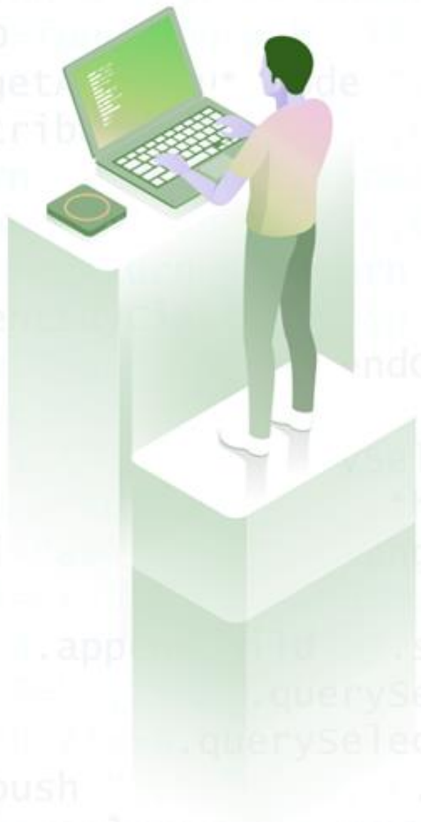
TECHNOLOGY

IIT KANPUR
Indian Institute of Technology, Kanpur

Professional Certification Program in Blockchain



Blockchain Pillars

TECHNOLOGY

Introduction to Blockchain Pillars

Learning Objectives

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

- Implement cryptographic algorithms
- Understand hashing and digital signing
- Execute Consensus algorithms
- Identify distributed ledger

Introduction to Blockchain Pillars

Three pillars of Blockchain technology:

Introduction to Blockchain Pillars

Cryptography

The science of making information secure to send it across two or more parties. Ciphers are used to encrypt data and a secret key is used for decryption.

Consensus

A method to ensure the nodes on a network verify the transactions and agree with their order and existence on a ledger to prevent double spending.

Distributed Ledger

A database of replicated, shared, and synchronized digital data geographically spread across countries, institutions, or multiple sites and accessible by multiple people.

TECHNOLOGY

Cryptography

Introduction to Cryptography

Information exchange without cryptography:

Hello User B

User A

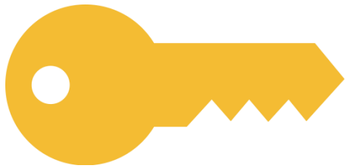
User B

Introduction to Cryptography

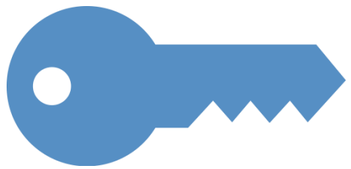
Information exchange with cryptography:

Keys in Cryptography

Keys in cryptography are used to secure the information. There are two types of keys:



Public Key



Private Key

Public Key

Public Key

- A public key is a publicly available cryptographic key that can be obtained and used by anyone to send the encrypted messages to a particular recipient.
- No one else would be able to decrypt the message because the corresponding private key is held securely by the intended recipient.
- Once the public key encrypted message is received, the recipient can decrypt the message using a second (private) key.

Private Key

Private Key

- A private key is a highly secure variable that is randomly generated and kept secretly by the owner of the key.
- It needs to be protected and no unauthorized access should be granted to it.
- It is used in cryptography with algorithms to encrypt and decrypt the data.

Generate Public and Private Keys

Problem Statement: You are given a task to generate public and private keys.

ASSISTED PRACTICE

Assisted Practice: Generate Public and Private Keys- Steps

Steps to perform:

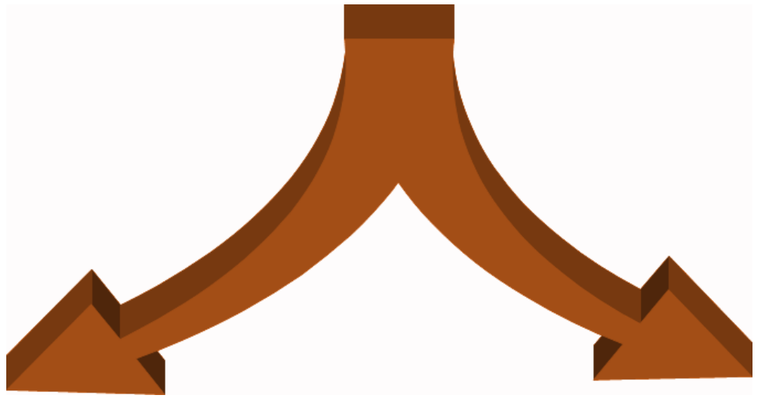
1. Visit https://andersbrownworth.com/Blockchain/public-private-keys/keys

1. Click on the **Random** button to generate public and private keys

Cryptography Categories

Cryptography is mainly divided into two categories:

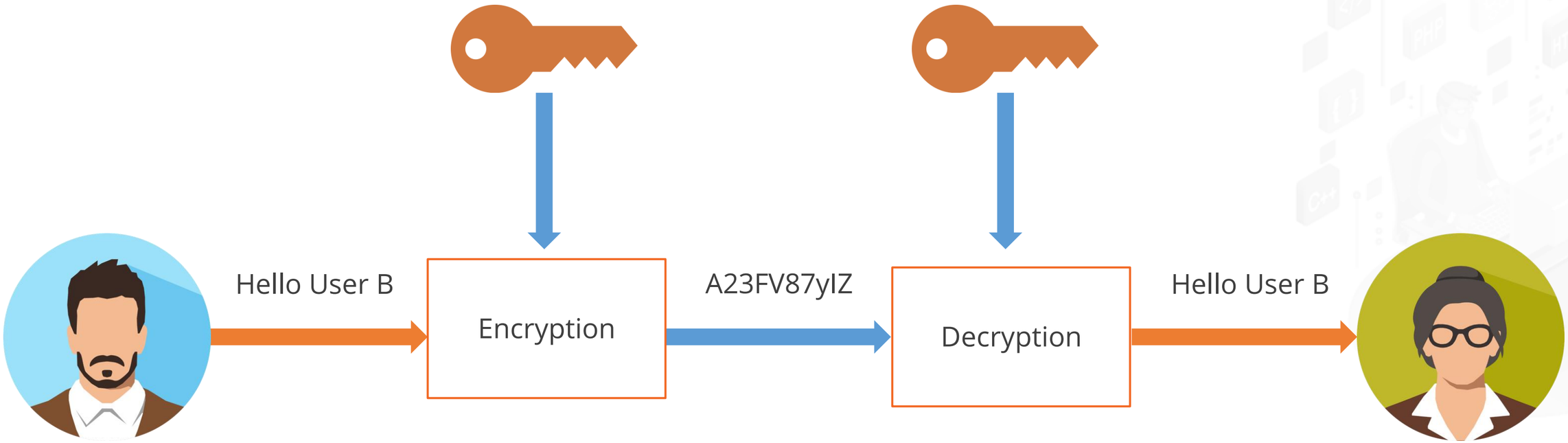
Symmetric Cryptography



Asymmetric Cryptography

Symmetric Cryptography

Symmetric cryptography is a type of cryptography where the same key is used for encryption and decryption of data, and thus it is also known as a shared key cryptography.



Send a Message Using Symmetric Cryptography

Problem Statement: You are given a task to first encrypt and then decrypt the message using symmetric cryptography.

ASSISTED PRACTICE

Assisted Practice: Send a Message Using Symmetric Cryptography

Steps to perform:

1. Visit https://www.kerryveenstra.com/cryptosystem.html

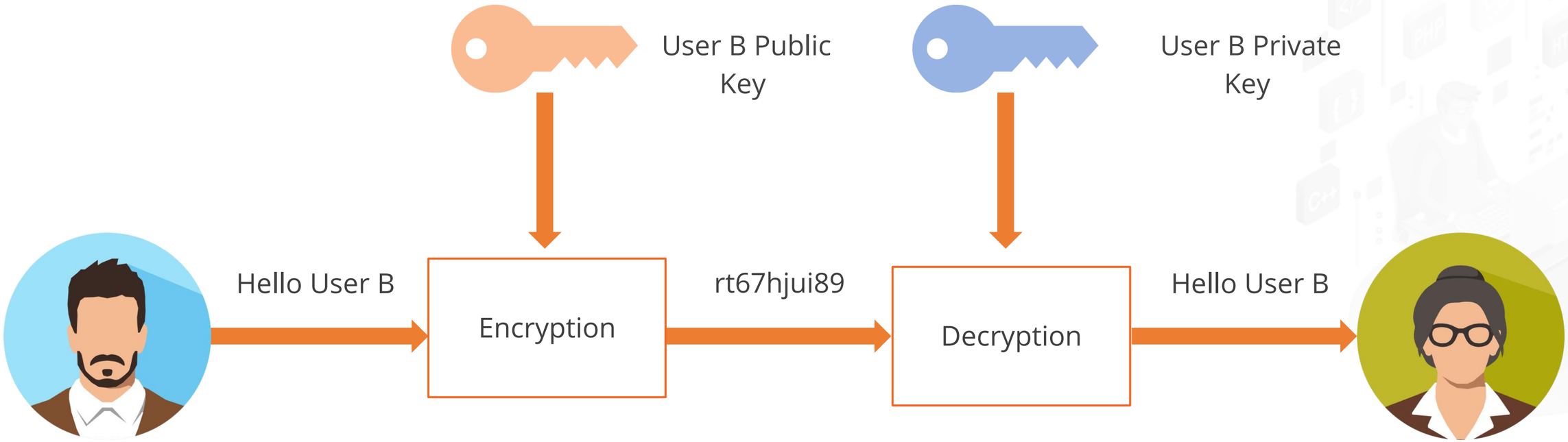
1. Click on **Generate a Symmetric Key** button under symmetric key encryption section, this will generate a key for you

