# Introduction

# Who we are


Winners of Microsoft x2,
IBM, WAVES, Blockchain
Founder x2 Binary
District hackathons

Fullstack developers (Node.JS, React.js, ASP.NET, Xamarin and others)
MSP (Microsoft Student Partners)
Solidity developers (BANKEX)

Have courses and
master classes  (HSE,
Bauman University,
MSU and some others)

# About

# About

# Why?

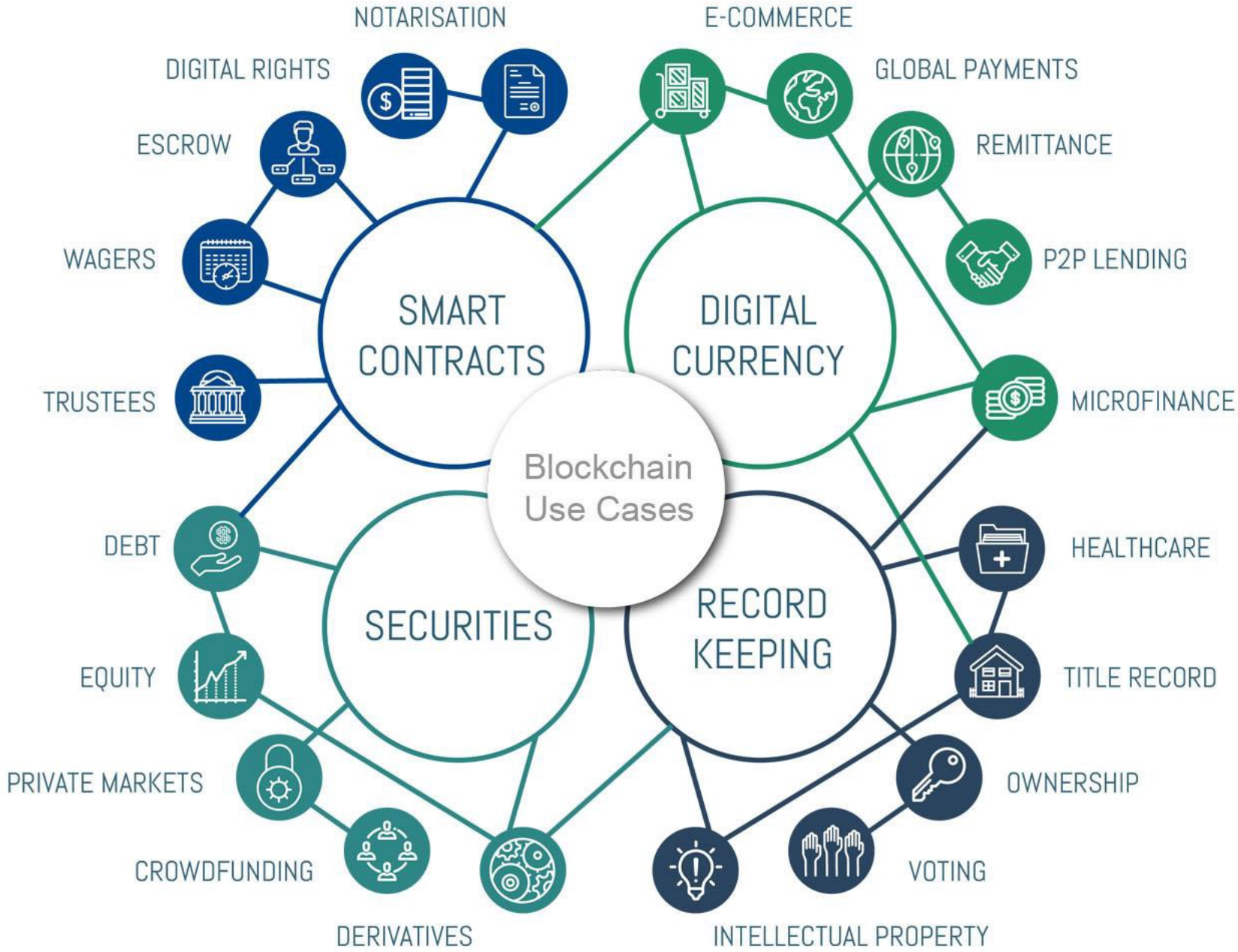
# Some Use Cases As Example

# Crowdfunding

# Exchange Data Between Corporations

# Secure Voting Solutions

# P2P Payments


Blockchain Use Cases
SMART CONTRACTS
DIGITAL CURRENCY
SECURITIES
RECORD KEEPING
NOTARISATION
DIGITAL RIGHTS
ESCROW
WAGERS
TRUSTEES
E-COMMERCE
GLOBAL PAYMENTS
REMITTANCE
P2P LENDING
MICROFINANCE
DEBT
EQUITY
PRIVATE MARKETS
CROWDFUNDING
DERIVATIVES
HEALTHCARE
TITLE RECORD
OWNERSHIP
VOTING
INTELLECTUAL PROPERTY

