Blockchain

What exactly is Blockchain?

The blockchain is general terms is defined in following manner:

- A technology that permits transactions to be recorded permanently.
- A technology that cryptographically secure the system and chains data in chronological order.
- A technology that remove intermediaries and create trust through the algorithm.

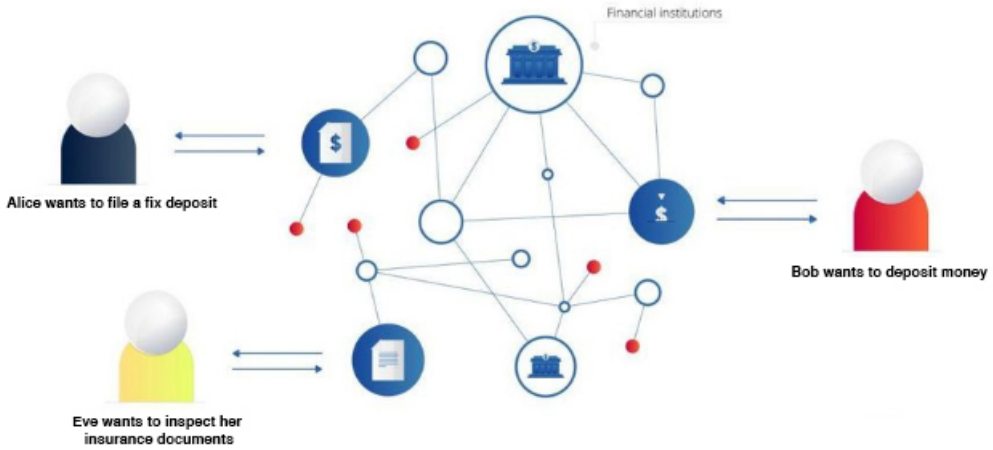
Blockchain was first introduced in the white paper for Bitcoin in 2009 by unknown person named as Satoshi Nakamoto. Currently, blockchain is used my multiple organizations to tackle their problems and provide a better solution.

Current Banking System

Problems with current system

- Account Hacking
- Internet Frauds
- High Transaction Costs
- High Transaction Time due to intermediaries
- Dependency on Banks

Blockchain Banking System



How Blockchain solves the current problem?

- Security through Cryptography
- Availability through multiple machines
- Low transaction costs
- Remove of central parties and intermediaries.

Summarizing Blockchain

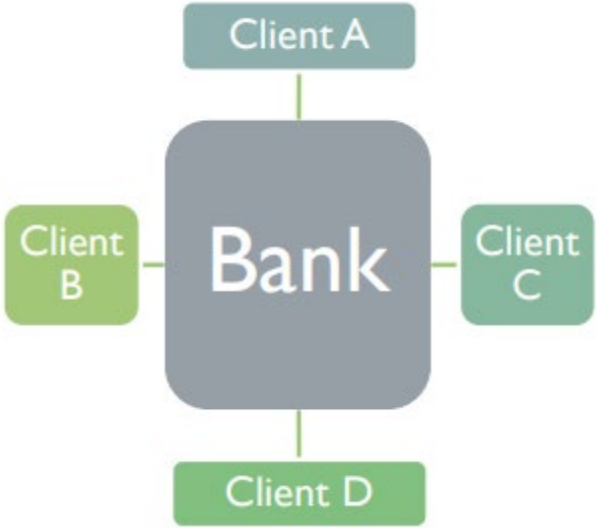
- It's a digitized store for information in the form of transactions.
- It is distributed. Thus, nobody controls it.
- Consensus algorithms make sure of the security and immutability.
- When a new block is added to a blockchain, it is linked to the previous block using a cryptographic hash.
- Data gets recorded in chronological order.
- Everyone present over the network can view the transactions.

Blockchain Definition:

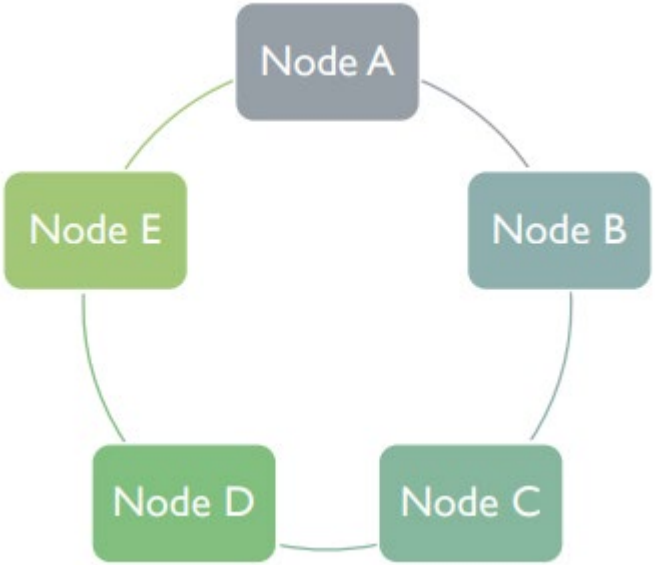
"A blockchain is a digitized, distributed, consensus-based secure storage of information protected from revision and tampering over the peer-to-peer network."

Database vs Blockchain

Typical Database Architecture



Typical Blockchain Architecture



Problems with Database

- Single Point of failure
- Administrator Privileges
- Security issues
- No Transparency

Advantages of Blockchain

- Decentralization
- Immutability
- Transparency
- Security
- Removal of Intermediaries

Difference between Blockchain and Database

Characteristic	Blockchain	Database
Authority	Decentralized	Centralized
Architecture	Distributed	Client-Server Architecture
Data Handling	Only Read and Write	CRUD operations
Integrity	Nobody can change	Alterations are allowed
Transparency	Built In	Not Transparent
Trust	Algorithms	Owner of the Database

greatlearning
Learning for Life

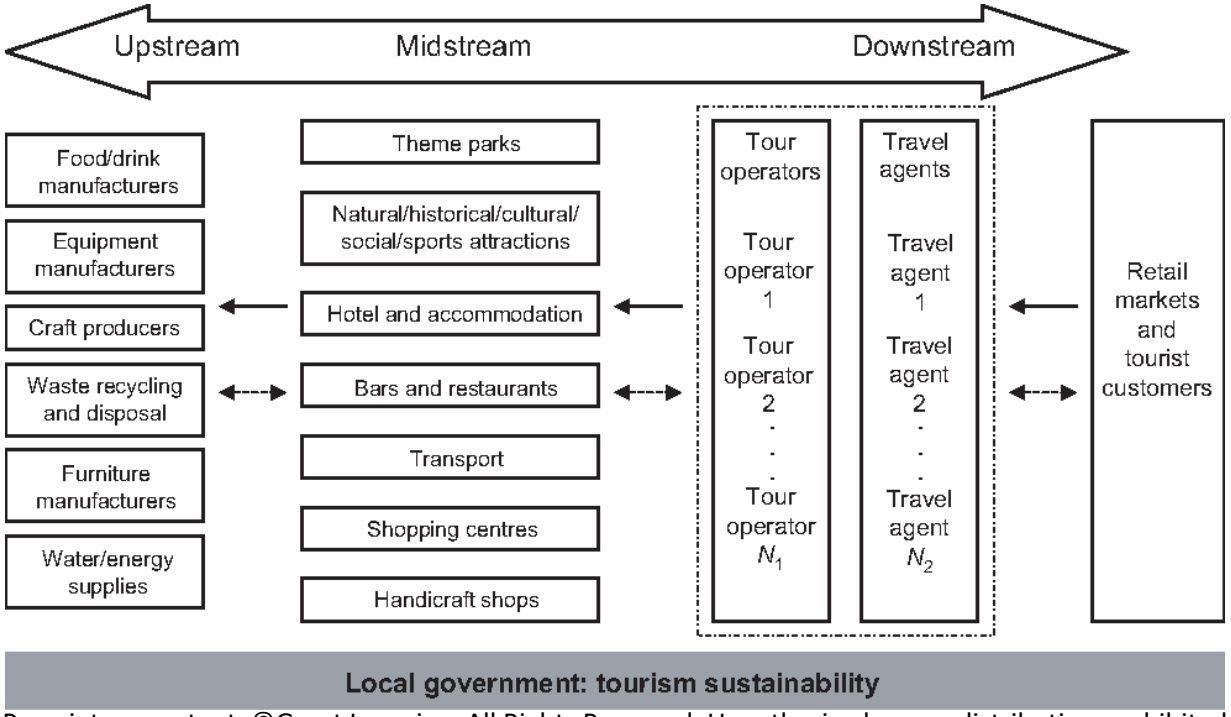
Thank You

Role of Intermediaries

Function of Intermediaries

- Information Gathering
- Promotion
- Contact
- Negotiation
- Physical Distribution
- Financing
- Risk Analysis

Example: Role of Intermediaries in Tourism Industry



Source: https://www.semanticscholar.org/paper/Game-Theoretic-Study-of-the-Dynamics-of-Tourism-for-Huang-Chen/50d2fec75a037be6dc262004fa009a52174b1a21/figure/0

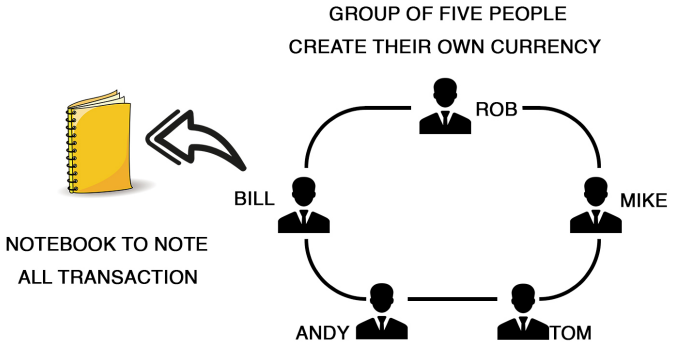
greatlearning
Learning for Life

Thank You

Blockchain Solution

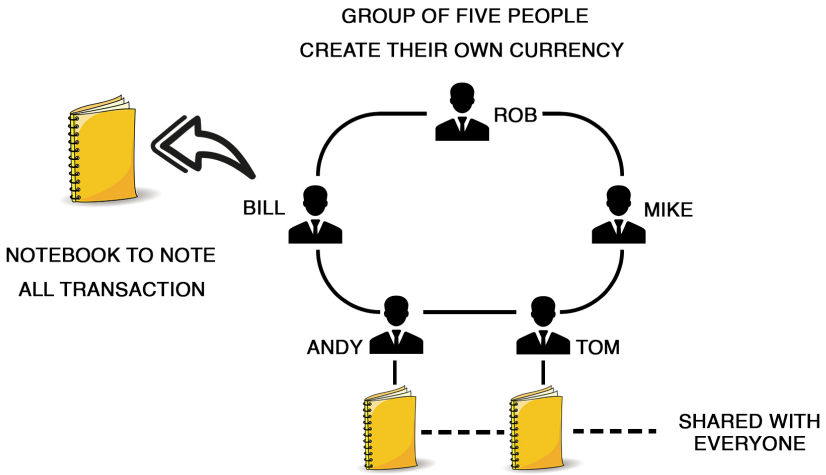
How Blockchain Works?

