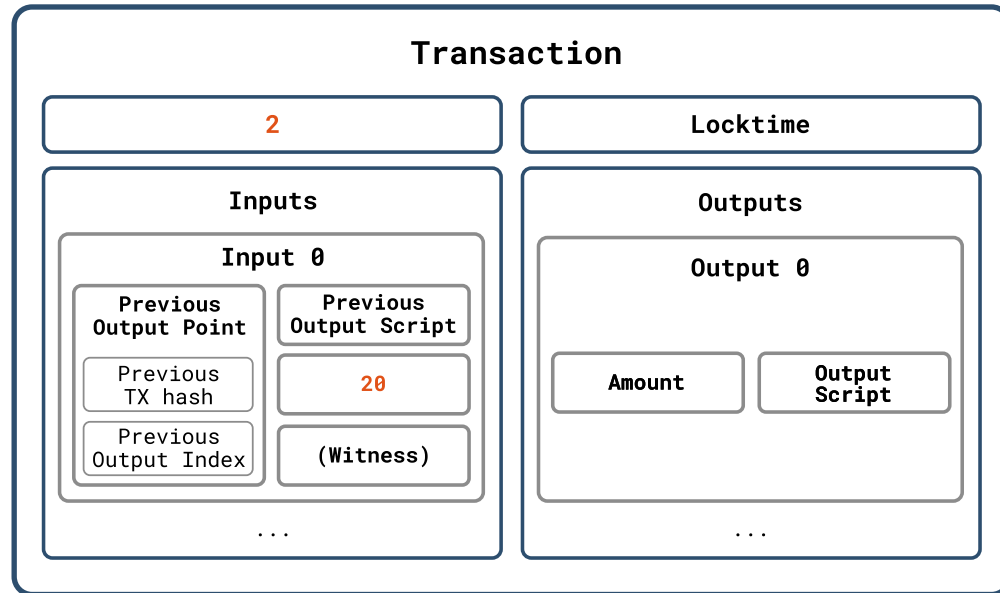
TX Input Sequence Field

- 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



Serialized TX

0200000001e1ae355a349c315d9a58410acdbfe9df6ac
abb8f45207a9b82be823d6a41f72b01000000...6c114
567a51cd8deb7157aeabcce46eb6138c3a1b314000000
...

Serialized Sequence (4B, Little Endian)
20 in decimal

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 significant 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

Output Script
(Previous TX)

[Delay]

OP_CSV

Compares

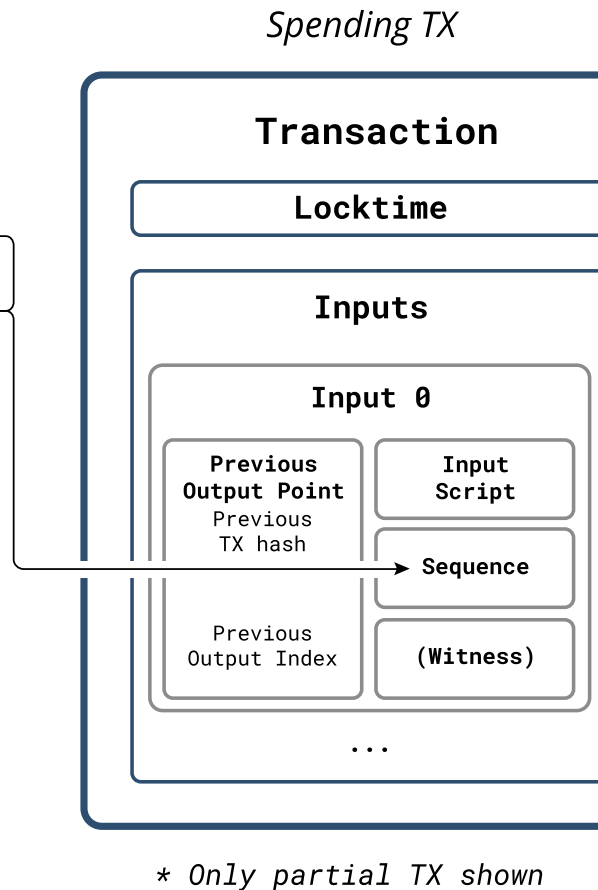
OP_DUP

OP_HASH160

[Public Key Hash']

OP_EQUALVERIFY

OP_CHECKSIG



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

OP_CHECKSEQUENCEVERIFY

- Validates:
 - Spending TX Input Sequence Delay \geq 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 significant bits.

Median time past

- Synchronizing time in a distributed system :(
- No way to reach consensus on timestamp 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: $\text{Timestamp} > \text{MTP} \Rightarrow \text{MTP increases monotonically}$

Timelocks resources

- [BitMex Research blog post](#)