TECHNOLOGY

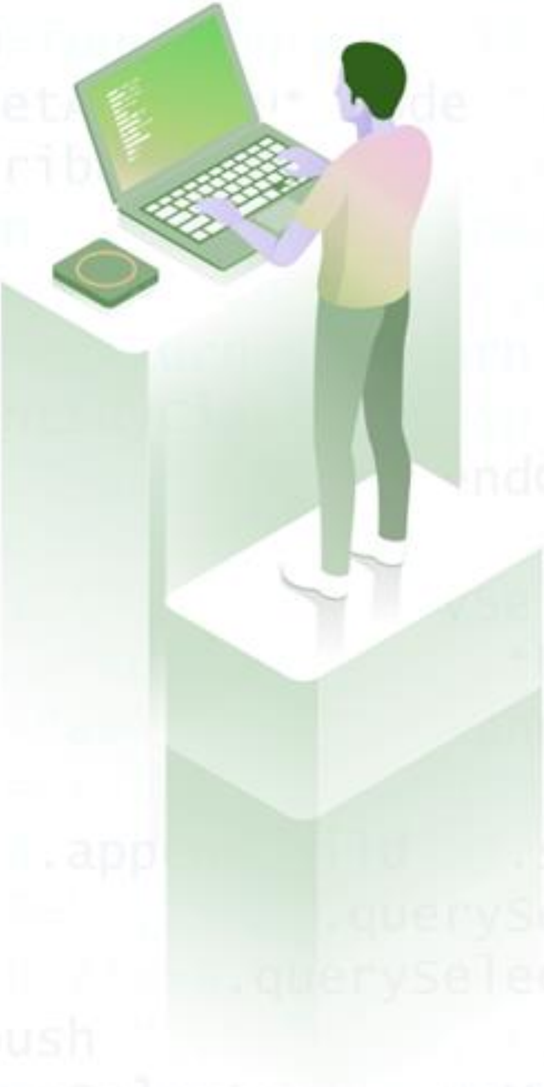
IIT KANPUR

Indian Institute of Technology, Kanpur

Professional Certification Program in Blockchain

Powered by simplilearn

TECHNOLOGY



Bitcoin Blockchain

Learning Objectives

By the end of this lesson, you will be able to:

- Explore Bitcoin and its elements
- Identify and create different wallets for Bitcoin
- Analyze the Bitcoin transaction mechanism
- Understand Bitcoin scripting and mining

Introduction to Bitcoin

Introduction to Bitcoin

Bitcoin is the first application of blockchain technology. It was introduced in 2008 through a paper called *Bitcoin: A Peer-to-Peer Electronic Cash System* and implemented in 2009.

Introduction to Bitcoin

- Bitcoin can be defined as a protocol, a digital currency, and a platform.
- It is a combination of network, protocols, and software that facilitate the creation and usage of the digital currency.
- Nodes in this peer-to-peer network talk to each other using the Bitcoin protocol.

Bitcoin Components

Bitcoin majorly consists of the following components:

Bitcoin Network

Wallets

Blockchain

Miners

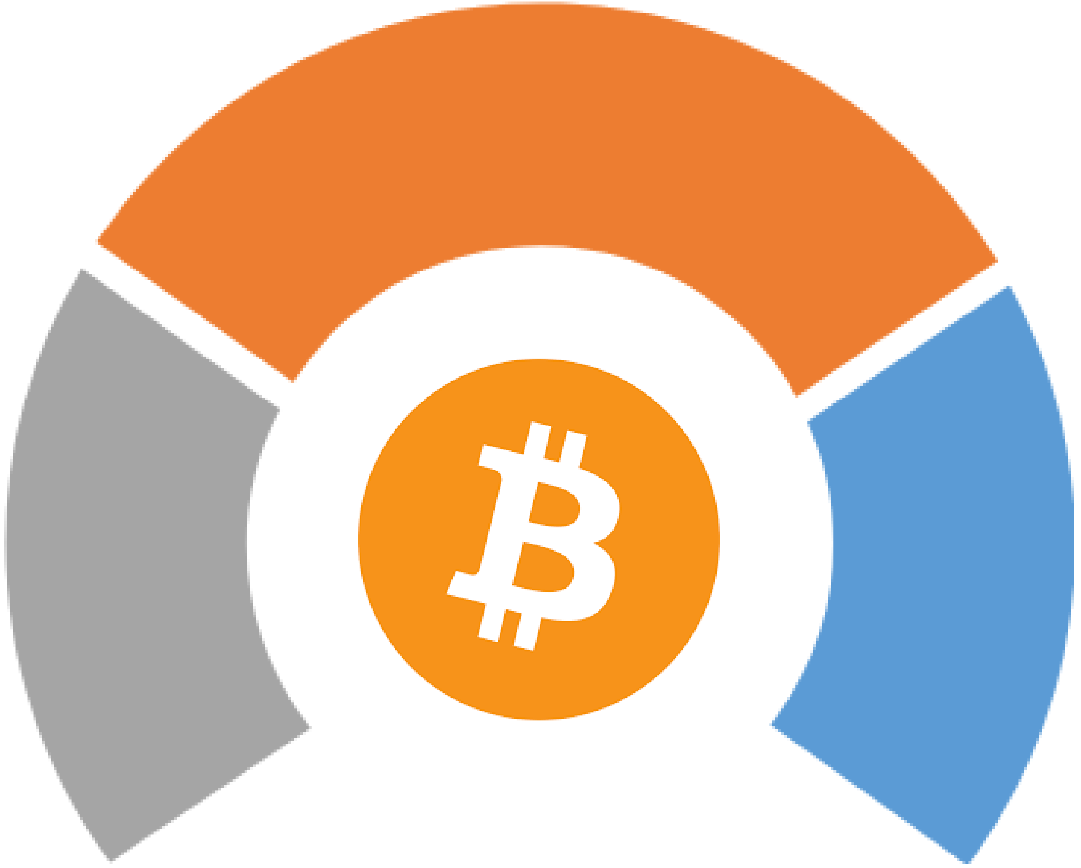
Transactions

Digital Keys

Hash Address

Limited Supply of Bitcoin

The number of Bitcoins mined will be halved after every 210,000 blocks



Only 21 million Bitcoins will be created for the currency to maintain value

The rate of block creation is moderated after every 2016 blocks

Addresses in Bitcoin

It is a 64-bit hash address that is generated by hashing the public and private keys of the user with SHA-256 algorithm first and RIPEMD-160 next.

A typical bitcoin address looks like this:

1ANAguGG8bikEv2fYsTBnRUmx7QUcK58wt

TECHNOLOGY

Bitcoin Wallets

Bitcoin Wallets

The wallet software is used to store private/ public keys and Bitcoin address. It also helps transact and store cryptocurrency. Wallets today act as both Bitcoin client and wallet.

Types of Bitcoin Wallets

Bitcoin wallets are mainly categorized in the below types:

Desktop/Software Wallet

Web Wallet

Mobile Wallet

Hardware Wallet

Software or Desktop Wallets

These wallets store your private keys on your computer

Example

ARMORY

BitcoinCore

MultiBit HD

Web Wallets

These wallets are accessed through an internet gateway from any capable device.

Example

BLOCKCHAIN

coinbase

CIRCLE

Mobile Wallets

These wallets store your private keys on your mobile.

Example

bread wallet

mycelium
ad-hoc economy

Bitcoin

Hardware Wallets

These wallets are most secure as private keys are stored in an external USB device.

Example

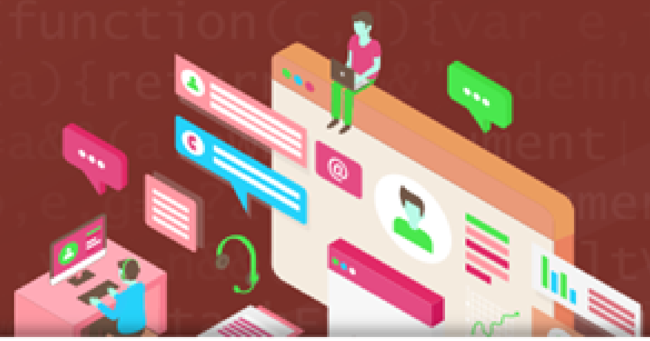
Ledger

TREZOR

OPENDIME

Bitcoin, like cash in hand.

Install a Software Wallet



Problem Statement: You are to install a software wallet in your lab system.

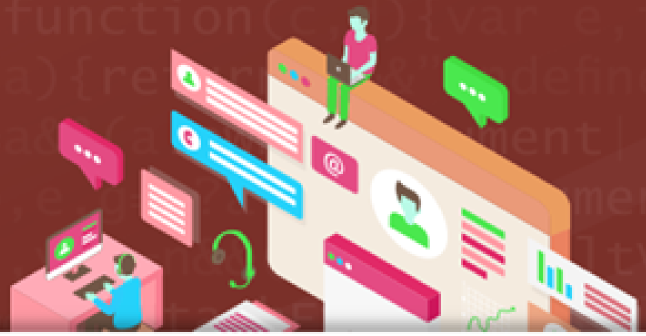
ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to install a software wallet:

1. Downloading and installing the Exodus software wallet

Generate a Paper Wallet



Problem Statement: You are to generate a paper wallet account.

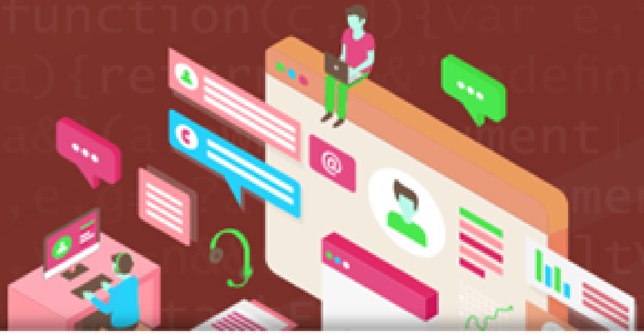
ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to generate a paper wallet:

1. Generating a Single Wallet and Paper wallet

Install a Web Wallet



Problem Statement: You must install a web wallet in your lab machine.