1. To encrypt the message, enter the plaintext of your message and your symmetric key. Then press the button to encrypt the plaintext of your message into its ciphertext

1. Now to decrypt the message, enter the ciphertext of the message followed by your symmetric key, and press the button to decrypt the ciphertext of the message into plaintext

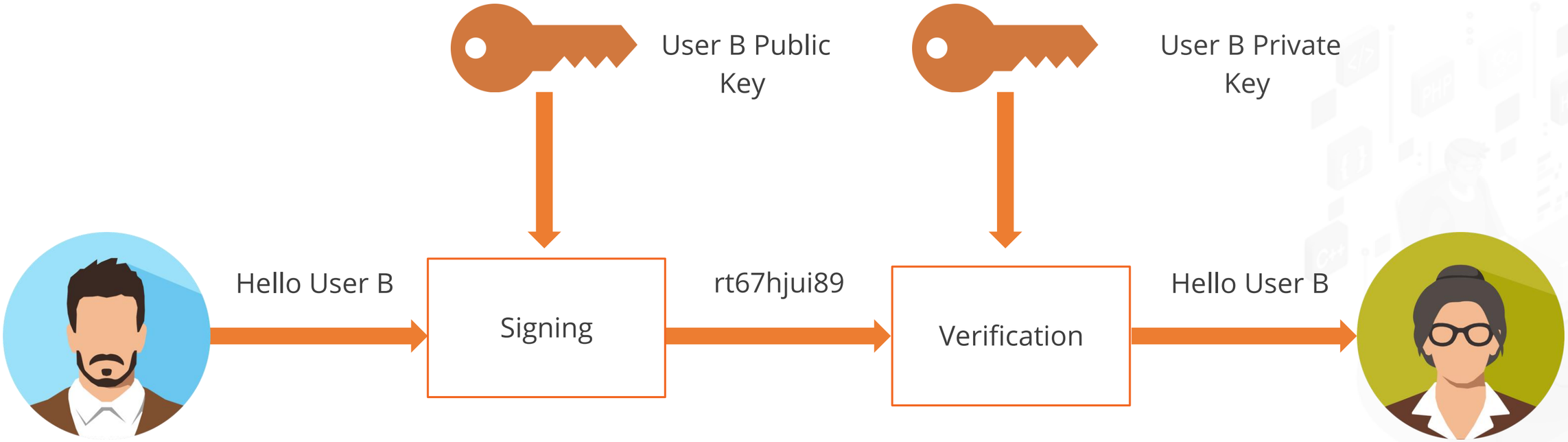
Asymmetric Cryptography

Asymmetric cryptography is a type of cryptography where the encryption key is different from the decryption key, and thus it is also known as public key cryptography.



Message Signing

Signing can be used to verify the integrity of the received message by the receiver.



Sign a Message Using Asymmetric Cryptography

Problem Statement: You are given a task to sign a message using asymmetric cryptography.

ASSISTED PRACTICE

Assisted Practice: Sign a Message Using Asymmetric Cryptography

Steps to perform:

1. Visit https://andersbrownworth.com/Blockchain/public-private-keys/signatures

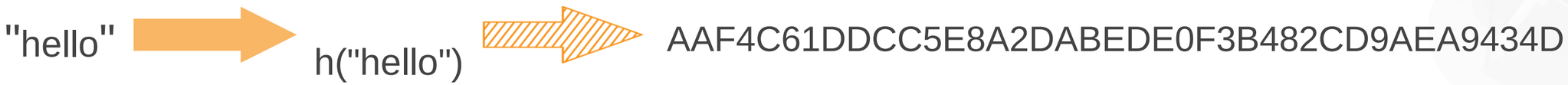
1. Enter the message and click on **Sign** to add digital signature

1. Click on the **Verify** tab to verify the signature

Hash Function

Introduction

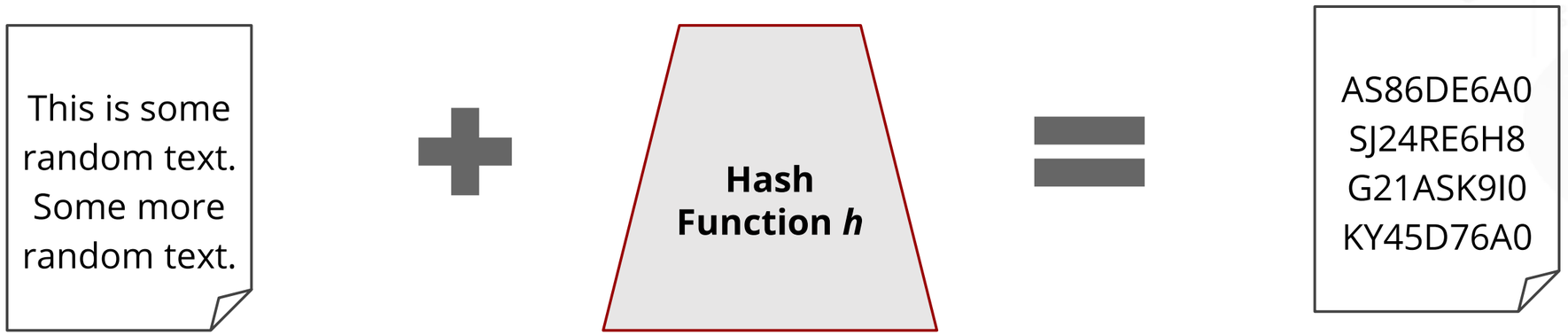
- A hash function is a mathematical function that converts a numerical input value into another compressed numerical value.
- The input to the hash function is of an arbitrary length but output is always of a fixed length. For eg: MD, SHA1, SHA-2, SHA-3, RIPEMD, and Whirlpool



Hash Function

Features

- It is impossible to produce the same hash value for differing inputs.
- You will get a new hash if you make any minute change in the input data.
- It is impossible to determine the input based on the hash value.



Generate Hash Using Hash Function

Problem Statement: You are given a task to generate the hash for a message using the hash function.

ASSISTED PRACTICE

Assisted Practice: Generate Hash Using Hash function

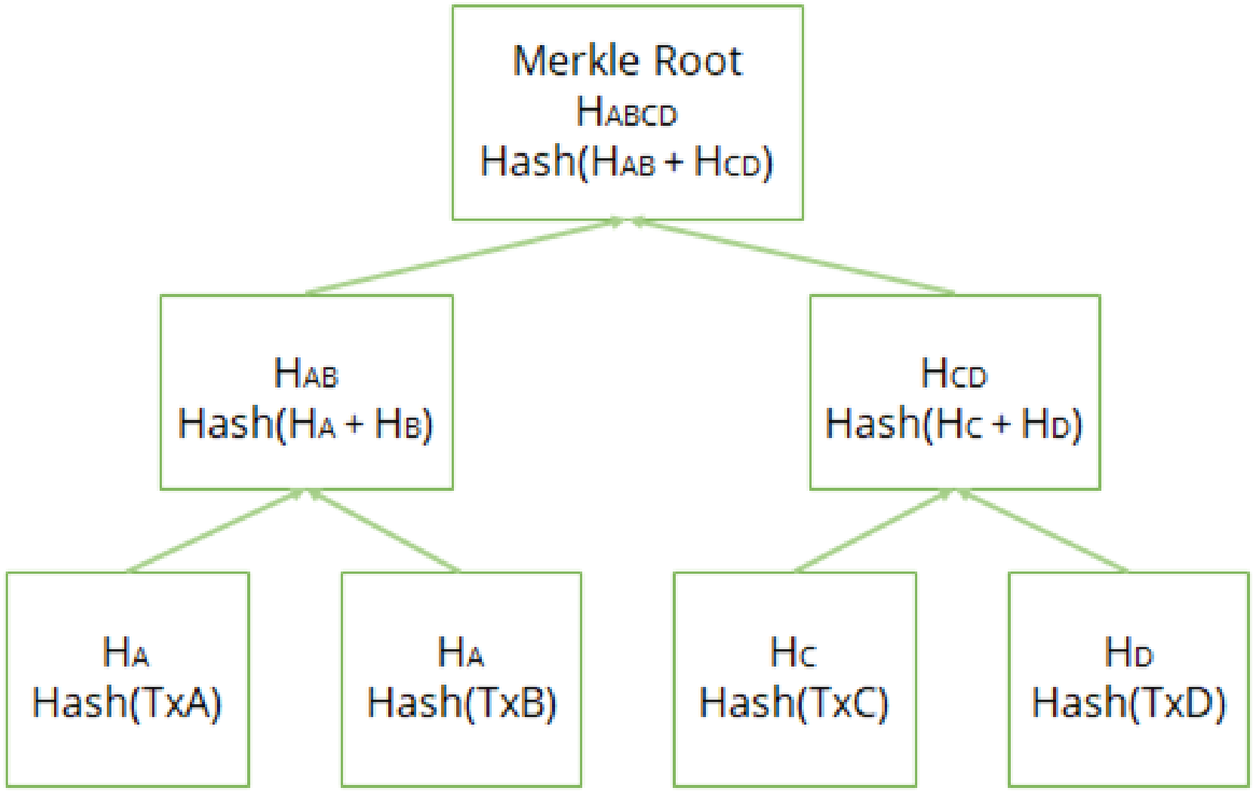
Steps to perform:

1. Visit https://andersbrownworth.com/Blockchain/hash

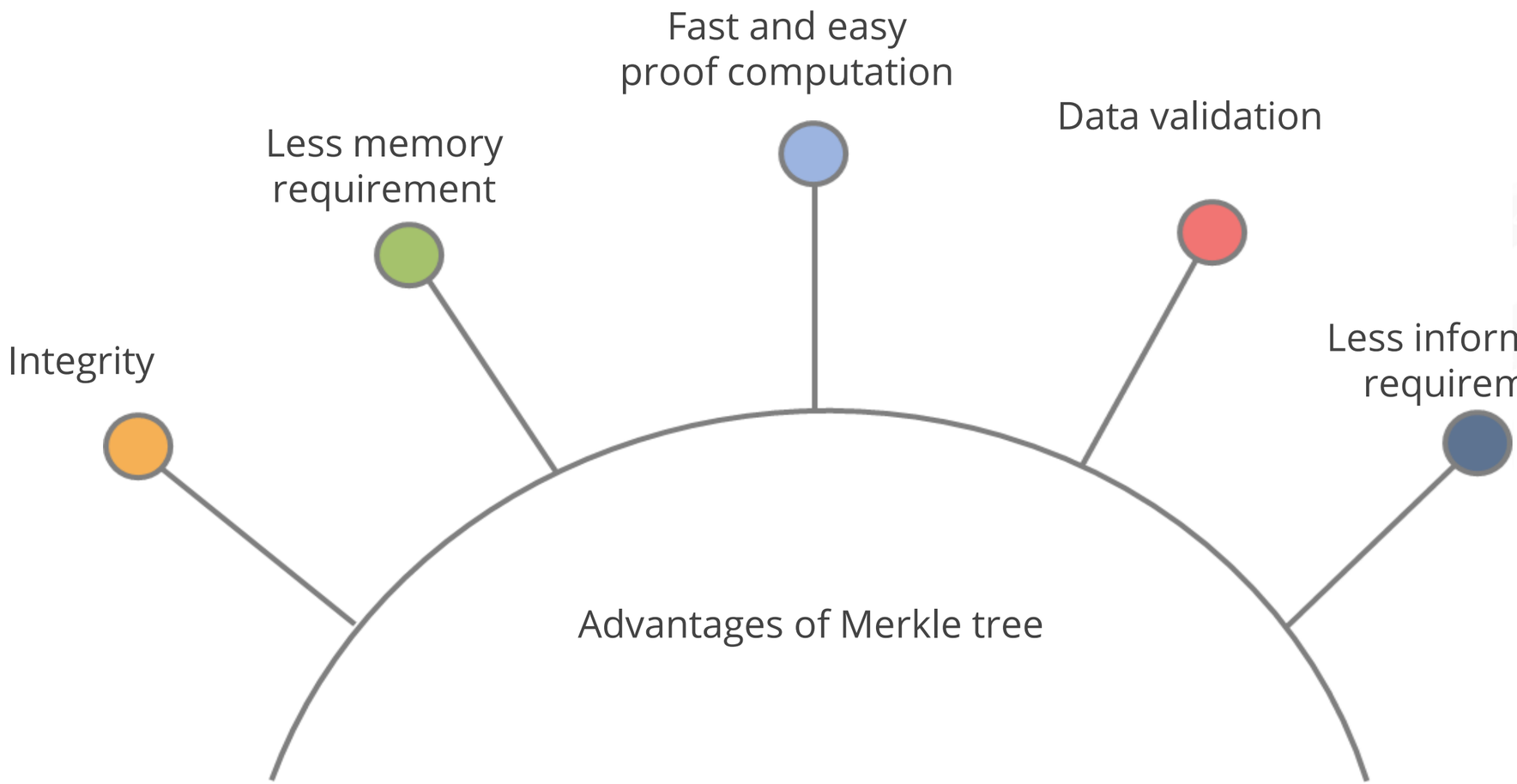
1. Enter the message and it generates the hash of that message

Merkle Tree

Merkle tree is a data structure that is used for summarizing and verifying the integrity of large data sets. It is also known as a binary hash tree.



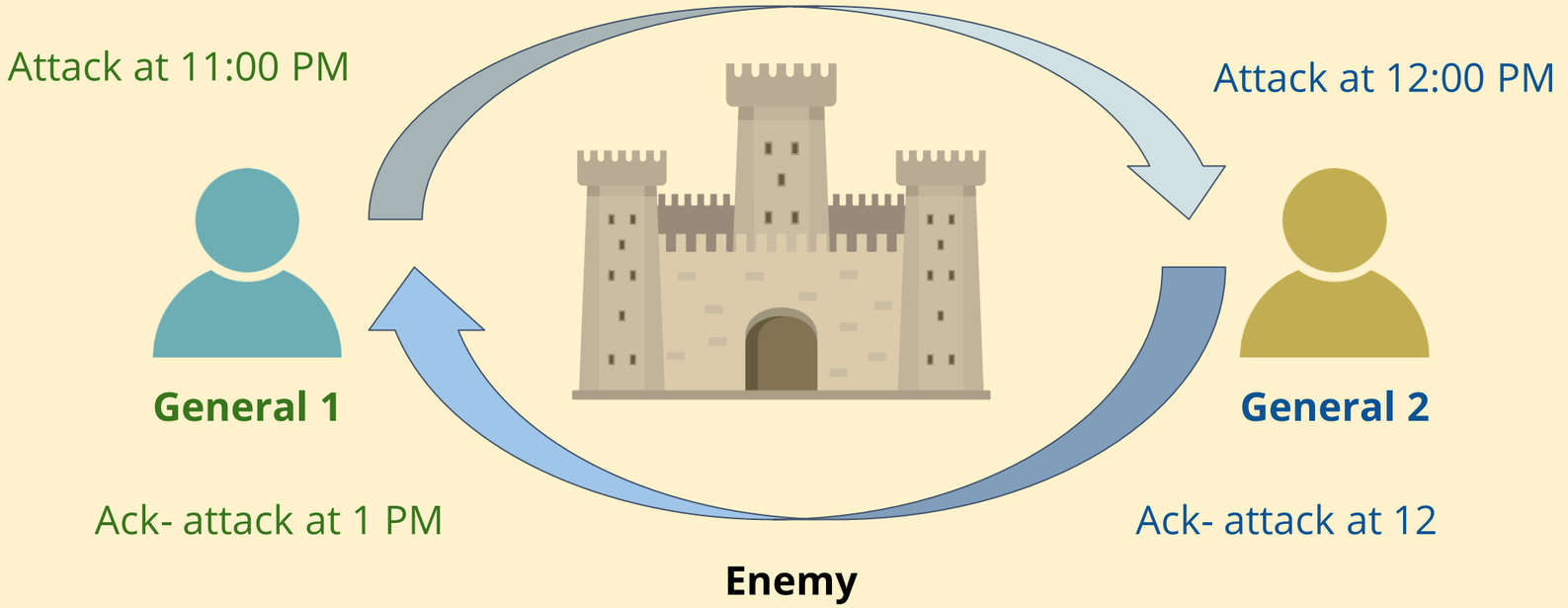
Merkle Tree


Fast and easy
proof computation
Less memory
requirement
Data validation
Integrity
Less information
requirement
Advantages of Merkle tree

Consensus

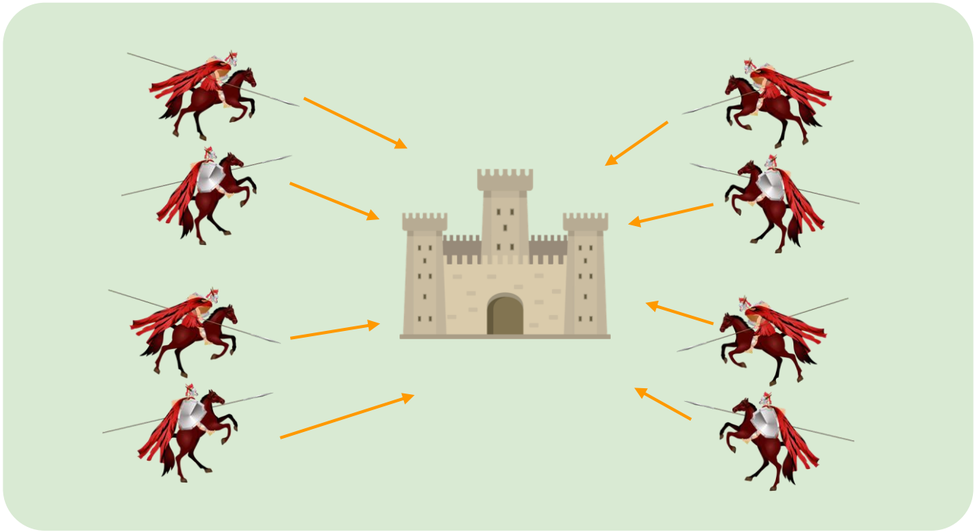
Two General Problem

- It is a scenario where two generals are attacking a common enemy.
- First general is considered the leader and the other is considered the follower.
- Each army on its own is not enough to defeat the enemy army, so they need to cooperate and attack at the same time.

