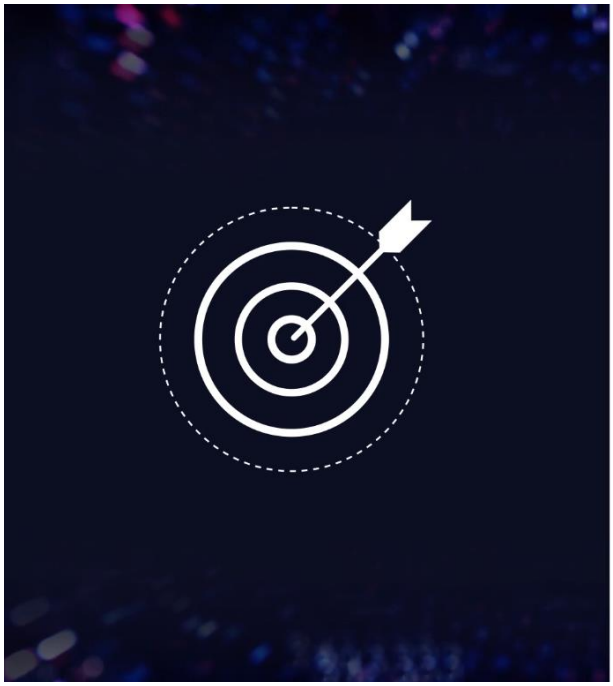
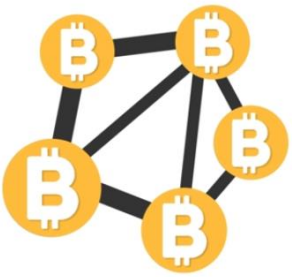


Objectives

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

- Describe the Blockchain transaction process
- Generate a public key and a digital signature
- Generate a nonce, a hash code, and a Blockchain block
- Work with a distributed system and perform Blockchain transactions

Overview of Blockchain



Blockchain can operate in a peer-to-peer fashion with zero intervention from third parties

Blockchain

BLOCKCHAIN

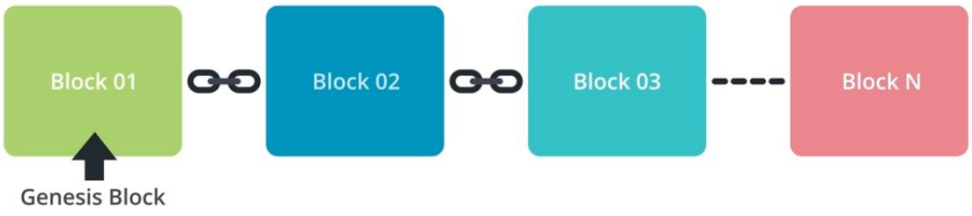
Blockchain is a decentralized ledger of all transactions across a peer-to-peer network.

It is a technology that enables Bitcoin and is also applied to many business processes.

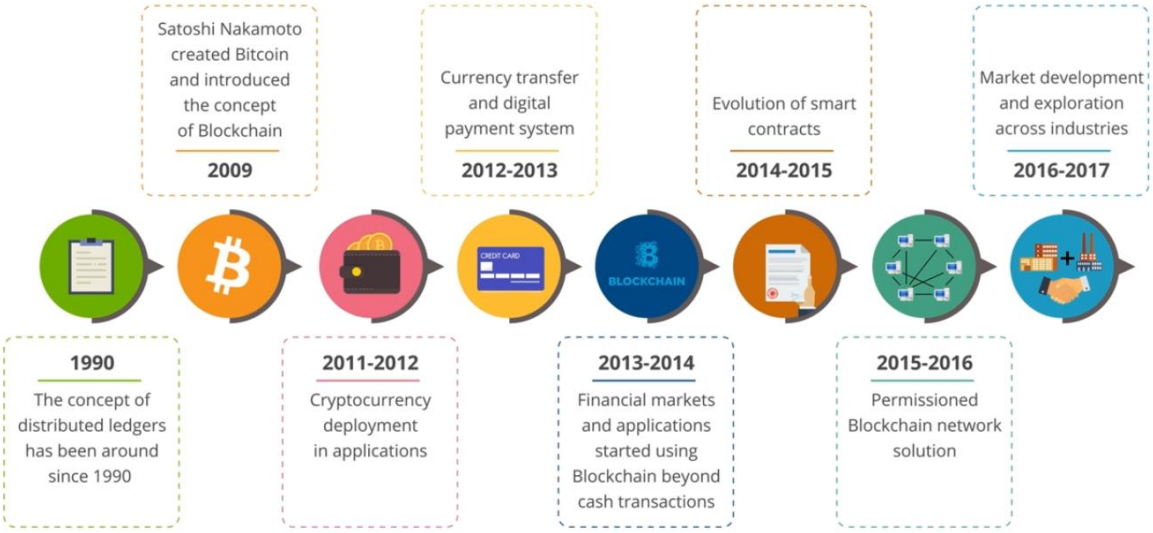
It not only performs transactions but also ensures anonymity and security of the users.

