

Unit 1

1.1. Introduction to blockchain

The fundamental issues solved by blockchain are security and Integrity among the peers. A blockchain is a peer to peer, shared network of a distributed ledger system without a central authority to govern. This can be thought of a database without a single point of failure that helps to maintain a secure and decentralized record of transactions. In other words Blockchain uses data structures that are maintained distributedly, That is permitted transactions (data) stored and recorded as blocks, These blocks are cryptographically secured by hash function. These blocks are chained to each other in a chronological order. This allows all servers/peers to view the ledger.

The Harvard business school review has described blockchain as "Open, Distributed ledger that can record transactions between two parties Efficiently and in a Verifiable and Permanent way". The keywords: open refers to the accessibility by all users, distributed refers to control of data by the users (blockchain doesn't allow a single user to have central control), verifiable refers to the validity checking i.e every user in the network has to validate all the transactions. Permanent refers to lifespan of the stored information. Blockchain underlies cryptocurrency networks used in a wide variety of applications.

Blocks are considered as the core components. These blocks contain information about transactions such as date, time, and amount of your most recent purchase. They also store information about the participant and identity of that block which distinguishes them from other blocks. Node which is part of the blockchain will collect the transaction information over a certain period and mine a block. This constructed block will be verified and validated by the validator nodes in the network and based on the consensus mechanism the block will be added to blockchain. Blockchain also maintains a local copy of global data at every node. The system ensures the consistency among all the copies of data in the network. Each local copy will get update based on the global data. These local copies are known as public ledger. Blockchain networks combine private key technology, distributed networks and shared ledgers technologies. Confirming and validating transactions is a crucial function of the blockchain for a cryptocurrency. Thus it is considered secure and solves the issue of security and Integrity

1.2. Need for blockchain

Let's consider 2 scenarios to better understand the need for blockchain. 1) The traditional way of sharing documents between two parties say Alice and Bob. Here both the parties cannot modify the data at a time in a centralized environment. If Alice's centralized environment might get affected by any vulnerability or system failure, Bob will not receive the document which results in data and integrity loss with this system. 2) google document shared between two parties, Here even though the both parties can modify the data its still considered a centralized. This is because any issues such as server down, deletion of document, user bandwidth will affect the availability of data. These situations cause "single point of failure" in a centralized environment. This problem can be solved by using blockchain,

1 Hash link e
time stamp → 2 Smart contract → 3 DApps → 4 Business oriented bc.

Feature of BC: Distributed, P2P, Anonymity, immutability, logical compute on chain

allows each user to edit data on their local copy of the document while the internet takes care ensuring updating and consistency.

1.3. Trust model

With the evolving technology, cyber security plays a major role. Cyber security revolves around whom do you trust. If Hardware can be trusted to not leak your cryptographic keys, OS to not peek into computation memory or Application to not be controlled by adversaries etc or Do you trust your banks, land record department and uidai officials to not commit any foul play, manipulation or data leak? These questions arise trust among a centralized systems. To get a better understanding lets check a scenario

1) Double spending attack:

This attack arises with transaction of cryptocurrencies. If user A send a transaction to user B then The amount is unknowingly deducted twice from User A's wallet. This is called as double spending attack. This problem can be resolved using blockchain which uses decentralized ledger and consensus to verify each mechanism.

2) Supply chain

In a scenario where ice cream is meted during the delivery from a storage factory to a restaurant through a delivery truck. Parties will not take the responsibility of the ice cream melting even though its monitored by a iot system. As iot system are susceptible to failures. To avoid this, blockchain could be used as it uses a decentralized ledger which displays the same temperature recordings across the servers.

