BLOCKCHAINS

ARCHITECTURE, DESIGN AND USE CASES

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING,
IIT KHARAGPUR

PRAVEEN JAYACHANDRAN
IBM RESEARCH,
INDIA

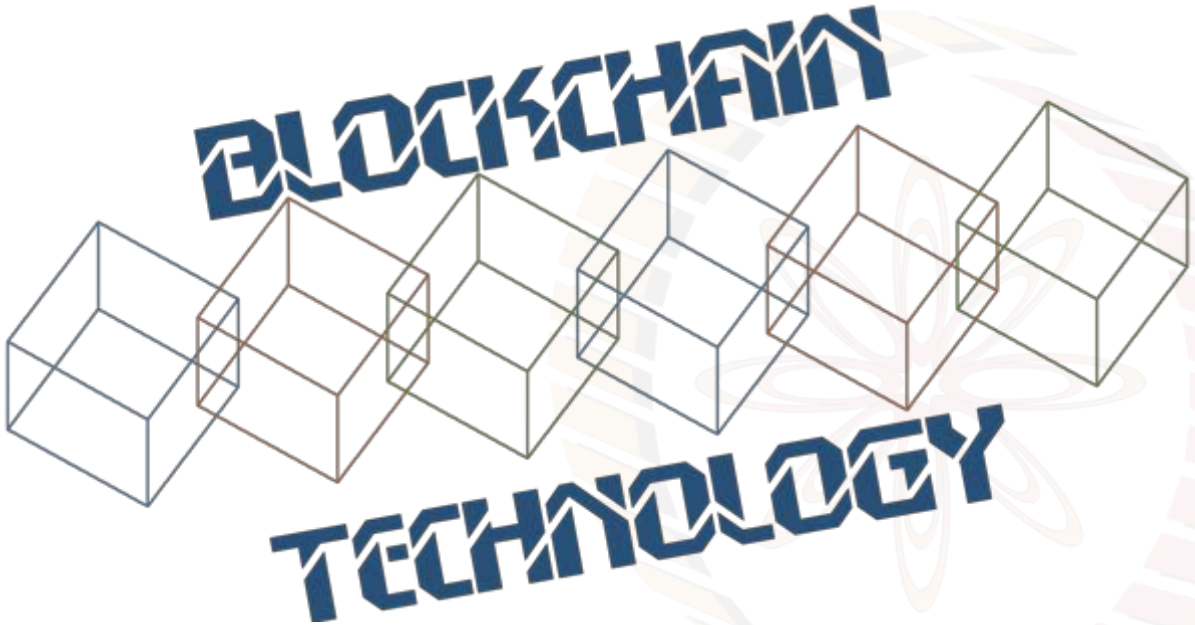
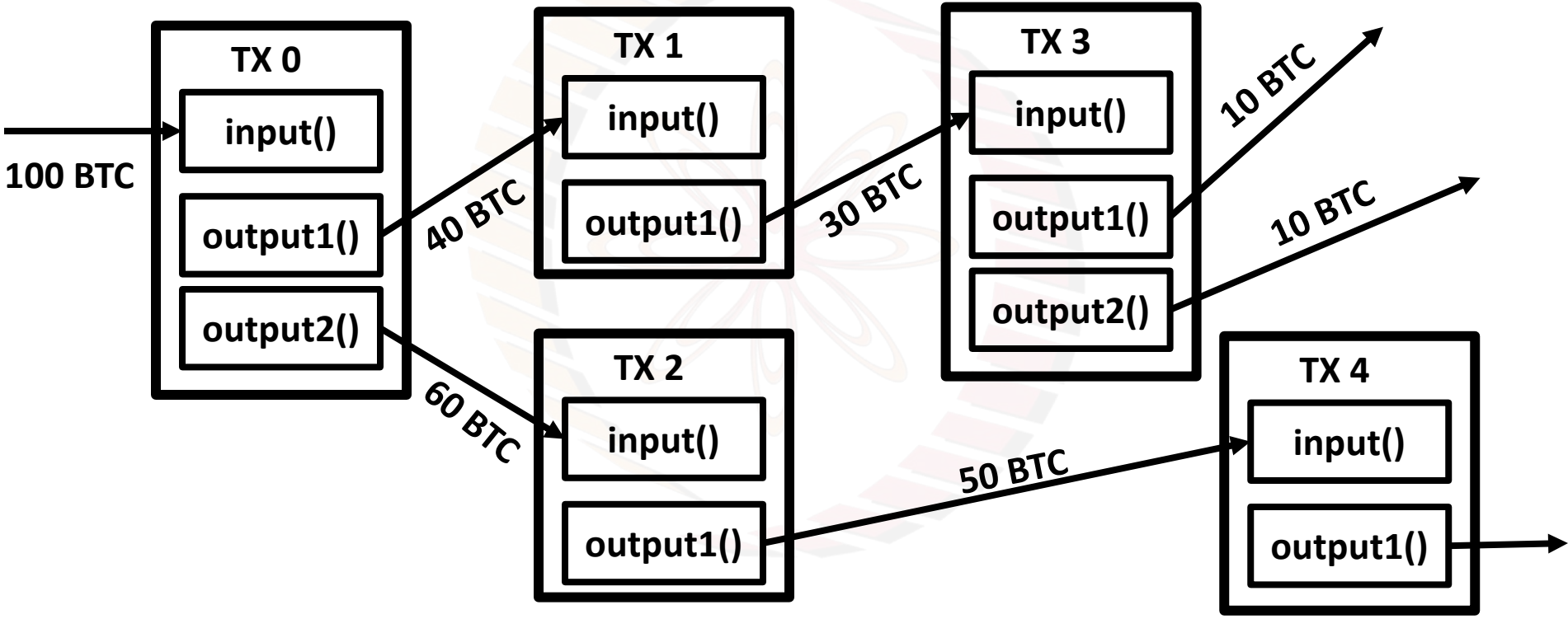