Blockchain

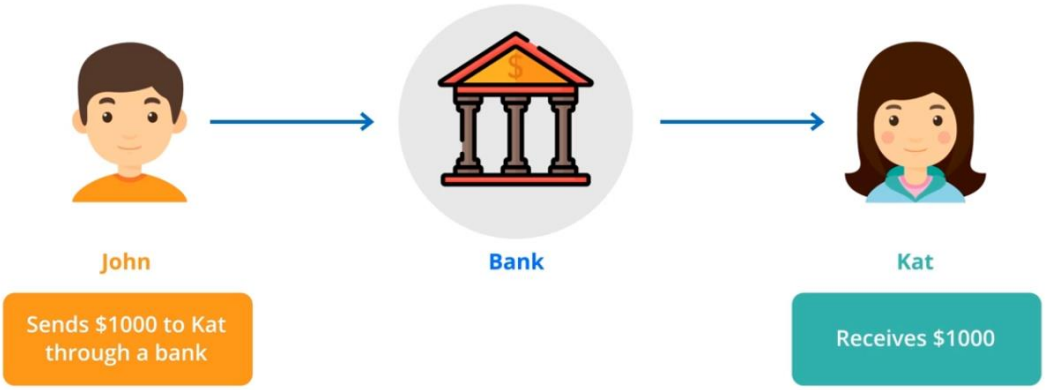
BLOCKCHAIN



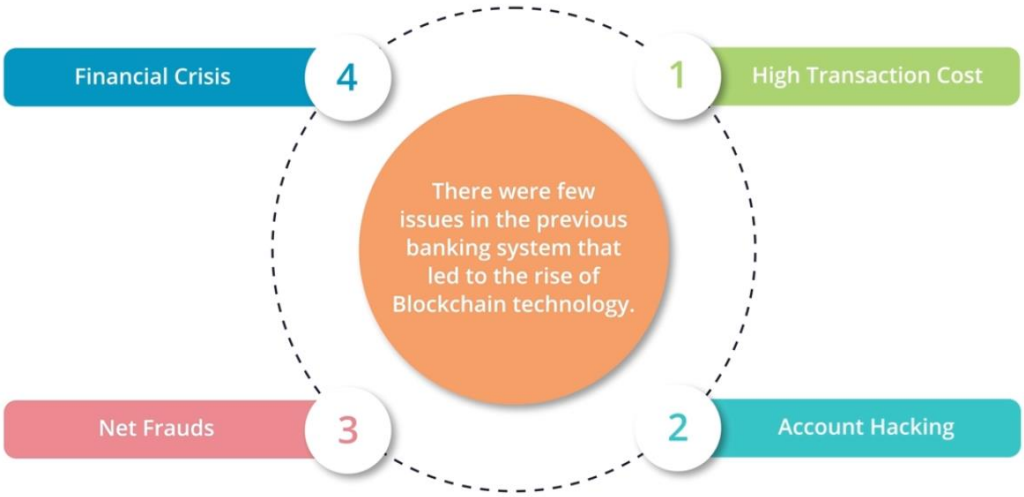
History of Blockchain



Current Banking System

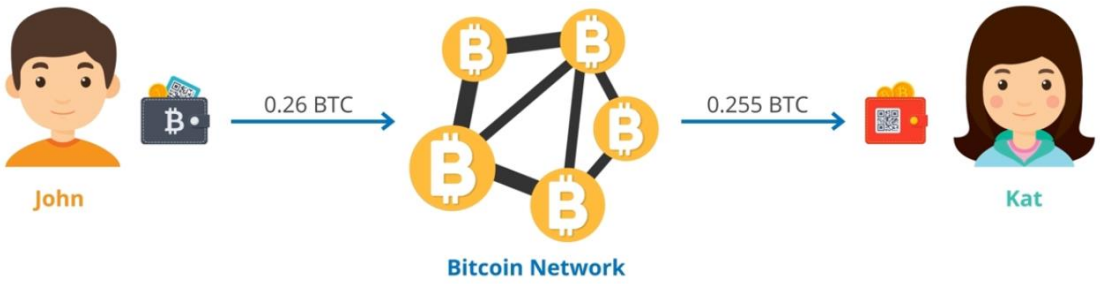


Issues in Banking System



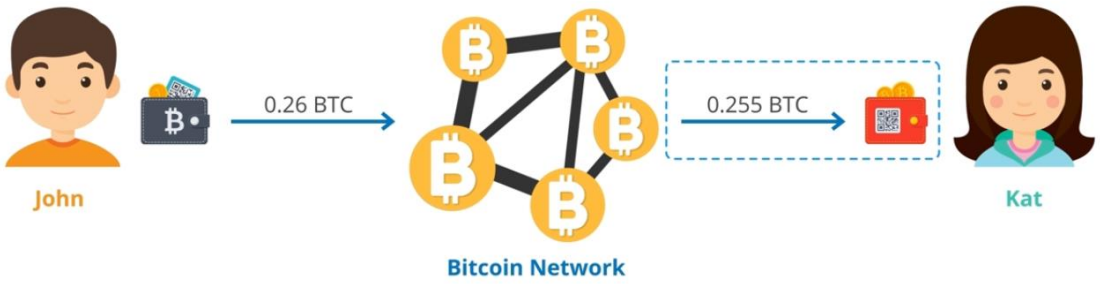
Blockchain Solution for the Issues

Scenario: Transaction between John and Kat in a Bitcoin Network



Blockchain Solution for the Issues

Scenario: Transaction between John and Kat in a Bitcoin Network

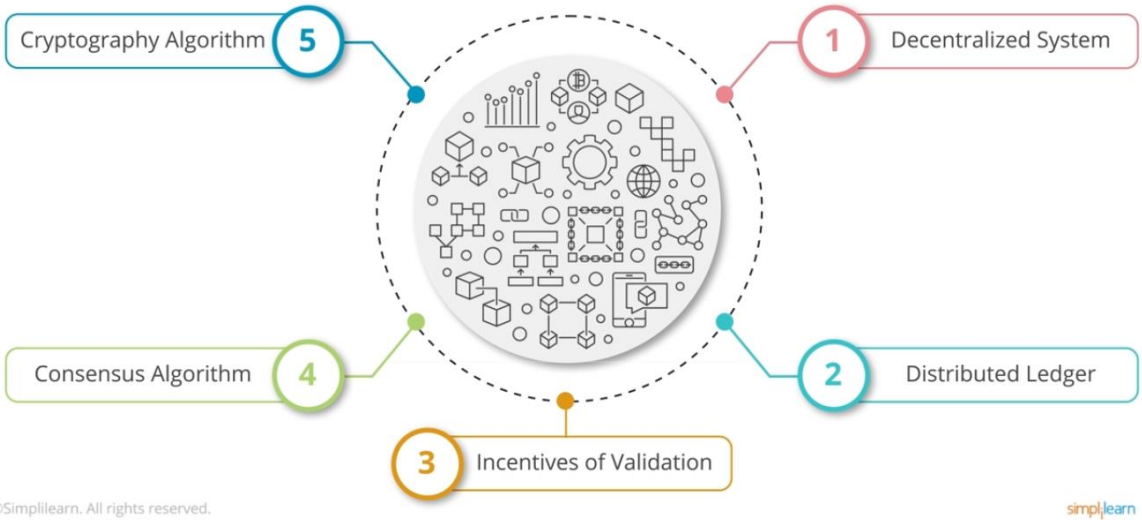


Blockchain Solution for the Issues

The blockchain comprises of a single ledger shared among all participants

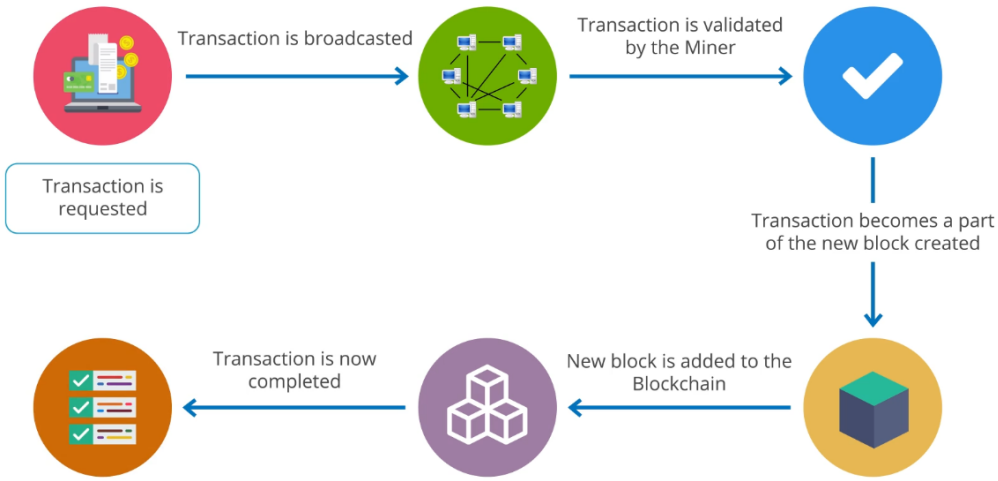
Blockchain Solution for the Issues

Blockchain tackled the issues in the previous system with some of its features mentioned below:



simplilearn

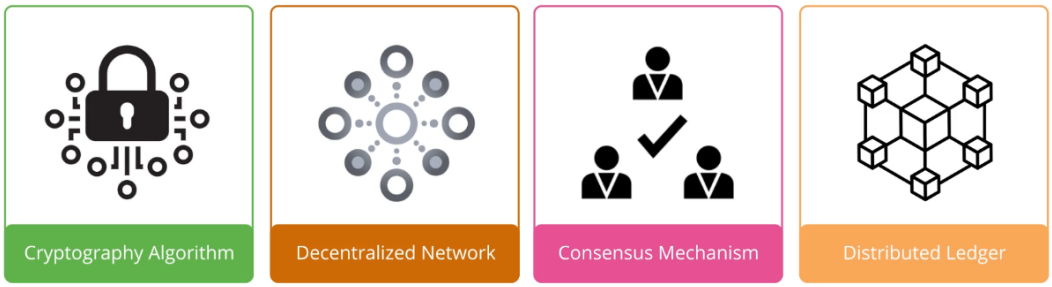
Blockchain Transaction Process



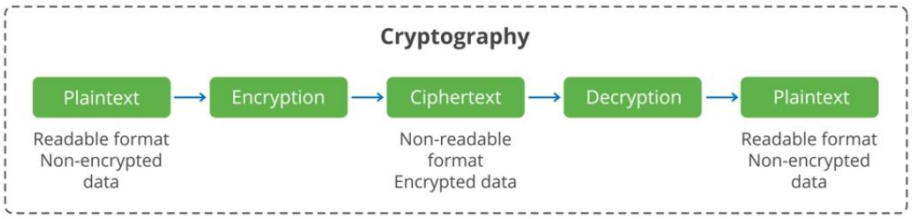
simplilearn

Steps of Blockchain Transaction

Blockchain transaction works by implementing one of the following features in each step:



Features of Blockchain

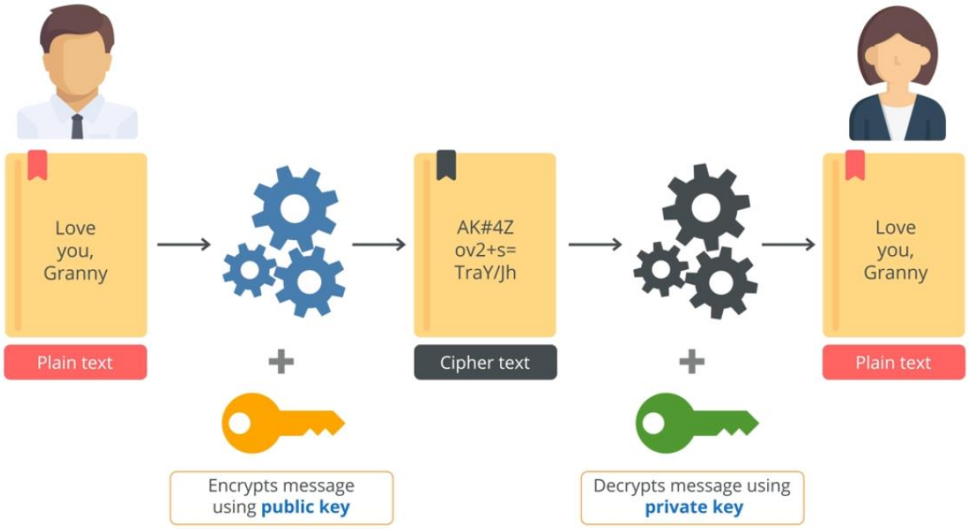


Features of Blockchain

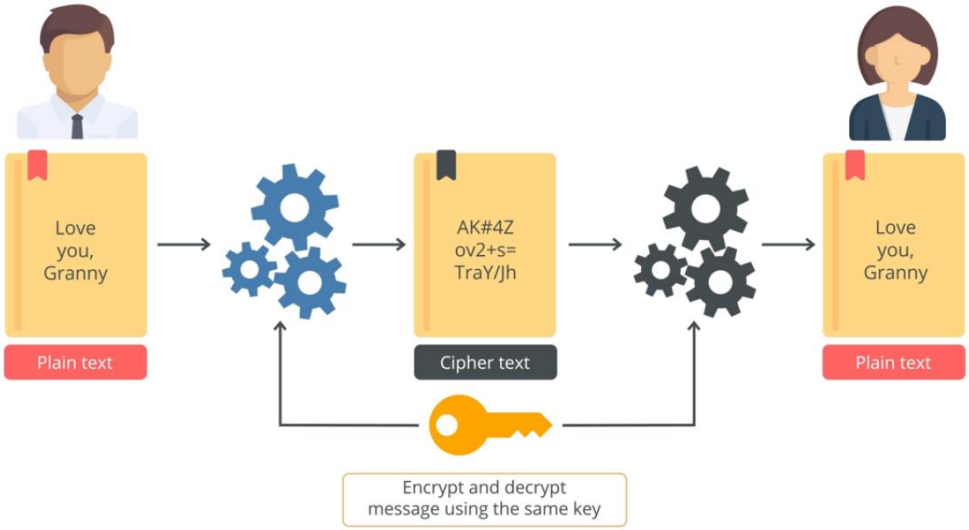
Asymmetric Key Cryptography

Symmetric Key Cryptography

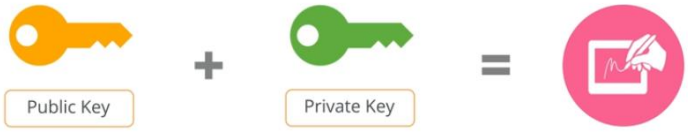
Asymmetric Key Cryptography



Symmetric Key Cryptography



Digital Signature



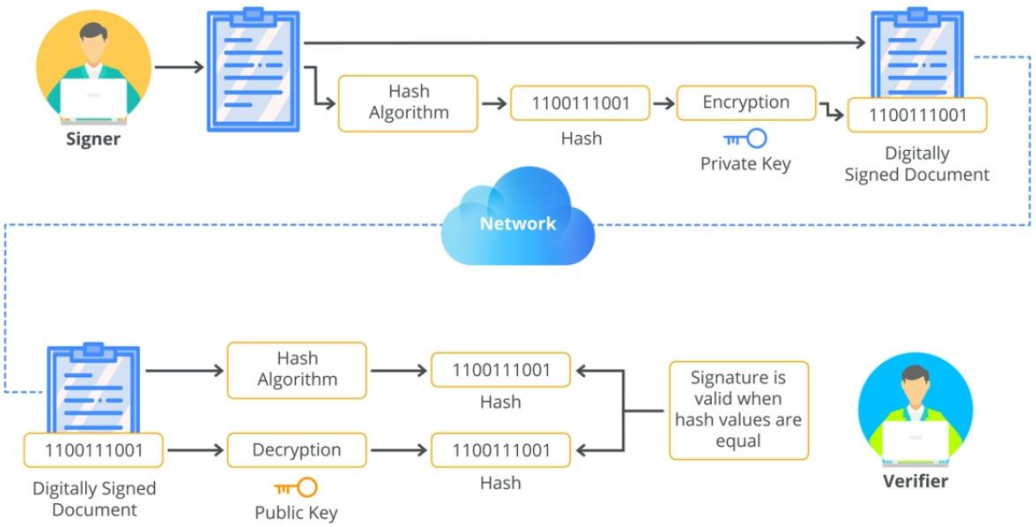
A digital signature provides authentication and validation like normal signatures.

It ensures the security and integrity of data recorded on the Blockchain.

It uses asymmetric cryptography in which information can be shared using a public key.

Primary keys are linked to users providing digital signatures a quality of nonrepudiation.