1.4. How the blockchain works

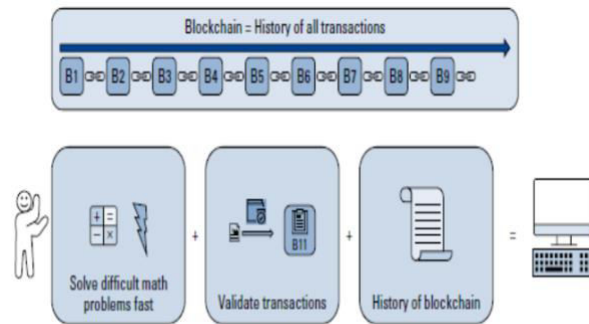
The blockchain procedure are as follows:

1. A user request to initialize a transaction.
2. A block representing the transaction is created i.e. block mining
3. A block is broadcasted to all the nodes in the network
4. Validators will validate the block and the transactions
5. The Block will be added to the chain and
6. Transaction gets verified and executed.

1.5. Node

When a computer connects to a blockchain network, the computer becomes a node. This node runs the blockchain software for the network and it keeps the network healthy by engaging in the transfer of information. **Nodes broadcast bitcoin transactions to other nodes throughout the network Anyone can run a node on a public network like Bitcoin.** Node solves mathematical problems to become a miner and adds their block into the blockchain network. Any node that is a part of these can validate the transactions. The history of this blockchain is stored in the node.

Full node has all blocks publishes & recv block validate all blocks
lightweight node, minor nodes
 Priv Pub pair headers of few blocks use SPU for verification
 helps create blocks



1.6. Types of nodes

There are three types of nodes namely public, permissioned (Hyperledger fabric) and federated nodes. In Public blockchain node, open to anyone in the world to participate in network depending on their hardware and internet access. This type of node allows you to mine and secure a block and start your cryptocurrency transactions. Here any node can either be a full node (check transactions) or lightweight node (send and receive message on n/w). This node has no license fee nor need a permission to join the network. They usually have an open license such as apache. Eg of public nodes are

The permission nodes are private nodes. They usually utilize only some of the blockchain technology. Thus, they do not include mining or a native cryptocurrency. All the blocks and transactions in this node are processed by known parties. These are often operated by consortium such as R3. Corda is a distributed blockchain technology behind R3. The Hyperledger fabric nodes are called peers or orderers. These nodes unlike the public node hosts the ledger's data in order. These data include information such as smart contracts, policies, orderers etc. These nodes can host more than one blockchain ledger which makes it distinguished from other nodes.

The federated nodes exist in both private and public blockchain. This nodes gets it name form the word federation because the user elects the node to process transactions. It selects some nodes to do most of the work, such as, maintenance of blockchain.

1.7. Cryptocurrency

A cryptocurrency is a new, non-tangible digital asset or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Most of the cryptocurrencies are decentralized networks based on blockchain technology. A defining feature of cryptocurrencies is that they are generally not issued by any central authority, rendering them theoretically immune to government interference or manipulation. The first blockchain-based cryptocurrency was Bitcoin created by Satoshi Nakamoto. Other cryptocurrencies are:

- 1) Bitcoin cash also referred as Bcash, split into Bitcoin cash and bitcoin sv.
- 2) Monero an open source cryptocurrency.
- 3) Dash which is also an open source crypto currency.
- 4) Dogecoin.
- 5) NEM is a peer to peer cryptocurrency.
- 6) NXT is an open source

C#

Java, C++

C++

Java POS

Ado: inflation, Central Auth, Secure, Private
DAO: illiquid stuff, Mining effects, Susceptible to hacks
c++

cryptocurrency and payment network.7) Peercoin is a peer-to-peer cryptocurrency utilizing both proof-of-stake and proof-of-work systems.8) Primecoin is a cryptocurrency that implements a proof-of-work system that searches for chains of prime numbers.

1.8. Tokens *Coins are a part of the chain, tokens are deployed using an existing chain. tokens have programmable access control*

Tokens are basically objects that have economic value. Such as money or coins. Tokens haven't been used through centuries. In olden days shells and beads were used as tokens for payments. Tokens are also used in computers to perform some kind of operations. In blockchain, Tokens are form of digital asset that represent programable asset or asset rights build for a specific blockchain. These are managed by smart contract and an underlying distributed ledger it gives a rise to lots of decentralized applications and decentralized autonomous organization(dao). Token is like a cryptocurrency, it can act as bearer instrument and used to transfer value between two parties over a network. They are accessible only by the person who has the private key for that address and can only be signed using this private key. It can be termed as a valuable object represents asset on a digital ledger. A token can be native which serves as an incentive to help protect the network from attack and has governance rule-set, example is Bitcoin which is being paid to miners for block creation and validation. Ether; which is used for payment of transactions to the nodes carrying out block validation and confirmation. This is a perfect example of a token economy as it is reward based on the systematic reinforcement of target behavior.