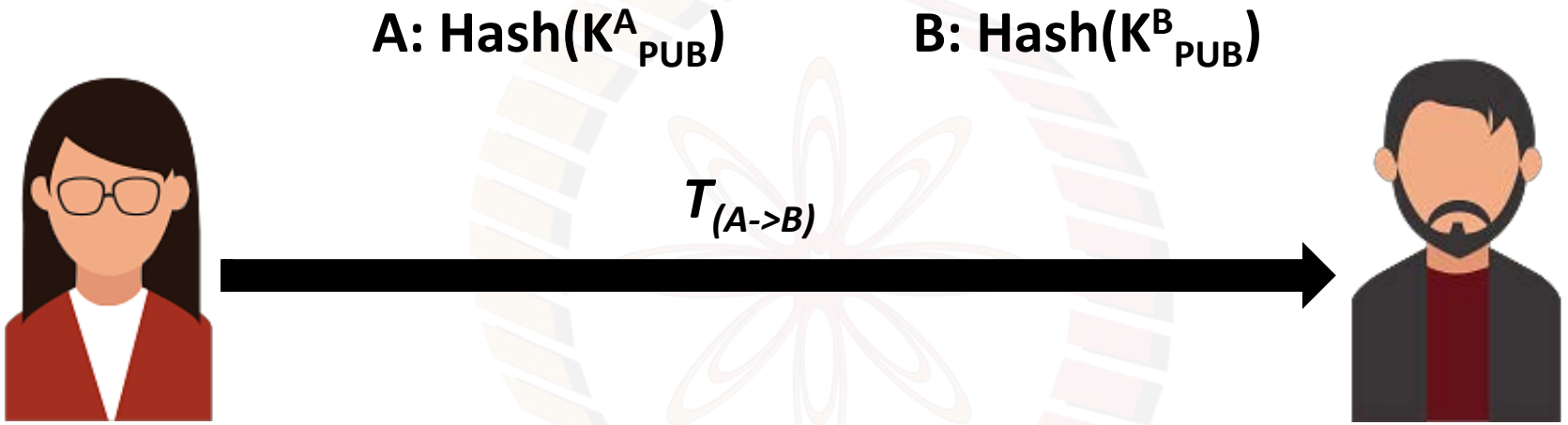
Image courtesy: http://beetfusion.com/

BITCOIN BASICS II

Bitcoin Transactions and Input and Output

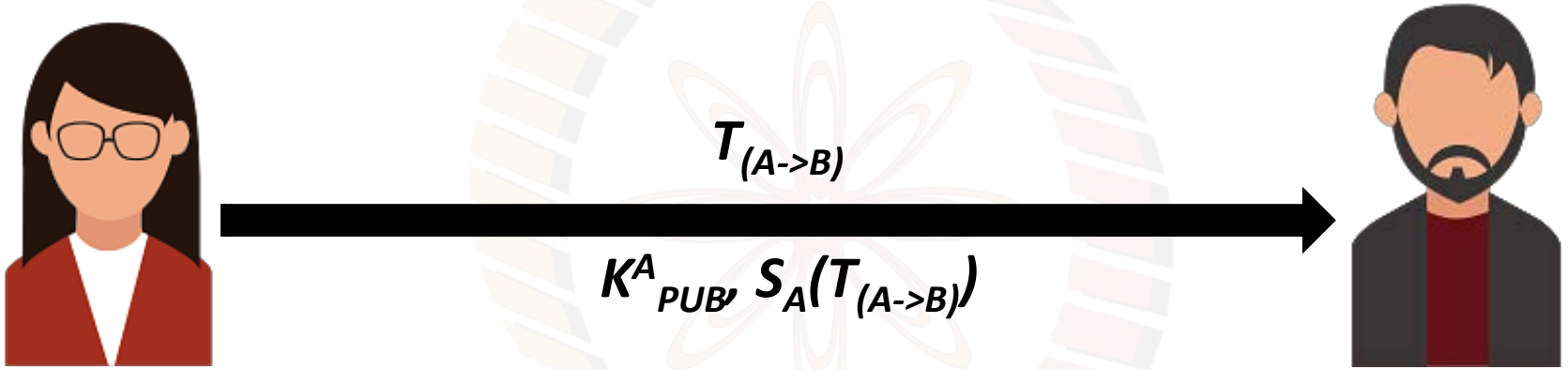


Bitcoin Scripts – A Simple Example



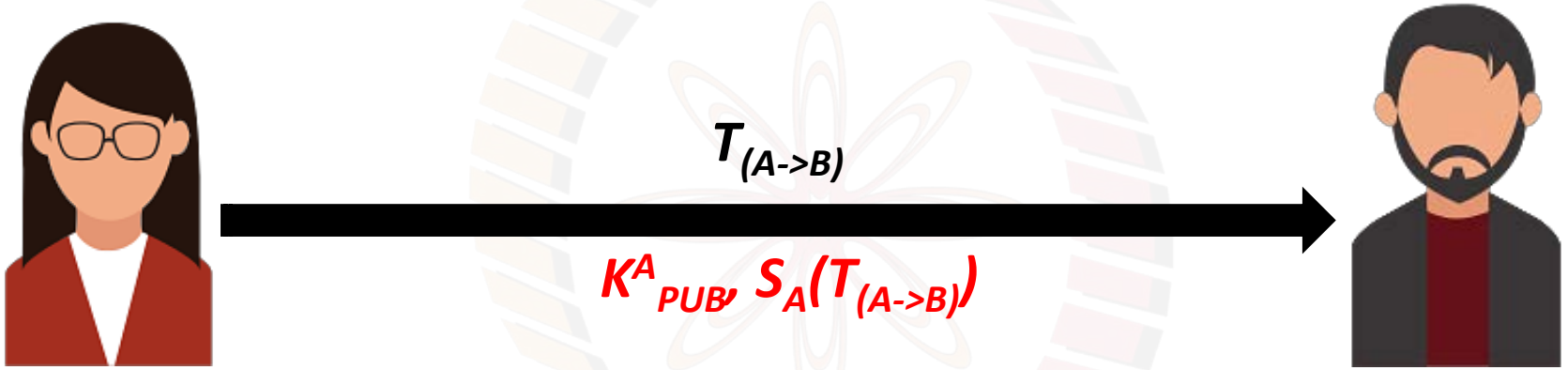
How Bob will verify that the transaction is actually originated from Alice?