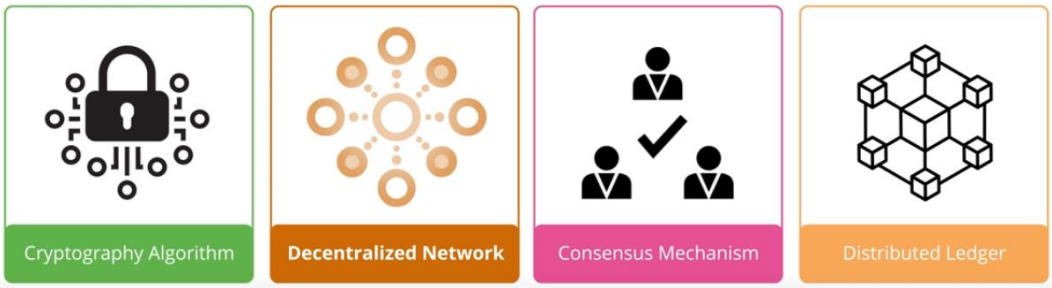
Digital Signature Creation



simplilearn

Features of Blockchain

It is a system where Miners play an important role in the validation of transaction taking place.



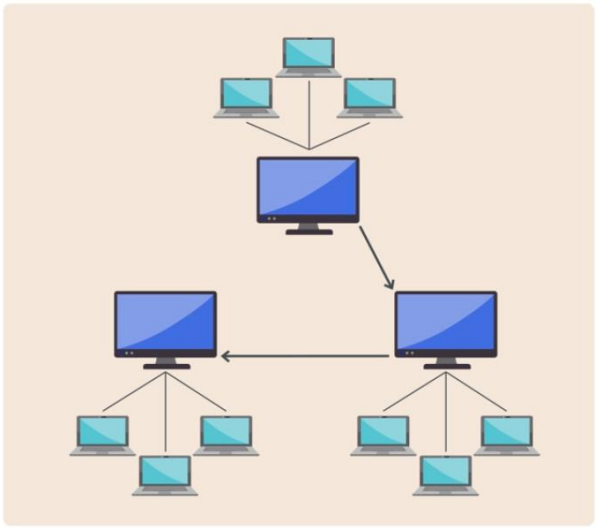
00:12 / 01:24

simplilearn

Types of Network

Decentralized Network

Centralized Network



simplilearn

Types of Network

Decentralized Network

Centralized Network

01:09 / 01:24

simplilearn

Features of Blockchain

It is an algorithm where Miners validate the transaction using mathematical puzzles.

Consensus Protocol

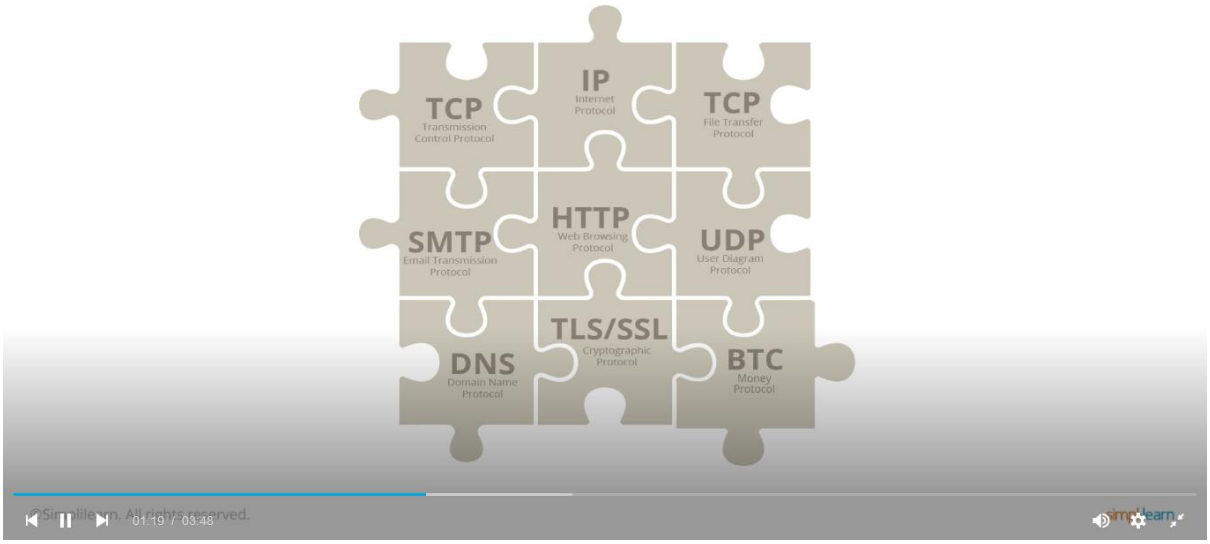
It is a fault-tolerant protocol that is used to achieve the necessary agreement on a single data value or a single state of network.

It is a set of rules that decides on the contribution of the various participants of the Blockchain.

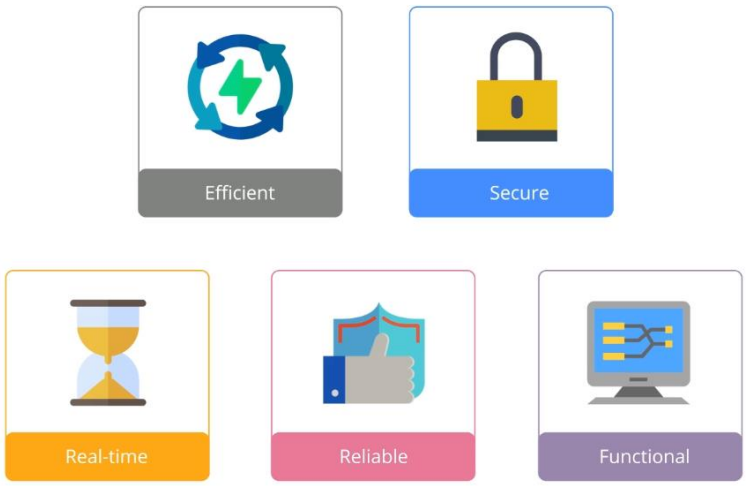
It ensures that all transactions occurring on the network are genuine and all participants agree on the consensus of the ledger.

Blockchain Protocols

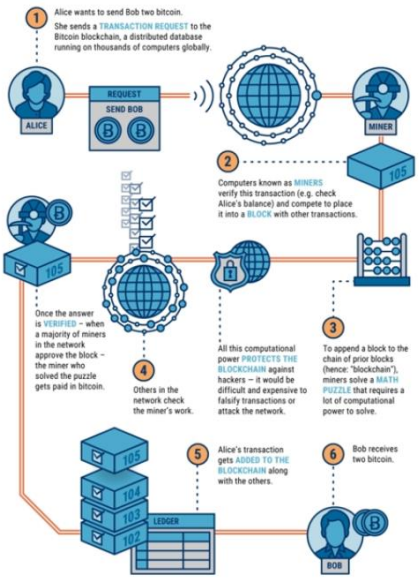
Blockchain Protocol holds the real transformative power of Bitcoin