ASSISTED PRACTICE

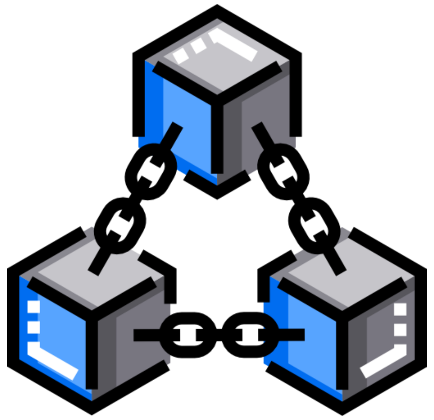
Assisted Practice: Guidelines

Steps to install a web wallet:

1. Generating a Jaxx web wallet

Bitcoin Block

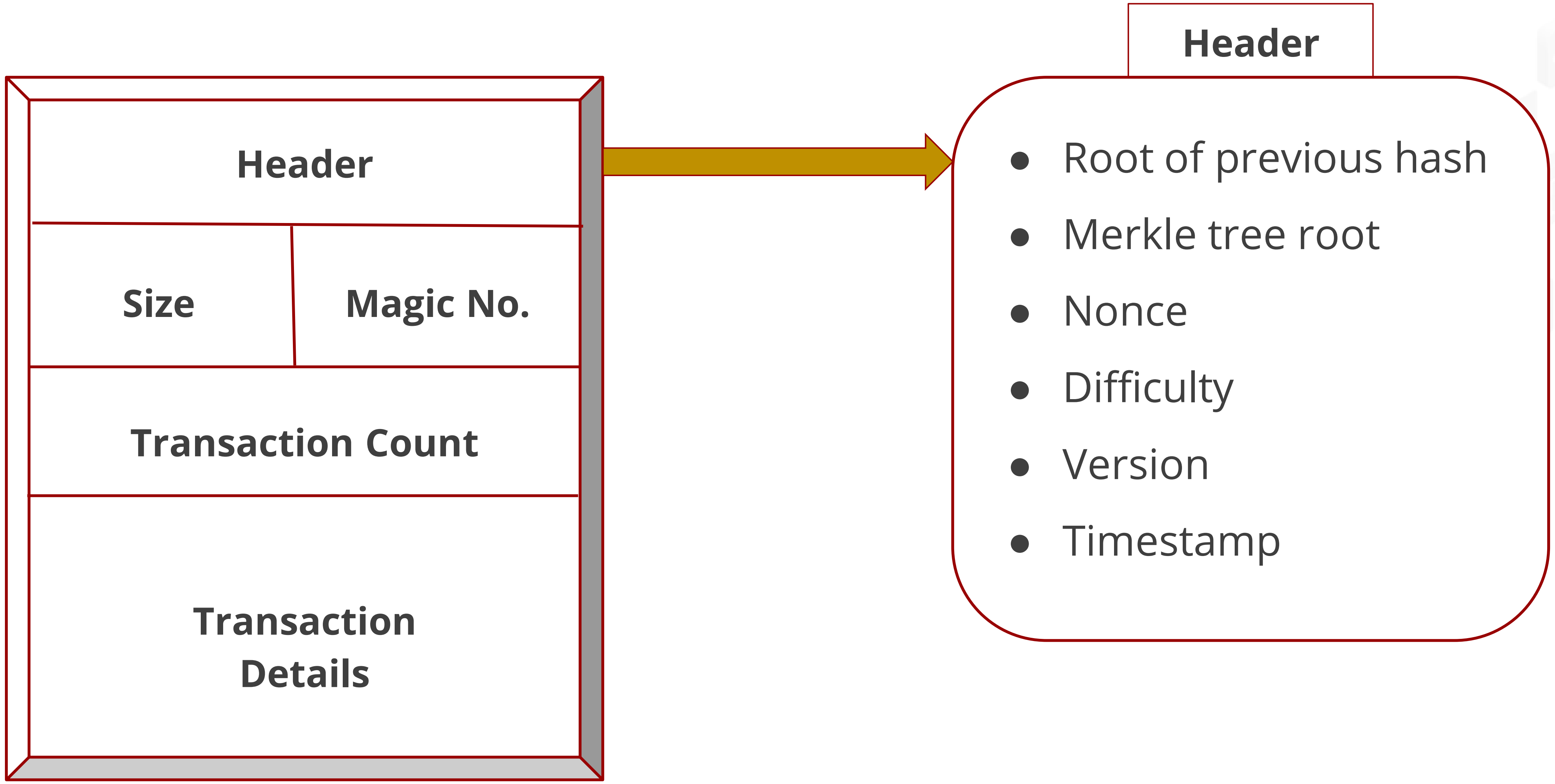
Bitcoin Block



Magic Number	A 4-byte value which is always 0xD9B4BEF9
Block Size	Average size of the block in bitcoin is 1 MB
Block Header	Contains important metadata such as hash values
Transaction Count	Depicts the number of transactions stored in that block
Transaction List	Lists the details of all transactions stored in that block

Bitcoin Block

A block in Bitcoin consists of a header, nonce, the size of the block, the number of transactions recorded, and the translation information itself.



Header

Size

Magic No.

Transaction Count

Transaction Details

Header

- Root of previous hash
- Merkle tree root
- Nonce
- Difficulty
- Version
- Timestamp

Bitcoin Block Header

Version

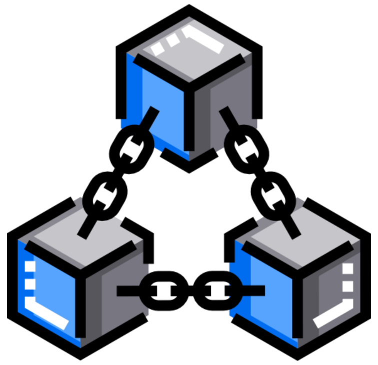
Version of the block and the technology used

Previous Block Hash

Is stored to maintain security and immutability

Nonce

A pseudo-random number generated to create a secure hash value



Merkle Root Hash

Stores the hash of all information in block to enhance security

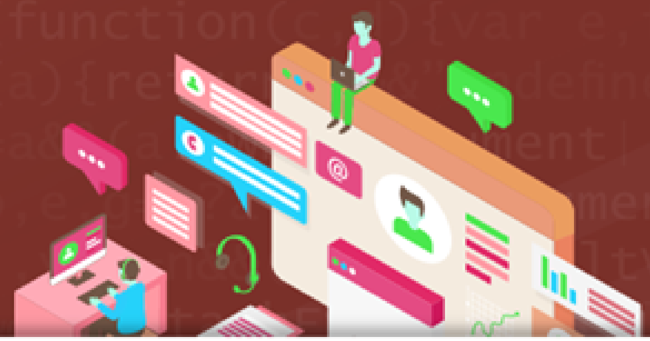
Difficulty

Decides the time taken to mine a block for rewards

Timestamp

A Unix timestamp of the creation of the block

Review and Analyze a Bitcoin Block on Explorer



Problem Statement: You must download the contents of a Bitcoin block and analyze the information in it using Explorer.

ASSISTED PRACTICE

Assisted Practice: Guidelines

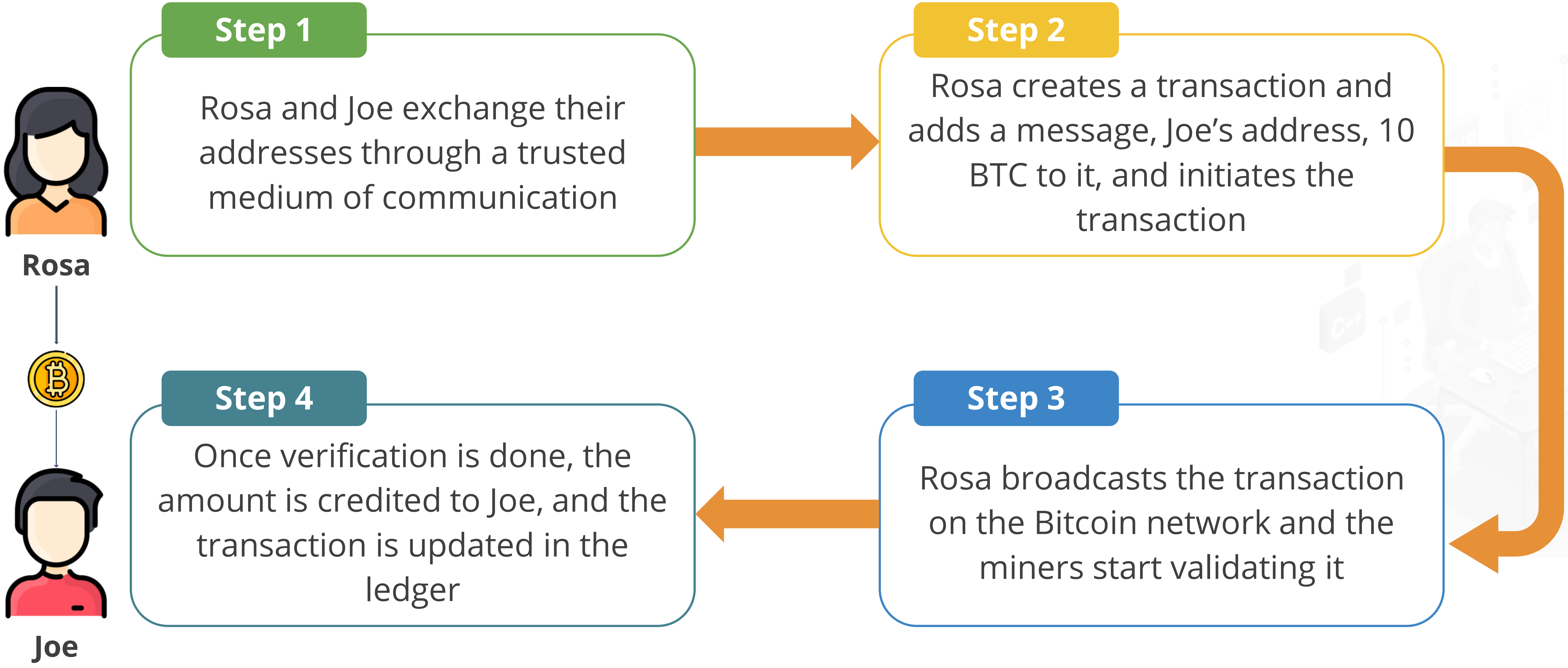
Steps to review and analyze a Bitcoin block on Explorer:

1. Reviewing the latest Bitcoin blocks

Bitcoin Transaction

Bitcoin Transaction

Scenario: Rosa wants to transfer 10 BTC to Joe.
These are the steps that occur for the transaction to be completed:



Rosa

Joe

Step 1

Rosa and Joe exchange their addresses through a trusted medium of communication

Step 2

Rosa creates a transaction and adds a message, Joe’s address, 10 BTC to it, and initiates the transaction

Step 3

Rosa broadcasts the transaction on the Bitcoin network and the miners start validating it

Step 4

Once verification is done, the amount is credited to Joe, and the transaction is updated in the ledger

Unspent Transaction Output (UTXO)

UTXO is the factor by which one determines the wallet balance of a user

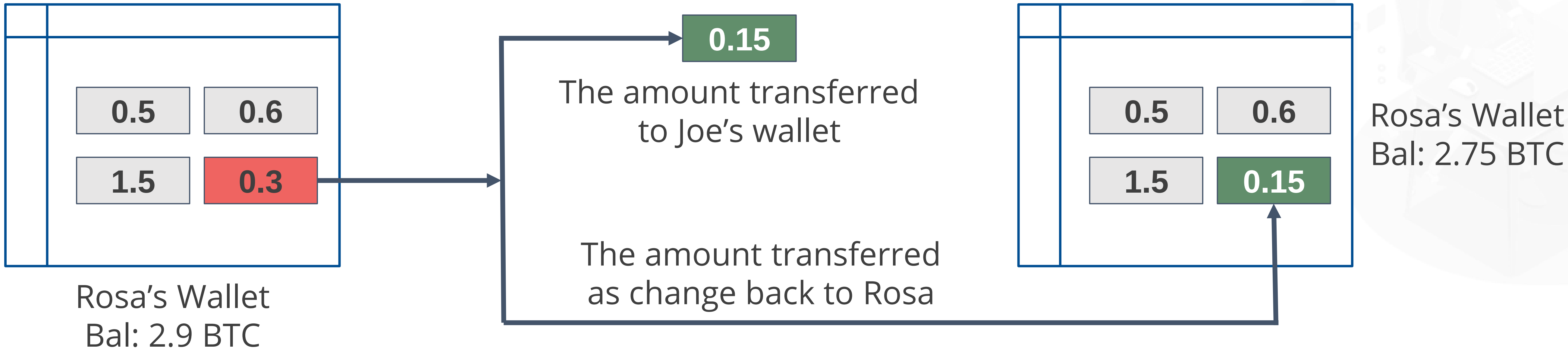
It is like a cheque or a coin. One cannot spend a partial amount of money, but instead must utilize the whole amount

Each UTXO represents a chain of ownership. The owner signs the transaction with his signature and transfers it to the recipient.

The UTXOs are all stored in a global register from which the miners can verify if the currency is legitimate or not

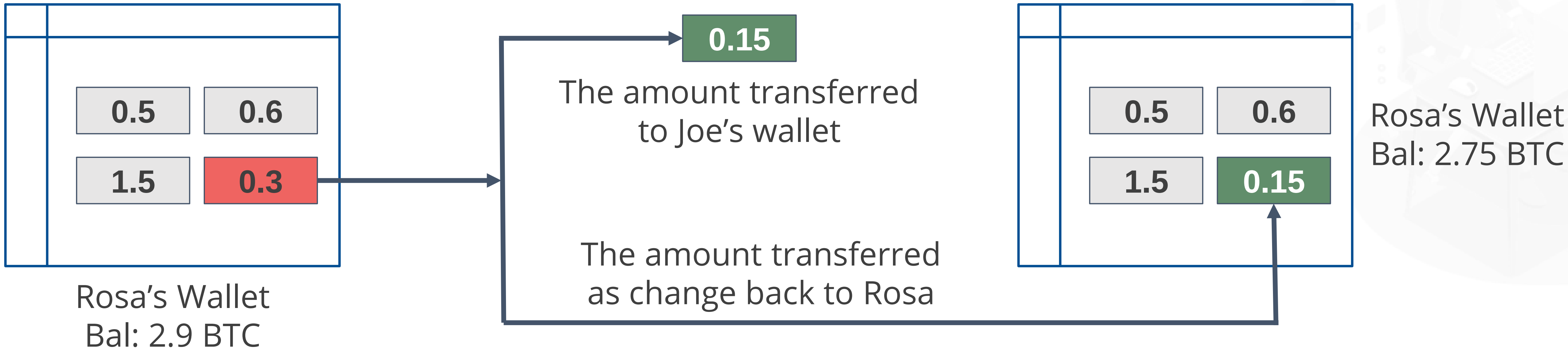
Unspent Transaction Output (UTXO)

- Let us consider an example where Rosa wants to transfer 0.15 BTC to Joe.
- The Bitcoin miners will look for the closest UTXO in amount.
- The whole UTXO will be entered into the transaction, breaking off into two parts.



Unspent Transaction Output (UTXO)

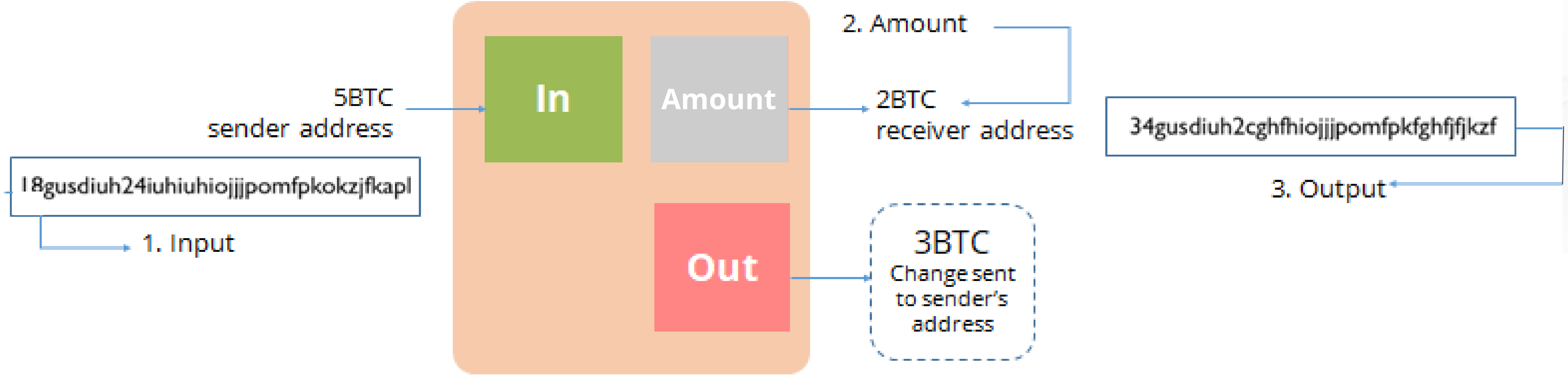
- The first part is 0.15 BTC that is to be transferred to Joe.
- The second part is the 0.15 BTC change that must be returned to Rosa.
- After the transaction is complete, Rosa's wallet will be updated with the 0.15 BTC and 0.3 BTC UTXO will be completely removed from the wallet to prevent double spend.



Blockchain Transaction Structure

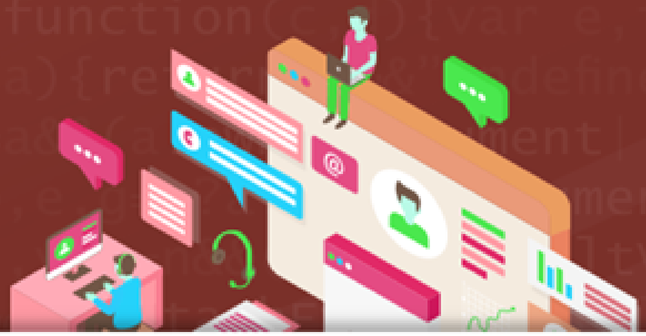
A Bitcoin transaction has three pieces of information:

- **Input**: This is a record of the Bitcoin addresses involved in the transaction
- **Amount**: The amount of Bitcoins that sender intends to transfer
- **Output**: The remaining amount of currency sent back to the sender as UTXO



5BTC
sender address
18gusdiuh24iuhiuhiojjjpomfpkokzjfkapl
1. Input
In
Amount
Out
2. Amount
2BTC
receiver address
34gusdiuh2cghfhiojjjpomfpkfghfjfjkzf
3. Output
3BTC
Change sent to sender's address

Analyze a Bitcoin Transaction



Problem Statement: You have to analyze a legacy Bitcoin transaction.

ASSISTED PRACTICE

Assisted Practice: Guidelines

Steps to analyze a Bitcoin transaction:

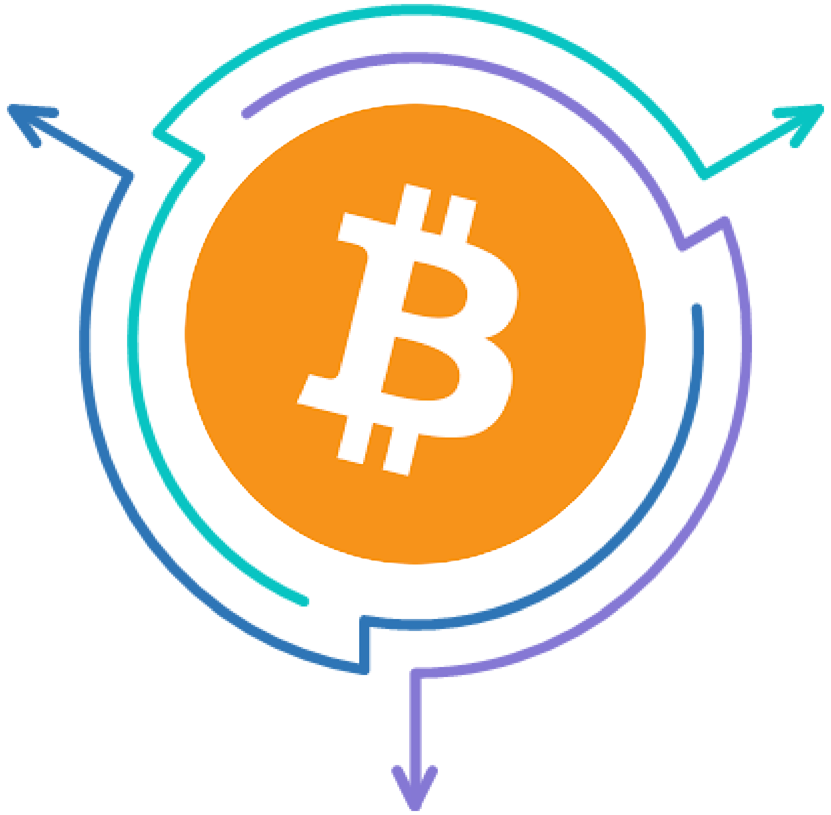
1. Reviewing the latest Bitcoin transactions