These cryptographic tokens represent a set of rules, encoded in a smart contract the token contract. Every token belongs to a blockchain address. These tokens are accessible with a dedicated wallet. It communicates with the blockchain and manages the public-private key pair related to the blockchain address. These are accessible by only the person who has the private key address. This person is regarded as the owner or custodian of that token. If the token represents an asset, the owner can initiate transfer of the tokens by signing with their private key, which in turn generates a digital fingerprint or digital signature. If the token represents an access right to something somebody else owns the owner of that token can initiate access by signing with their private key, thereby creating a digital fingerprint. If the token represents a voting, the owner of that token can vote by signing with their private key, creating a digital signature.

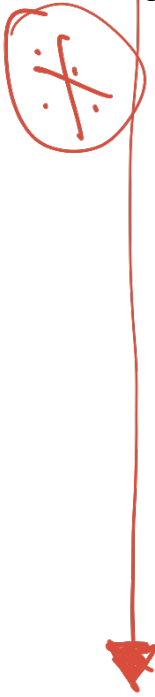
There are different types of tokens namely:

- 1) **Utility token:** It can be used as access right to contribute to a network like a DAO and receive reward for carrying out a particular task. These kind of token can also be exchanged for a service or product.
- 2) **Security token :** it gives holders right of equity in your venture. Holders can lay claim to revenue or profit of the venture. Issuers of such tokens promise returns to holders. Any token that passes the Howey Test is considered an investment contract.
- 3) **Governance token :** it can be used to represent each users stake in DAO's. They also used to assign control in blockchain as these token have have voting powers.

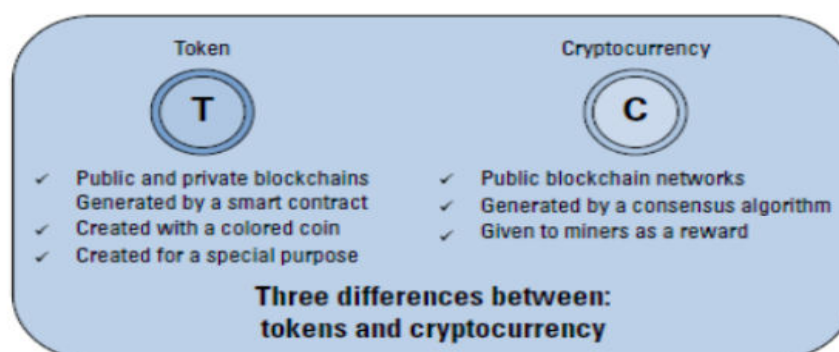
- 4) **Transactional tokens:** These tokens are similar to traditional currency where units of account and are exchanged for goods and services.
- 5) **Platform tokens:** It can be used as a plug and play solution to simplify the implementation of Blockchain and Decentralized technologies within Public Services which are easily accessible to any developer.
- 6) **NFT : Non fungible token** that can be used to represent real world objects such as music, art etc. These tokens can easily be traded or exchanged for one another.

SECURITY TOKEN PROTOCOL STACK.

The Security Token Stack, it is essential that marketplaces have met the regulatory guidelines required for operating as an exchange

- 
- 1) The blockchain : is the foundation offering trustless transactions, fast settlement times, security and the network on which all higher levels in the stack are built. The blockchain offers issuers and regulators visibility and provides investors with connectivity and discoverability leading to liquidity.
 - 2) The security token: is the on-chain technology layer that, in combination with the compliance platform, enforces compliant transactions required by issuers and regulators.
 - 3) The compliance platform: consists of off-chain processes that conduct due diligence, ensure that investors are qualified to participate in offerings and later trades, and update rules and permissions dynamically over time to ensure compliant secondary trading.
 - 4) Exchange protocols: such as 0x and Swap are an essential layer to ensure a global liquidity pool. Exchange protocols connect order books from different marketplaces and enable the exchange of tokenized securities by providing developers an open protocol to build on. The decentralized protocols lower the cost of trading, remove barriers for overseas investors, and enhance security as it is not a centralized third party that holds funds or securities.
 - 5) Exchanges (exchanges, 0x relayers, second-layer protocols) : provide a venue for liquidity, where buyers and sellers find trade execution once secondary trades are allowed to occur.