Features of Consensus Protocol



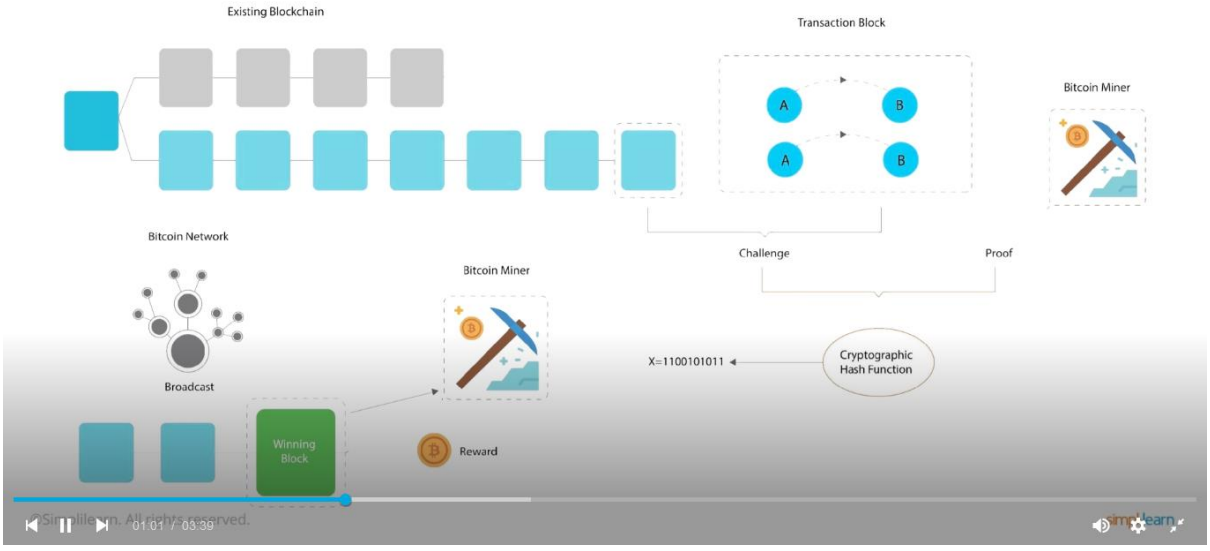
Role of Miner



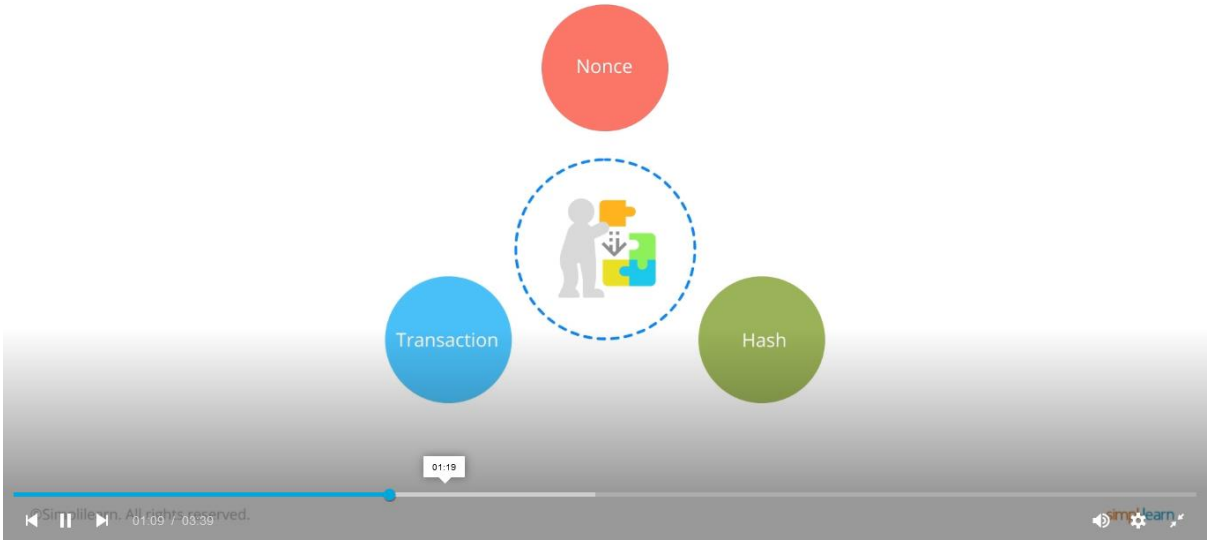
simplilearn

Proof of Work

Consensus algorithm is used to confirm transactions and produce new blocks to the chain.



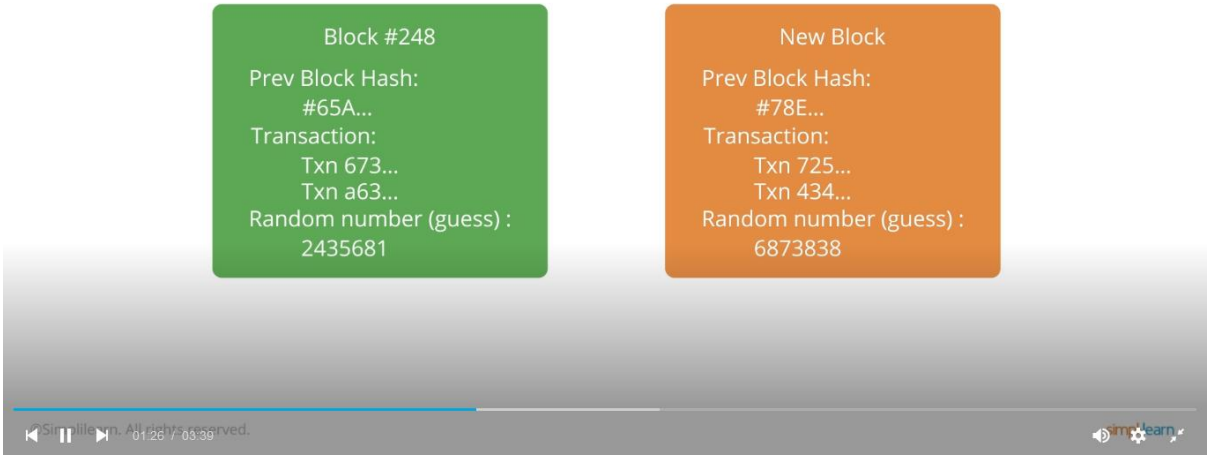
Proof of Work



Nonce

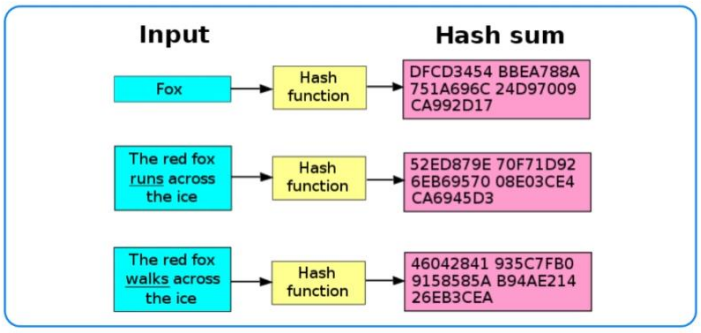
Nonce: Number Used Once

A random number whose value is set so that the hash of the block will contain a run of leading zeros.