Bitcoin Scripts – A Simple Example



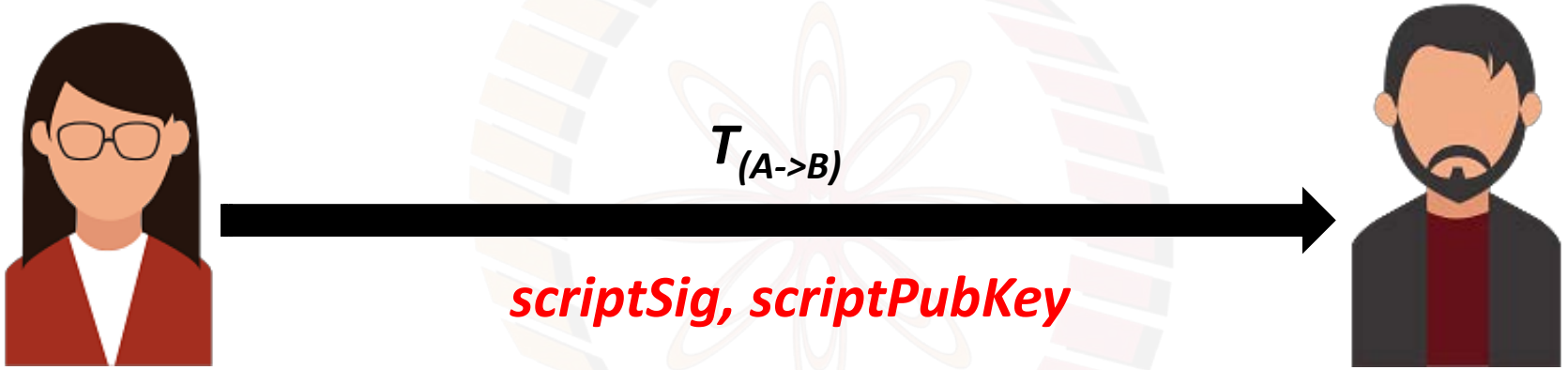
Send the public key of Alice along with the signature -> Bob can verify this

Bitcoin Scripts – A Simple Example



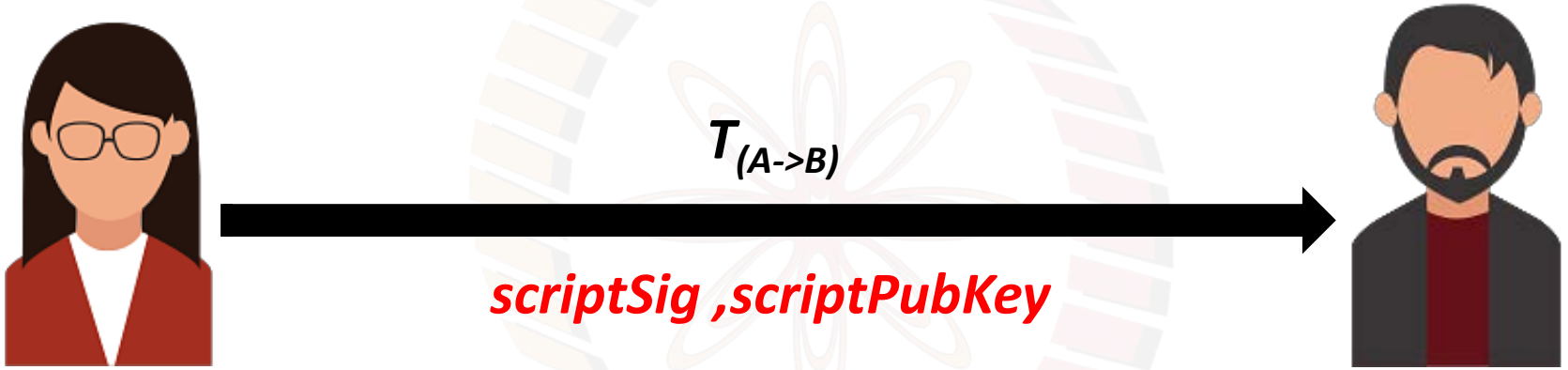
Bitcoin indeed transfers scripts instead of the signature and the public key

Bitcoin Scripts – A Simple Example



Bitcoin indeed transfers scripts instead of the signature and the public key

Bitcoin Scripts – A Simple Example



Bob can spend the bitcoins only if both the scripts return true after execution

Bitcoin Scripts

- Simple, compact, stack-based and processed left to right
  - FORTH like language

- **Not Turing Complete** (no loops)
  - Halting problem is not there

Bitcoin Scripts

- With every transaction Alice must provide
  - A public key that, when hashed, yields the address of Alice embedded in the script
  - A signature to provide ownership of the private key corresponding to the public key of Alice

Bitcoin Scripts

Transaction Input → **scriptSig:**

```
18E14A7B6A30…
D61967F63C7DD…
```

Transaction Output → **scriptPubKey:**

```
OP_DUP
OP_HASH160
16UwLL9Risc3QfPqBUvKof…
OP_EQUALVERIFY
OP_CHECKSIG
```

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

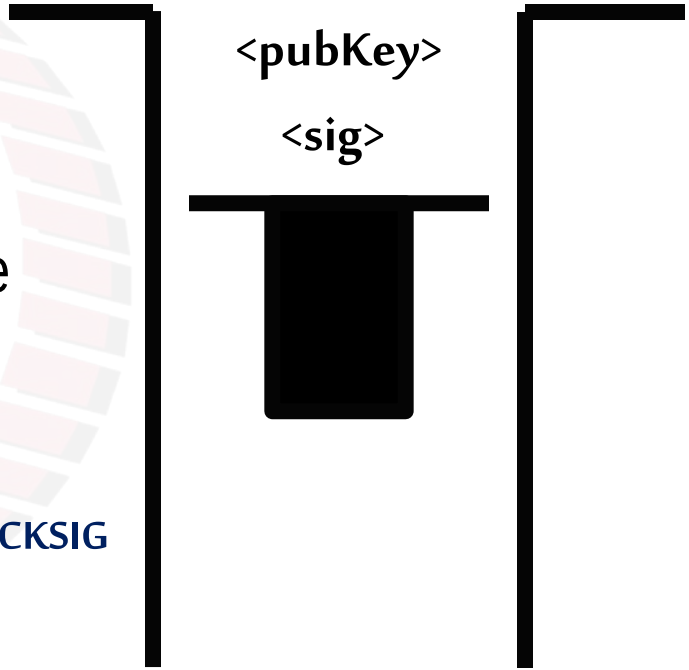
<sig> <pubKey> OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