# So, That's Why

# Let’s Start From Our Plan

## Today

Understanding of basics (PoW, Merkle tree, CAP and e.t.c)

Ethereum Solidity introduction on practice

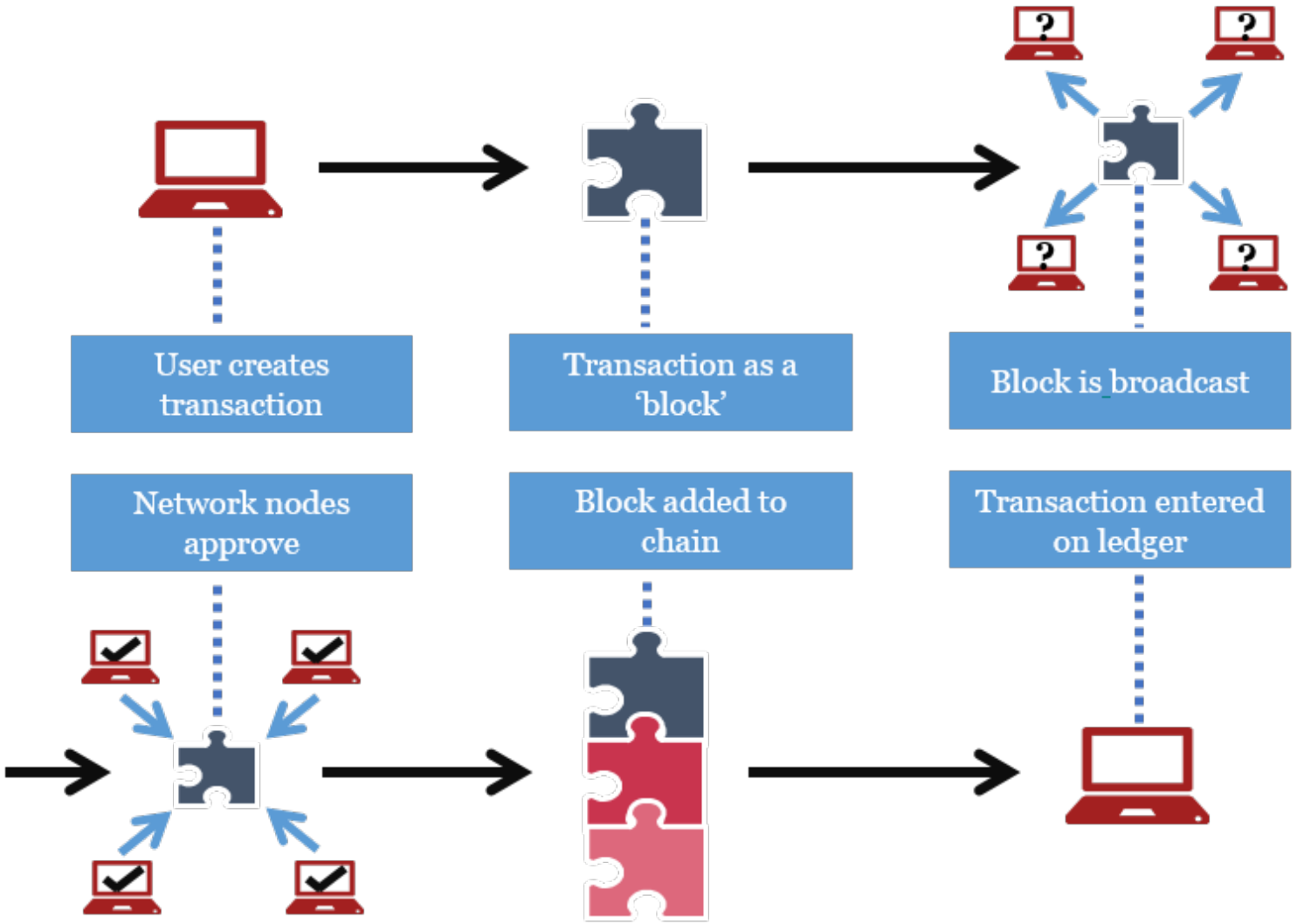
## Tomorrow

Ethereum Solidity practice on some cases

Making DApp with web3.js

Best backend practices from DevOps position for DApps

# Abstract Blockchain




Transaction

Block

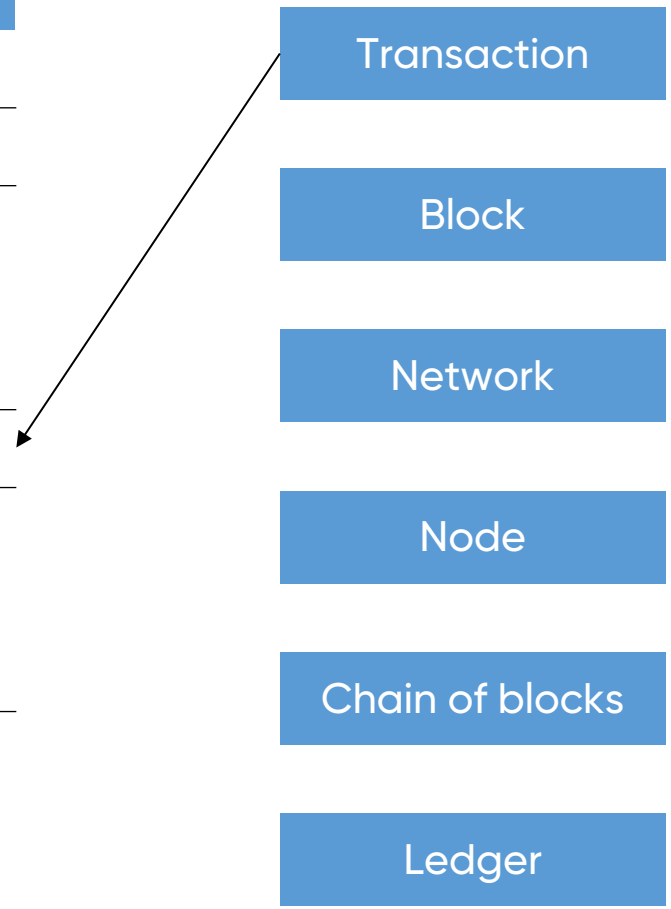
Network

Node

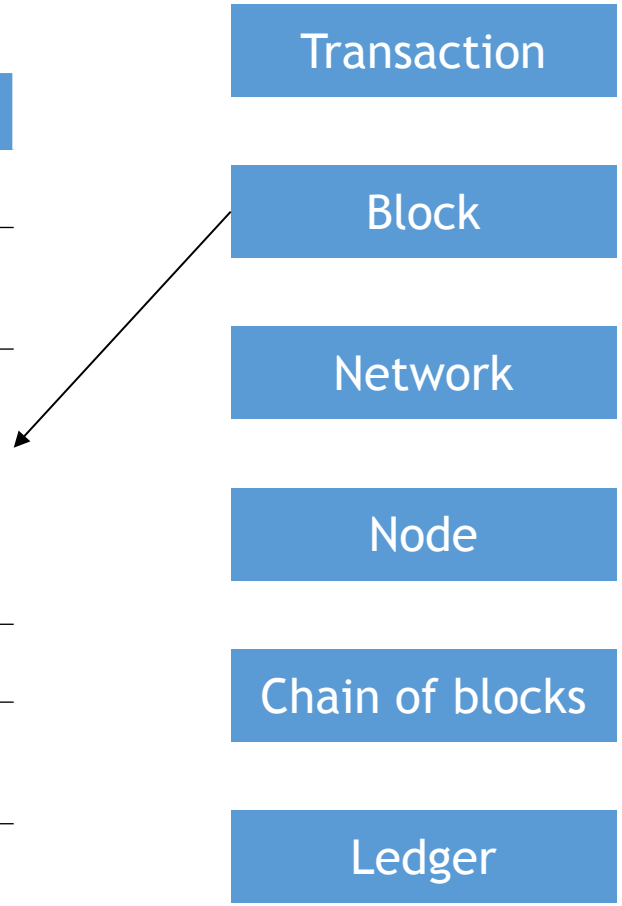
Chain of blocks

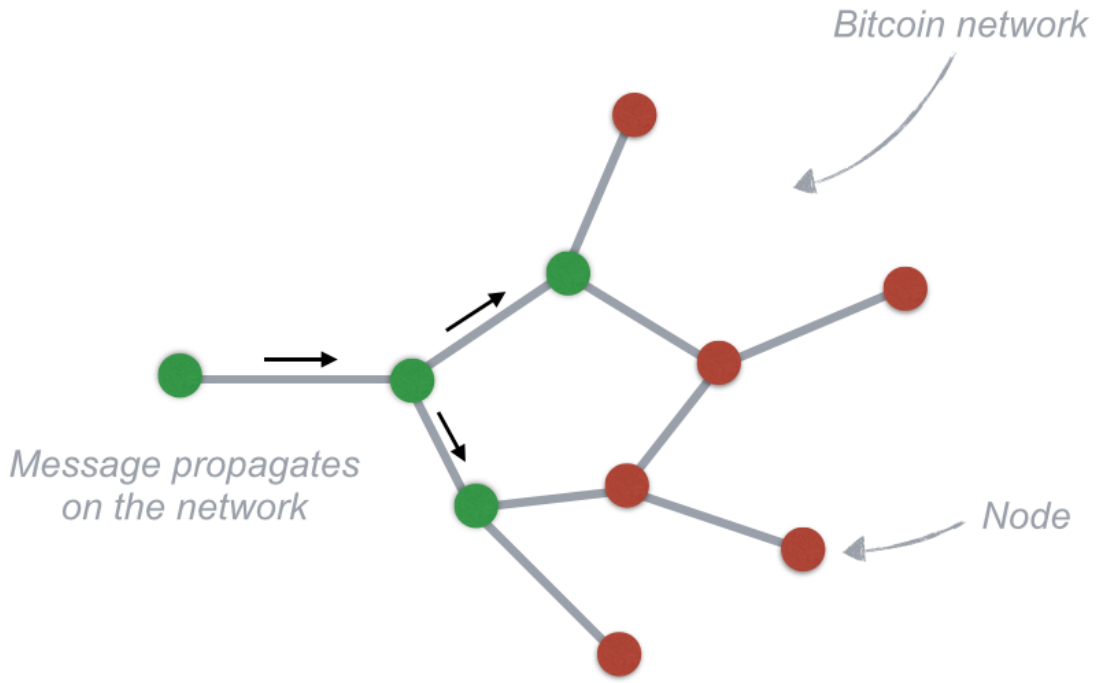
Ledger

| Field | Description | Size |
|---|---|---|
| Version nomber | Is 1 now | 4 bytes |
| In-counter | Positive integer VI = VarInt | 1 – 9 bytes |
| List of inputs | The first input of the first transaction is also called "coinbase" (its content was ignored in earlier versions) | Depends on inputs |
| Out-counter | Positive integer VI = VarInt | 1 – 9 bytes |
| List of outputs | The outputs of the first transaction spend the mined bitcoins for the block | Depends on outputs |
| Lock time | if non-zero and sequence numbers are<0xFFFFFFFF: block height or timestamp when transaction is final | 4 bytes |



| Field | Description | Size |
|---|---|---|
| Magic number | value always 0xD9B4BEF9 | 4 bytes |
| Blocksize | Number of bytes following up to end of block | 4 bytes |
| Blockheader | 6 items :<br>Version, hashPrevBlock, hashMerkleRoot, Time, Bits, Nonce | 80 bytes |
| Transaction counter | Positive integer VI = VarInt | 1 – 9 bytes |
| Transactions | List of transactions (non empty) | A lot of bytes |