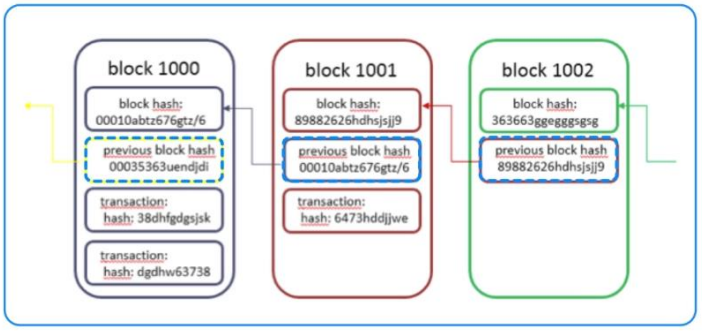
Hash Code

The main purpose of hash code is to assist with efficient lookup and insertion in data collections that are contingent on a hash table.



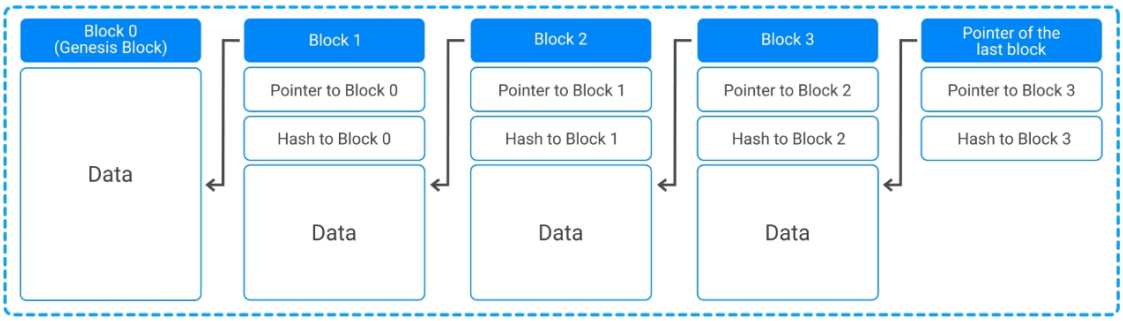
Hash Code

Transaction



Hash Pointer

- Hash pointer is a pointer to the location where information or hash of that information is stored
- If we retrieve information that the pointer points at, we can get hash of the information and confirm it to be unchanged
- It requires information of previous hash



simplilearn

Summary

Step 1 Visit the link https://anders.com/blockchain/block.html and observe the Nonce value

Step 2 Enter some data in the data field and click on Mine

https://andersbrownworth.com/blockchain/public-private-keys/signatures

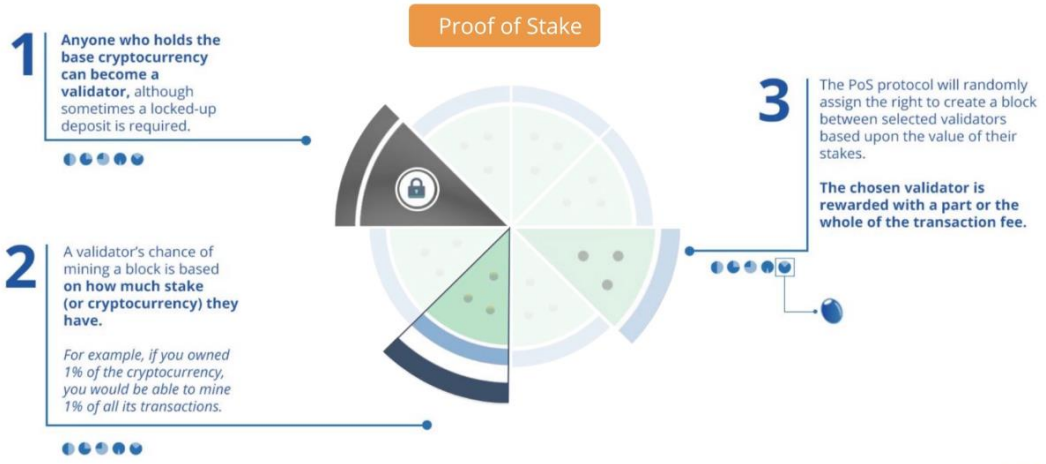
Summary

Step 1 Visit the link https://anders.com/blockchain/hash.html

Step 2 Enter some data in the data field and observe the change in the Hash value

Proof of Stake

A low cost, low energy consuming algorithm which states that a person can mine and validate transaction based on how many coins he or she holds.



Proof of Elapsed Time

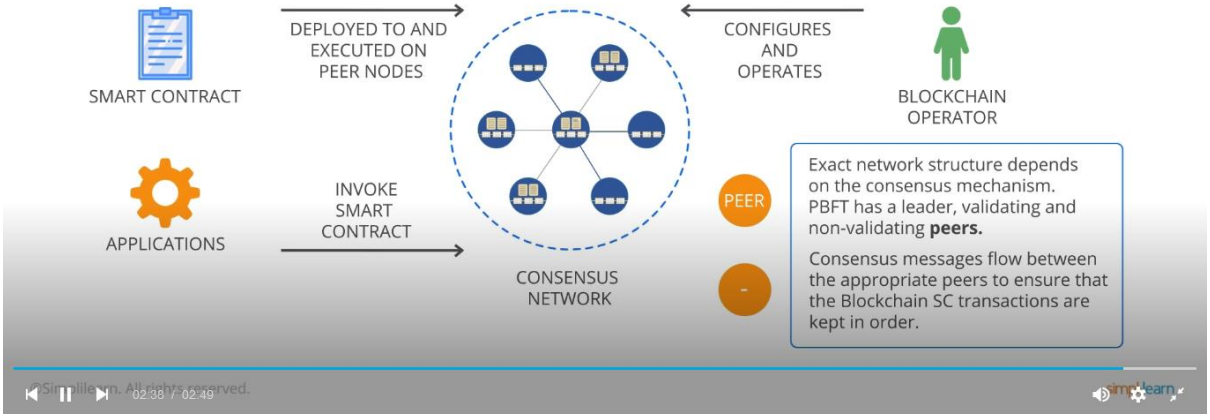
Consensus algorithm prevents high energy consumption and resource utilization following a lottery system.

simplilearn

PBFT

Practical Byzantine Fault Tolerance (PBFT) improves the robustness and performance of transaction by directing peer-to-peer messages with minimal latency.