Bitcoin Scripts

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

- The stack is initially empty. Both the scripts are combined

OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

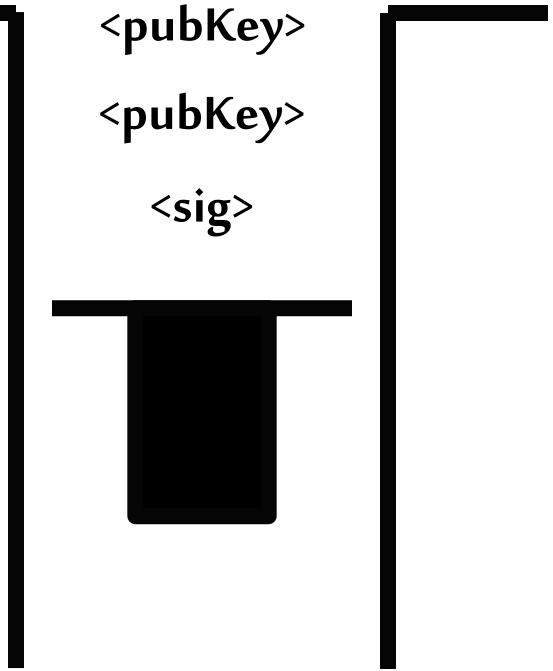


Bitcoin Scripts

OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

- Top stack item is duplicated

OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

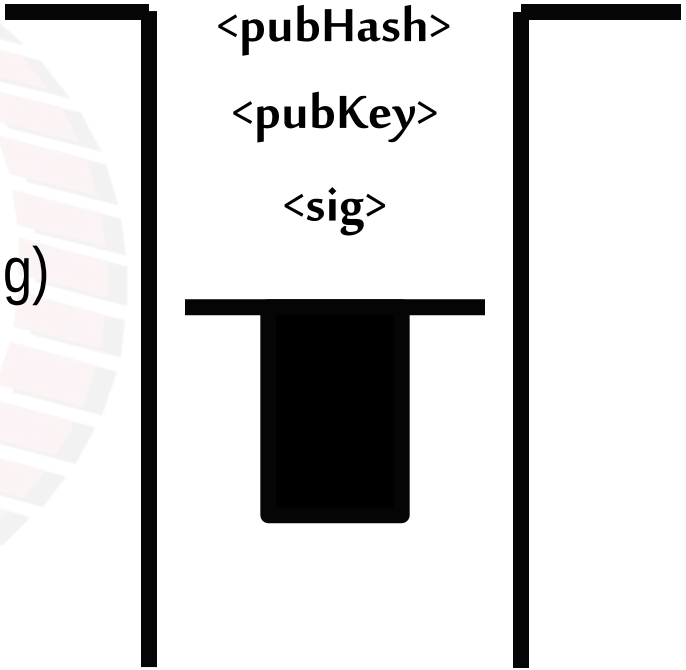


Bitcoin Scripts

OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

- Top stack item is hashed (RIPEMD-160 hashing)