Transaction

Block

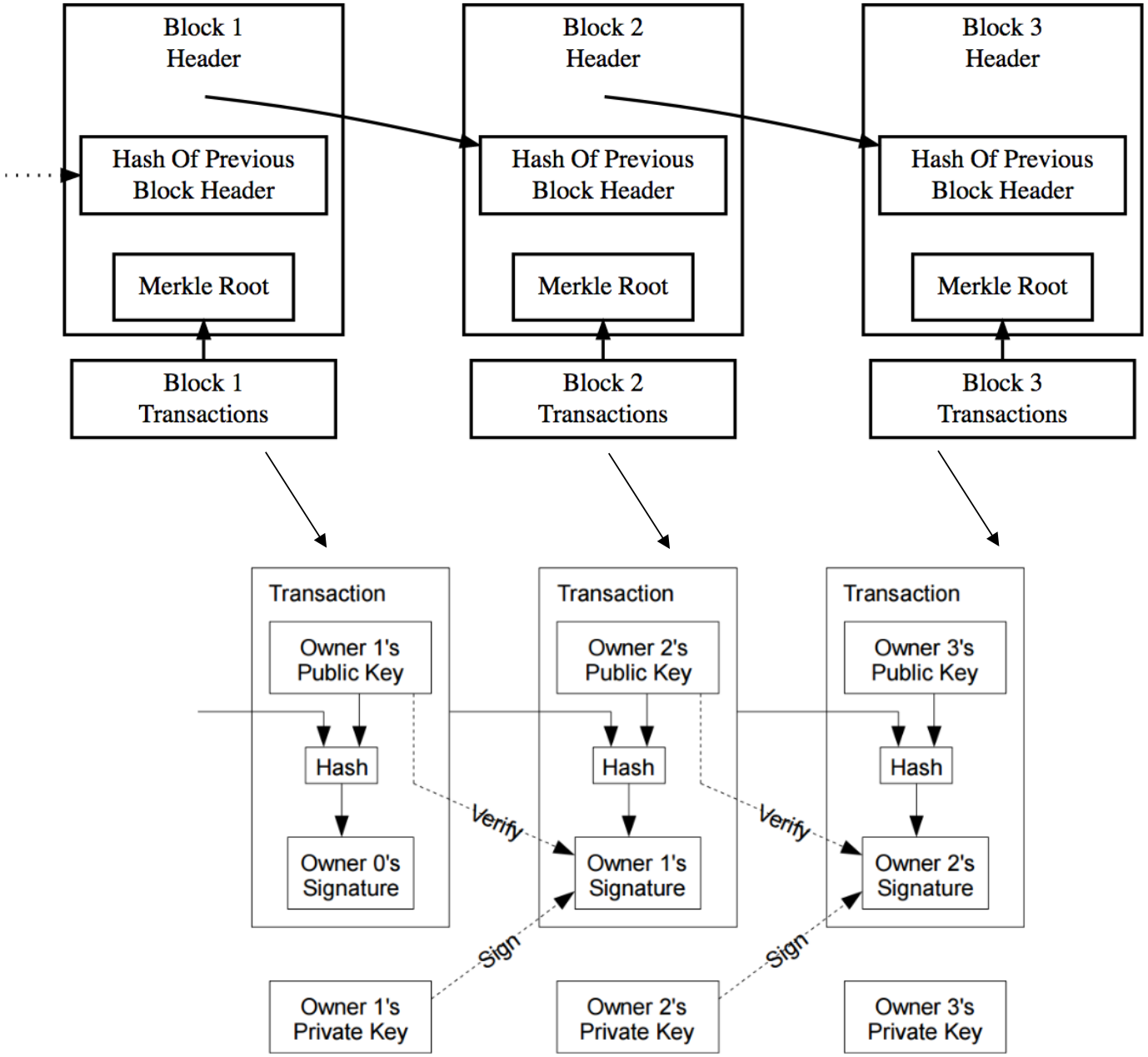
Network

Node

Chain of blocks

Ledger

Any computer that connects to the Bitcoin network is called a node.