DIFFERENCE BETWEEN CRYPTOCURRENCY AND TOKEN

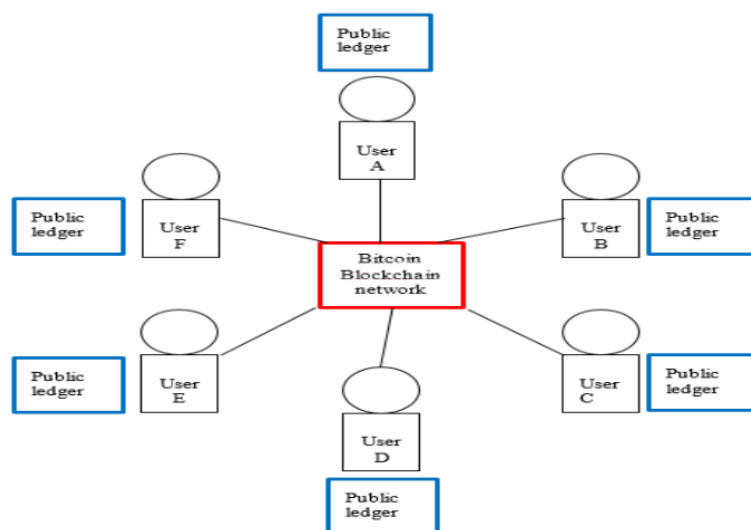


1.9. Ledger

Ledger is a series of blocks or a database which record the transaction after they are authenticated and verified. Ledger cannot be viewed as a collection assets. There ledgers are immutable meaning they cannot be changed. There are 2 types of ledgers, namely, centralized ledger that is maintained by a single node or a third party and public or distributed ledger where every node has a local copy of the ledger. It can also be defined as the ledger is a distributed immutable record of a collection of transactions.

PUBLIC LEDGER

A Public ledger is also called as a distributed ledger. It is a database, consensually shared and synchronized across multiple sites, institutions, or geographies. It is accessible by multiple people. It allows transactions to have public witnesses. The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it. Any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes. When a buyer and a seller engage in a transaction, the blockchain verifies the authenticity of their accounts. This is done by using the public ledger and by checking if the funds are available then proceeds with the transactions. However, if the funds are either not available in the buyer's account or Funds promised to another party, then the sale is prevented effectively making double spending attack impossible.



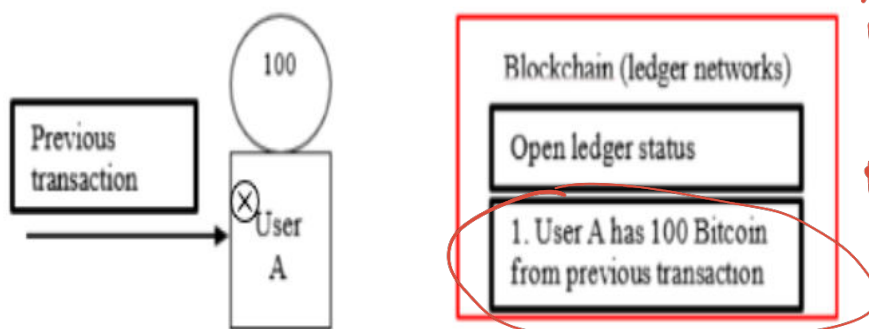
The working of a public ledger could be understood with this scenario where there exists 2 customers, Alice and Bob. Both Alice and Bob will be having their own ledgers. Say if Alice is having 100 Bit coins in his wallet. This information should get updated in the Bobs public ledger. If Alice transfers a 60 bit coins to bob that information should be also updated in the bobs ledger. In our example we are taken only 2 nodes, if there exist n nodes all the n nodes should get update with each transaction data.



