Standard Script Notation

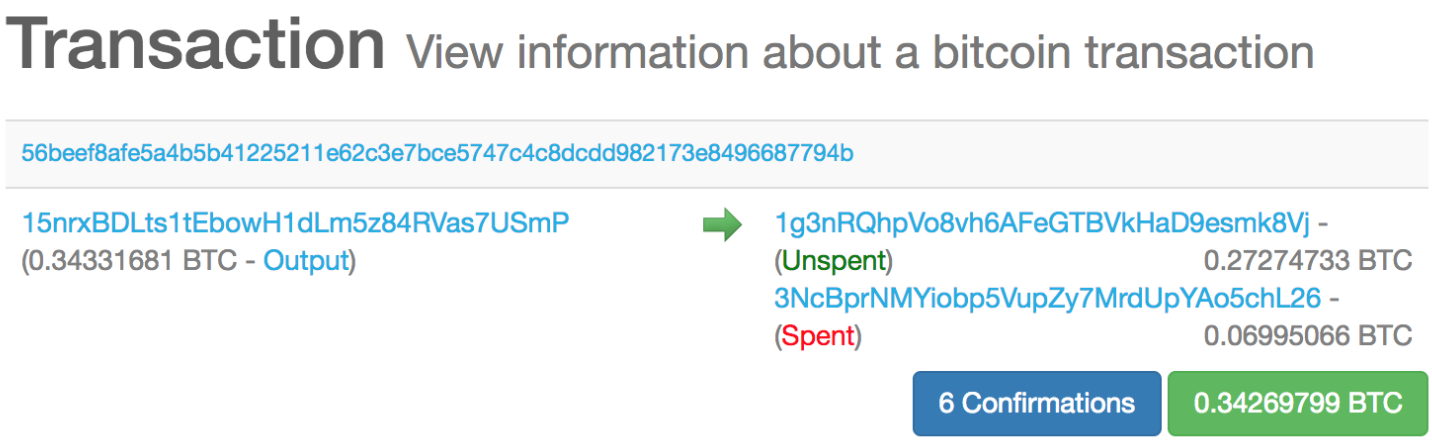
Let's discuss standard script notation using this example, `<sig><pubKey> OP_CHECKMULTISIG`

- Bracketed values are data to be pushed to the stack.
  - For example, `<sig>`.
- Non-bracketed words are opcodes.
  - For example, `OP_CHECKMULTISIG`
- Sometimes you may see the `OP` prefix omitted.
  - For example, `<sig><pubKey> OP_CHECKMULTISIG` may be abbreviated to `<sig><pubKey> CHECKMULTISIG`

Exploring Live Scripts

Using an online block explorer, we can see examples of live Unlocking and Locking Scripts.

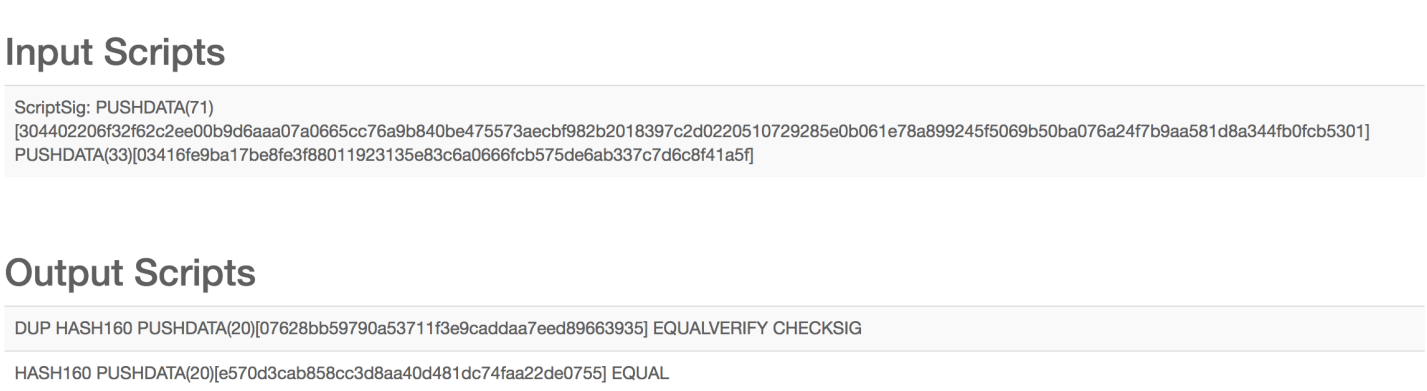
Step 1: Checkout this TXID: 56beef8afe5a4b5b41225211e62c3e7bce5747c4c8dcdd982173e8496687794b that has 1 input and 2 outputs.



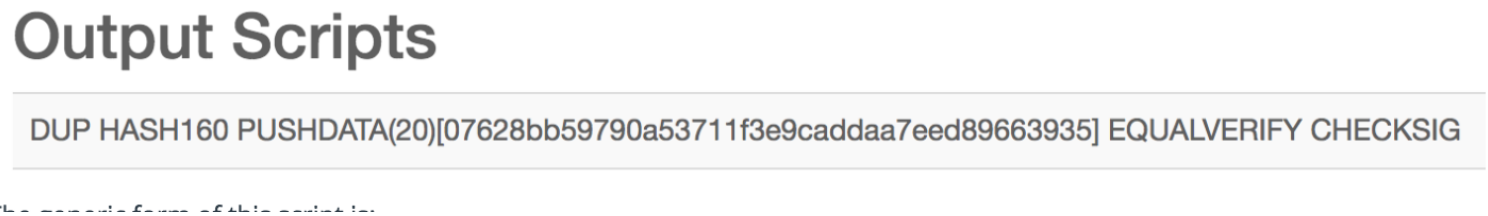
Example transaction with 1 input and 2 outputs.

Step 2: Scroll down to the bottom to see the Unlocking Scripts (scriptSig) of the one input and the two Locking Scripts (scriptPubKey) from the two outputs.

If you don't see it check **Hide scripts & coinbase** link in the **Inputs and Outputs** section.



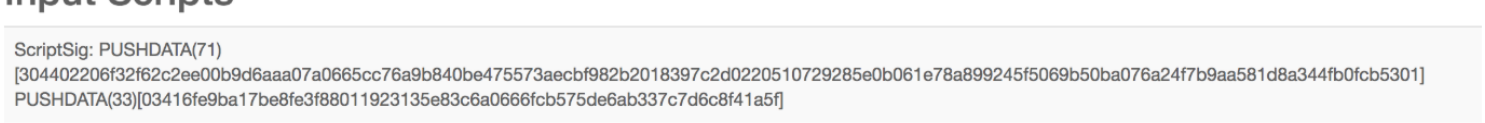
Step 3: Focus on the Locking Script of the first Output (output 0):



The generic form of this script is:

```
OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
```

Step 4: Now focus on the Unlocking Script of the Input:



The generic form of this script is:

```
<sig> <pubKey>
```

Which is a Standard Unlocking Script for Standard Transactions to Bitcoin addresses.

That wraps it up for your overview to Script Opcodes. In this concept, we:

- Demoed how to evaluate an example script and you got to practice solving an example
- Saw some examples of simple Unlocking and Locking Scripts
- Reviewed standard script notations
- Explored live scripts using an online block explorer