Transaction

Block

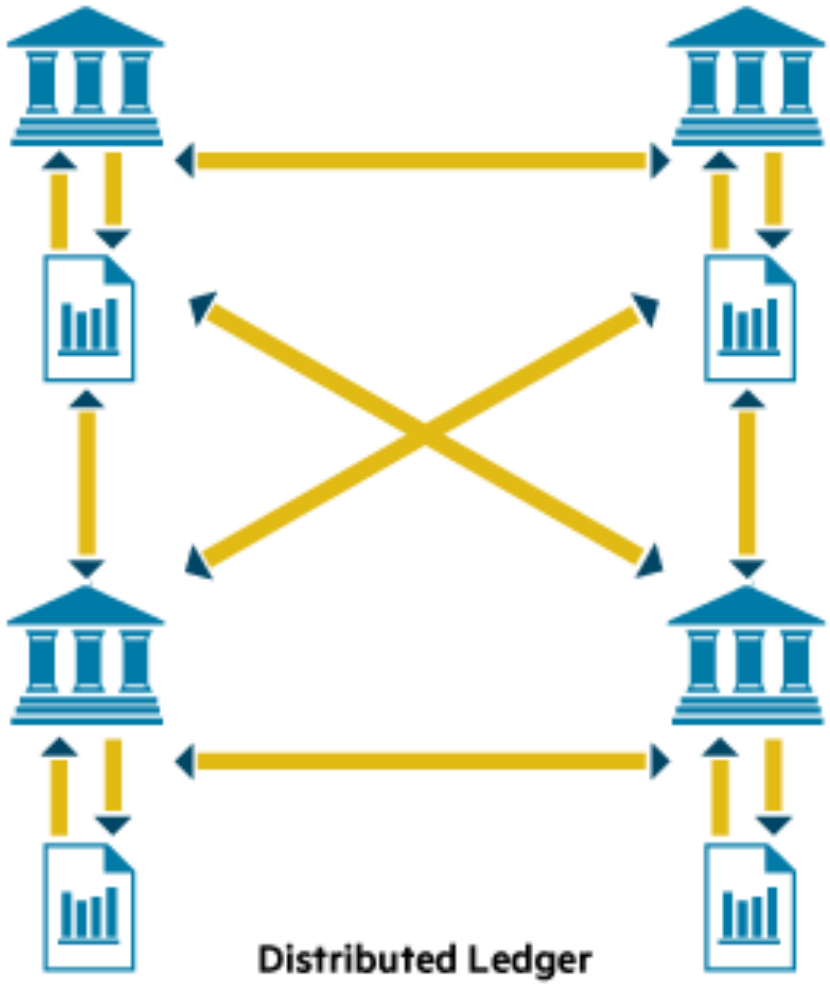
Network

Node

Chain of blocks

Ledger

steemit.com




Transaction

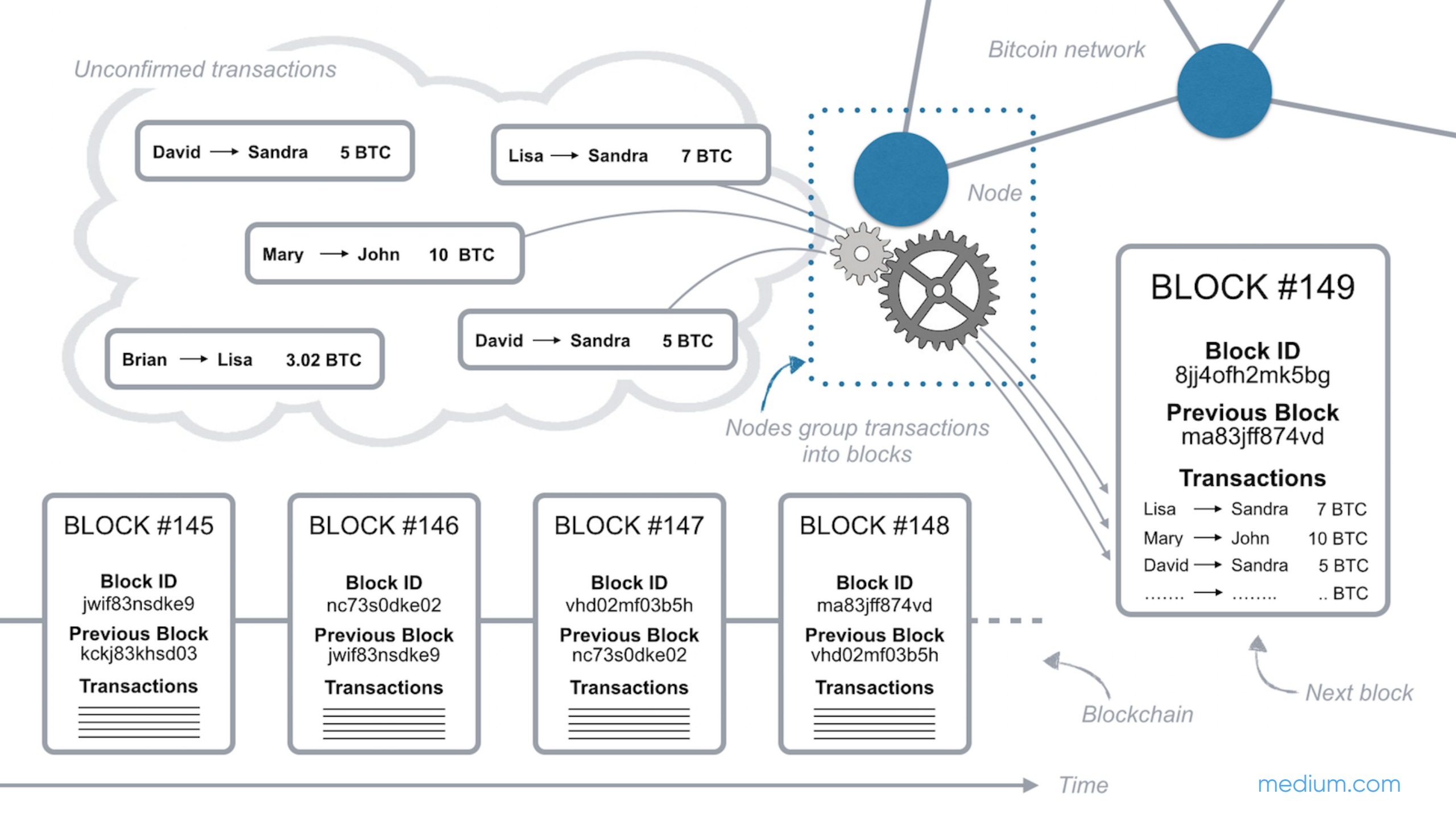
Block

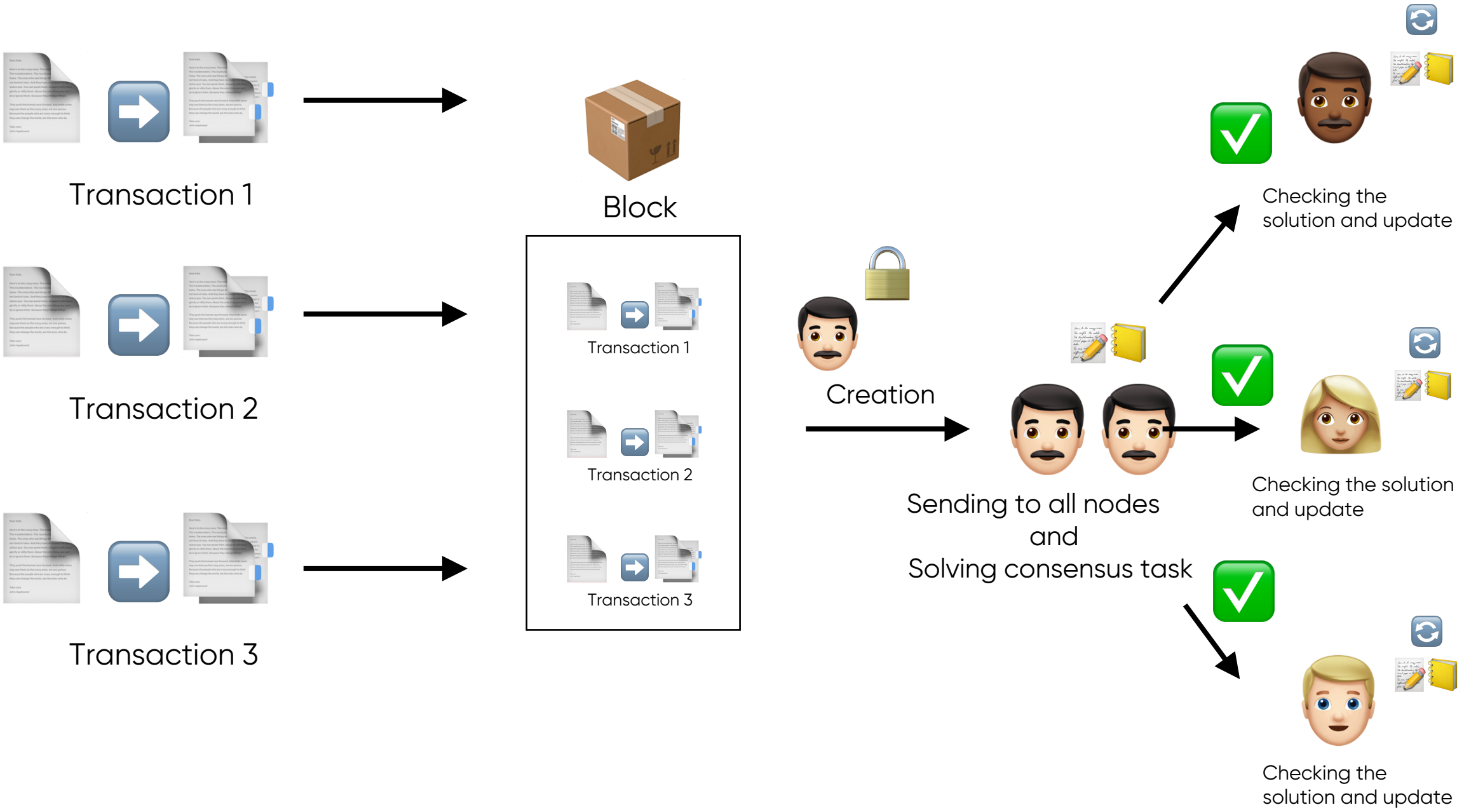
Network

Node

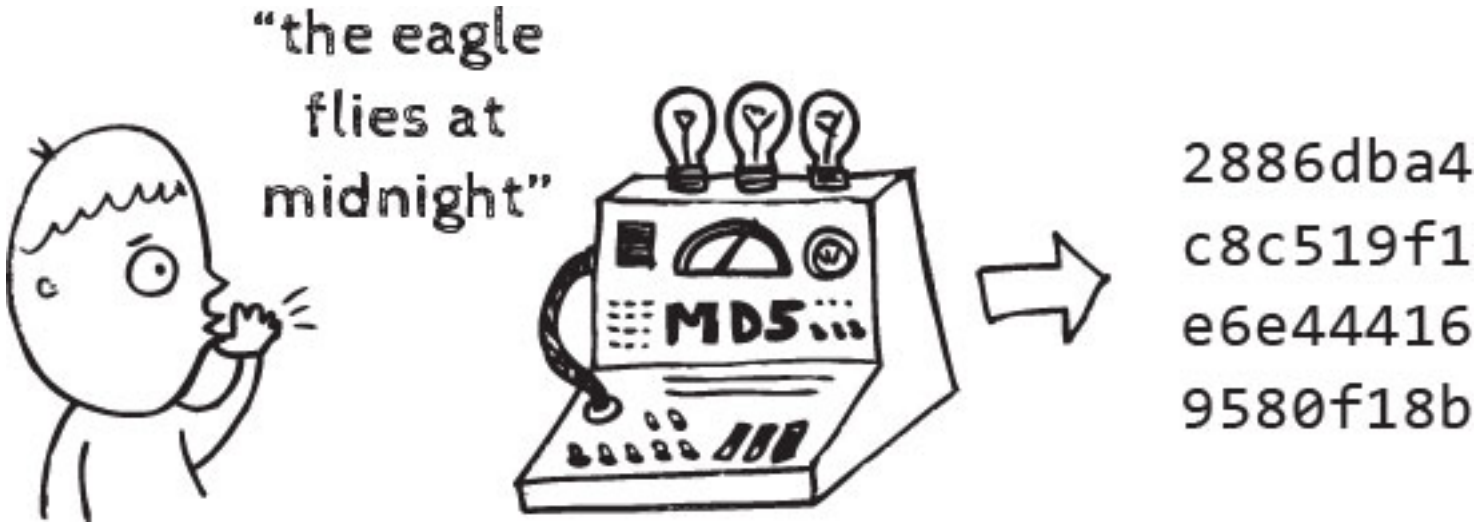
Chain of blocks

Ledger


Unconfirmed transactions
David → Sandra 5 BTC
Lisa → Sandra 7 BTC
Mary → John 10 BTC
David → Sandra 5 BTC
Brian → Lisa 3.02 BTC
Bitcoin network
Node
Nodes group transactions into blocks
BLOCK #149
Block ID
8jj4ofh2mk5bg
Previous Block
ma83jff874vd
Transactions
Lisa → Sandra 7 BTC
Mary → John 10 BTC
David → Sandra 5 BTC
..... → ..... .. BTC
BLOCK #145
Block ID
jwif83nsdke9
Previous Block
kckj83khsd03
Transactions
BLOCK #146
Block ID
nc73s0dke02
Previous Block
jwif83nsdke9
Transactions
BLOCK #147
Block ID
vhd02mf03b5h
Previous Block
nc73s0dke02
Transactions
BLOCK #148
Block ID
ma83jff874vd
Previous Block
vhd02mf03b5h
Transactions
Blockchain
Next block
Time
medium.com


