Tutorial 2:
Bitcoin Scripts: Multisig

CSCD71: Blockchains & Decentralized Applications

Nikhil Lakhwani, Oct 6 2023.

Multisignature wallet

A **multisignature** (*multisig*) wallet is a Bitcoin wallet that requires multiple private keys to authorize and complete a transaction.

Purpose: Enhances security, enables shared control, and supports complex spending conditions.

Setup for this demo.

1. Installed Bitcoin Core.
2. Set up a local testnet node
3. RPC Configuration

Reference:
https://github.com/BlockchainCommons/Learning-Bitcoin-from-the-Command-Line/blob/master/02_1_Setting_Up_a_Bitcoin-Core_VPS_with_StackScript.md

Objectives

1. Generate 3 private/public keys on a single machine.
2. Create a 2 of 3 multisignature wallet.
3. Create a raw transaction.
4. Sign the transaction from 2 out of 3 private keys, and the specific redeem script.
5. Send transactions from the multisignature wallet and broadcast to the testnet.

How does it work?

1. *https://learnmeabitcoin.com/technical/p2ms#why-use-p2sh-instead-of-p2ms*

Sending a **transaction**

The locking script contains the *hash* of another locking script (the "`script hash`"), surrounded by the `HASH160` and `EQUAL` opcodes:

scriptPubKey	OP_HASH160	748284390f9e263a4b766a75d0633c50426eb875	OP_EQUAL

P2SH

hex | opcodes inline | stack

The unlocking script then contains your original custom locking script (the "`redeem script`"), preceded by the data/opcodes needed to unlock it:

scriptSig	OP_0 3046022100a07b2821f96658c938fa9c68950af0e69f3b2ce5f8258b3a6ad254d4bc73e11e022100e82fab8df3f 7e7a28e91b3609f91e8ebf663af3a4dc2fd2abd954301a5da67e701 5121022afc20bf379bc96a2f4e9e63ffceb8652b2b6a097f63fbee6ecec2a49a48010e2103a767c7221e9f15f87 0f1ad9311f5ab937d79fcaeee15bb2c722bca515581b4c052ae

hex | opcodes inline | stack

1. *https://learnmeabitcoin.com/technical/p2ms#why-use-p2sh-instead-of-p2ms*

Thanks!

Do you have any questions?