TECHNOLOGY

Bitcoin Scripts

Bitcoin Scripts

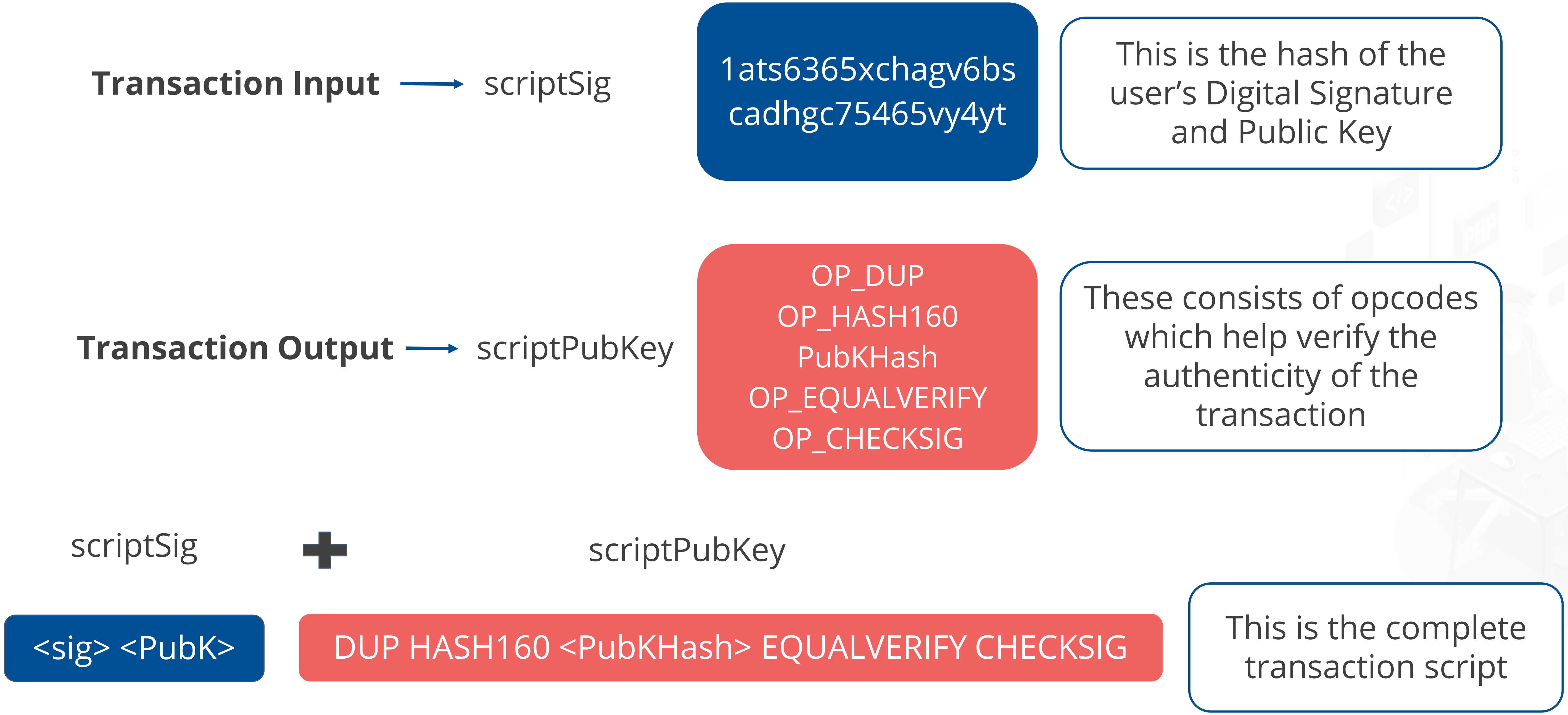
All Bitcoin transactions have scripts embedded into their inputs and outputs



Bitcoin script describes how a user can access the Bitcoin. Bitcoin script is a stack-based programming language like Forth.

A list of instructions are present with each transaction. Instructions in Bitcoin are composed of opcodes