Transaction using ledger

There are three stages of transaction procedure .

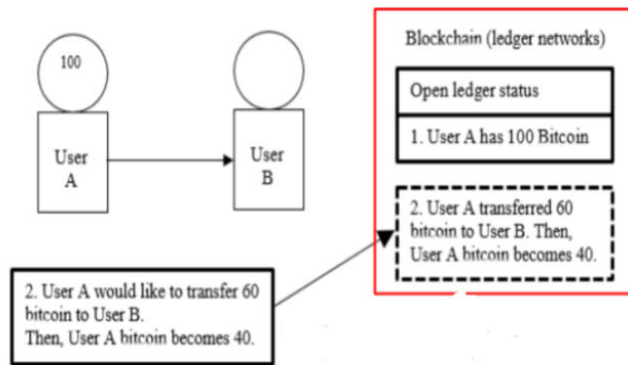
- 1) A transaction is a transfer of Bitcoin value that is broadcast to the network and collected into blocks. A transaction typically references previous transaction outputs as new transaction inputs and dedicates all input Bitcoin values to new outputs. Bitcoin transaction defined as a chain of digital signatures.



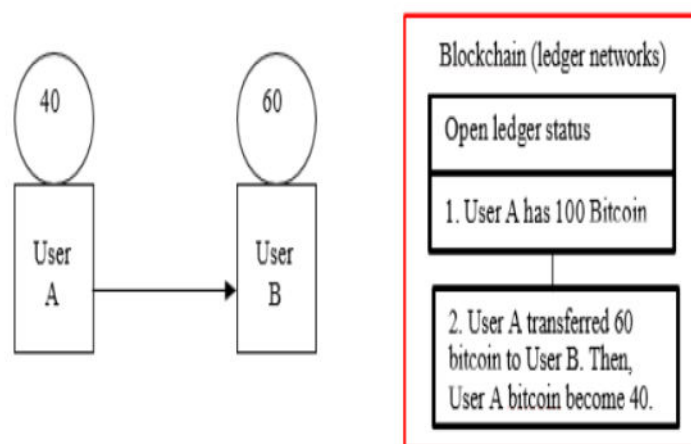
(a) First stage: The current condition

All the ledger has to do is to check previous transaction output

- 2) This step has 3 sub steps
 - a. This transaction will be valid across all ledger network whether user A Has 100 bit coins
 - b. This network will identify transactions 60 bitcoins to user B. IF the transactions is valid then the transaction can add to open ledger.
 - c. Will be included in the transaction chain



- 3) The transaction will get approved and executed after approval they can be added to chain



(c) Third stage: Approval of transaction chain

PUBLIC BLOCKCHAIN LEDGER

Public ledger blockchain is totally open to all and anybody can join the system.

Each member on the chain has full power to access, read and write transactions.

Since it is decentralized and wholly distributed, every node gives verification to approve any transaction. Data can not be altered or manipulated once it is placed on the block. Public blockchains are also called permissionless blockchains. Being totally open to everyone is the biggest drawback of this type of ledger, since it offers complete transparency with little privacy. Time taken to reach consensus by the network is high because of the numerous nodes present, therefore resulting in high computational power. examples Bitcoin, Ethereum, etc

PRIVATE BLOCKCHAIN LEDGER

Private blockchain ledger have limitations on who is participating in the network. A user is granted access only by the network initiator or by a predefined set of rules. Once a user is given entrance to the network, it can perform the same duties as that of other users.

Again, the degree of permissions is decided by the one who initiated the network.

DIFFERENCE BETWEEN PERMISSIONED AND PERMISSIONLESS BLOCKCHAIN LEDGER.



