Scripts

Introduction to Scripts

Ira A. Fulton Schools of Engineering
Arizona State University

Objectives

Objective

Describe what transaction scripts are

Objective

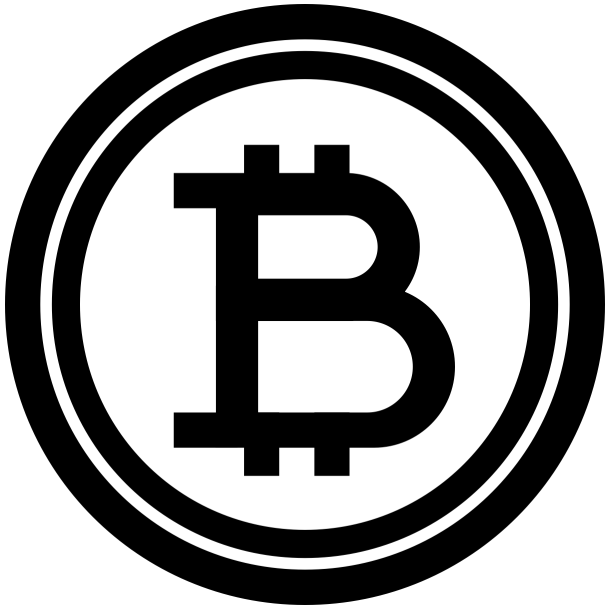
Identify the language Bitcoin scripts are written in

Objective

Explain script operations

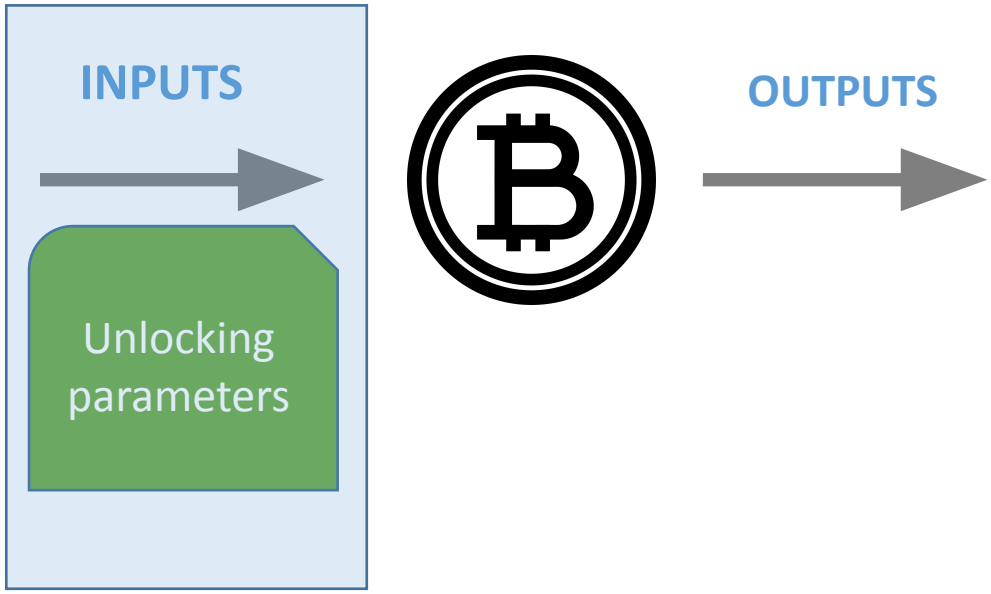
What are Bitcoin Transactions?

- Transfer of rights to certain denominations of Bitcoins
- Each denomination has its own lock
- Only certain parameters unlock the lock condition



Script Operations: Inputs and Outputs

- Unlocking parameters placed in inputs of a transaction
- Inputs are pointers to previous outputs in an unlocking script
- Outputs are scripts and associated value transfer
- With necessary rights, concatenation enables execution



Use inputs to unlock outputs

Input / Unlocking scripts

Output / Locking scripts

Script Language

Script

- Stack-based with reverse-polish notation
- "Turning Incomplete"
  - No loops
  - Not for general use

Stack
=
Data Structure

LIFO
=
Last-In-First-Out

Script Operations

Two main components

1. Simple data (numbers)
2. Operations (functions)

Script Operators (OP Codes) – 1/2

- **OP_DUP** => Duplicates the top stack item
- **OP_HASH160** => The input is hashed twice, first with SHA-256, then with RIPEMD-160
- **OP_EQUAL** => Returns 1 if the inputs are exactly equal, otherwise 0
- **OP_VERIFY** => Marks transaction as invalid if top stack value is not true (the top stack value is removed)
- **OP_EQUALVERIFY** => Same OP_EQUAL but runs OP_VERIFY afterward

Script Operators (OP Codes) – 2/2

- **OP_CHECKSIG** => The entire transaction's outputs, inputs, and script (from the most recently executed OP_CODESEPARATOR to the end) are hashed.
  - The signature used by OP_CHECKSIG must be a valid signature for this hash and public key.
    - If valid, 1 is returned
    - Otherwise, 0