- Let's imagine that five people in one room decided to make their currency. They need to know the flow of the funds. They appointed one person to track the flow of funds For our example Bill is tracking the flow of funds:



How Blockchain Works?

- After some time Bill decided to cheat the system by changing entries in notebook, so the group decided to share the notebook with everyone.



How Blockchain Works?

- Now, to forge transactions, Bill would need to change all the notebooks.
- Sometime after, the group realized that there were too many transaction records and that he couldn't keep the diary like this forever. After reaching 10,000 transactions, they converted them to a one-page spreadsheet. Andy checked that all transactions are right.
- The group spread his spreadsheet diary over 10,000 computers located globally.
- These computers are called nodes. Every time a new transaction occurs, it has to be validated by the nodes.
- Once every node has received/checked a transaction there is a sort of electronic vote, as some nodes may think the transaction is valid and others believe it is a fraud.
- Now, if Bill changes one entry, all the other computers will have the original entries. They would not allow fraud entries to occur.

Summarising

- This spreadsheet created in the example is called a block.
- The whole chain of blocks is collectively called as Blockchain. Every node holds a copy of the Blockchain. Once a block reaches a certain number of approved transactions, then a new block is formed.
- The Bitcoin Blockchain updates itself every ten minutes.
- As soon as the spreadsheet or ledger or registry is updated, it can no longer be changed. Thus, it’s impossible to forge it.

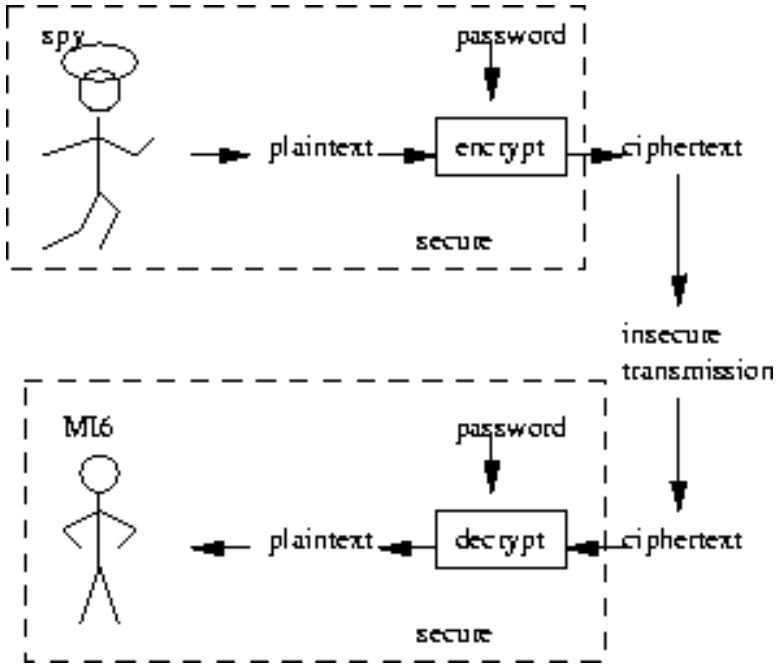
greatlearning
Learning for Life

Thank You

Blockchain Cryptography

Introduction to Cryptography

Cryptography is an important aspect when we deal with network security. ‘Crypto’ means secret or hidden.

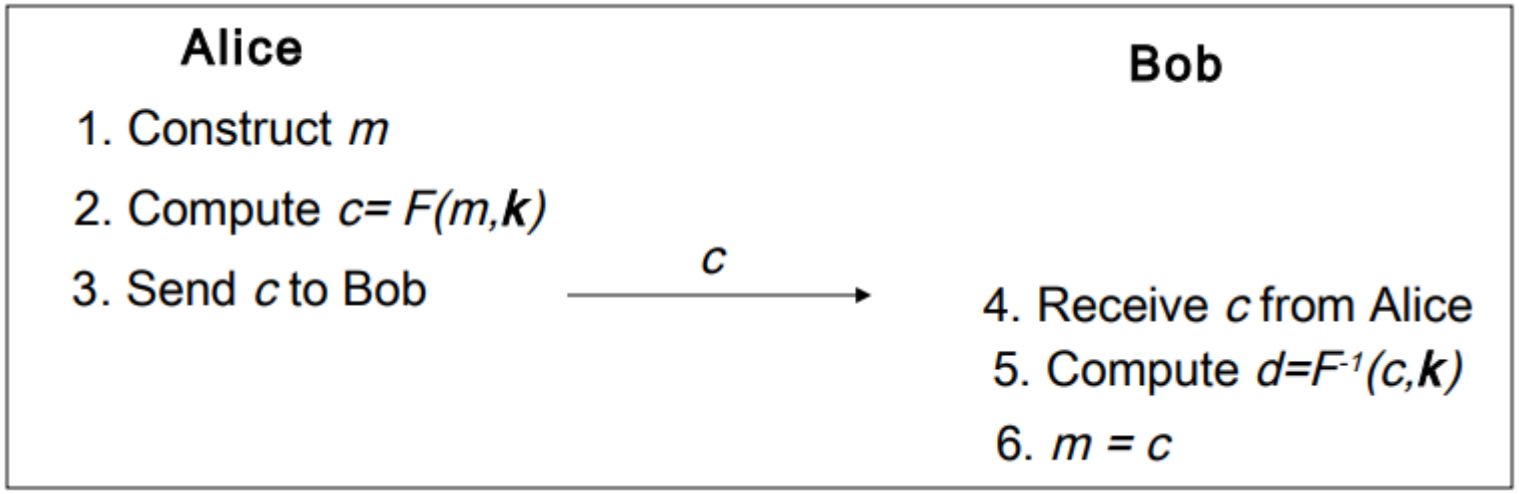


Source: Stanford

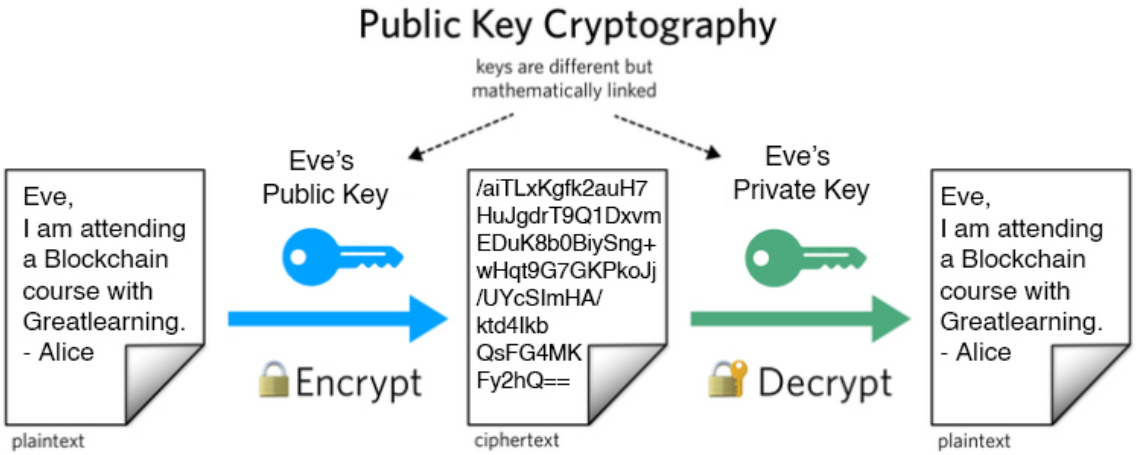
Types of Cryptography

- Symmetric aka Private Key Cryptography
- Asymmetric aka Public Key Cryptography