<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

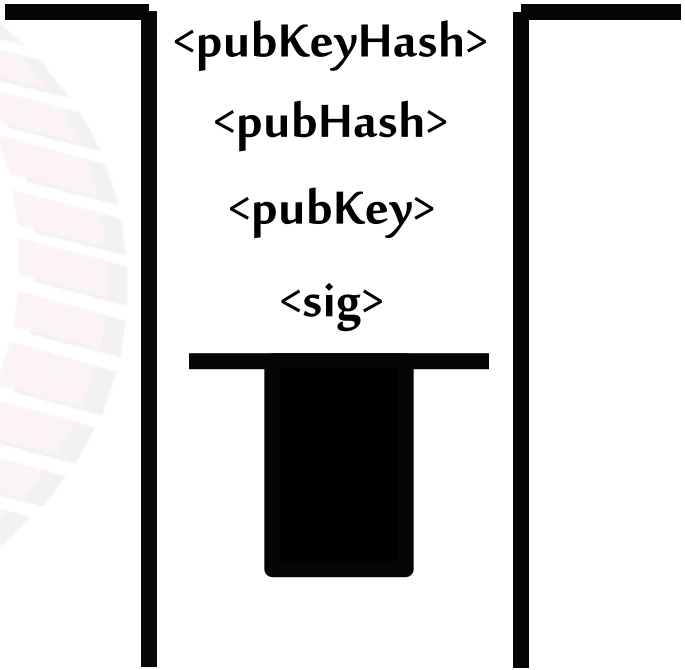


Bitcoin Scripts

<pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

- The constant is pushed in the stack

OP_EQUALVERIFY OP_CHECKSIG

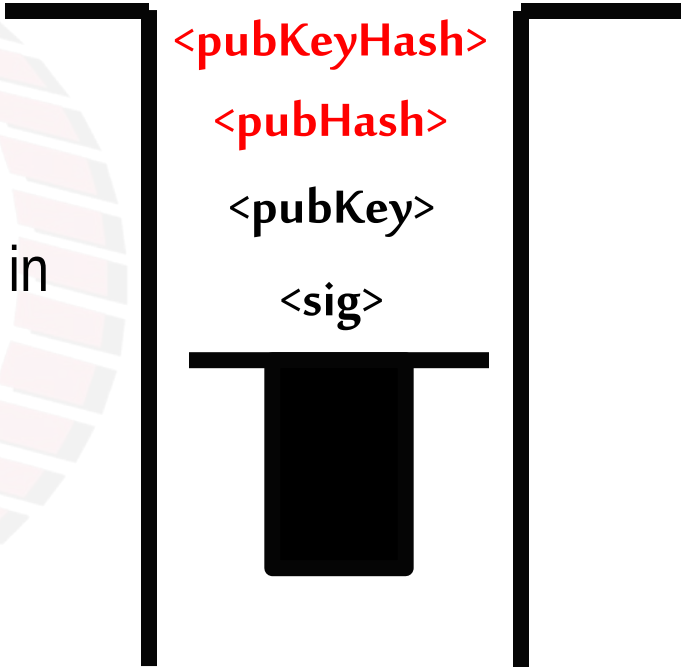


Bitcoin Scripts

OP_EQUALVERIFY OP_CHECKSIG

- Equality is checked between the top two items in the stack

OP_CHECKSIG

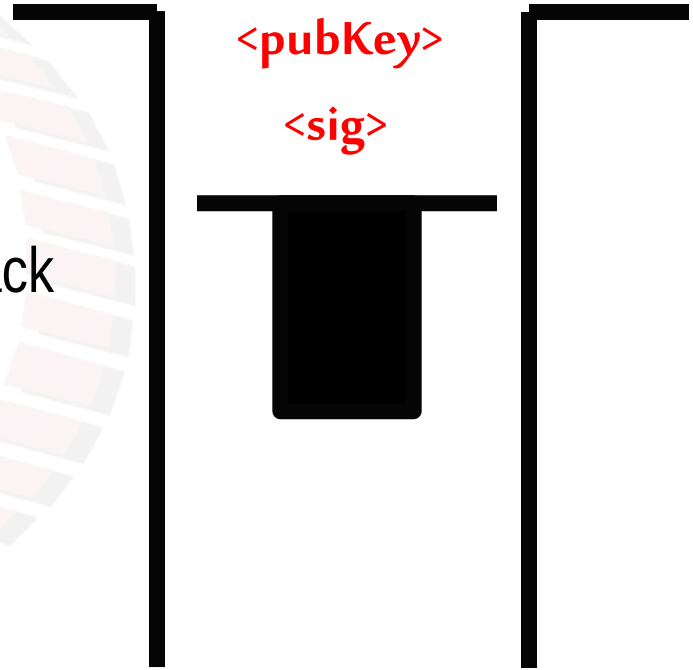


Bitcoin Scripts