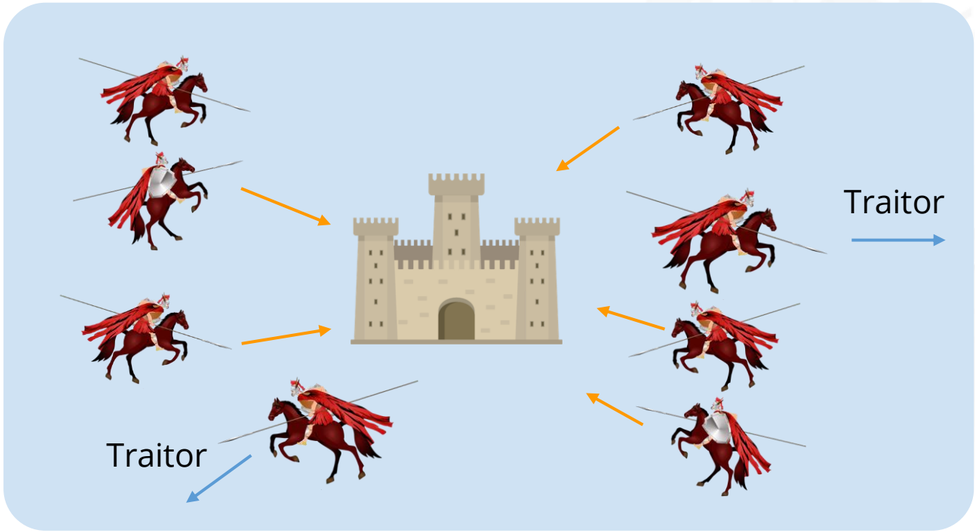


Byzantine Generals' Problem

- It is an advanced version of **Two General Problem** where there can be many generals.
- Generals not only need to agree on time of attack but here one or more generals can be a traitor.



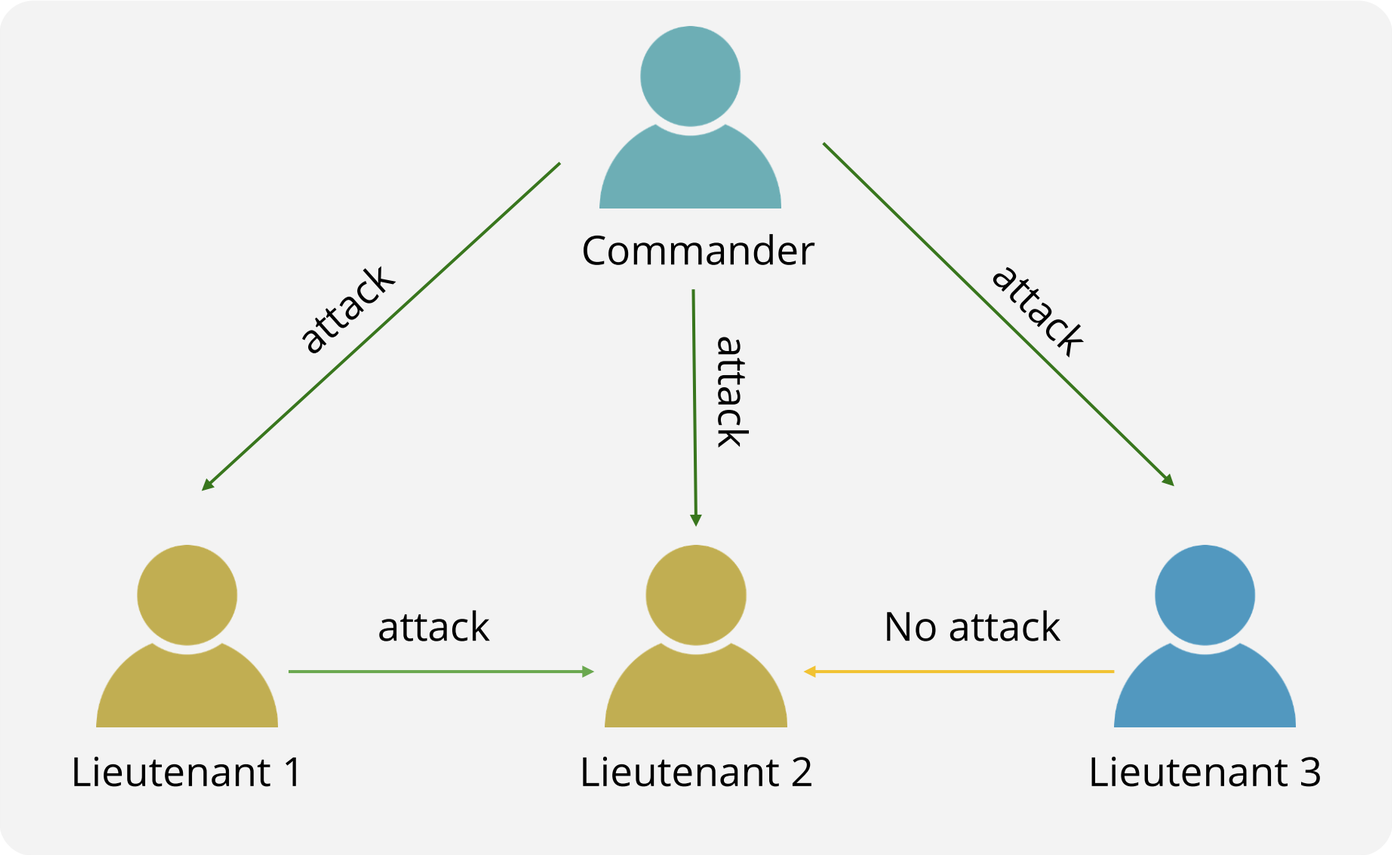
Coordinated attack leading to victory



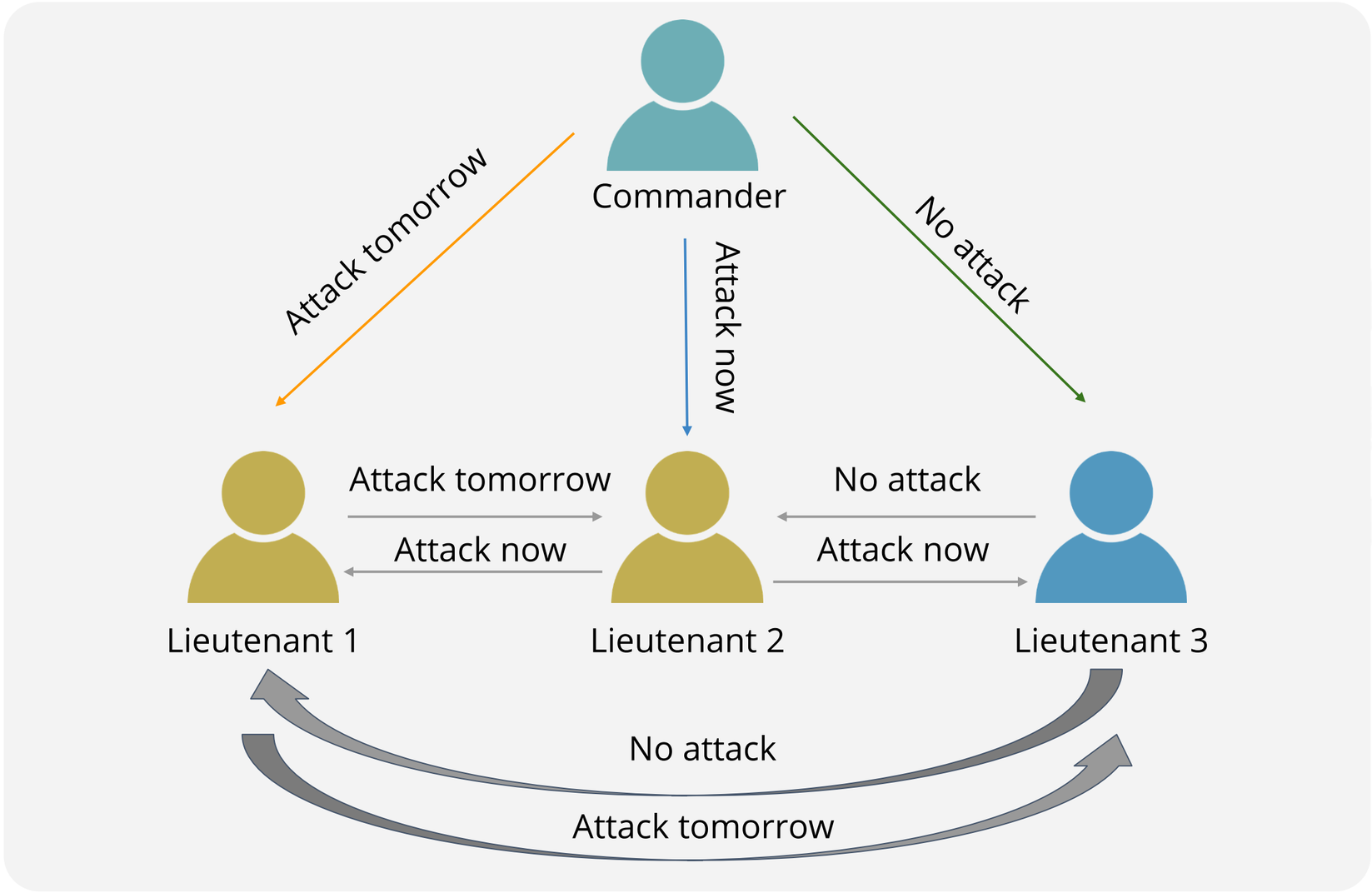
Uncoordinated attack leading to defeat

Byzantine Fault Tolerance

Byzantine Fault Tolerance is a characteristic that defines a system which tolerates the class of failures that belong to the Byzantine Generals' Problem.