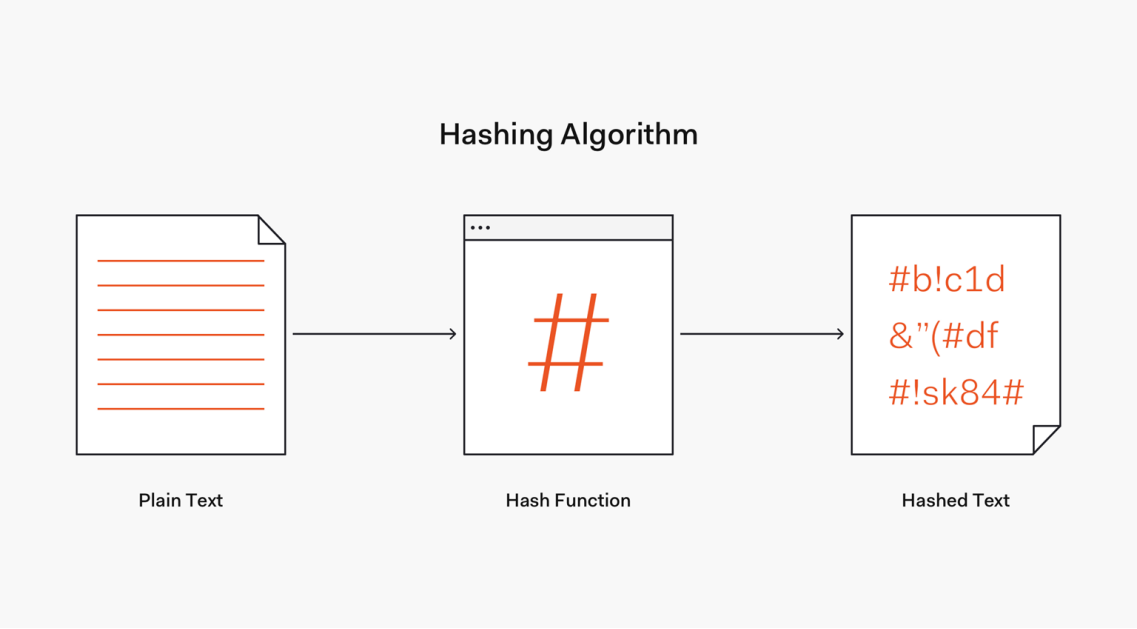
Symmetric Cryptography



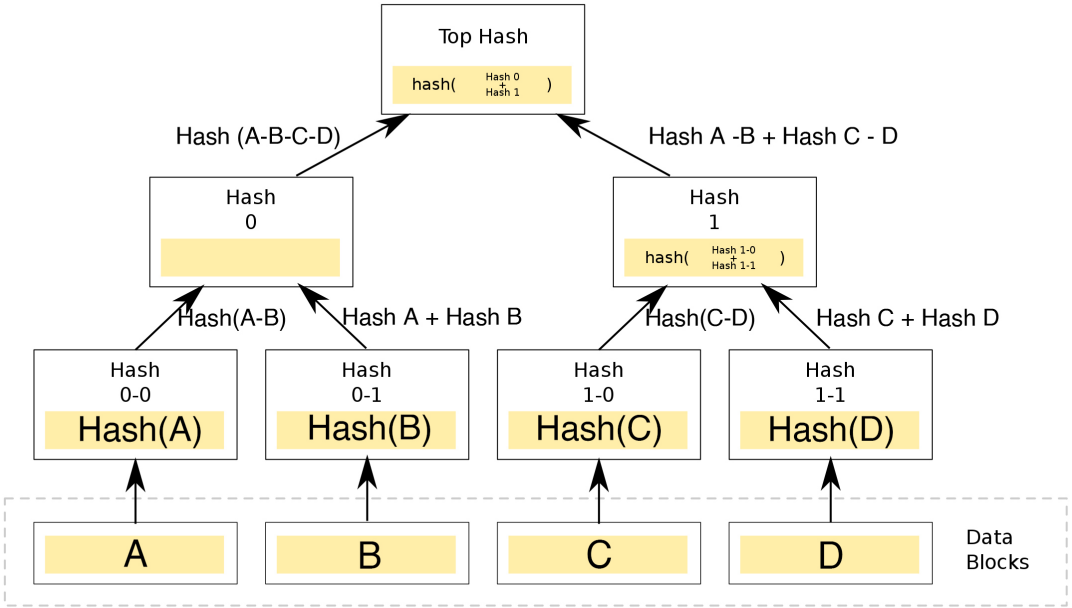
Asymmetric Cryptography



Hashing


Hashing Algorithm
#
#b!c1d
&”(#df
#!sk84#
Plain Text
Hash Function
Hashed Text

Merkle Trees



Thank You

Accounts, Blocks, Transactions and Merkle Trees

Blockchain Accounts - Private Key

- In general once you create an account on Blockchain, you will get a Private Key and a public address.
- Private Key is used to generate a signature for each transaction over the blockchain.
- The generated signature is used to confirm that the transaction has come from a specific user, and also prevents the transaction from being altered by any malign entity.
- In simple words - “Private Keys are used to sign the cryptocurrencies you send to others.”
- Example: **L34EXrFCuxQCorfE66sxQe8Tyh71SyU8cc9z7HnbEWwW8YsgbvTw**

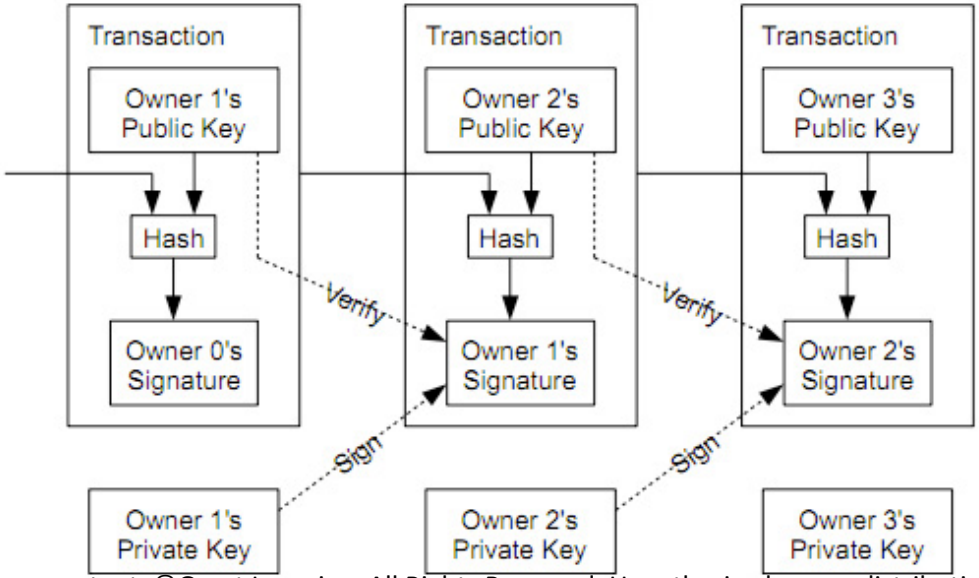
Blockchain Accounts - Addresses

- A cryptocurrency address in a core is a representation of the public key.
- One-way cryptographic hash functions are used to derive address from the public key.
- For example in Bitcoin, the algorithms that are being used to generate a bitcoin address from the public key are the Secure Hash Algorithm 256 (SHA-256) and the RACE Integrity Primitives Evaluation Message Digest 160 (RIPEMD-160)
- The address appears typically in a transaction between two parties, with the address signifying the recipient of the funds.
- Example: **1JPgMJuAvYJU6mxxbJdmf1XBd7bBPdPV3a**

Transactions

- Transactions are records of data in chronological order
- Transactions are stored in a Merkle tree inside the Block.
- The transactions, when submitted, are picked up by the blockchain network and is inserted into a ‘pool of unconfirmed transactions.’ The transaction pool is a collection of all the transactions on that network that have not been confirmed yet.
- Miners on the network select transactions from this pool and add them to their ‘block.’
- Transactions also contain metadata information which can be utilized to store data over the Blockchain.

Transactions



Source: https://bitcoin.org/bitcoin.pdf

Blocks

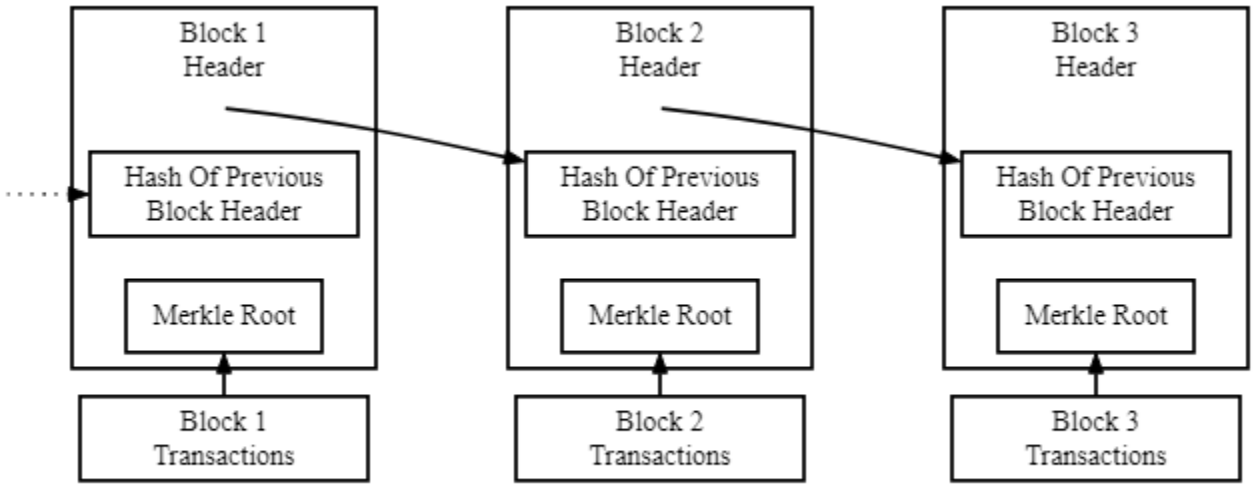
- A Block is a container data structure which contains a set of confirmed transactions.
- A block could contain different information, and a chain of these blocks evolves into a blockchain as long as it links one and the other.
- The blocks are stored on the hard drives of many miners spread across the globe on a peer to peer network.
- In the Bitcoin algorithm, a block is created every 10 minutes. All the transactions happening over the network within 10 minutes interval are crunched into that block and added to the chain.

Structure of Blocks

All blocks in the Blockchain are composed of a header, identifiers and a long list of transactions. The structure of a block is as follows:

- Block Header
- Block identifiers
- Merkle Trees

Blocks



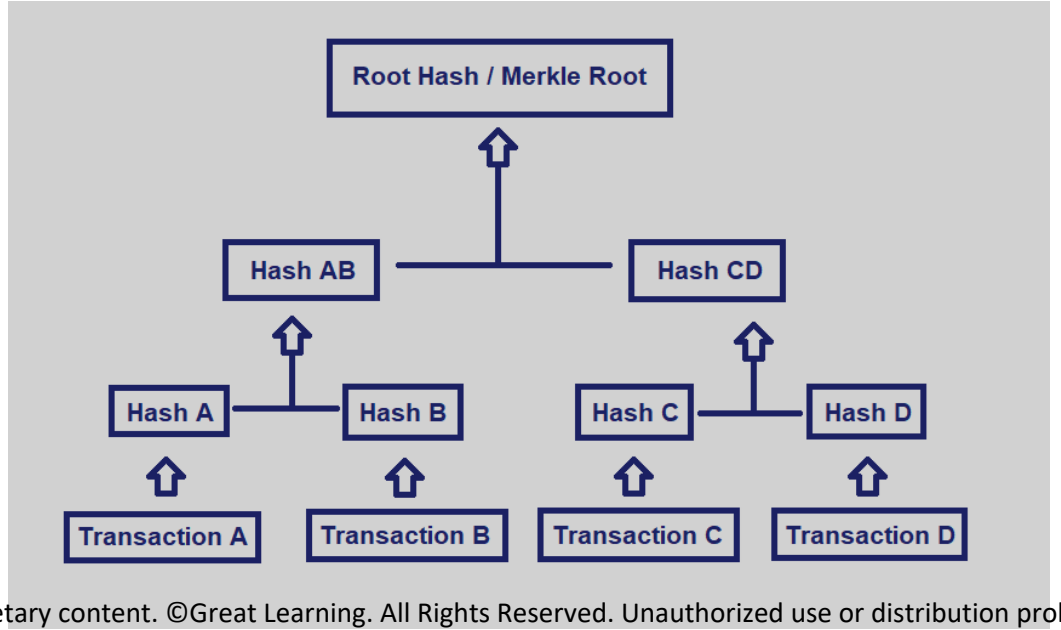
Simplified Bitcoin Block Chain

Source: https://bitcoin.org/en/blockchain-guide

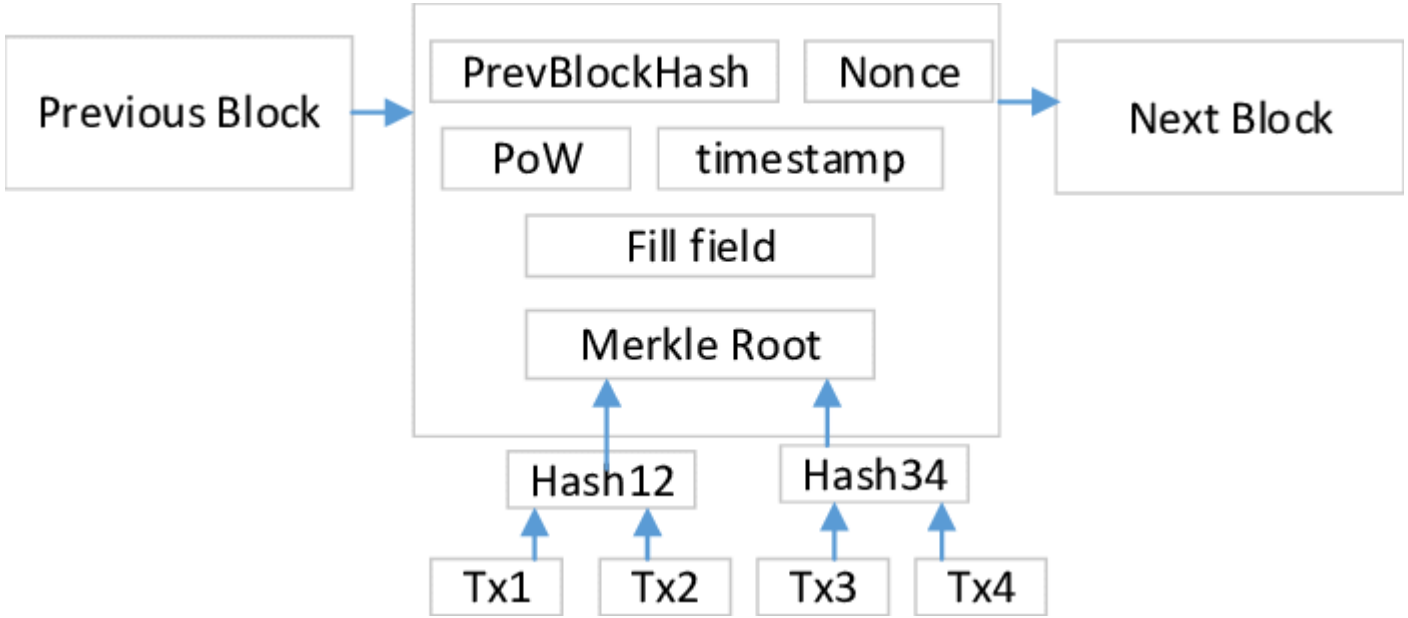
Example of Bitcoin Block

Field	Description	Size
Magic No	value always 0xD9B4BEF9	4 bytes
Blocksize	number of bytes following up to end of block	4 bytes
Blockheader	consists of 6 items	80 bytes
Transaction Counter	positive integer VI = VarInt	1 - 9 bytes
Transactions	The (non empty) list of transactions	Transaction counter-many transactions

Merkle Tree



Merkle Tree with a Block



greatlearning
Learning for Life

Thank You

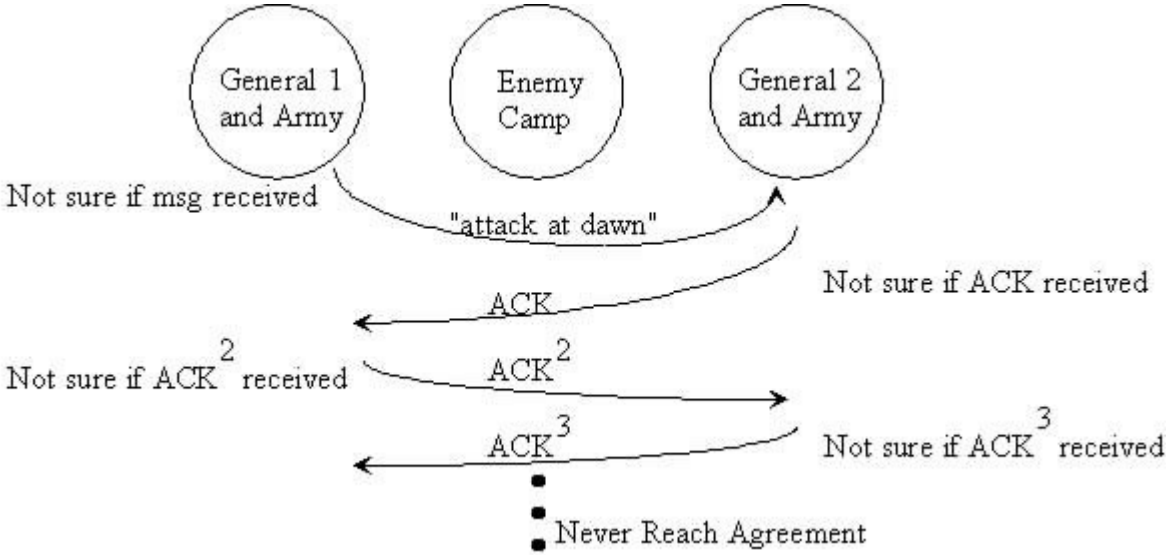
Consensus Mechanism

What is Consensus?

- Blockchains are decentralized systems which consist of different participants who act depending on incentives they receive and the information that is available to them.
- When a new transaction gets broadcasted on the network, nodes connected to the network have the option to either include that transaction to their copy of ledger or to ignore it. When the majority of the nodes which comprise the network decide on a single state, the **consensus** is achieved.

Let’s dive into 2 Generals Problem and understand the consensus better.

Two Generals Problem

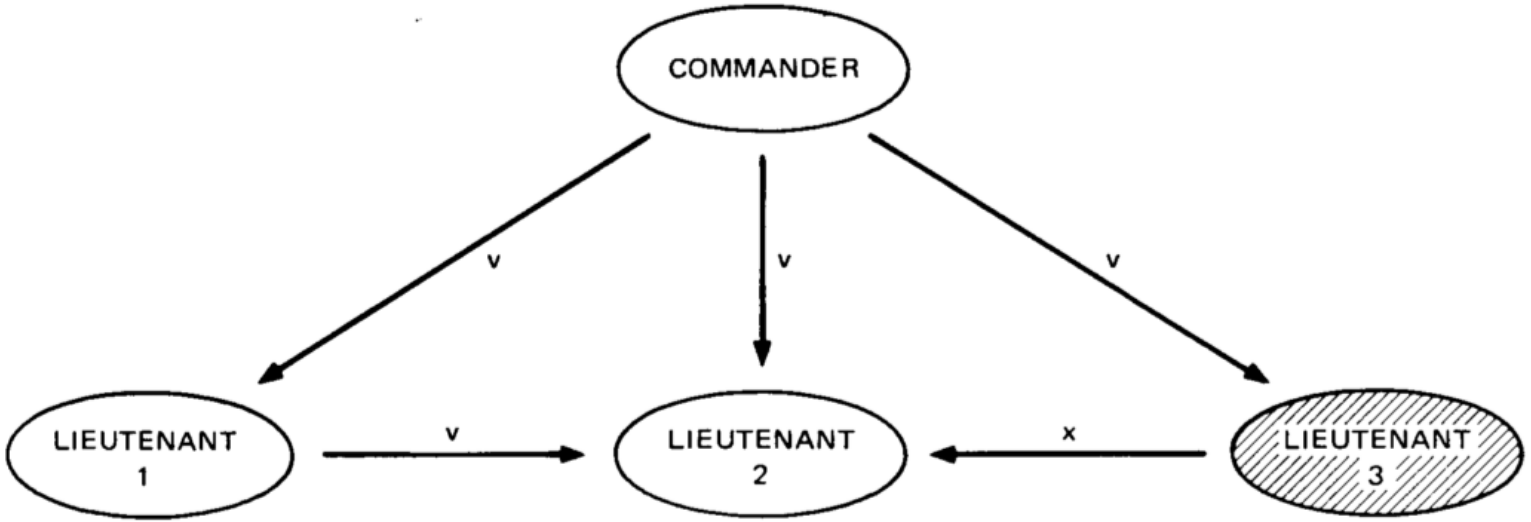


Source: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-1-byzantine-fault-tolerance-245f46fe8419

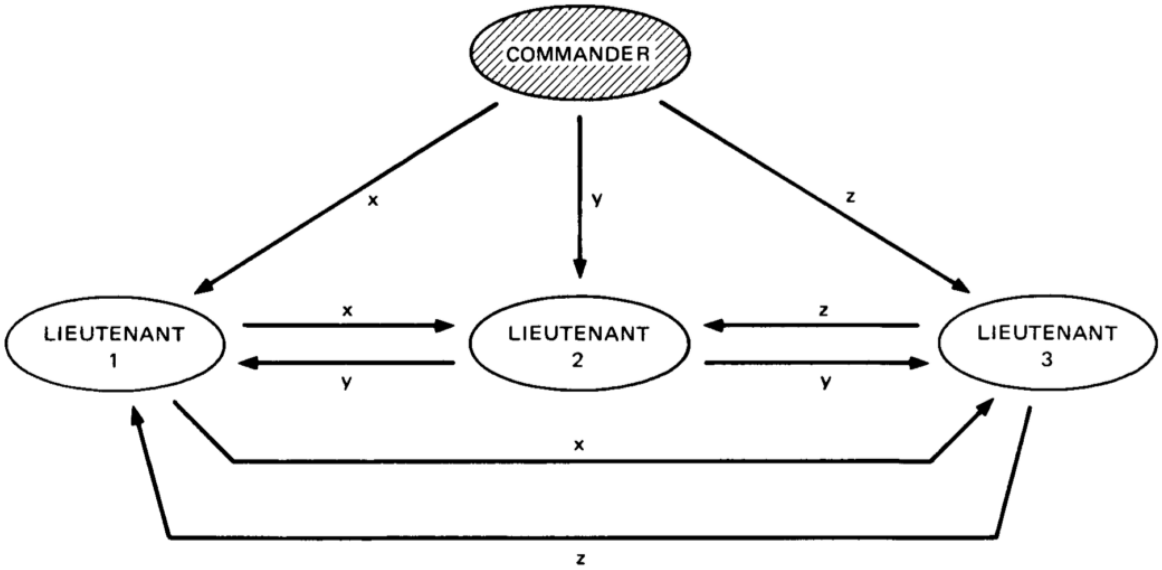
Byzantine Generals Problem

- A more generalized version of the Two Generals Problem describes a group of generals agreeing on the time of the attack. Apart from that, one or more generals can be the traitors, meaning that they can lie about their attack choice (e.g., they say that they agree to attack at 9 am, but instead they do not attack).
- To reach a consensus here, all the generals must agree on the same decision.
- Let's change the scenario to a Commanding General who issues the attack and all others as who will follow the same to attack.
- If the Commanding General is a traitor, the consensus is still achieved. As a result, all lieutenants take the majority vote over the Default value.
- This implies that the algorithm can reach a consensus as long as 2/3 of the actors are honest. If the traitors are more than 1/3, the consensus is not reached, the armies do not coordinate their attack, and the enemy wins.