Components of Bitcoin Scripts



Transaction Input → scriptSig

1ats6365xchagv6bs cadhgc75465vy4yt

This is the hash of the user’s Digital Signature and Public Key

Transaction Output → scriptPubKey

OP_DUP
OP_HASH160
PubKHash
OP_EQUALVERIFY
OP_CHECKSIG

These consists of opcodes which help verify the authenticity of the transaction

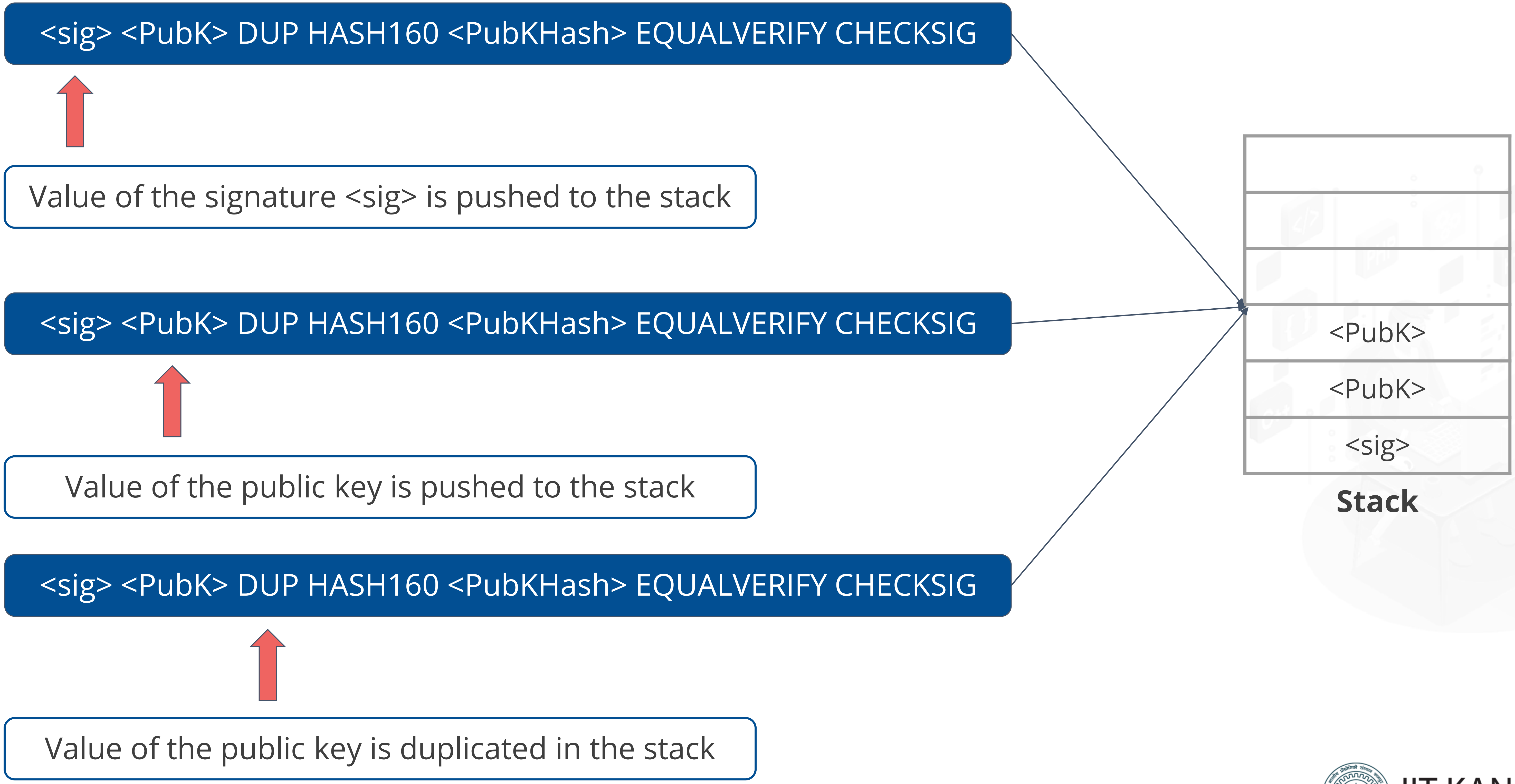
scriptSig ➕ scriptPubKey

<sig> <PubK>

DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG

This is the complete transaction script

Bitcoin Transaction Script Execution



<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG

Value of the signature <sig> is pushed to the stack

<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG

Value of the public key is pushed to the stack

<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG

Value of the public key is duplicated in the stack

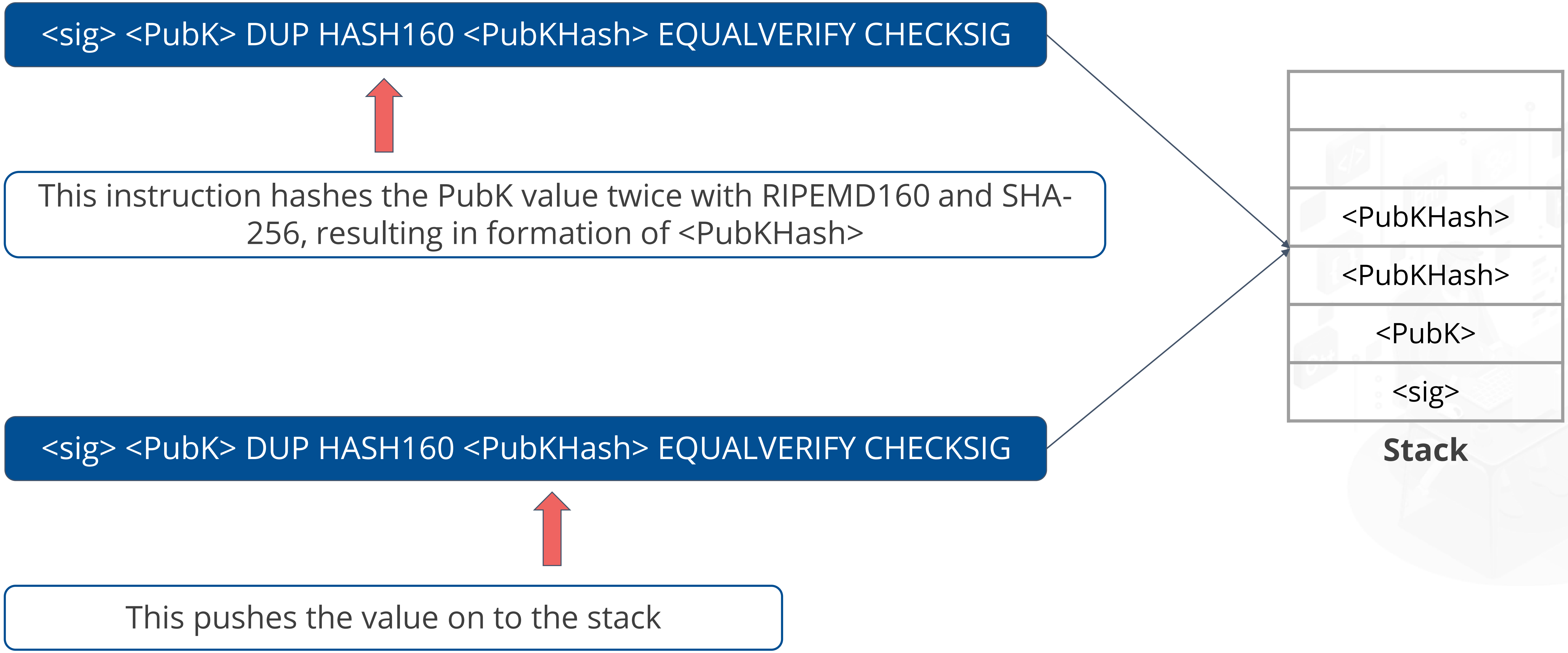
<PubK>

<PubK>

<sig>

Stack

Bitcoin Transaction Script Execution



<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG

This instruction hashes the PubK value twice with RIPEMD160 and SHA-256, resulting in formation of <PubKHash>

<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG

This pushes the value on to the stack

<PubKHash>

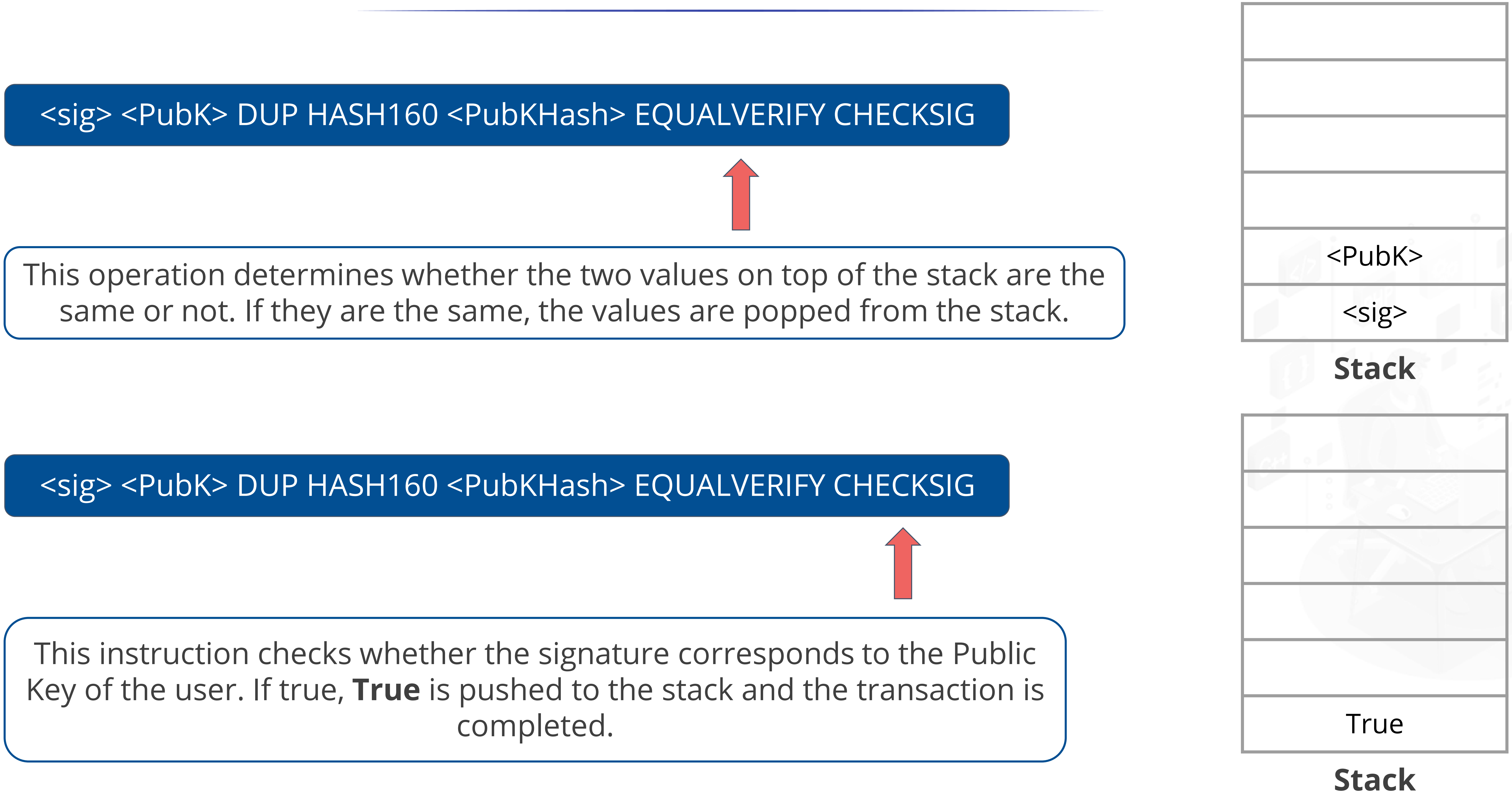
<PubKHash>

<PubK>

<sig>

Stack

Bitcoin Transaction Script Execution



<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG

This operation determines whether the two values on top of the stack are the same or not. If they are the same, the values are popped from the stack.

<PubK>
<sig>

Stack

<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG

This instruction checks whether the signature corresponds to the Public Key of the user. If true, **True** is pushed to the stack and the transaction is completed.

True

Stack

TECHNOLOGY

Bitcoin Network

Bitcoin Networks

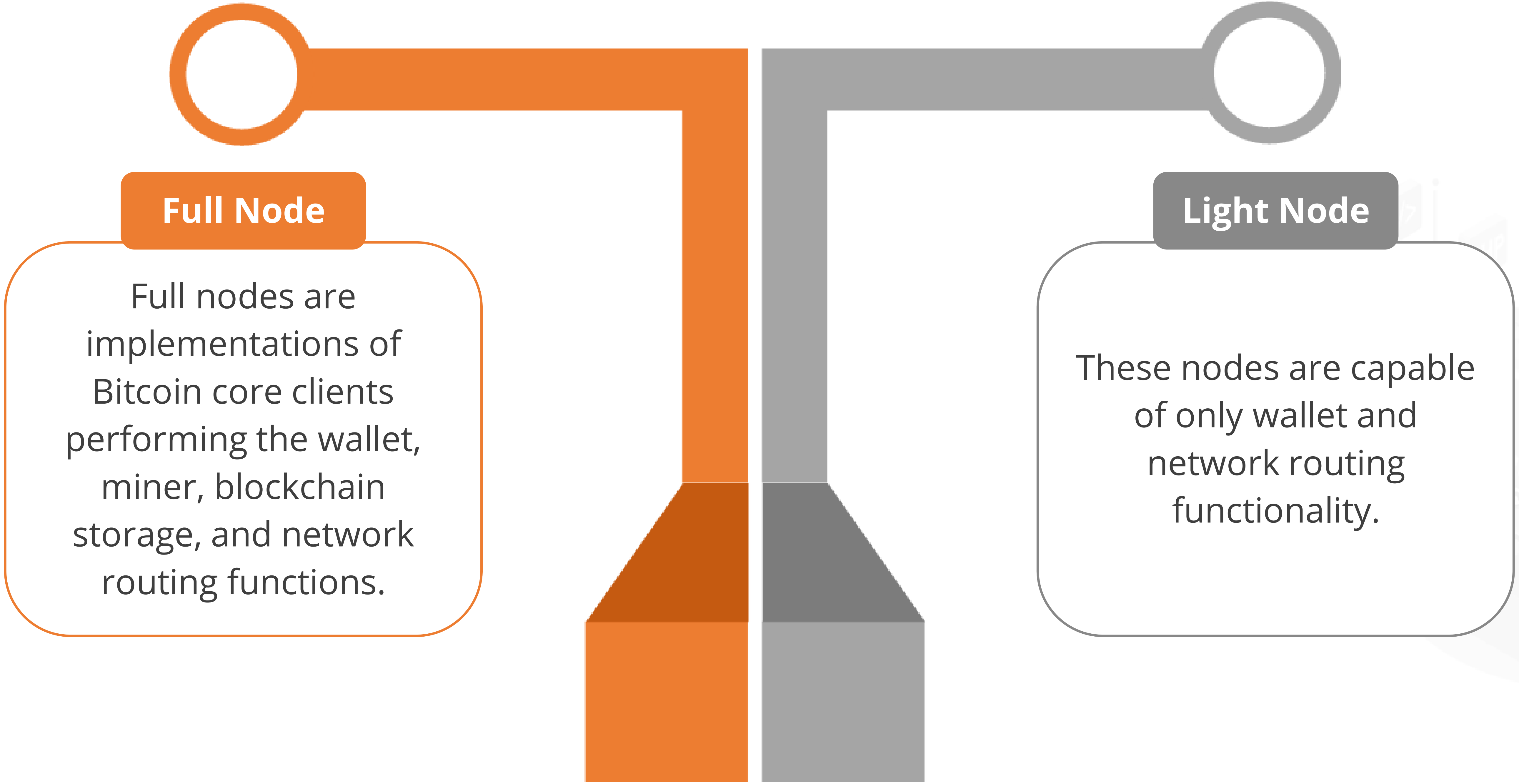
Main Network

The actual network on which all the cryptocurrency exchanges and transactions are conducted.