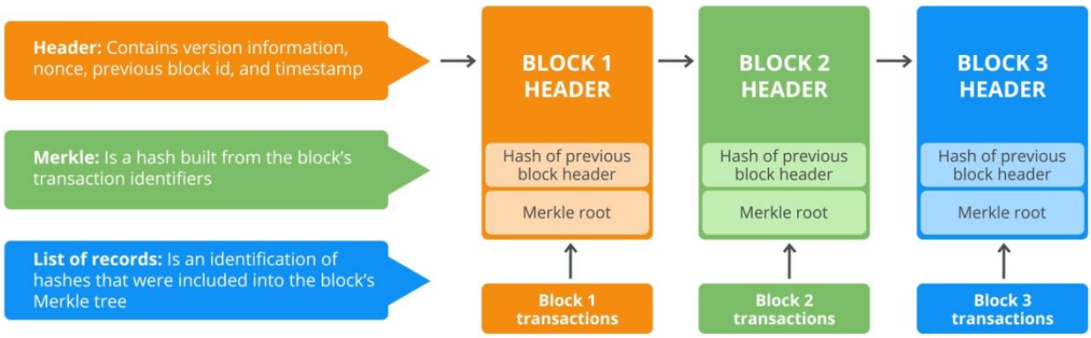
PRACTICAL BYZANTINE FAULT TOLERANCE



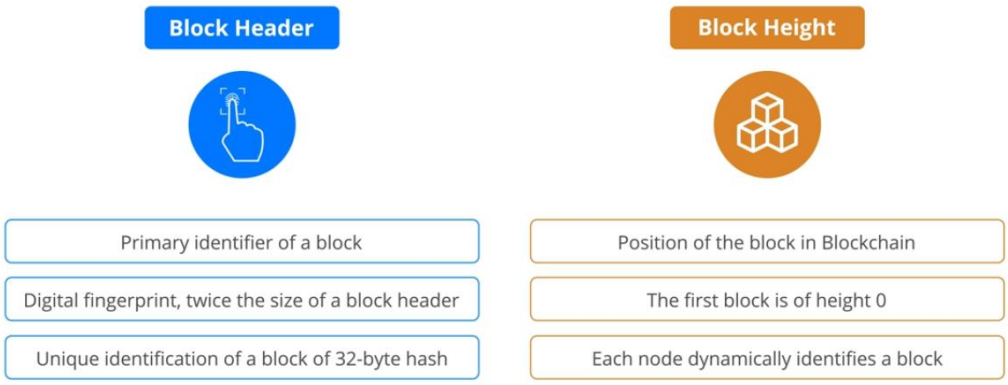
02:38 / 02:49

simplilearn

Blockchain Block Structure

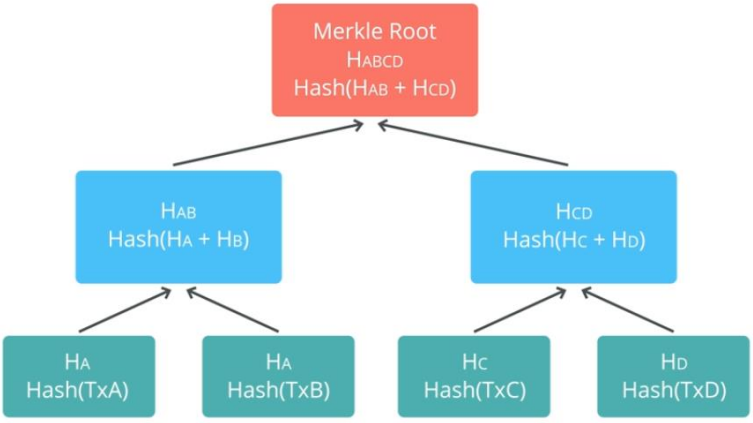


Blockchain Identifiers



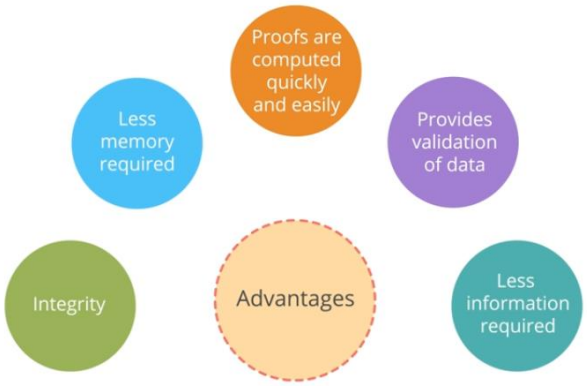
Blockchain Merkle Tree

Data structure used for summarizing and verifying the integrity of large sets of data. It is also known as **Binary Hash Tree.**



simplilearn

Advantages of Merkle Tree



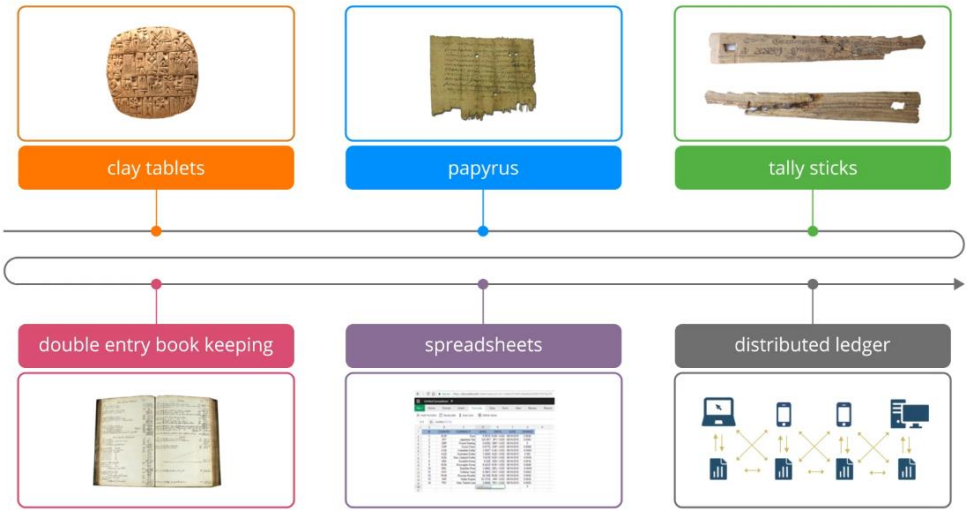
simplilearn

Summary

Step 1 Visit the link https://anders.com/blockchain/block.html and observe the Hash value

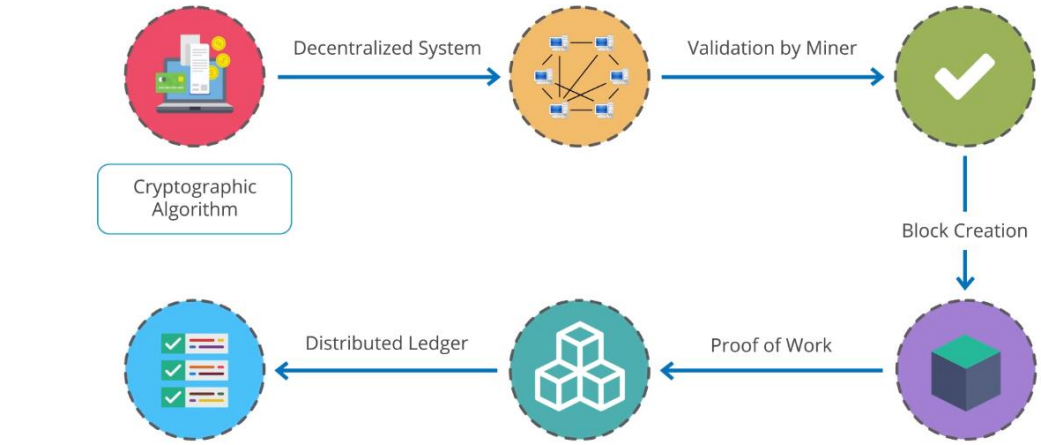
Step 2 Enter some data in the data field, mine the block, and note the Hash value

Evolution of Ledgers



Features of Blockchain in Transaction Process

The diagrams show the usage of Blockchain features in every step of the Blockchain transaction process.



simplilearn

Summary

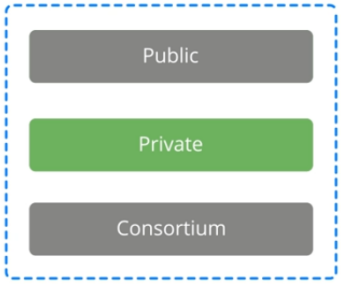
Step 1	Visit the link https://anders.com/blockchain/distributed.html and note the Hash value for Peer A - Block 1
Step 2	Enter data in the data field of Peer A, click on Mine button, and observe the change in Hash value of Block 1
Step 3	Mine the other blocks and verify if the Hash value of the previous block is the same in the next block

