Scripts

Advanced Scripts

Ira A. Fulton Schools of Engineering
Arizona State University

Objectives

Objective

Explain advanced script components

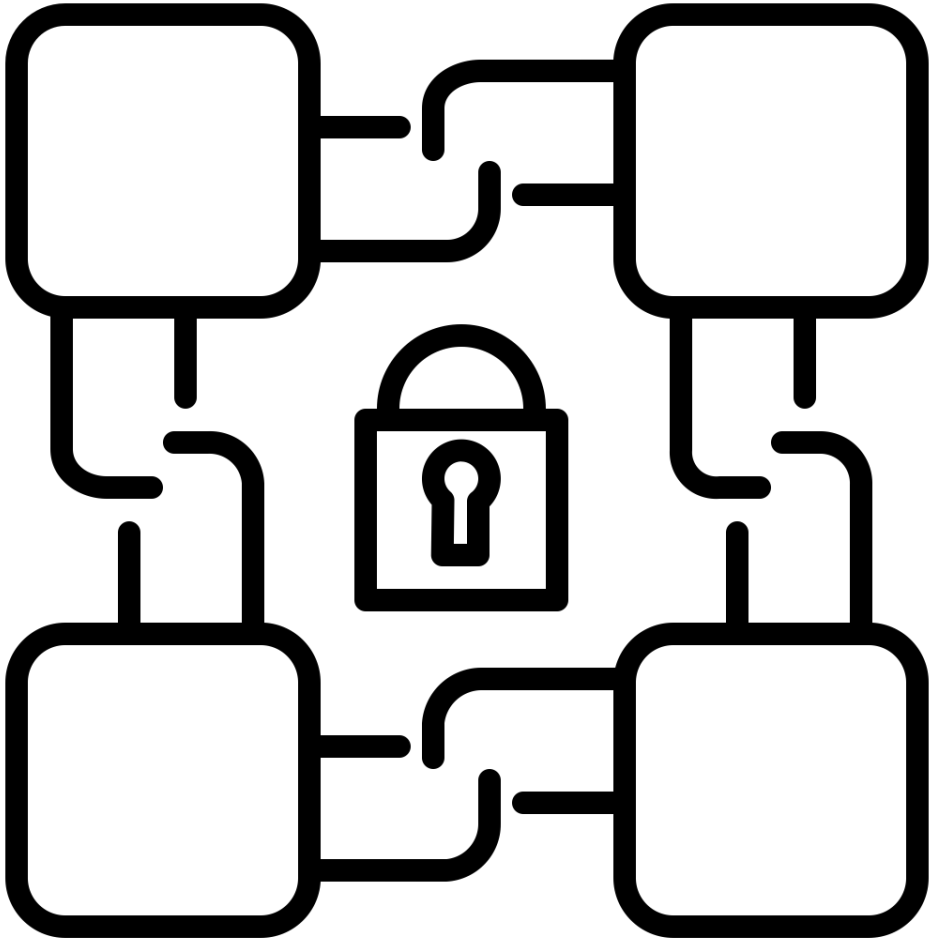
Objective

Interpret advanced scripts

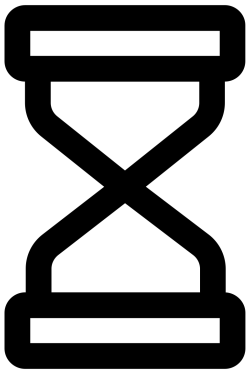
Objective

Create advanced scripts

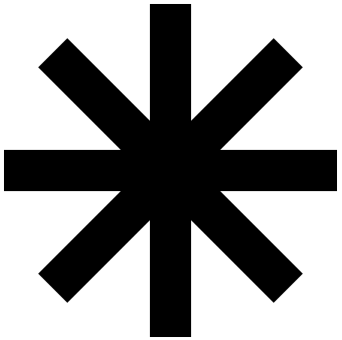
Introduction



Advanced Capabilities

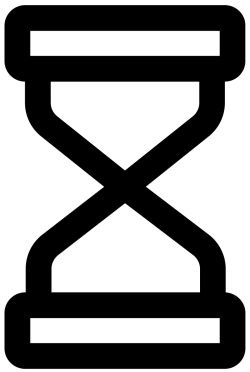


Time component



Conditional clauses

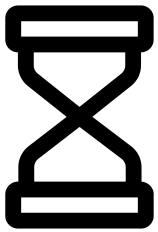
Advanced Capabilities



Time component

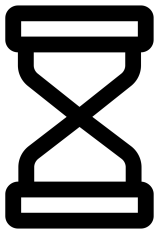
Time Locks

- nLockTime
- nSequence
- OP_CODES
  - CHECKLOCKTIMEVERIFY
  - CHECKSEQUENCEVERIFY



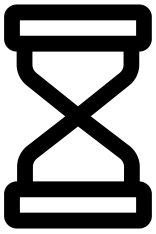
nLockTime

- Transaction-level setting (a field in the transaction data structure)
- Defines the earliest time that a transaction is valid and can be relayed on the network or added to the blockchain



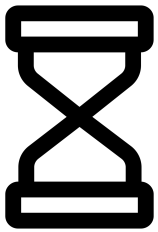
OP_CODE: Check Lock Time Verify (CLTV)

- Allows transaction outputs (rather than whole transactions) to be encumbered by a timelock
- When called, causes the script to fail unless the nLockTime on the transaction is equal to or greater than the time parameter provided to the CLTV opcode
- Ensures the CLTV-based timelock has expired before the transaction may be included in a valid block



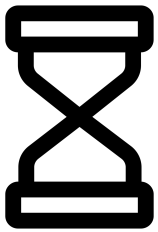
Relative Lock Time (nSequence)

- Result of BIP68/112/113
- Gave new meaning to nSequence creating a relative time lock
- Allows an input to specify the earliest time it can be added to a block based on how long ago the output being spent by that input was included in a block

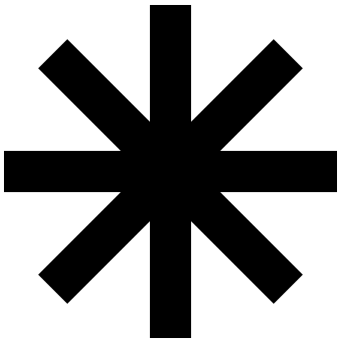


OP_CODE: Check Sequence Verify (CSV)

- Also part of the BIP68/112/113 soft fork
- Provides for relative locktime the same feature CLTV provides for absolute locktime
- Causes the script to fail unless the nSequence on the transaction indicates an equal or greater amount of relative locktime has passed than the parameter provided to the CSV opcode
- Ensures the CSV-based timelock has expired before the transaction may be included in a valid block



Advanced Capabilities



- Conditional clauses

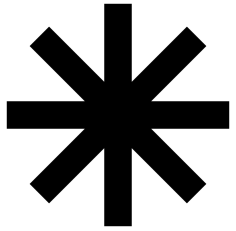
Conditional Clauses – 1/2

```
if (condition):

    code to run when condition is true
else:

    code to run when condition is false

code to run in either case
```



Conditional Clauses – 2/2

In Script, the condition precedes the IF Opcode:

```
condition
IF
    code to run when condition is true
ELSE
    code to run when condition is false
ENDIF
code to run in either case
```