Test Network

This is a network which mimics the behavior of the main network and is used to test new applications and scripts.

Bitcoin Nodes



Full Node

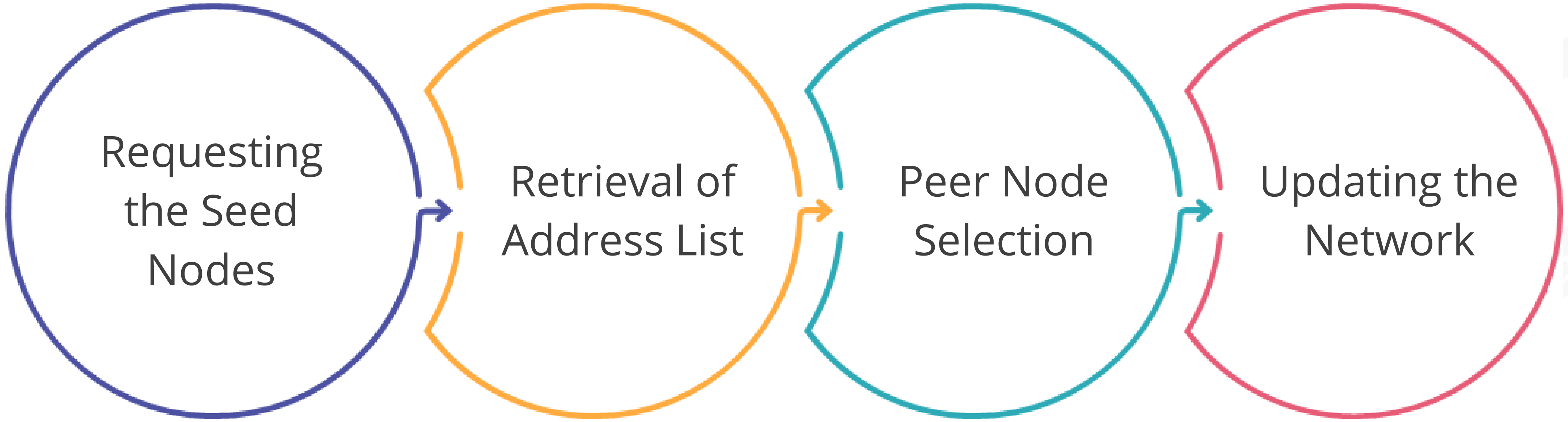
Full nodes are implementations of Bitcoin core clients performing the wallet, miner, blockchain storage, and network routing functions.

Light Node

These nodes are capable of only wallet and network routing functionality.

Joining the Bitcoin Network

Following are the steps performed to join the Bitcoin network as an active node (miner):



Requesting the Seed Nodes

Retrieval of Address List

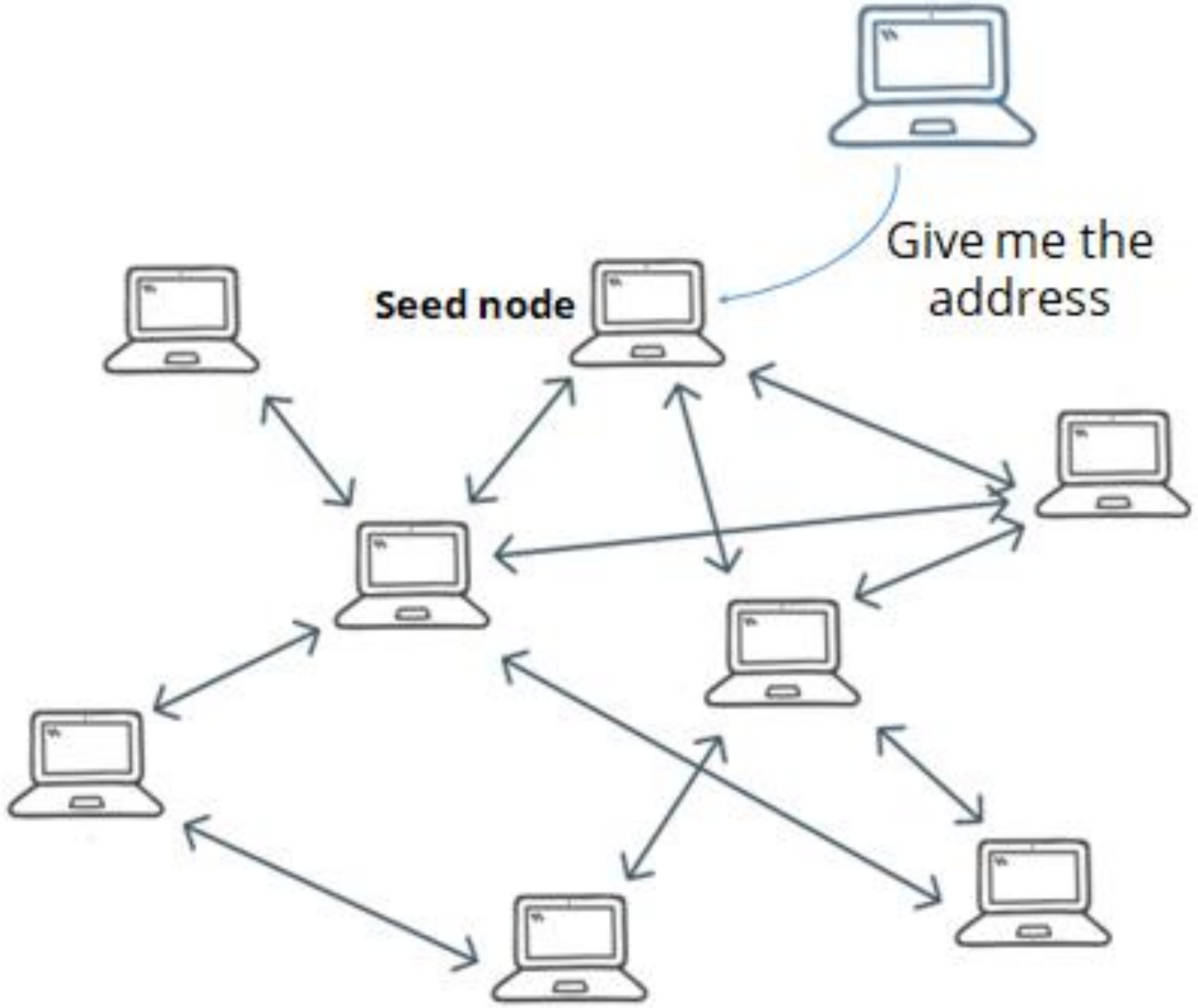
Peer Node Selection

Updating the Network

Joining the Bitcoin Network

Step 1: Requesting the Seed Nodes

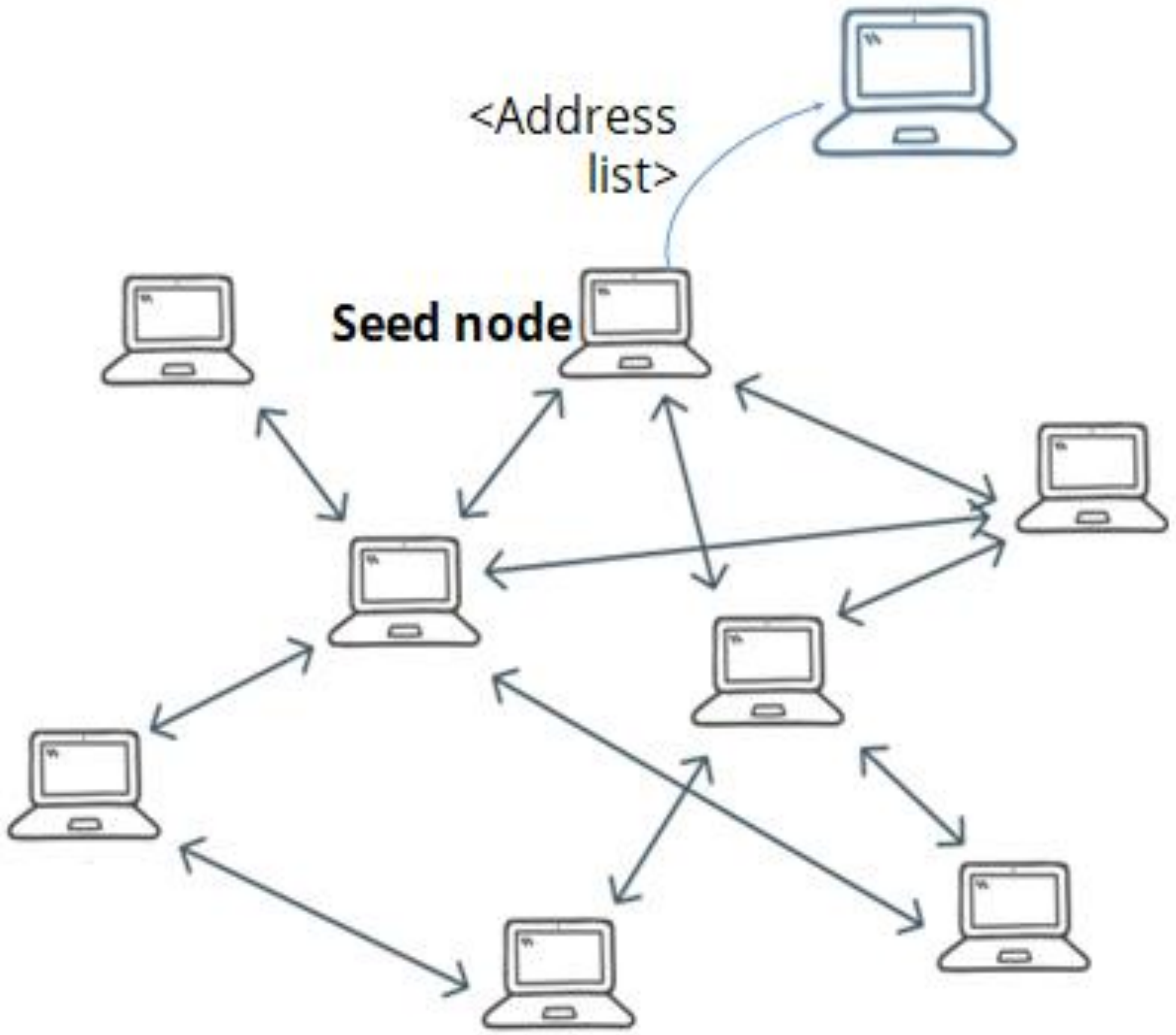
There are certain special nodes in the Bitcoin network called seed nodes which have list of all the active (full) nodes. New joining nodes ask for the list of addresses from the seed node.