Summary

Step 1	Visit the link https://anders.com/blockchain/blockchain.html and enter data in the data field. Observe the change in Hash
Step 2	Change the information in any block and observe how the Hash values change in the subsequent blocks
Step 3	Visit the link https://anders.com/blockchain/tokens.html
Step 4	Change Tx value in Block 1 from 25.00 to 100.00 and mine the block

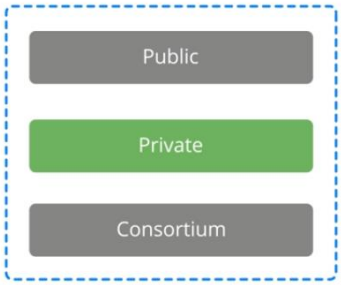
Types of Blockchain

Types of Blockchain



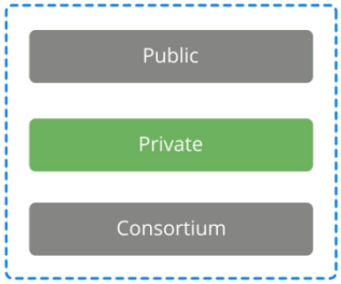
Only authorized users can add or verify the blocks, but anyone can view it.

Types of Blockchain



A private Blockchain is a closed network that offers its participants the benefit of the technology

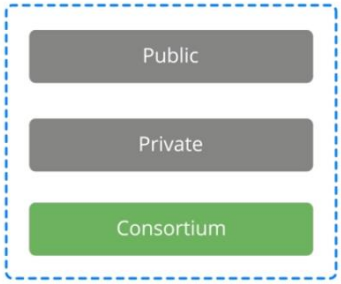
Types of Blockchain



MultiChain BLOCKSTACK

A private Blockchain is a closed network that offers its participants the benefit of the technology

Types of Blockchain

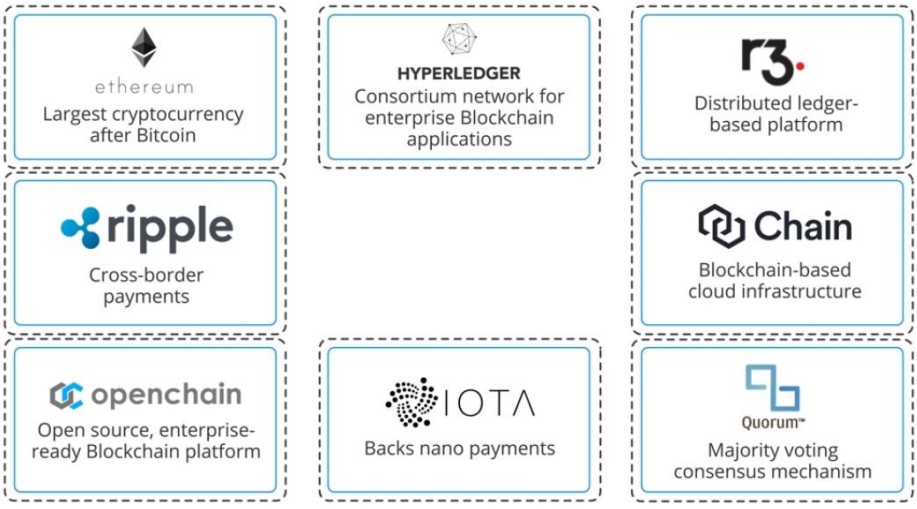




Hyperledger 1.0 | R3 | Ripple

Only a predefined set of nodes has permission to write the block, since it is a semi-centralized Blockchain.

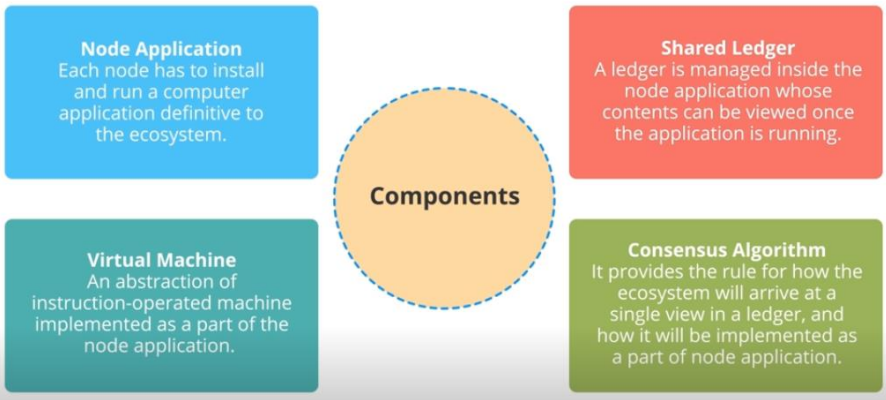
Blockchain Platforms



simplilearn

Blockchain Application Components

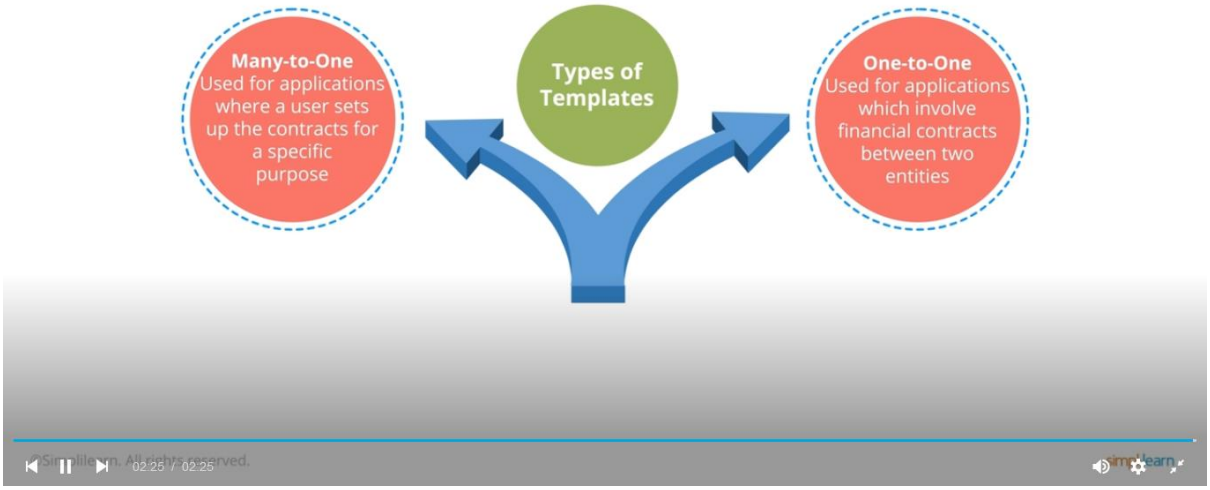
simplilearn.com is now full screen Exit Full Screen (Esc)



02:22

01:54 / 02:25

Blockchain Application Templates



Key Takeaways

You are now able to:

- Describe the Blockchain transaction process
- Generate a public key and a digital signature
- Generate a nonce, a hash code, and a Blockchain block
- Work with a distributed system and perform Blockchain transactions