Lieutenant is the Traitor



Commander is the Traitor



Solution

- Take an example; every Lieutenant take 10 mins to convey orders. In other words, 10 minutes are required for communicating a message for an attack.
- Moreover, the passing of messages is in a way where each message is appended to the last message before sending it to the next Lieutenant.
- Example:
  - General - Attack at 9 am
  - Lieutenant 1 - Attack at 9 am, Attack at 9 am
  - Lieutenant 2 - Attack at 9 am, Attack at 9 am, Attack at 4 am
- If the Lieutenant 2 is a traitor, then the 3rd Lieutenant can verify that the incoming message is not in synchronization.
- Moreover, if Lieutenant 2 decides to change all the previous messages too, then each message would take 10 minutes thus Lieutenant 2 will be working for 30 mins.
- But Lieutenant 3 expects the message to come in 10 minutes, thus again giving in that Lieutenant 2 is a traitor.
- If the commander is a traitor, then he might send different orders to different Lieutenants, which will come into consensus but since the messages don't follow the structure of providing in the same attack time, the default option of retreat will come to action.

How does it relate to Blockchain?

- This is solution which is described with Proof of Work for Bitcoin Blockchain.
- Each block has to follow the formulation guidelines of 10 mins in Bitcoin.
- Each block is appended to the last one by incorporating the Block hash.
- Consensus is achieved once ⅔ of the actors agree on a block.
- Verification of the Blocks is done by the miners.

greatlearning
Learning for Life

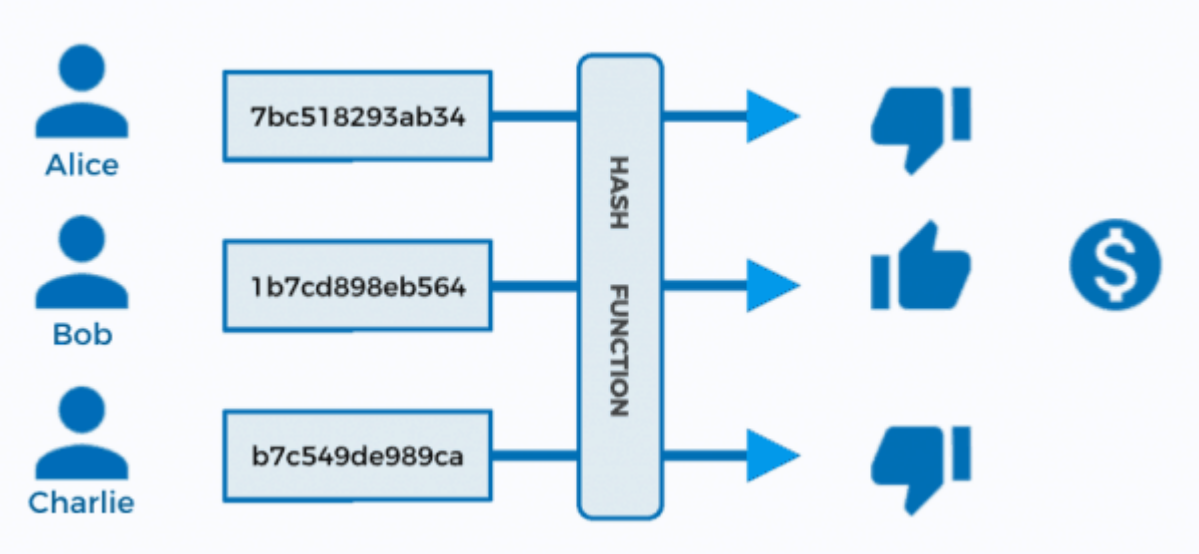
Thank You

Proof of Work and Proof of Stake

Proof of Work

- Proof of Work is the consensus algorithm where miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm.
- Some of the problems included with Proof of Work are:
  - Hash function - how to find the input knowing the output.
  - Integer factorization - how to present a number as a multiplication of two other numbers.
  - Guided tour puzzle protocol - If the server suspects a DoS attack, it requires a calculation of hash functions, for some nodes in a defined order. In this case, it's a 'how to find a chain of hash function values' problem.
- Miners receive a reward when they solve the complex mathematical problem.
- For example in Bitcoin miners receive 12.5 bitcoins for solving the puzzle.
- Miners can also receive transaction fees in addition to rewards.

Proof of Work



Proof of Stake

- Proof-of-Work algorithm rewards miners who solve complex mathematical problems with the end goal of validating transactions and creating new blocks. On the other hand, in the Proof-of-Stake algorithm, the creator of a new block is chosen in a deterministic way, depending on its wealth/stake in the blockchain.
- No block reward
- All the digital currencies are created at the start of the chain, and their number never changes. Miners only take the transaction fees.

Proof of Stake

Proof of stake

The blocks are validated as per the stake held by the person over the Blockchain.

Miners/Validators only collect the transaction fees as per the stake.

There is no complex computation involved that's why they are more efficient then proof of work systems

Proof of Work VS Proof of Stake

Mining is dependent upon the computational power of the nodes

Mining is dependent on the stake of the validators.

Miners receive block rewards with transaction fees for guessing the value of nonce.

Miners don't receive block rewards, only transaction fees are distributed to miners.

Nobody can modify the blockchain until and unless they have more than 51% power of the complete blockchain.

Attackers require 51% or greater stake on blockchain to take over blockchain, the cost is very high compared to the POW 51% attack.

greatlearning
Learning for Life

Thank You

Mechanism of Blockchain Transaction

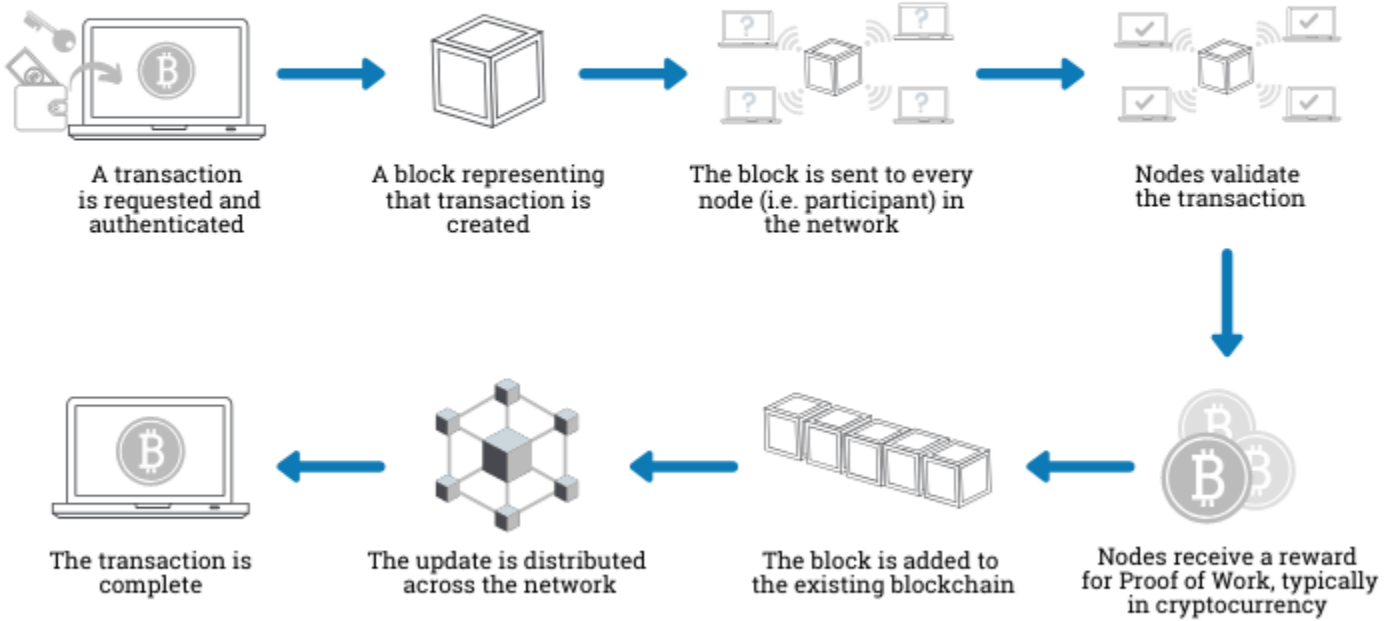
How a Blockchain Transaction Works?

- **Step 1**: A user creates a transaction from their wallet,, attempting to send currency or data to someone else.
- **Step 2**: The transaction is put across a ‘pool of unconfirmed transactions’. This pool is a collection of unconfirmed transactions that are waiting to be processed by the miners.
- **Step 3**: Miners on the blockchain select transactions from these pools and form them into a ‘block’. A block is basically a collection of transactions with some extra metadata. Every miner creates their own block. Multiple miners can put in the same transactions in their block.

How a Blockchain Transaction Works?

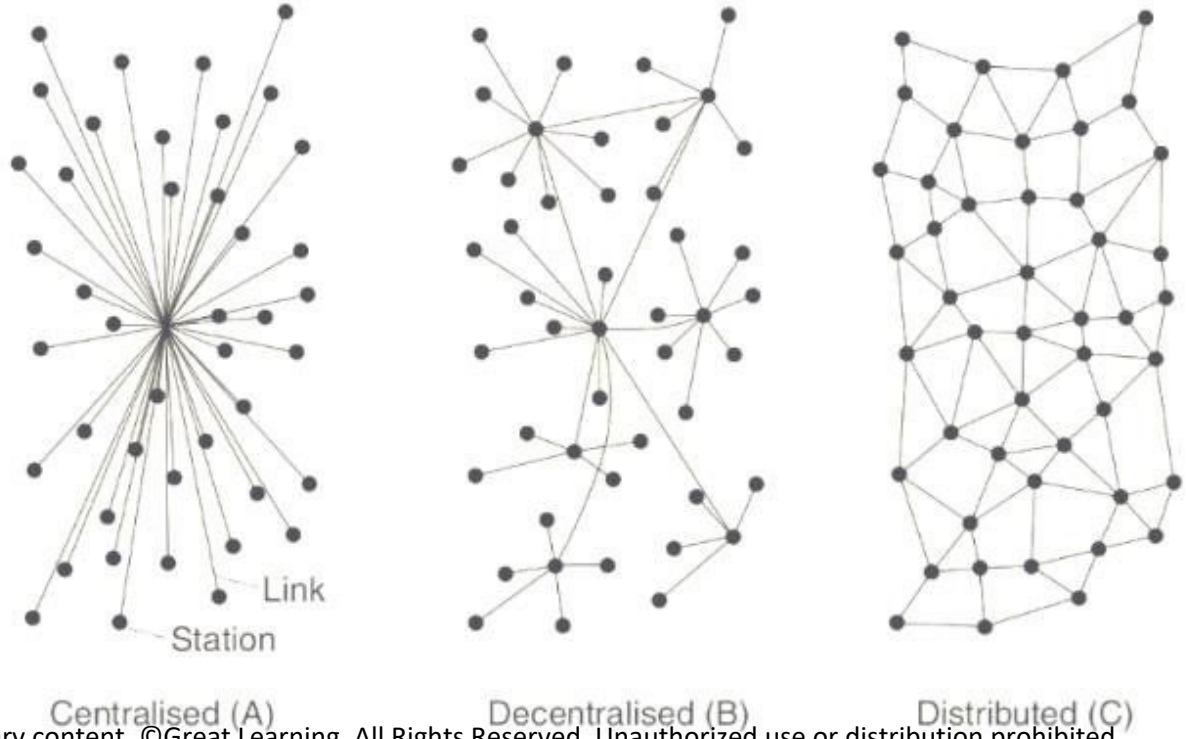
- **Step 4**: Once the block is created, miners generates a block signature. This signature is created by solving a complex mathematical problem. Each block has a different mathematical problem as per the transactions.
- **Step 5**: The miner that finds a target signature for its block first, broadcasts this block and the signature to all the other miners.
- **Step 6**: Other miners verify the signature If it is valid, the other miners will confirm its validity and agree that the block can be added to the blockchain. This process is also termed as consensus.