Joining the Bitcoin Network

Step 2: Retrieval of Address List

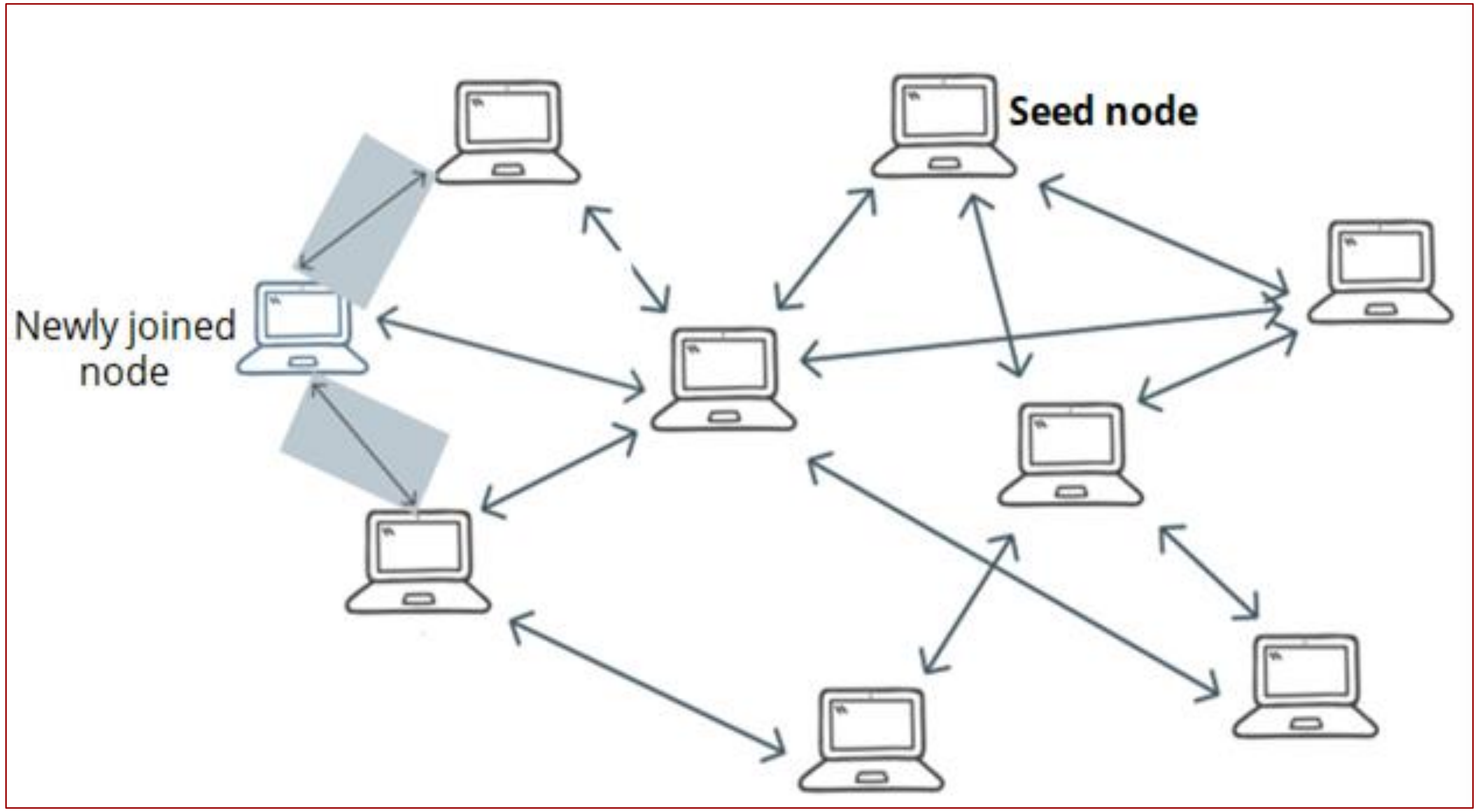
In response to the node's request to join the network, the seed node sends them the address list.



Joining the Bitcoin Network

Step 3: Peer Node Selection

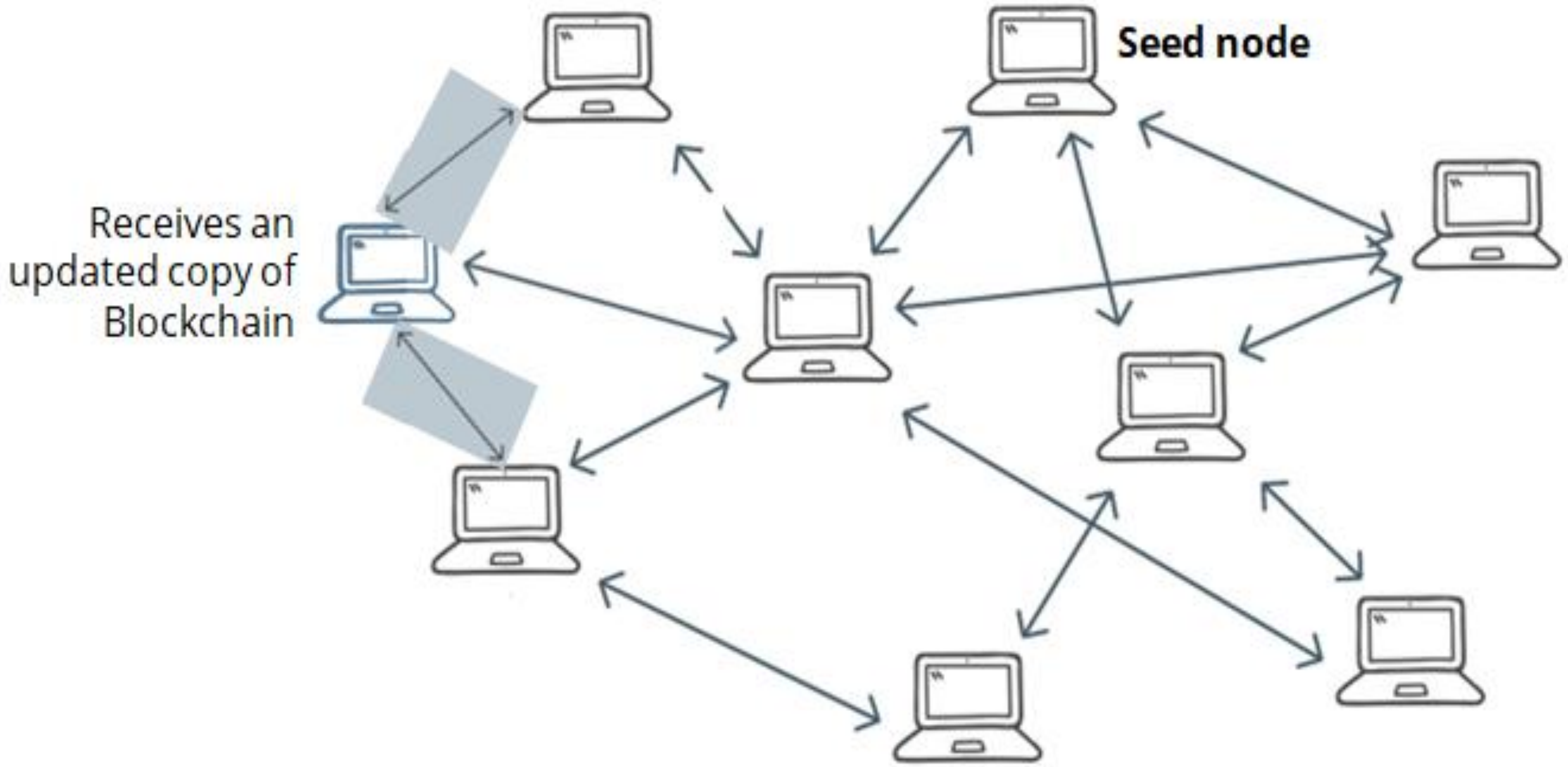
Joining node selects an address from the list and requests to join the network.



Joining the Bitcoin Network

Step 4: Updating the Network

Newly joined node then gets the most recent copy of Blockchain from its peers.