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

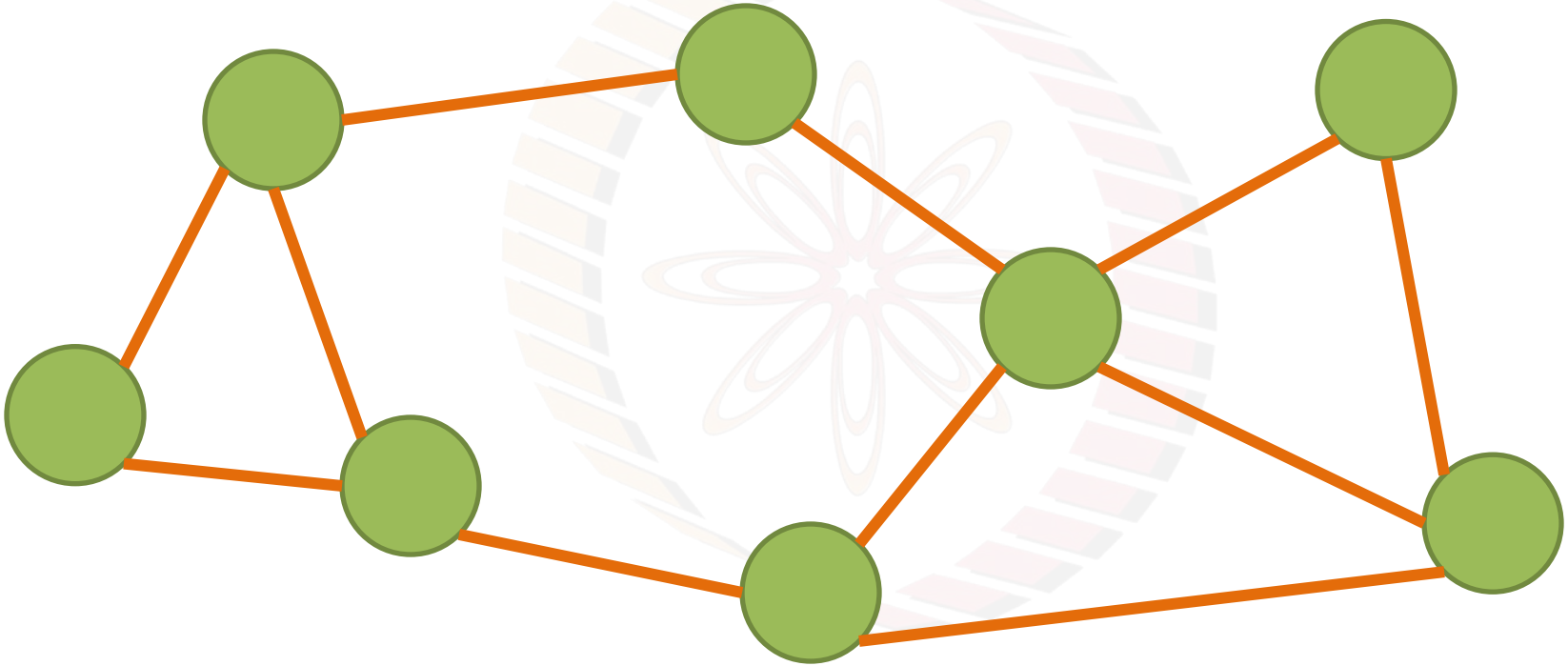
scriptSig: <sig> <pubKey>

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

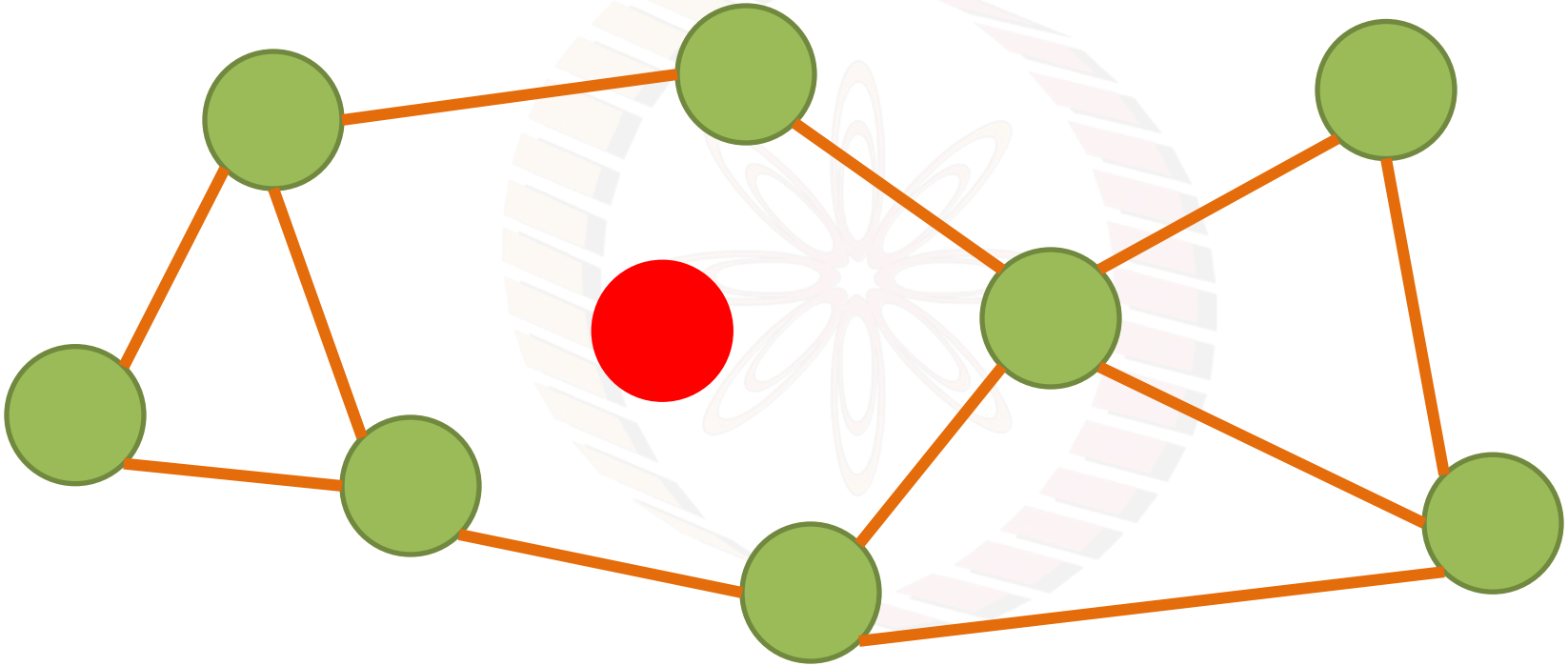
Bitcoin P2P Network

- An ad-hoc network with random topology, Bitcoin protocol runs on TCP port 8333
- All nodes (users) in the bitcoin network are treated equally
- New nodes can join any time, non-responding nodes are removed after 3 hours