How does a transaction get into the blockchain?



Source: https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain

Transaction Distribution



greatlearning
Learning for Life

Thank You

Blockchain Ecosystem

Blockchain Projects

The Blockchain ecosystem is currently running with some major projects and more are under pipeline. Some of the major projects on Blockchain are:

- **Bitcoin** - This project introduced the world to Blockchain.
- **Ethereum** - This project came with concept of Smart Contracts where two parties adhere to certain rules and create a trust. This opens the world for more decentralized applications.
- **Neo** - This project positioned itself as the “Chinese Ethereum” but it bought the Python as the main language for the creation of Applications.
- **Hyperledger Fabric** - This is an enterprise graded project which can be easily programmed as per the enterprise needs. This is a modular project which supports multiple consensus algorithms.

Blockchain Users

- Blockchain users are normal people like you and me, who make use of the blockchain or cryptocurrency to achieve some results. They can also be investors who buy cryptocurrencies to sell at a later date.
- For creating a Blockchain user base the technology or cryptocurrency should have some utility related to the problem being tackled.

For Example:

- Bitcoin serves the major utility of payment for goods and services. Currently there are over 50,000 merchants registered with Bitcoin including - Microsoft, PayPal and Subway.
- Bitcoin was the first mover in Blockchain and it's high utility as payment system made sure that a large part of its ecosystem is based upon users.

Blockchain Exchanges

- Every Blockchain project has a robust ecosystem working under it, and it always include a decentralized exchange. These are developed by the Blockchain team or the community of other developers.
- A typical exchange is designed to find the cheapest rates of exchange between any two cryptocurrencies, making it more affordable to trade tokens/cryptocurrencies.
- Exchanges used for trading also might integrate with hardware wallets, or users can create their own wallet on the exchange website.

Blockchain Verfiers/Miners

- To function a blockchain and maintain its integrity, it needs a large network of independent nodes around the world to maintain it continuously. In private blockchains, a central organisation has the authority over every node on the network. In the case of public blockchains, on the other hand, anyone can set up their computer to act as a node. The owners of these computers are called miners.
- Since the integrity of the blockchain is directly related to the number of independent nodes on the network, there also needs to be some incentive to mining. Different blockchains utilize different mining systems however most of them contain some form of:
  - An incentive system
  - A consensus algorithm

Blockchain Developers

- Blockchain technology is built by the potential of developers working behind it. A strong team of developers can lead to a successful Blockchain project. Currently there are two types of developers in the blockchain ecosystem:
  a. Blockchain developers
  b. dApp developers

- Blockchain developers build new blockchains with different levels of functionalities and Consensus Algorithms.
- dApp developers work with decentralized applications that can run on blockchains thus providing a similar functionality like Google Play Store over the Blockchain Technology.
- The development of Smart Contracts over the Blockchain has open possibility for the developers to create extensive applications and use cases for the industries.

Blockchain Applications

Apart from exchanges, platforms and users, another important aspect of the Blockchain ecosystem is the applications that industries, developers and communities build to serve a specific purpose.

There are various examples of Applications being build upon Blockchain, some of the major working applications are:

- **CryptPad** - A decentralized document creation application.
- **Humaniq** - A fintech startup which connects unbanked people with global economy.
- **Augur** - A peer to peer oracle and prediction market place.
- **Filament** - Building the IoT applications over the Blockchain.

greatlearning
Learning for Life

Thank You

Why Industries need Blockchain?

Current Blockchain Implementations

- **Pharmaceuticals** - DHL worked with Accenture to establish a blockchain-based track-and-trace system in six areas worldwide. Currently, the system has 7 billion unique pharmaceutical serial numbers and handling more than 1,500 transactions per second.
- **Fashion** - CGS has developed a system for tracking garments and compliances on raw materials for many apparels and fashion clients.
- **Cross-Border Payments** - IBM has developed a new blockchain banking solution that allows financial institutions to move quickly and cost-effectively process payments globally.
- **Food Safety** - IBM has partnered up with Dole, Nestlé, and Walmart to set up a blockchain for better regulation of food.
- **United Nations** - United Nations is currently using Blockchain for 16 agencies including Human Trafficking and World Food Program.
- **Jewelry** - Brilliant Earth has partnered up with Everledger to use blockchain in tracking and tracing the provenance of diamonds and other gemstones. This will also ensure that they are conflict-free.

Blockchain Revolution

Exciting Disruptions Coming Soon

- **Entertainment Industry** - Movie Braid was the first movie to be produced by doing an ICO.
- **Property Rental** - Rentberry aims to address the common pitfalls and headaches of the traditional rental model.
- **Politics** - Sierra Leone carried out their elections on Blockchain.
- **Education** - Socrates Coin is making big moves to change the traditional approach to a “3DInternet”.
- **Digital Advertising** - Basic Attention Token is taking a crack to solve the problems with Digital Advertisements.
- **Internet of Things** - Waltonchain, an award-winning Chinese project that seeks to integrate IoT and blockchain technology on an unprecedented scale.

greatlearning
Learning for Life

Thank You

Industry Challenges for Blockchain Adoption

Energy Consumption

- Some major public Blockchains use Proof-of-Work algorithms.
- PoW involves the use of the computational power of a machine to solve a complex mathematical puzzle to verify a transaction and add it to a block.
- Current Bitcoin energy consumption is almost equal to the consumption by Ireland.
- By 2020 it's estimated that Bitcoin will utilize more energy consumption than the entire world currently uses.
- A probable solution for this has emerged in the form of different consensus mechanisms like Proof-of-Stake, Delegated-Proof-of-Stake, etc.

Scalability

- Scalability has appeared as a significant issue for the Blockchain networks like Bitcoin and Ethereum.
- Blockchains are having trouble effectively supporting a large number of users on the network.
- Moreover, the size of public blockchains keeps on increasing. Currently, Bitcoin ledger size is above 100 GB.
- One possible solution which has emerged is storing a hash of data over the network.

Public Perception

- Presently, blockchain technology is almost synonymous with Bitcoin.
- The majority of the public is still oblivious to the existence and potential uses of Blockchain technology.
- As Bitcoin is anonymous and is used for shadowy dealings of money laundering, black market trade, and other illegal activities. The blockchain is also getting a bad reputation due to the same.
- Mainstream adoption is needed to remove the sometimes-negative undertones of Bitcoin.

Standards and Regulations

- Blockchains are continuously evolving, but still, countries are skeptic about it as there is no proper definition for standards and regulations.
- Enterprises and Governments require regulations to protect their customers.
- To tackle this problem, certain countries are trying to launch their regulations over the technology.
- Mass adoption might also standardize the Blockchain.

greatlearning
Learning for Life

Thank You

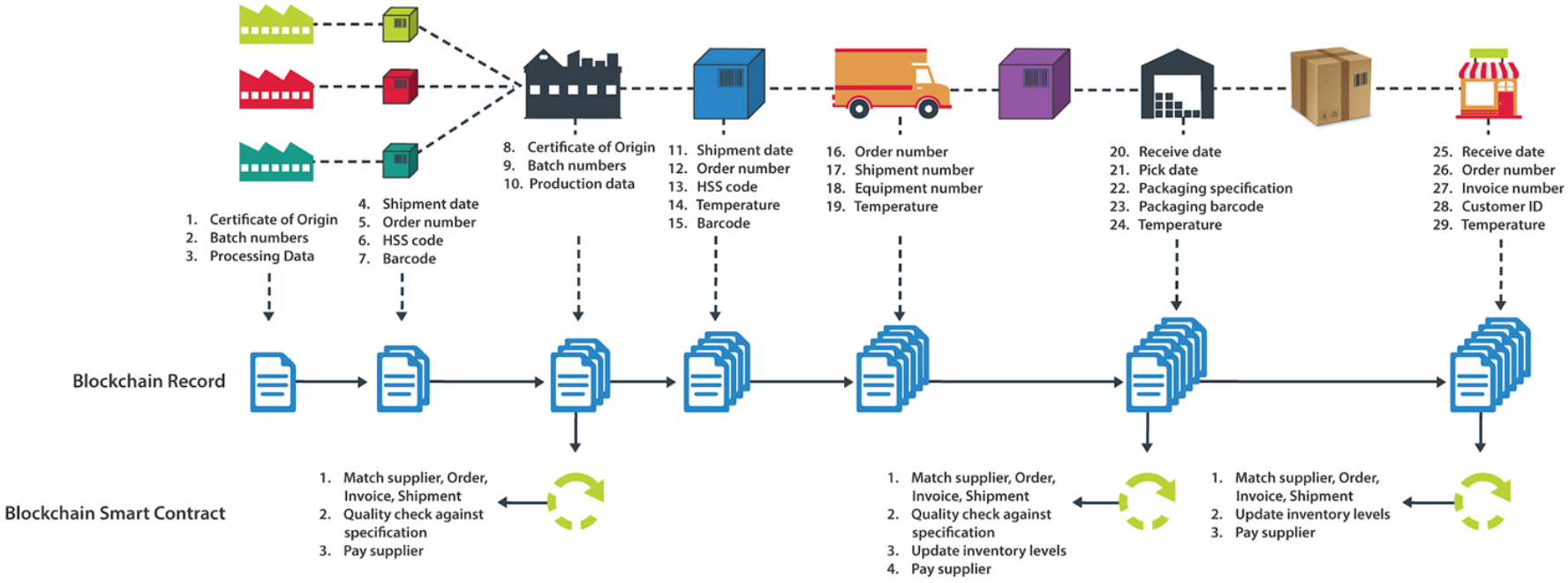
Blockchain Examples

Walmart Food Tracking

Challenge: It can take upto days weeks to track the source for an outbreak of a food-borne disease.

Benefit: Better traceability could help save lives by allowing companies to act faster and protect the livelihoods of farmers by only discarding produce from the affected farms.

Approach: Walmart created a food traceability system based on Hyperledger Fabric. Walmart, together with IBM, ran two POCs to test the system. First one for tracing mangos sold in Walmart US stores and the other one to trace pork sold in its China stores. The tracing improved from 7 days to 2.2 seconds.