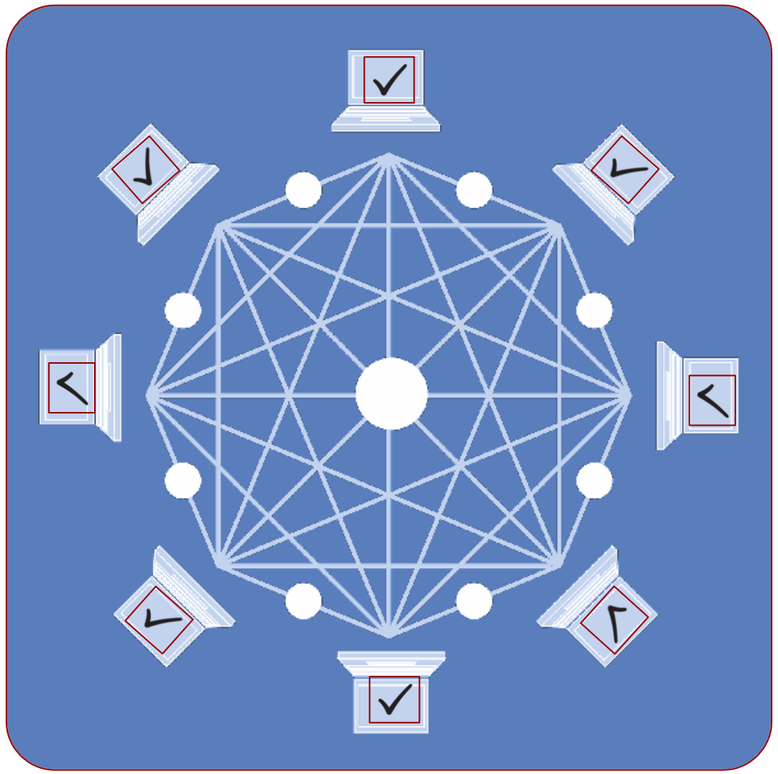
Byzantine Fault Tolerance



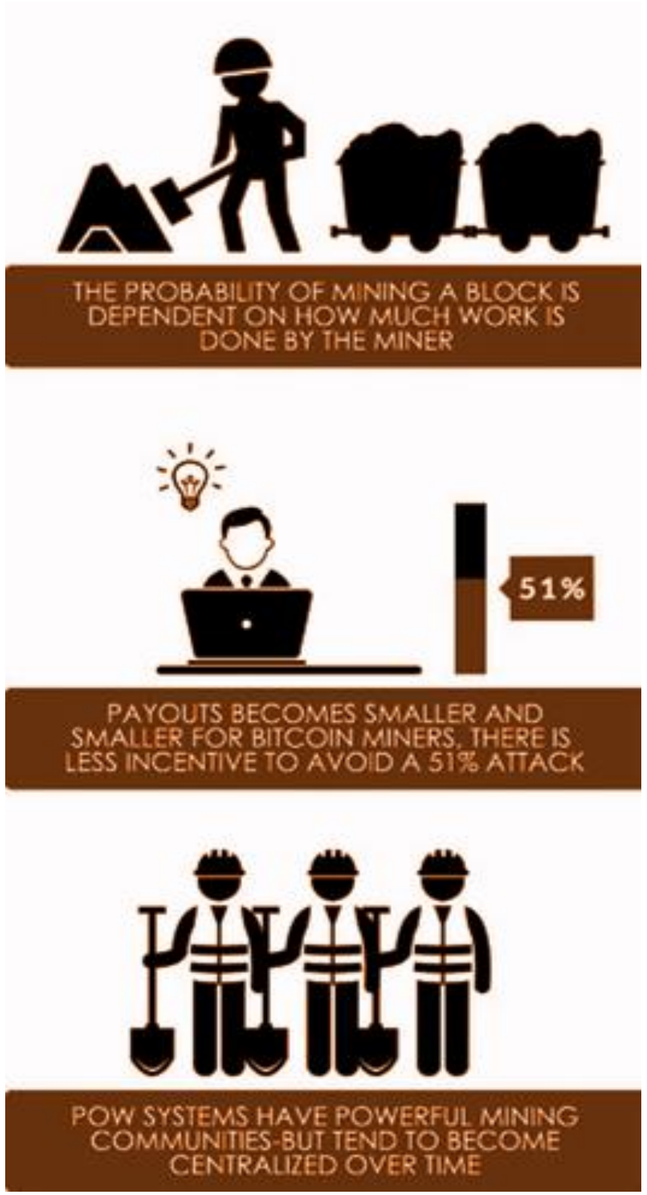
Understanding Byzantine Fault Tolerance

Introduction to Consensus

Consensus is a process of agreement between distrusting nodes on a final state of data. In order to achieve consensus different algorithms can be used.



Proof of Work



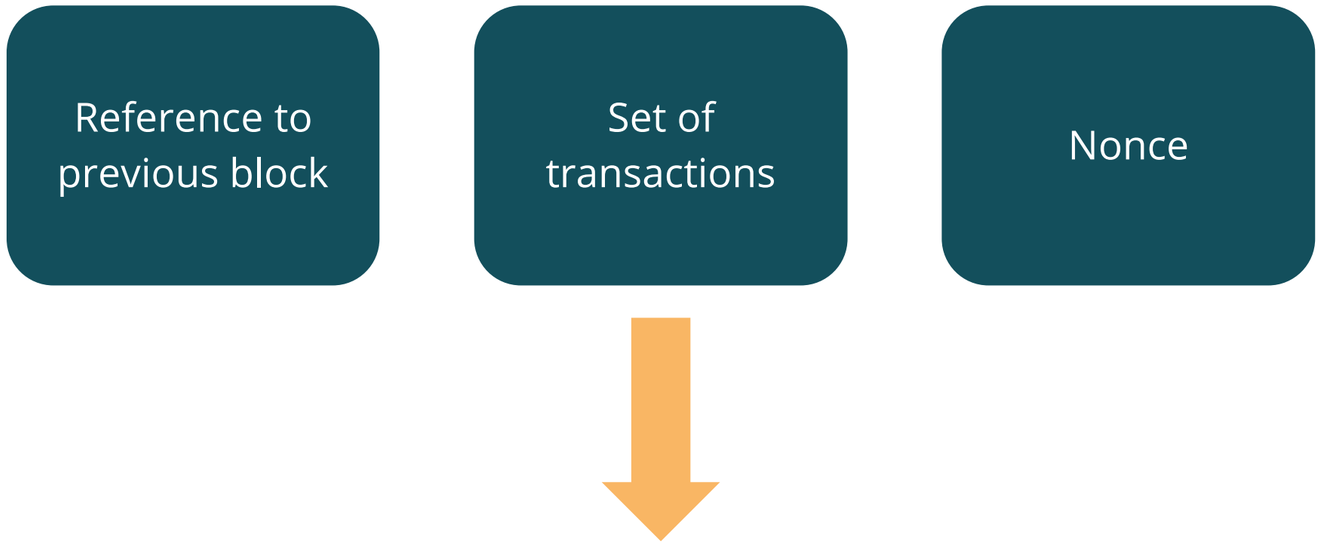
- Proof of Work (PoW) is an algorithm that is used to confirm transactions and produce new blocks to the chain.
- With PoW, miners compete against each other to complete transactions on the network and get rewarded.
- The main working principles are a complicated mathematical puzzle and a possibility to easily prove the solution.

Proof of Work Consensus

Hashcash Proof of Work system is used in Bitcoin as the mining basis. A *hard mathematical problem* can be written in an abstract way as follows:

Given data A, find a number x such as that the hash of x appended to A results in a number less than B.

