NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 15: Blockchain Elements - III

CONCEPTS COVERED

- Understanding Bitcoin Scripts
- Some Interesting Bitcoin Scripts

KEYWORDS

- Bitcoing Script
- scriptPubKey
- scriptSig
- Stack

Bitcoin Scripts

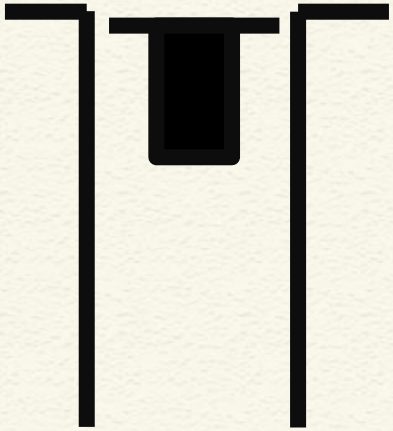
Transaction Input → **scriptSig:** 18E14A7B6A30… D61967F63C7DD…

Transaction Output → **scriptPubKey:**

OP_DUP
OP_HASH160
16UwLL9Risc3QfPqBUvKof…
OP_EQUALVERIFY
OP_CHECKSIG

See for detailed steps:
https://developer.bitcoin.org/devguide/transactions.html

Bitcoin Scripts



scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

scriptSig: <sig> <pubKey>

The stack is initially empty. Both the scripts are combined – input followed by output

<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

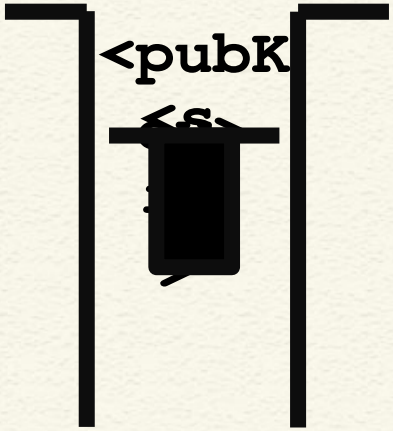
A real example from Bitcoin

For more examples to explore: https://btc.com/btc/blocks

Bitcoin Scripts

<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

The top two items are pushed to Stack one after another

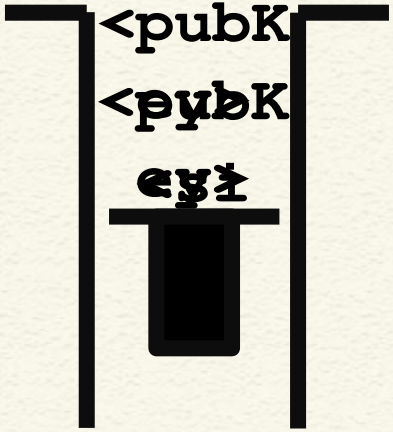


OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

Bitcoin Scripts

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

Top stack item is duplicated

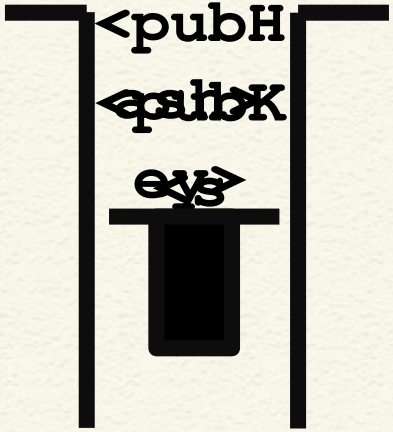



```
OP_HASH160 <pubKeyHash>
OP_EQUALVERIFY OP_CHECKSIG
```

Bitcoin Scripts

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

Top stack item is hashed (RIPEMD-160 hashing)



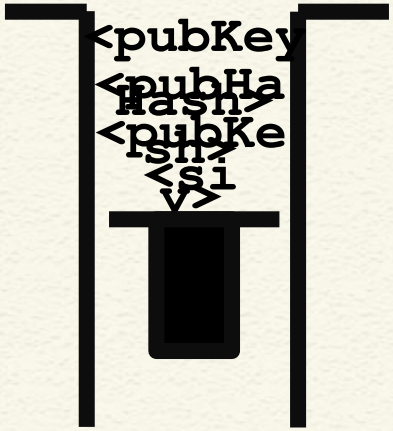

```
<pubKeyHash> OP_EQUALVERIFY
OP_CHECKSIG
```

Bitcoin Scripts

<pubKeyHash>

OP_EQUALVERIFY OP_CHECKSIG

The constant is pushed in the stack



OP_EQUALVERIFY OP_CHECKSIG

Bitcoin Scripts

OP_EQUALVERIFY OP_CHECKSIG

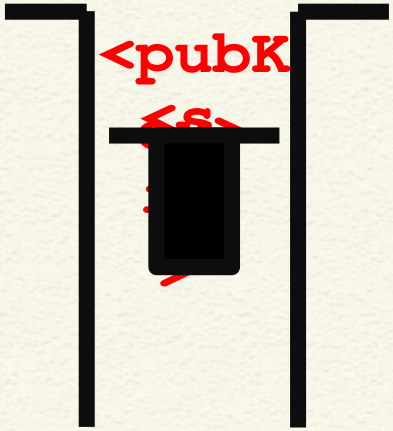
Equality is checked between the top two items in the stack

OP_CHECKSIG

Bitcoin Scripts

OP_CHECKSIG

Signature is checked based on the top two stack item



TRUE

Bitcoin Script Instructions

- Total 256 opcodes (15 disabled, 75 reserved)
  - Arithmetic operations
  - if-then conditions
  - Logical operators
  - Data handling (like OP_DUP)
  - Cryptographic operations
    - Hash functions
    - Signature verification
    - Multi-signature verification

Interesting Bitcoin Scripts

- Provably un-spendable or prunable outputs

```
scriptPubKey: OP_RETURN
{zero or more ops}
```

- Anyone-can-spend outputs

```
scriptPubKey: {empty}
scriptSig: OP_TRUE
```

Source: https://en.bitcoin.it/wiki/Script

Interesting Bitcoin Scripts

- **Freezing funds until a time in the future**

```
scriptPubKey: <expiry_time>
OP_CHECKLOCKTIMEVERIFY OP_DROP
OP_DUP OP_HASH160 <pubKeyHash>
OP_EQUALVERIFY OP_CHECKSIG
scriptSig: <sig> <pubKey>
```

Source: https://en.bitcoin.it/wiki/Script

CONCLUSIONS

- Use of scripts in generating input and output of bitcoin transactions
- Public key cryptography and digital signature for cryptographically protecting transactions

REFERENCES

- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress (2017)
- Any other standard textbook on blockchain/bitcoin


Thank
you