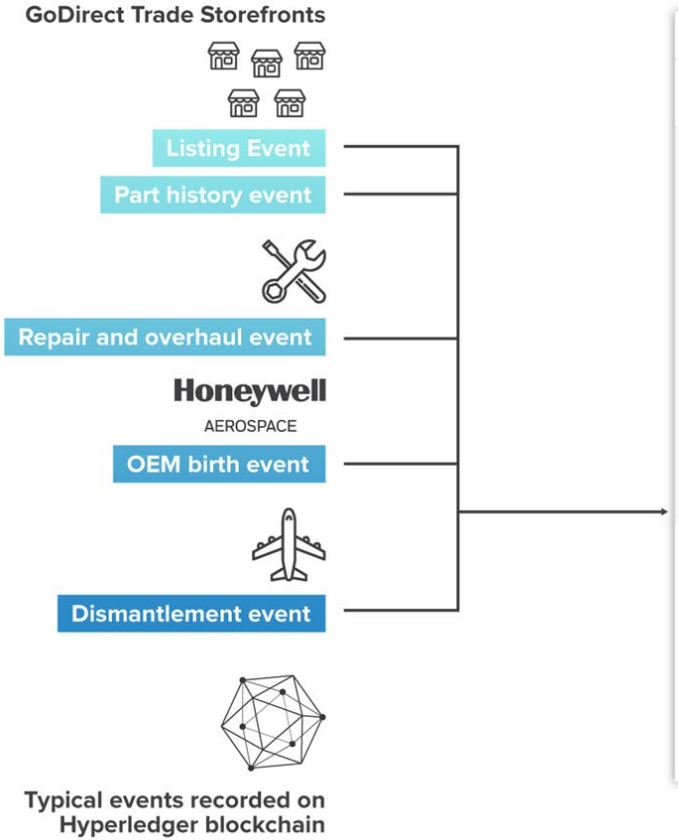
Source: https://aqurus.ca/blockchain-crucial-link-supply-chain/

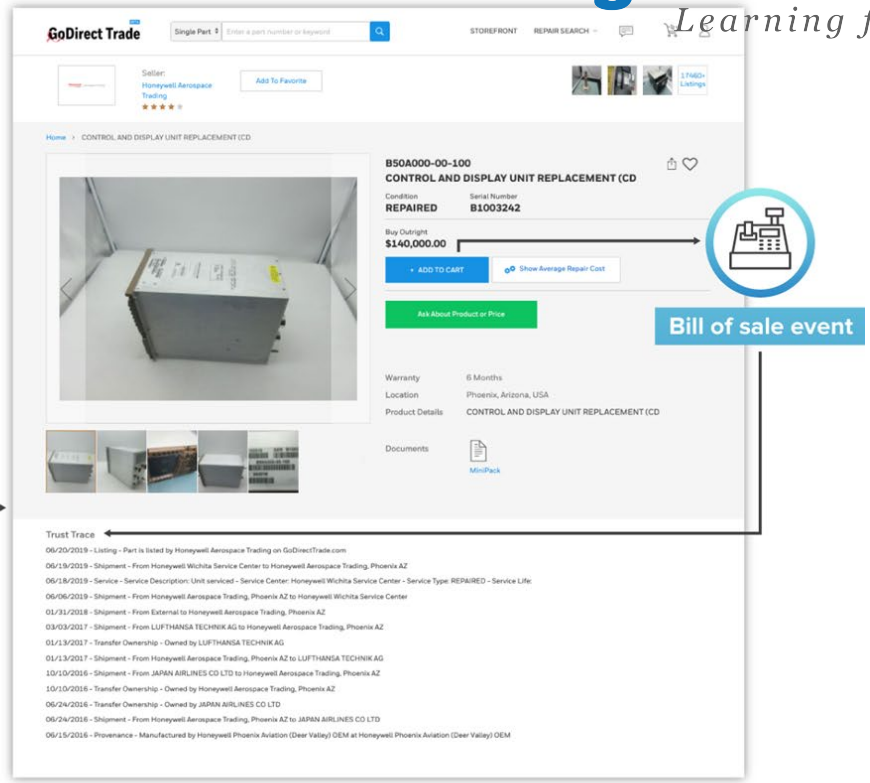
Honeywell Marketplace

Challenge: To cut purchasing time for aerospace products from days or weeks down to seconds. Also, to connect each physical part to its digital equivalent.

Benefit: Purchased time reduced from days to minutes and boost to anti-counterfeit measures.

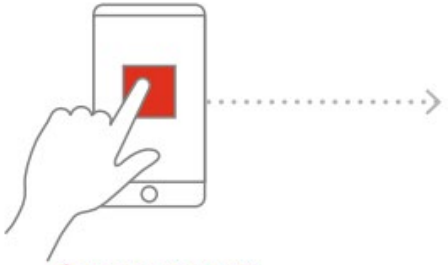
Approach: Honeywell created a online marketplace system based on Hyperledger Fabric. Tracking of new and old parts for aircrafts is done with the same. Also, it created a trust system due to cryptography as most purchases happened using bonds. Any seller can launch his/her own selling system for aircraft parts using Honeywell solution known as Go Direct.



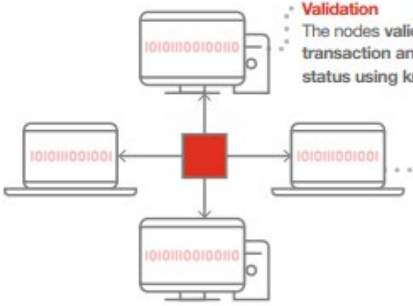


Typical Screen in GoDirect Trade

Source: https://www.hyperledger.org/wp-content/uploads/2019/12/Hyperledger_CaseStudy_Honeywell_Printable_12.12.19.pdf

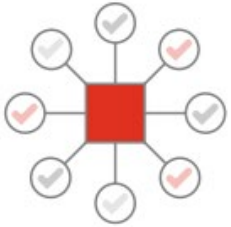


Someone requests a transaction.

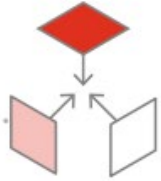


Validation
The nodes **validate the transaction and the user's status using known algorithms.**

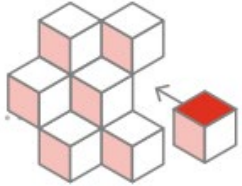
The requested transaction is broadcast to a peer-to-peer **network consisting of nodes.**



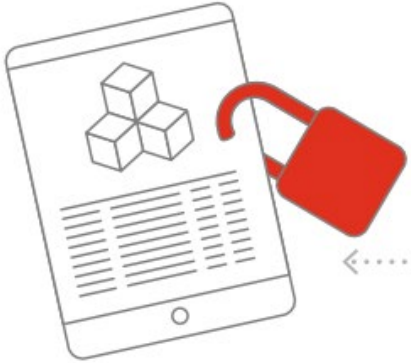
A verified transaction can involve cryptocurrency and other **digital tokens,** records, or other information.



Once verified, the transaction is combined with other transactions **to create a new block of data for the ledger.**



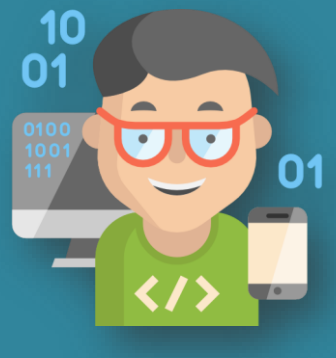
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.



The transaction is complete.

greatlearning
Learning for Life

Thank You



Bank Database Management System

Sampriti Chatterjee (Great Learning)

What is a Database?

A database is a container where data can be collected systematically. Managing, manipulation of those data are easy

Example of Databases

Suppose an online telephone directory uses a database to store their data, Like: Name, address. phone numbers, other contact details.

Example of Databases

Or an online library who has millions of books. In order maintain their data they use database

What is a Database management System?

A Database Management System (DBMS) is basically a software where you can store, retrieve, define, and manage your data in a database.

Most used Databases Management systems Software

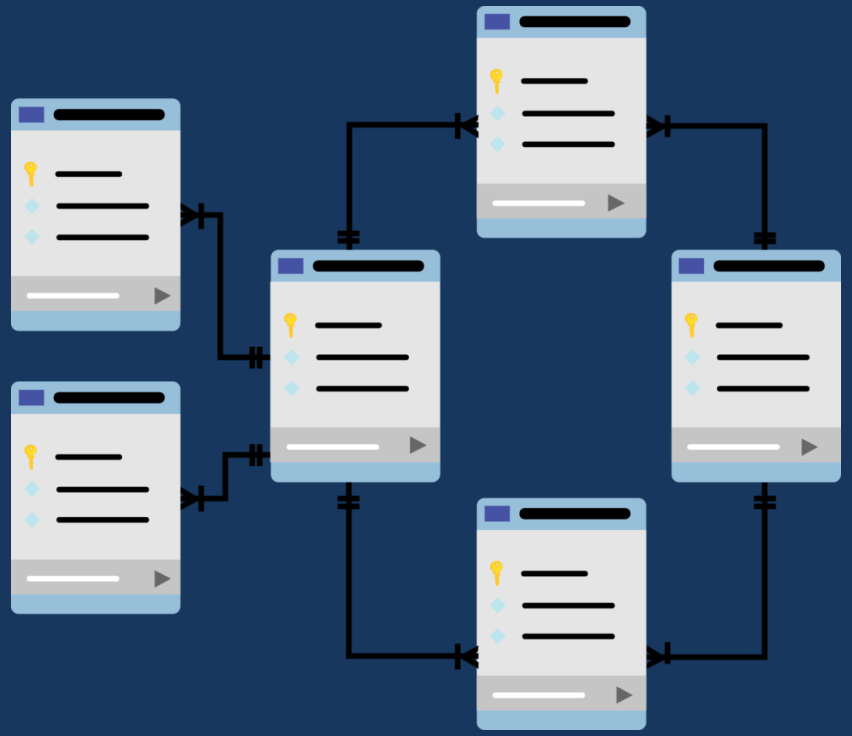
- MySQL
- Oracle
- PostgreSQL
- SQLite
- Maria DB
- PostgreSQL

Types of Databases Management systems

- Hierarchical database
- Network database
- Relational database
- Object-Oriented database

What is Relational Database management System?

A Relational database management system (RDBMS) is used for the database management system (DBMS). The concept is based on the relational model as introduced by E. F. Codd.



Key Concept In DBMS

What is Key in RDBMS?