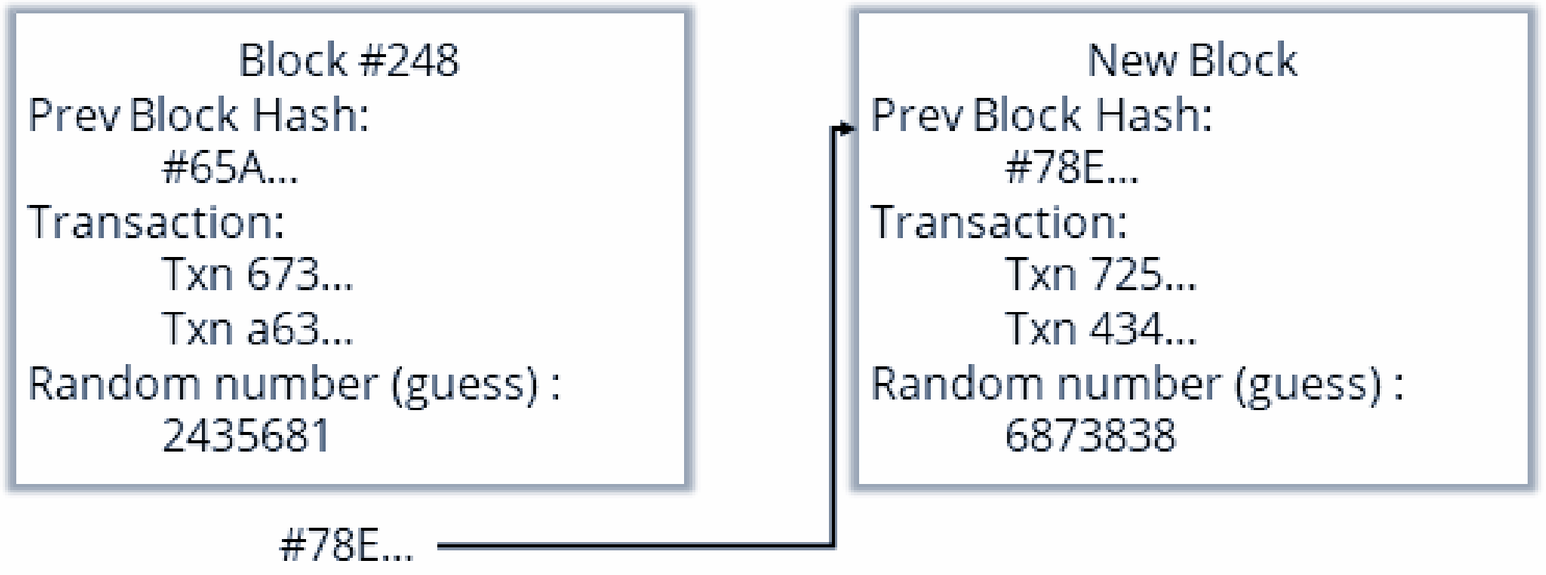
Mathematical Problem



00000000000000000149e18da3aebbe10087a34867338ab828d58b68a699a58

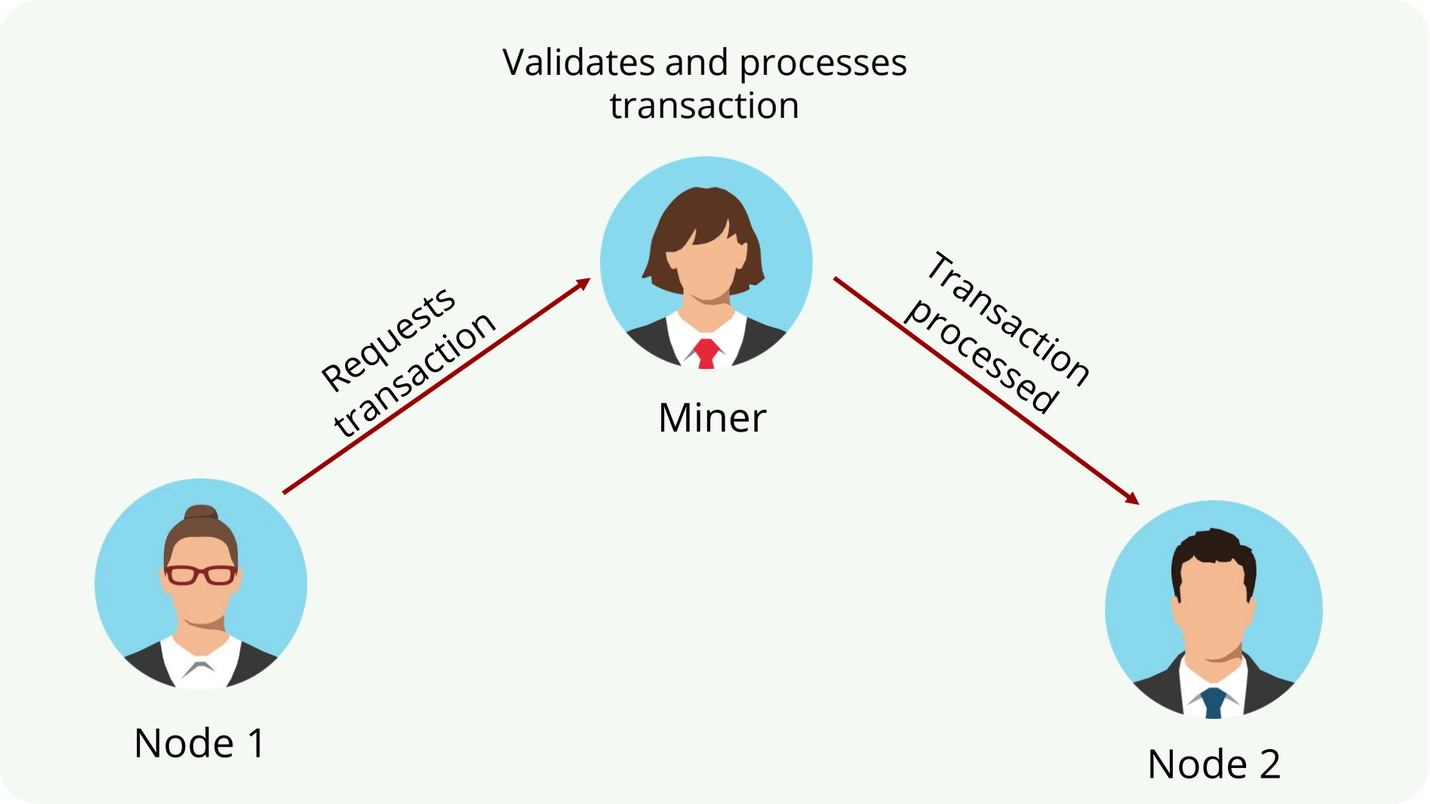
Nonce

Nonce is a random number that can be used just once in a cryptographic communication and is added to a hashed or encrypted block in a Blockchain that, when rehashed, meets the difficulty level restrictions.



Role of Miners

Bitcoin miners verify the new Bitcoin transactions and record them in the public ledger. Miners receive rewards for providing processing power to the bitcoin network by mining.



Generate a Nonce Value

Problem Statement: You are given a task to generate a nonce value.

ASSISTED PRACTICE

Assisted Practice: Generate a Nonce Value

Steps to perform:

1. Visit https://andersbrownworth.com/Blockchain/block

1. Enter some data in data field and click on **Mine**

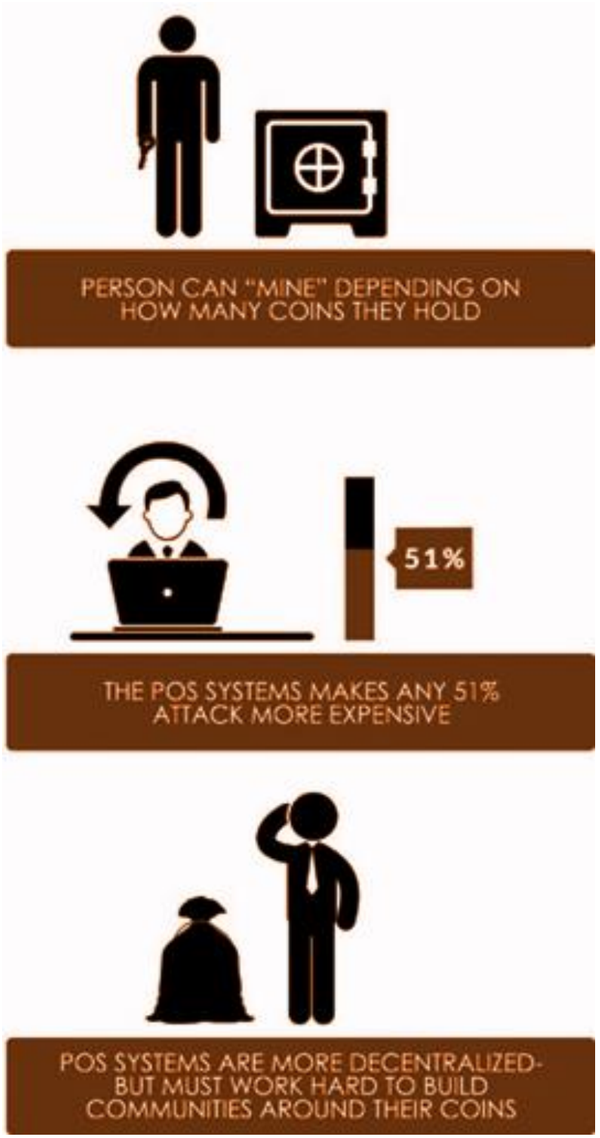
1. Observe the generation of nonce value

Drawbacks of Proof of Work

- **Energy consumption:** Miners' **supercomputers** test millions of computations per second, making PoW highly costly and energy intensive.

- **Vulnerability:** PoW is vulnerable to a **51% attack**, that means theoretically nefarious miners could capture 51 percent of a network's computing power and manipulate the Blockchain to their advantage.