Transaction 1
Transaction 2
Transaction 3
Block
Transaction 1
Transaction 2
Transaction 3
Creation
Sending to all nodes
and
Solving consensus task
Checking the
solution and update
Checking the solution
and update
Checking the
solution and update

# Hash Functions



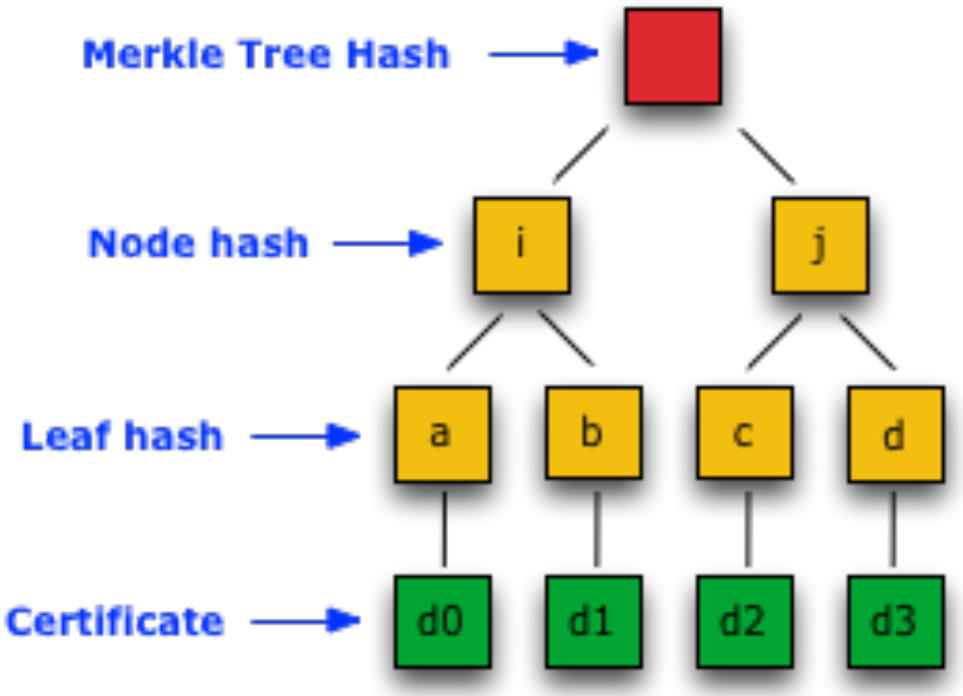
Hello  185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969

hello  2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

2cf24dba5fb0a30e26e83b2ac5b9e29
e1b161e5c1fa7425e73043362938b9824  d7914fe546b684688bb95f4f888a92dfc680603a75f23eb823658031fff766d9

Hello MSU students  ea526da0ea9e2f472afbdb647ffad0cd63567f59fb9a4bfa12429f5dbfed5c1e

# Merkle tree




KECCAK In Ethereum

# PoW

“hello world!” = J  and X = “0
We have :

H("Hello, world!0")=1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64

Find X such that when we append X to J
We will have:

H("JX")=

0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

# CAP

Consistency

Согласованность данных

Availability

Доступность

Partition tolerance

Устойчивость к разделению

**Can't have all three!**

# Ethereum

contract Option {

trikePrice = $50

holder = Alice

seller = Bob

asset = 100 shares of Acme Inc.

expiryDate = June 1st, 2016

function exercise ( ) {

If Message Sender = holder, and

If Current Date<expiryDate, then

holder send($5,000) to seller, and

seller send(asset) to holder

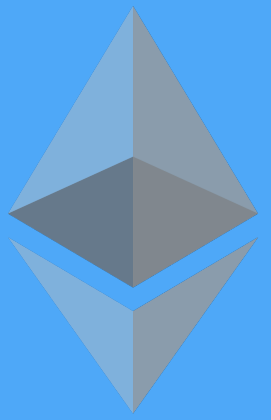
}}

Public

Blockchain-based
distributed computing platform

Features smart contract
(scripting) functionality

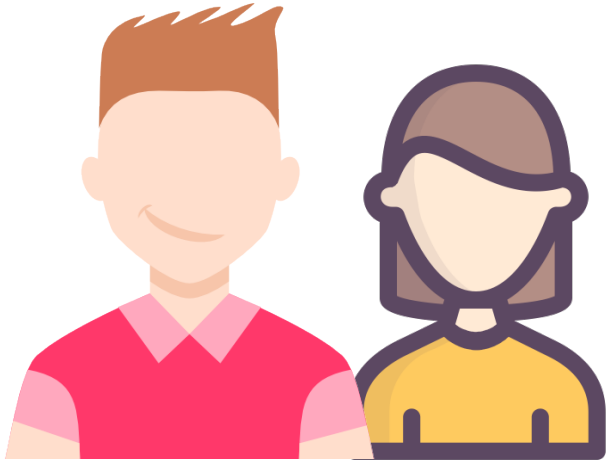
Open-source



ethereum

# Two types of accounts


Controlled by code



Controlled by humans

# Solidity

# remix.ethereum.org