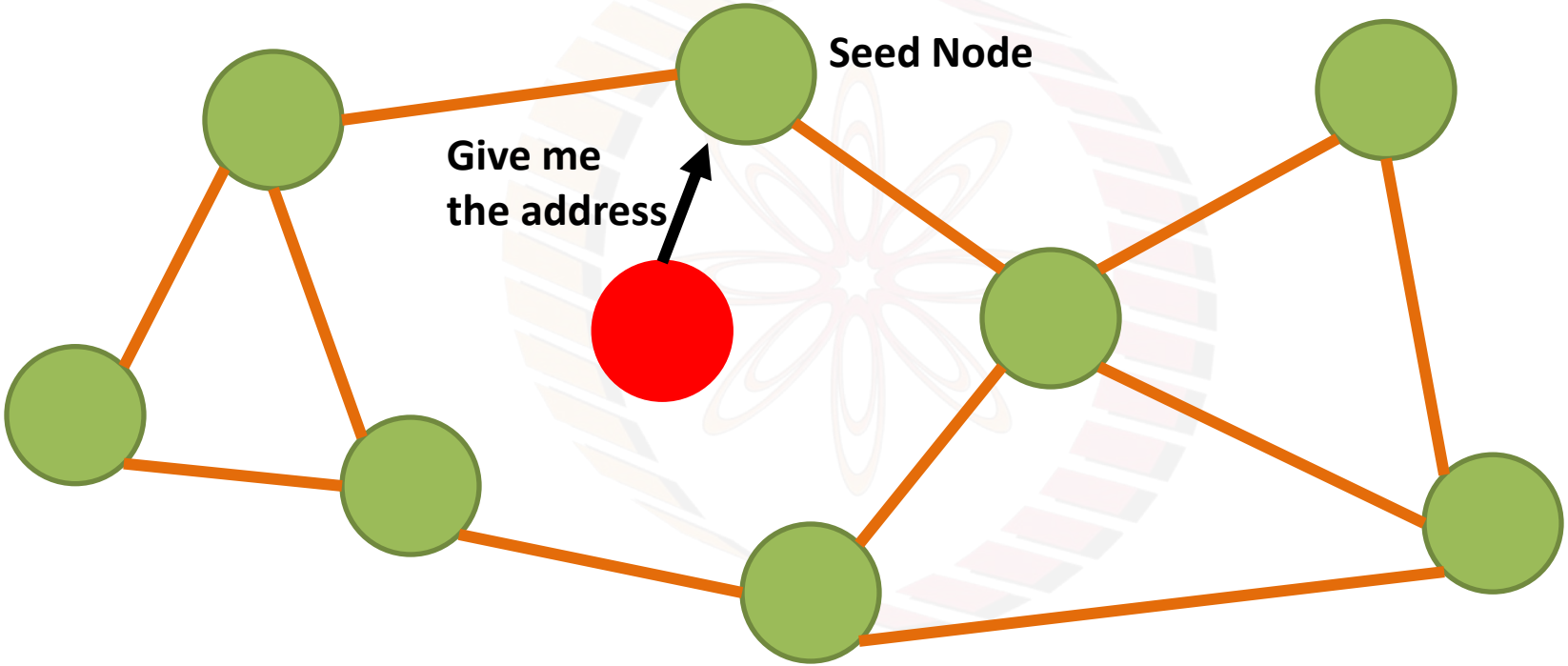
Joining in a Bitcoin P2P Network



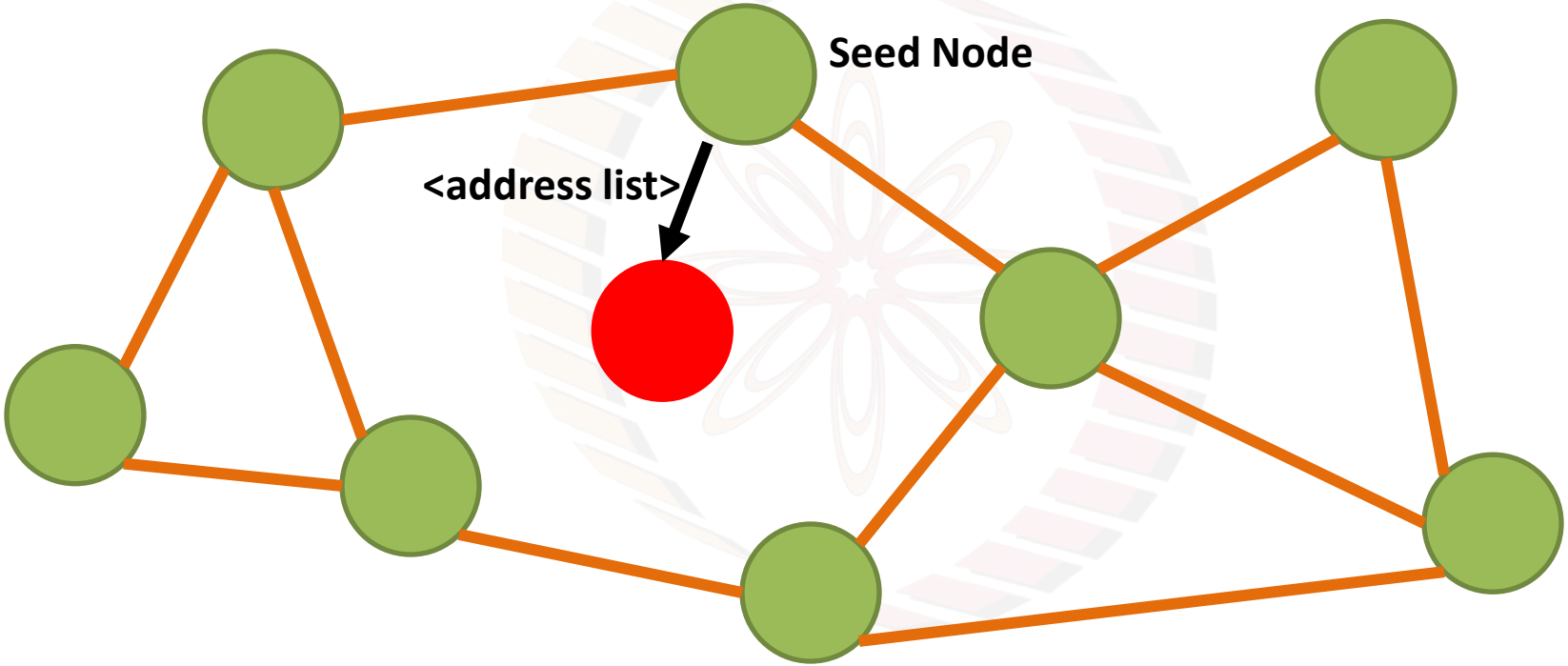
Joining in a Bitcoin P2P Network



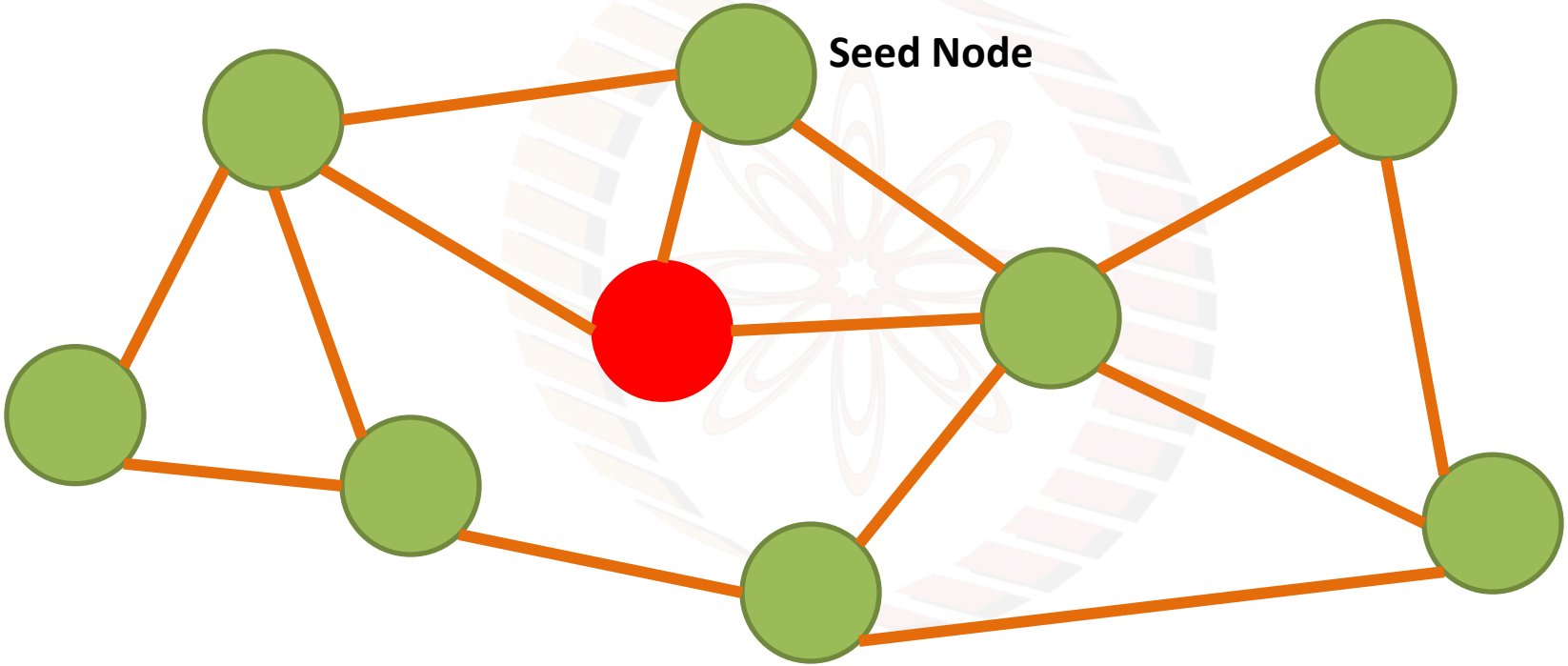
Joining in a Bitcoin P2P Network



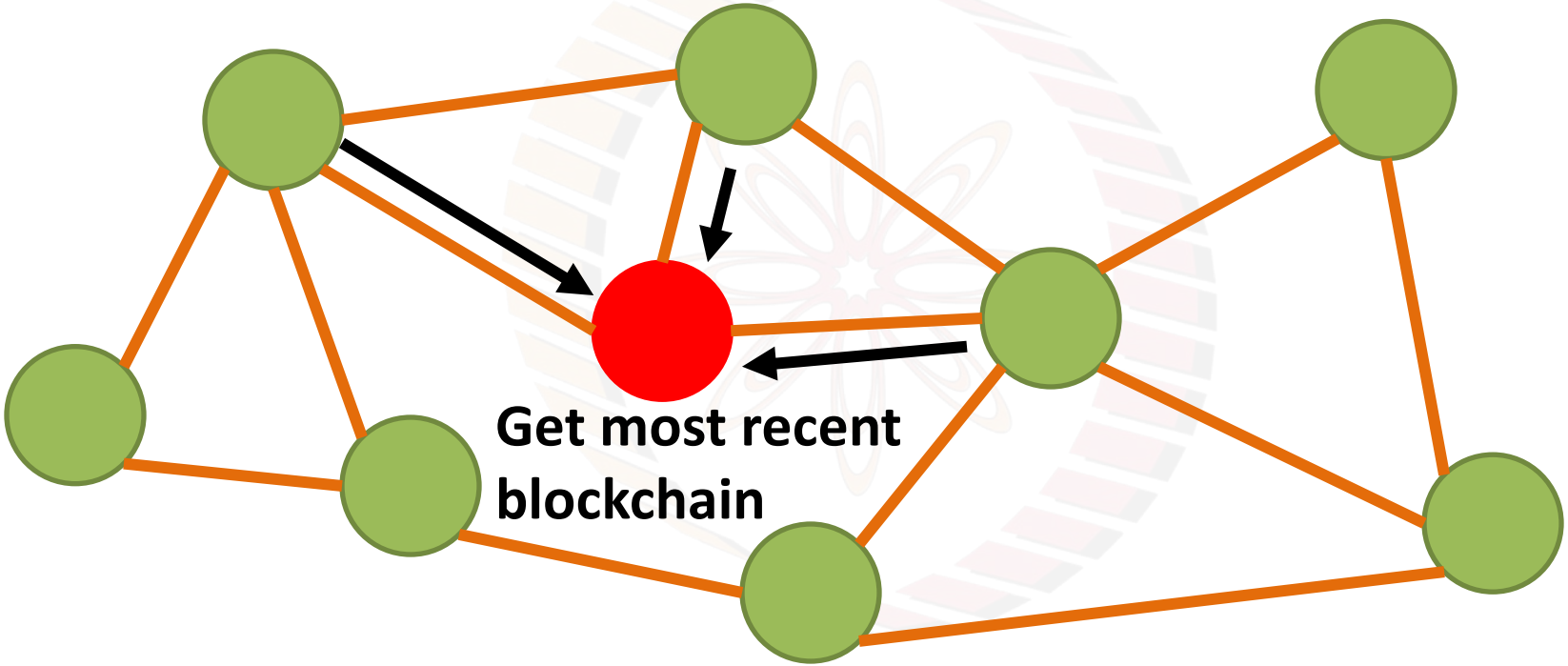