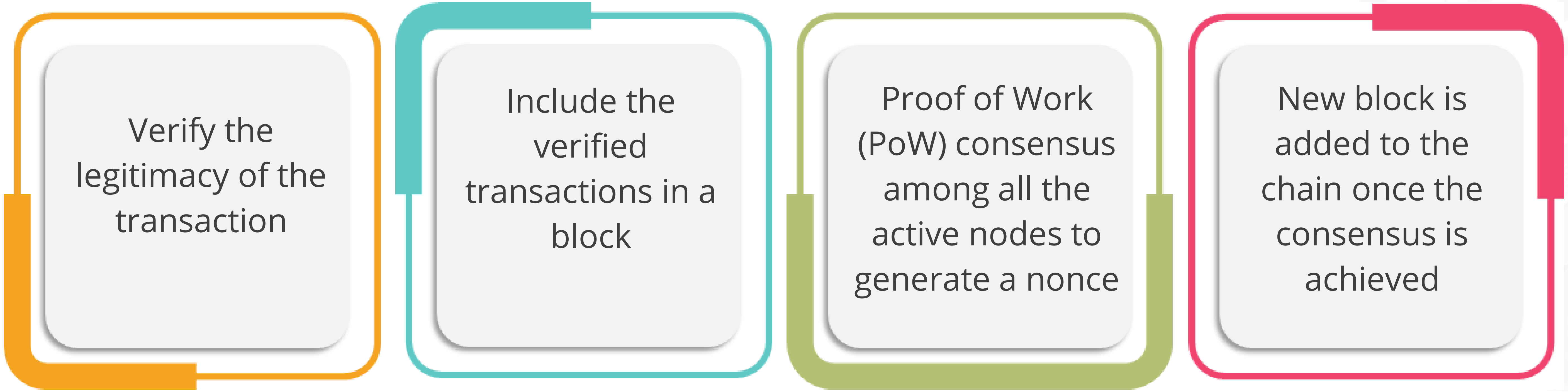


TECHNOLOGY

Bitcoin Mining

Bitcoin Mining

Bitcoin mining is the process of creating new Bitcoins by solving complex mathematical problems. Following are the steps performed during bitcoin mining:



Verify the legitimacy of the transaction

Include the verified transactions in a block

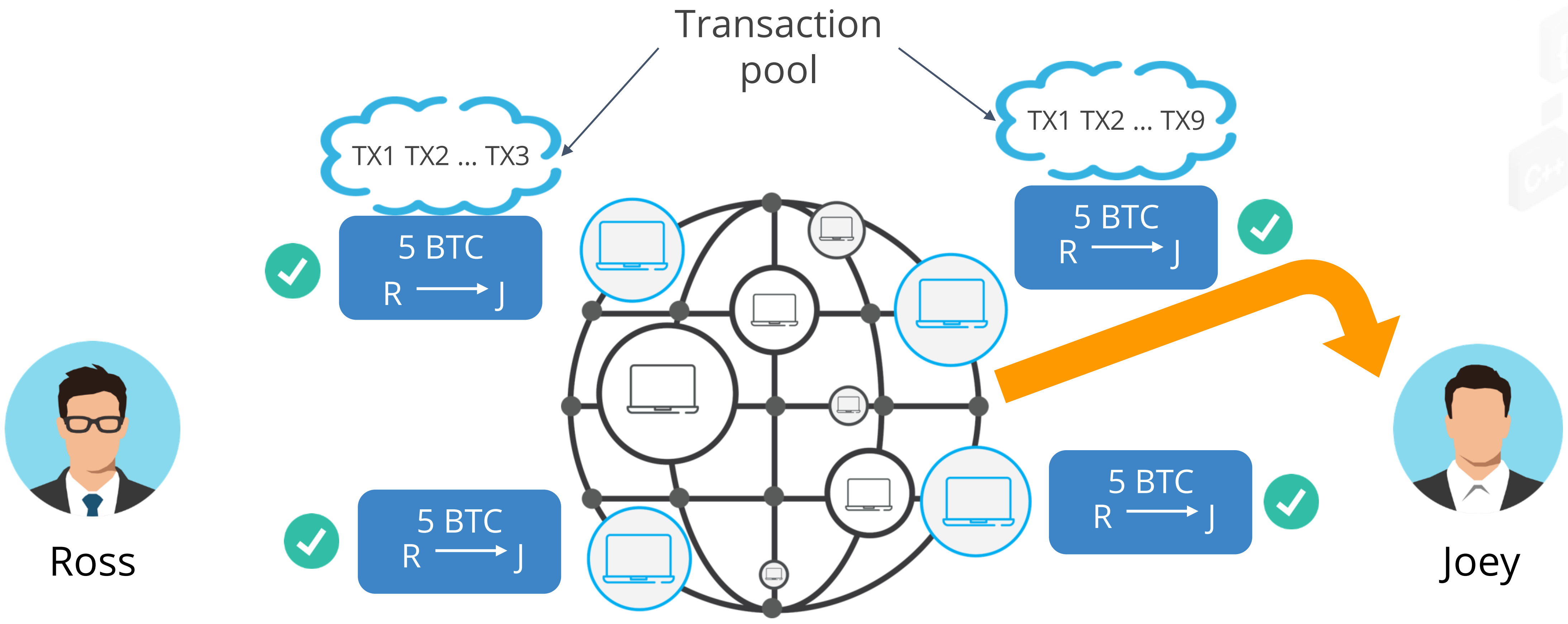
Proof of Work (PoW) consensus among all the active nodes to generate a nonce

New block is added to the chain once the consensus is achieved

Bitcoin Mining

Step 1: Transaction Verification and Inclusion

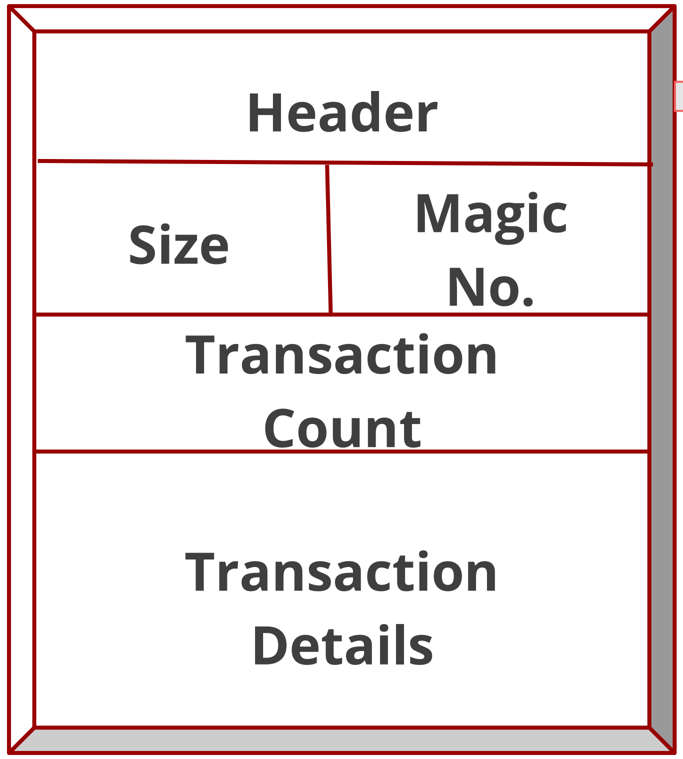
- Each node that receives the transaction copy verifies the transaction.
- All validated transactions get stored in a pool called mempool.
- Miners then bundle these transactions to the candidate block.



Bitcoin Mining

Step 2: PoW Consensus

- Miners now start looking for a nonce value to generate block hash that requires certain leading zeros.
- Miners construct the block and block header that contains version, merkle root, previous block hash, difficulty target, and nonce.

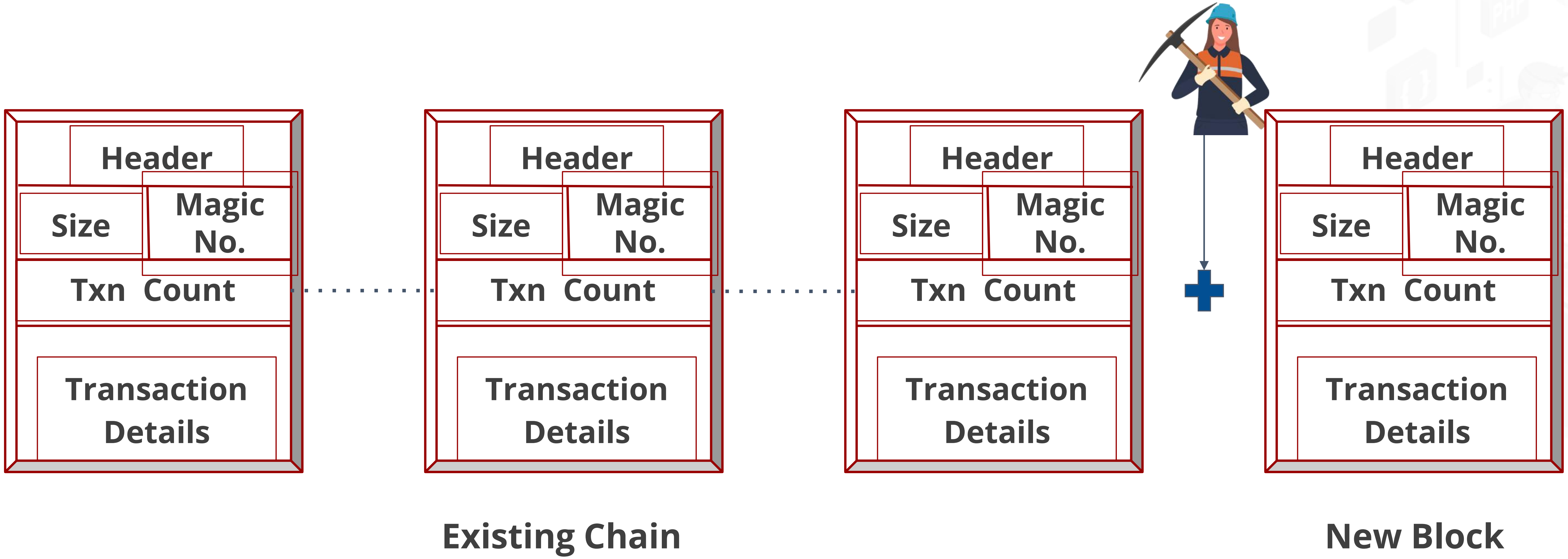


- Root of previous hash
- Merkle tree root
- Nonce
- Difficulty
- Version
- Timestamp

Bitcoin Mining

Step 3: Creation of New Block

Once miners create a new block, it gets added to the blockchain network.



Powered by simplilearn

IIT KANPUR
Indian Institute of Technology, Kanpur

Key Takeaways

- Bitcoin is a crypto-currency introduced in 2009 and consists of various elements such as miners and wallets.
- There are four different types of wallets: hardware, software, desktop, and mobile.
- Bitcoin scripts consist of the scriptSig and scriptPubKey along with the opcodes.
- Anyone can join the Bitcoin network as a miner by following four steps and can help verify transactions.

Conduct a Transaction Using Electrum Wallet

You must install Electrum software wallet and perform a transaction. Perform the following steps:

1. Download and set up the Electrum software wallet
2. Create a new Electrum wallet
3. Perform a transaction of Bitcoins using the Electrum wallet

LESSON-END PROJECT