Proof of Stake



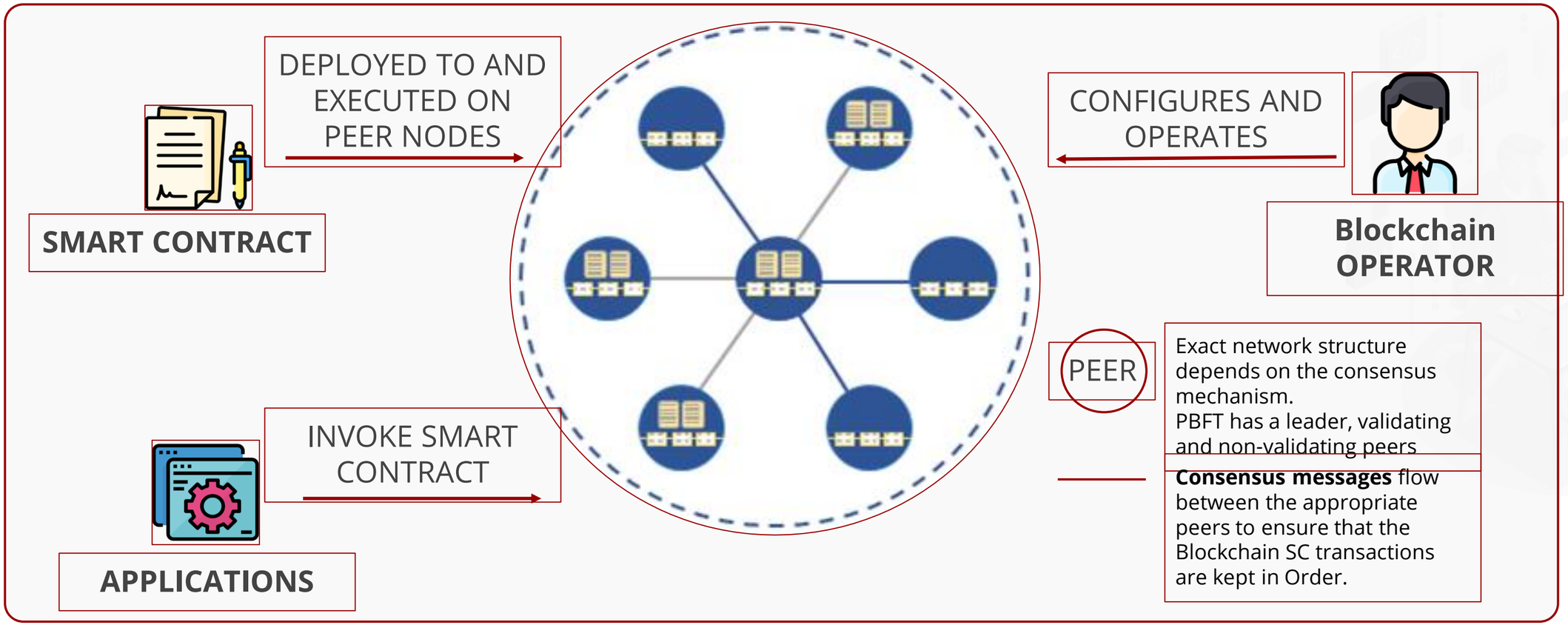
- Proof of Stake (PoS) is a low cost and low energy consuming algorithm that allows people to mine and validate the transaction based on how many coins they hold.
- With PoS, miners only get transaction fees for making a block.
- No competition for mining as the block creator is chosen by the algorithm based on user's stake.

Proof of Elapsed Time

Proof of Elapsed Time (PoET) is a consensus algorithm that prevents high energy consumption and resource utilization by following a lottery system. It enables permissioned Blockchain networks to determine block winners and mining rights.

Practical Byzantine Fault Tolerance

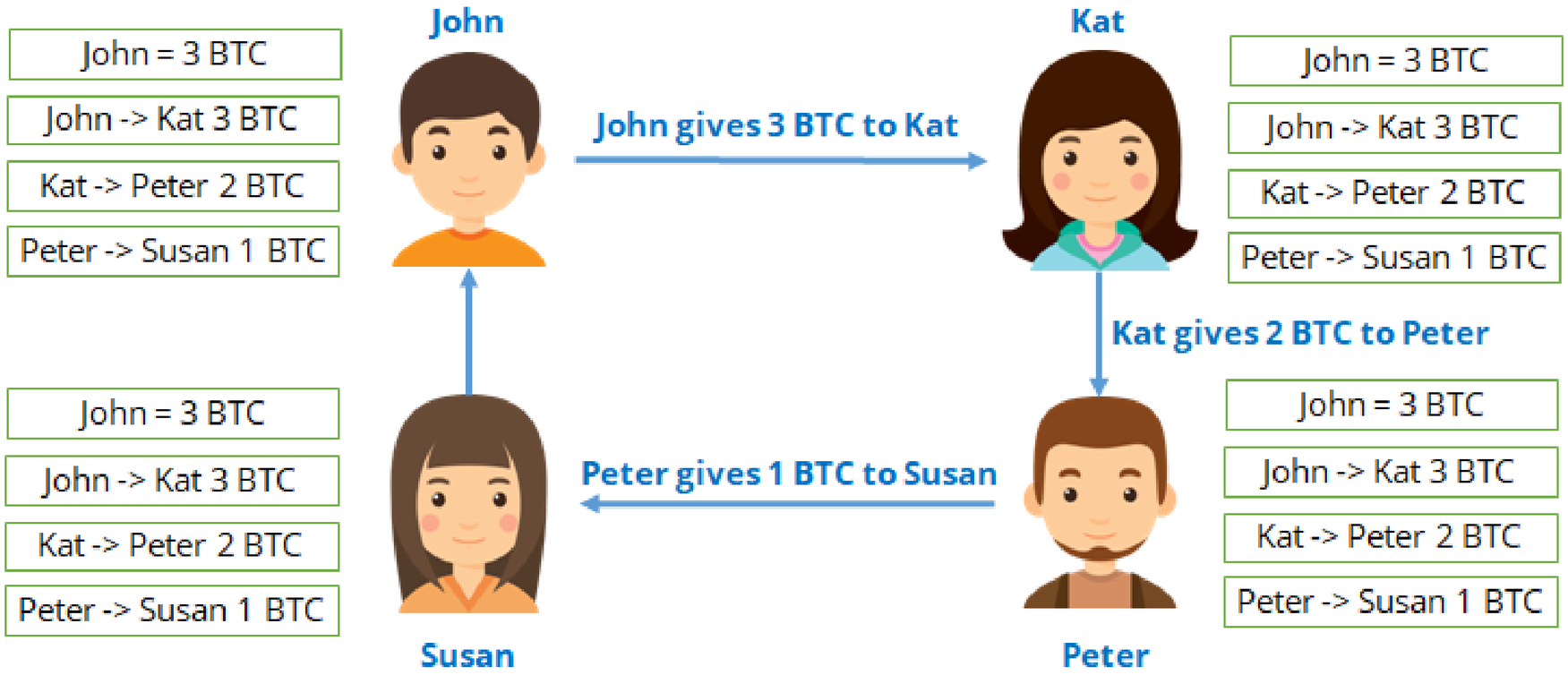
Practical Byzantine Fault Tolerance (pBFT) is a consensus algorithm that improves the robustness and performance of transaction by directing peer-to-peer messages with minimal latency.



Distributed Ledger

Distributed Ledger

Distributed ledgers are databases that store the copy of all the transactions that have happened. Every single person in the Blockchain network has a copy of the ledger.



Working of Distributed Ledger

Problem Statement: You are given a task to demonstrate the working of distributed ledger.

ASSISTED PRACTICE

Assisted Practice: Working of Distributed Ledger

Steps to perform:

1. Visit https://andersbrownworth.com/Blockchain/distributed

1. Note the hash value of Node 1 Peer A

1. Enter data in the data field of Peer A, click **Mine** and note the hash value

1. Enter data and mine the other blocks of Peer A

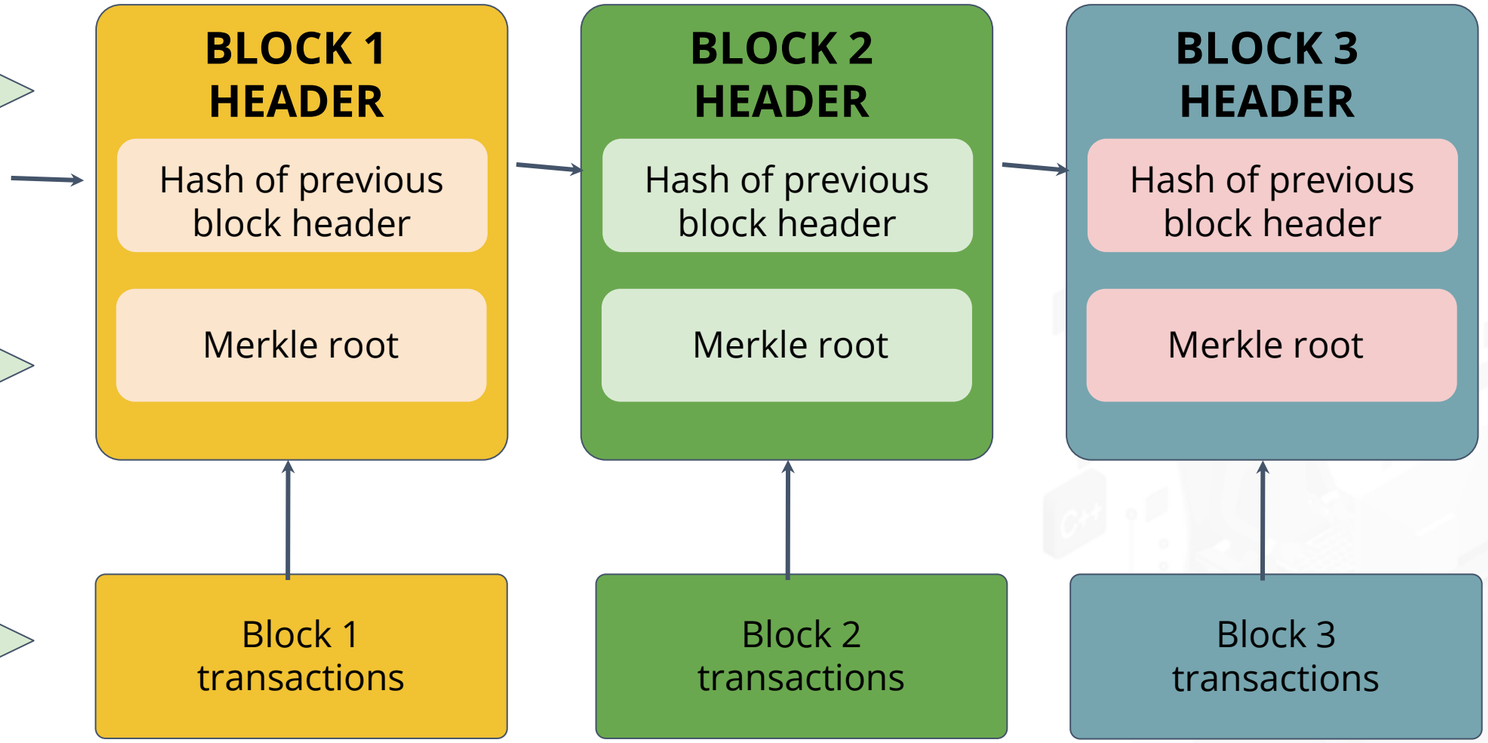
1. Verify if the hash of previous block is same in the next block