Permission-less blockchain ledger	Permissioned blockchain ledger
Open to everyone hence anyone can participate in the network	Only users who have been granted permission by network starter can join
More transparency, less privacy	More security, limited permissions
High computing power due to a greater number of users	Efficient and well organized due to limited number of users
E.g:- Bitcoin, Ethereum	E.g:- Hyperledger Fabric, Corda

UE19CS335

Blockchain Notes

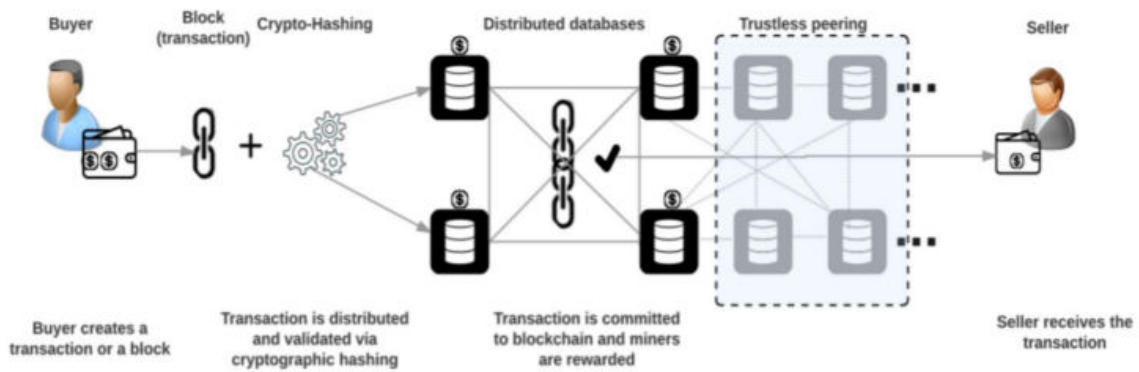
Types of Blockchain

- Public
- Private
- Hybrid
- Consortium

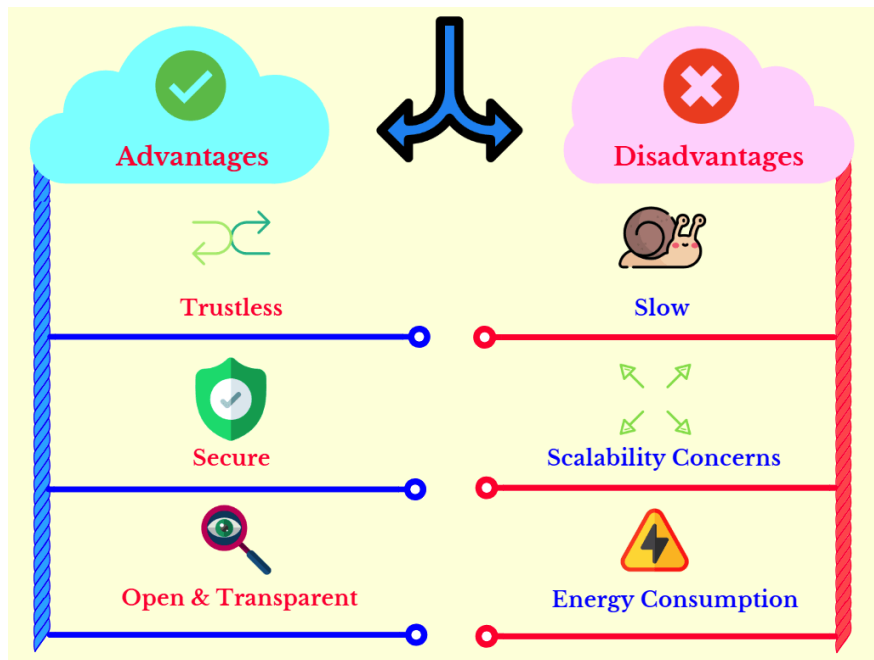
Public Blockchain

- Permissionless blockchain
- It is a complete decentralization system
- Anyone can join the network
- Anyone can read and write to the ledger
- Users are anonymous in the network
- Examples- Bitcoin, Ethereum, Litecoin