Key concept has an important role in relational database management system. This technique is used for identifying the unique rows from table and also help to establish relationship among the tables

Types of Key in RDBMS

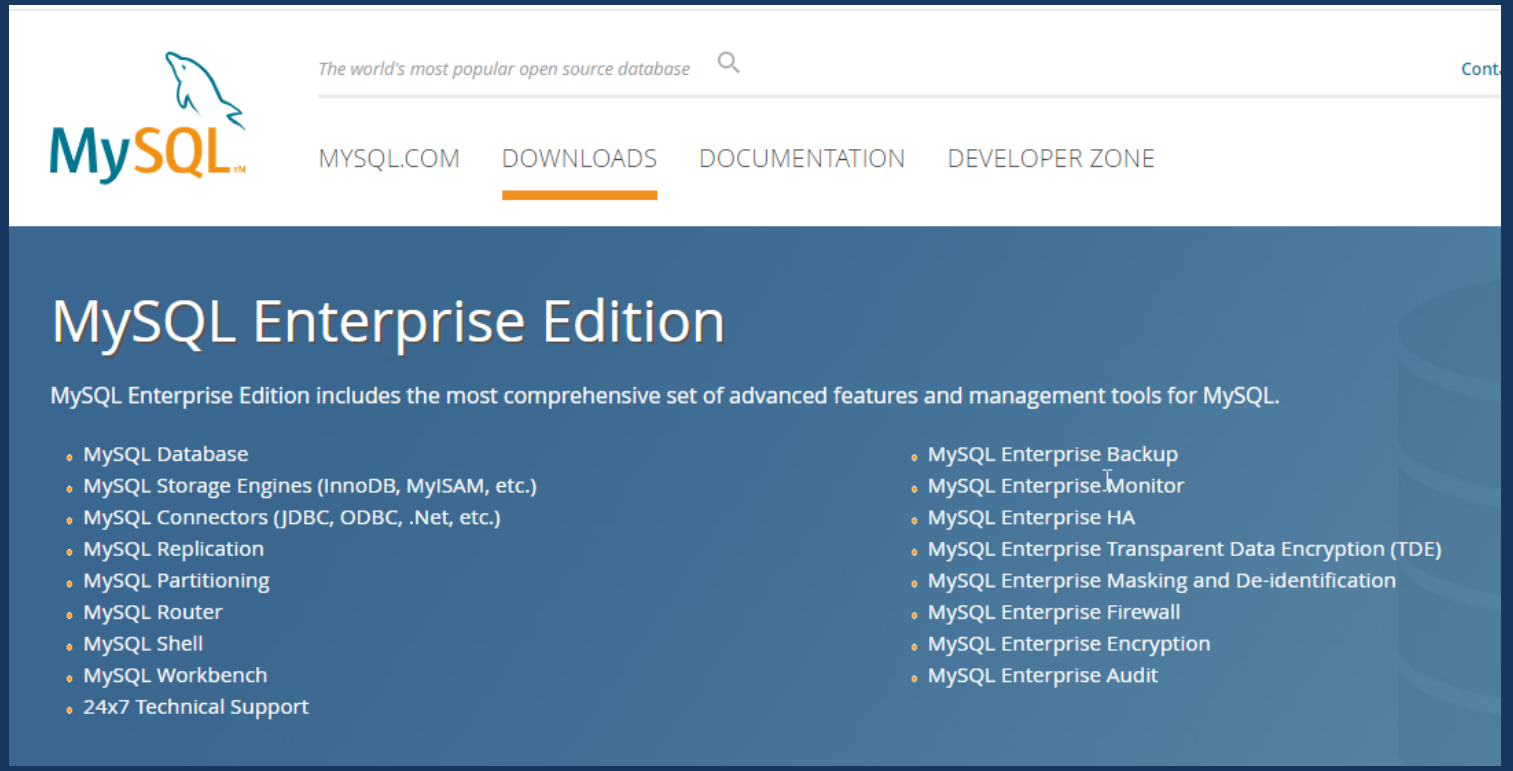
What is SQL?

- SQL stands for Structured Query Language
- SQL helps to access and manipulate your databases
- SQL became a standard of the American National Standards Institute (ANSI) in 1986, and of the International Organization for Standardization (ISO) in 1987

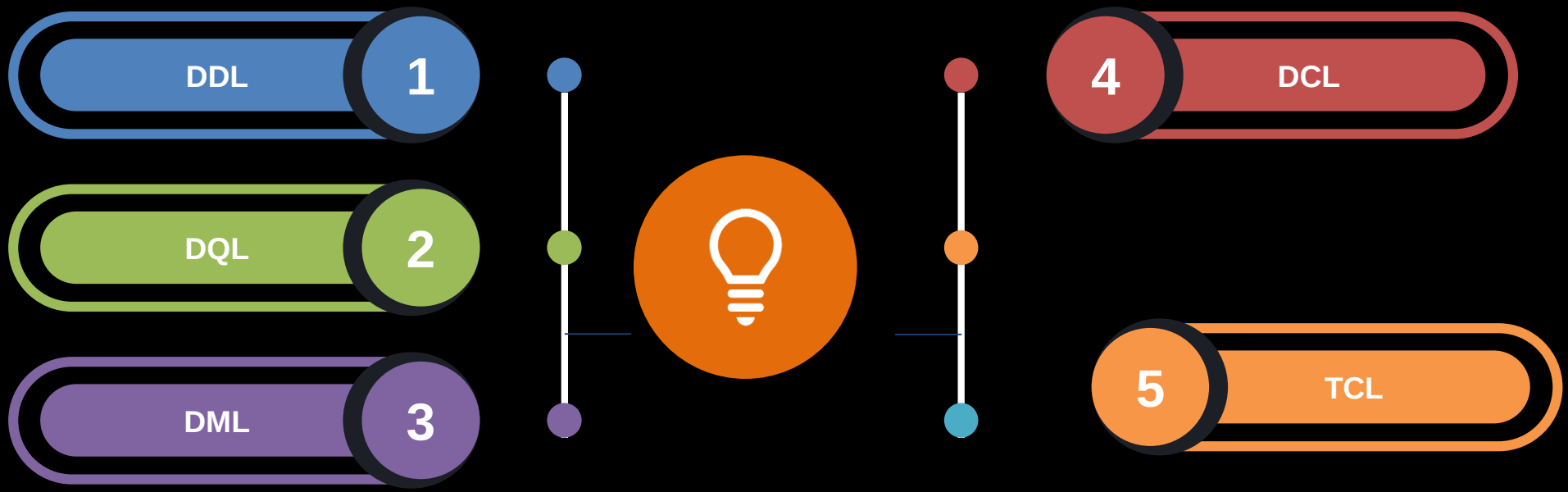
Getting started with MySQL

Installing MySQL

This is the site to install MySQL -> https://www.mysql.com/downloads/



Types of command in MySQL: DDL



Proprietary content. ©Great Learning. All Rights Reserved. Unauthorized use or distribution prohibited

Basic commands for MYSQL

```
INSERT INTO Customers (CustomerName, ContactName, Address, City,
PostalCode, Country)
VALUES (‘Priti', Ms. Chatterjee', ‘4/56 College street
21', ‘Kolkata', ‘70032', ‘India');
```

```
SELECT * FROM Customers
```

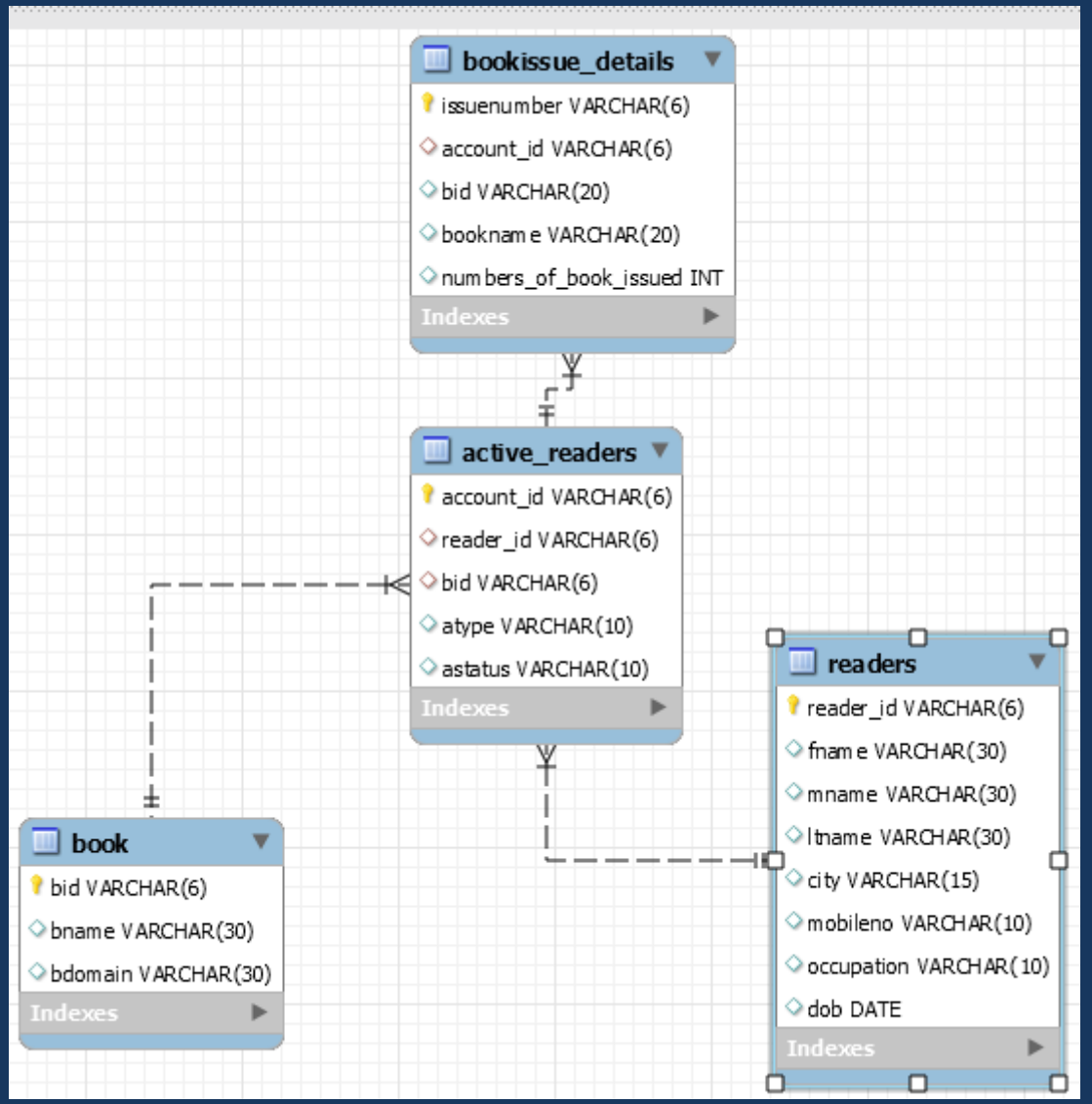
```
show databases;
```

```
create database demo;
```

```
use demo;
```

Bank Database Management System

Table schema



Thank You