Block Structure

Header: Contains version information, nonce, previous block ID, and timestamp

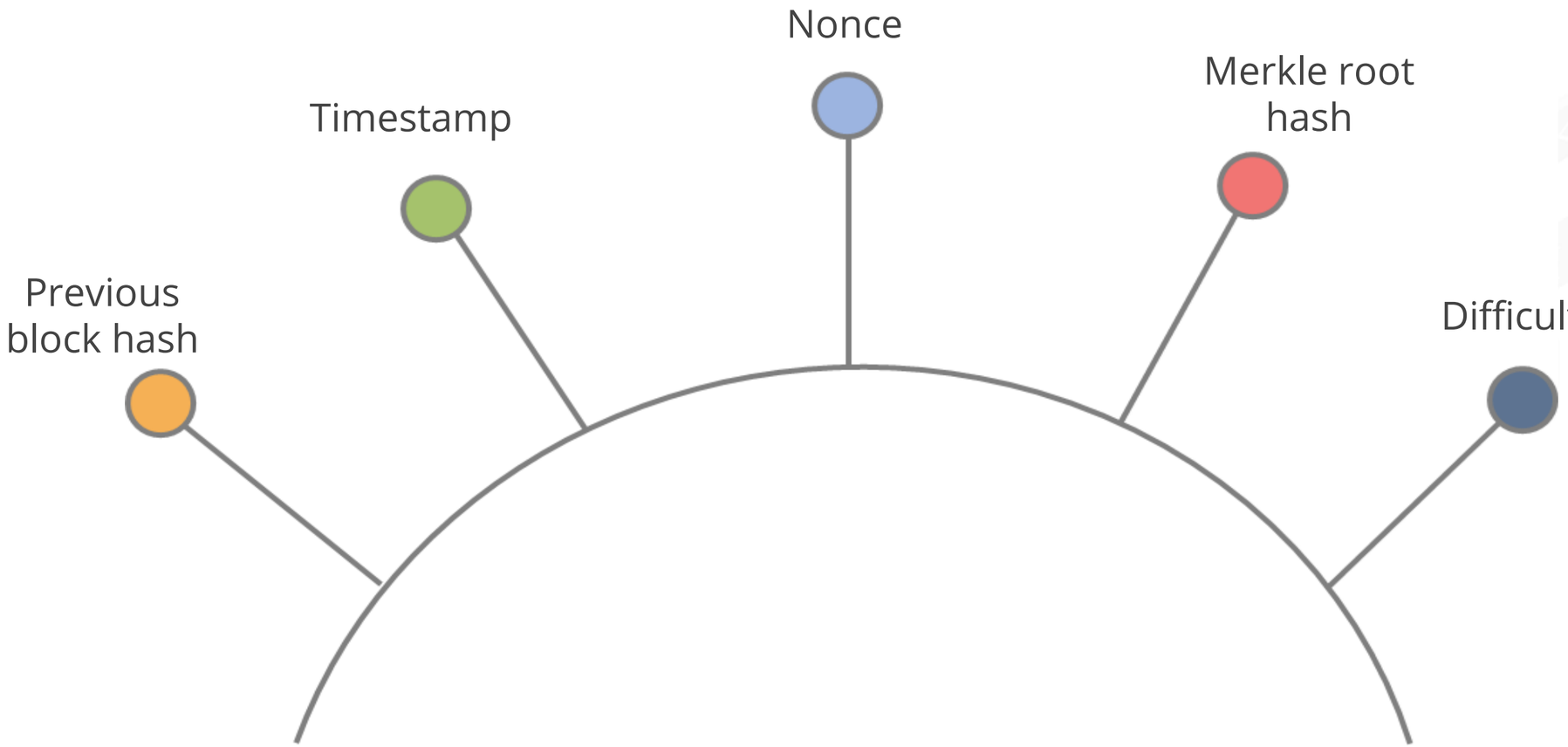
Merkle: A hash built from the block's transaction identifiers

List of records: Identification of hashes that were included into the block's Merkle tree



Block Header

Block Header generally contains the following items:

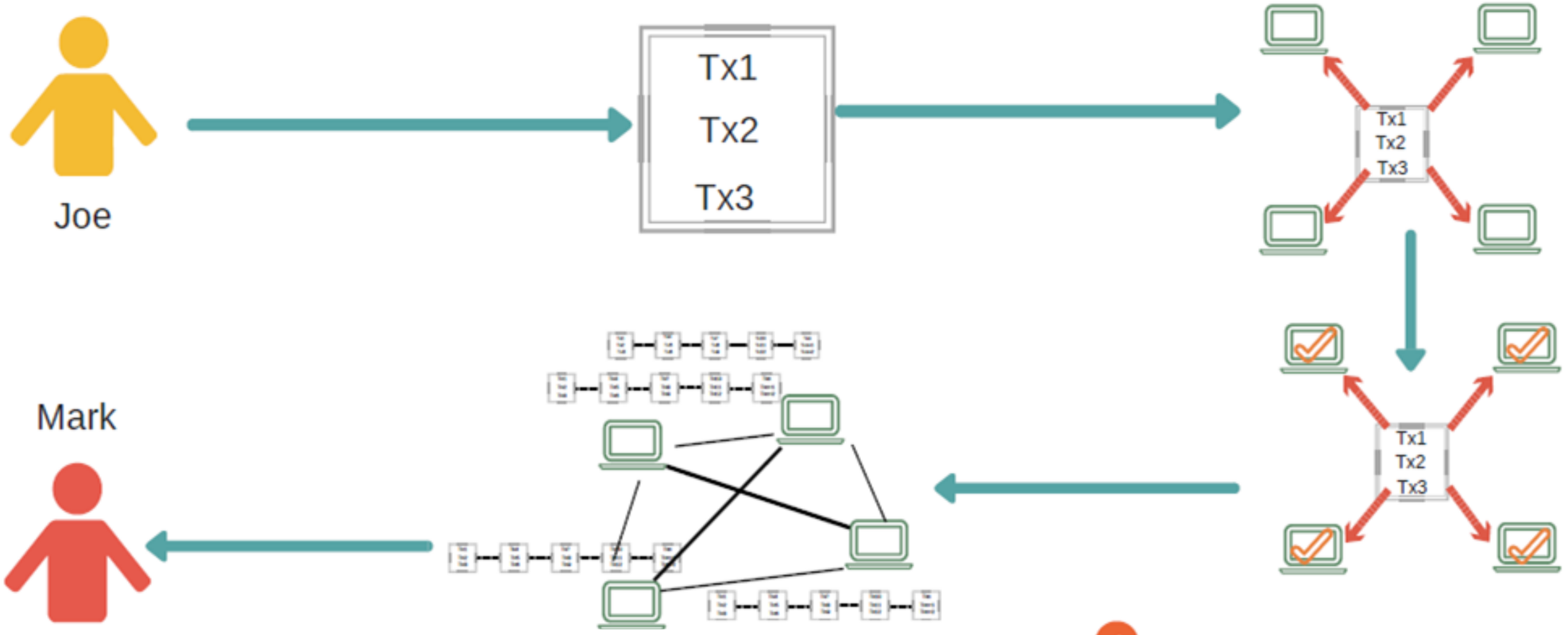


Blockchain Transaction

1. Joe wants to send money to Mark so he initiates the transaction

2. Transaction gets stored in a block

3. Block gets broadcasted to network



4. Network approves if the transaction is valid

5. Block gets added to the Blockchain

6. Mark receives the money

Working of Blockchain Transaction

Problem Statement: You are given a task to demonstrate the working of Blockchain transaction.

ASSISTED PRACTICE

Assisted Practice: Working of Blockchain Transaction

Steps to perform:

1. Visit https://andersbrownworth.com/Blockchain/Blockchain

1. Enter any data in the data field and observe the change in hash

1. Change the information in any block and observe the change in hash value

1. Observe how the hash value changes in the subsequent blocks

Key Takeaways

- Cryptography is the science of making information secure to send it across two or more parties using Ciphers.
- Consensus ensures that the nodes on a network verify the transactions and agree with their order and existence on a ledger.
- A hash function is a mathematical function that converts a numerical input value into another compressed numerical value.
- Distributed ledger is a database of replicated, shared, and synchronized digital data geographically spread across multiple sites and accessible by multiple people.

Lesson-End Project

Create Blockchain Network

You are an employee of a company and have been asked to create a Blockchain network to demonstrate the working of Blockchain. You need to perform the following actions:

1. Create blocks of an existing peer
2. Create another peer and block for this new peer
3. Connect the newly created peer with the existing peer

LESSON-END PROJECT