Joining in a Bitcoin P2P Network



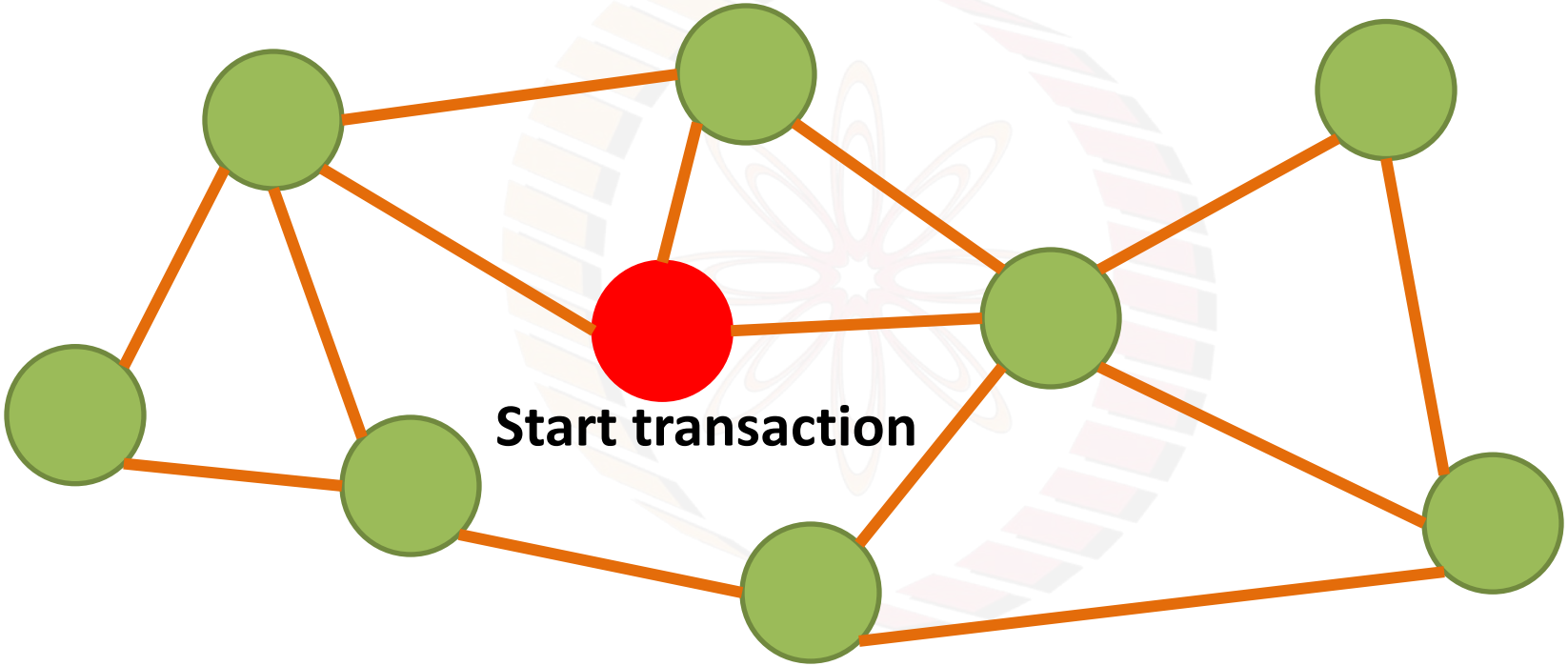
Joining in a Bitcoin P2P Network



Joining in a Bitcoin P2P Network



Joining in a Bitcoin P2P Network




BITCOIN • DIGITAL • DECENTRALIZED • PEER TO PEER
1 TROY OZ .999 FINE COPPER
BTC

thank you!