➔ Transaction in a Public Blockchain



➔ Advantages and Disadvantages of Public Blockchain



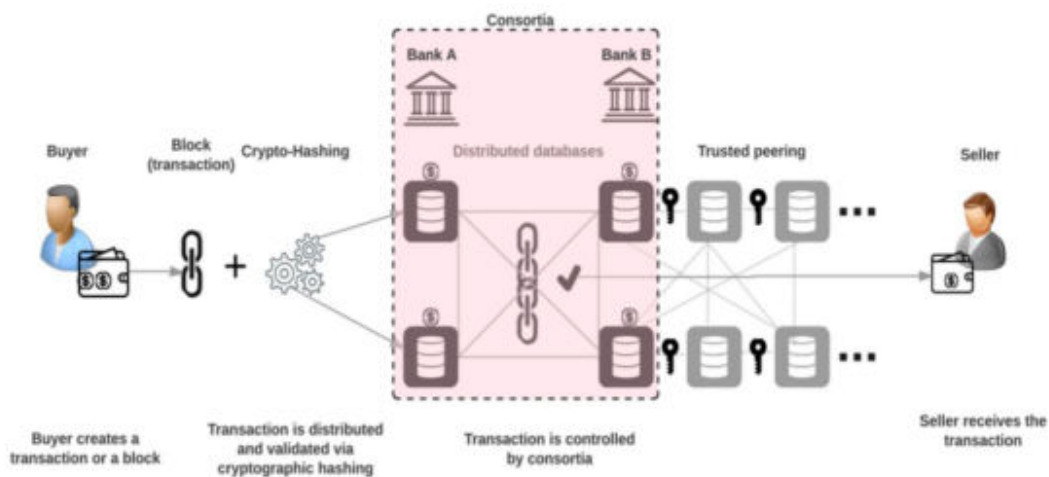
(source: masterthecrypto.com)

Private Blockchain

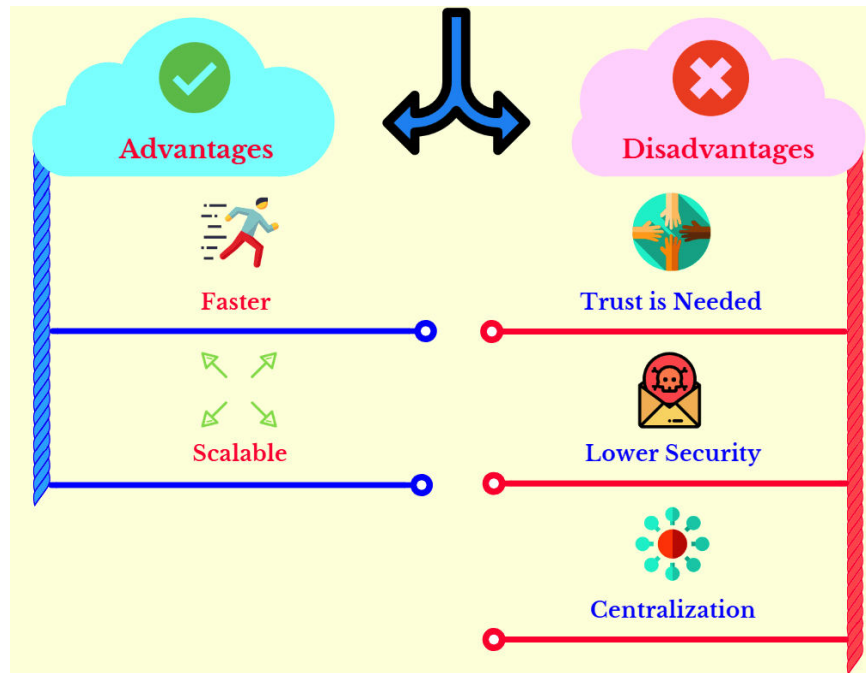
- Permissioned blockchain system
- Controlled by a single organization

- A user cannot freely join the network nor can he read and write to the ledger
- User identity is known to everyone in the network
- Transactions are only visible to those who have permission
- Only access controllers are allowed to make a decision
- Organizations that want control over data and can provide more privacy use private blockchain
- Examples- Hyperledger fabric, Corda

→ Transaction in a Private Blockchain



→ Advantages and Disadvantages of Private Blockchain

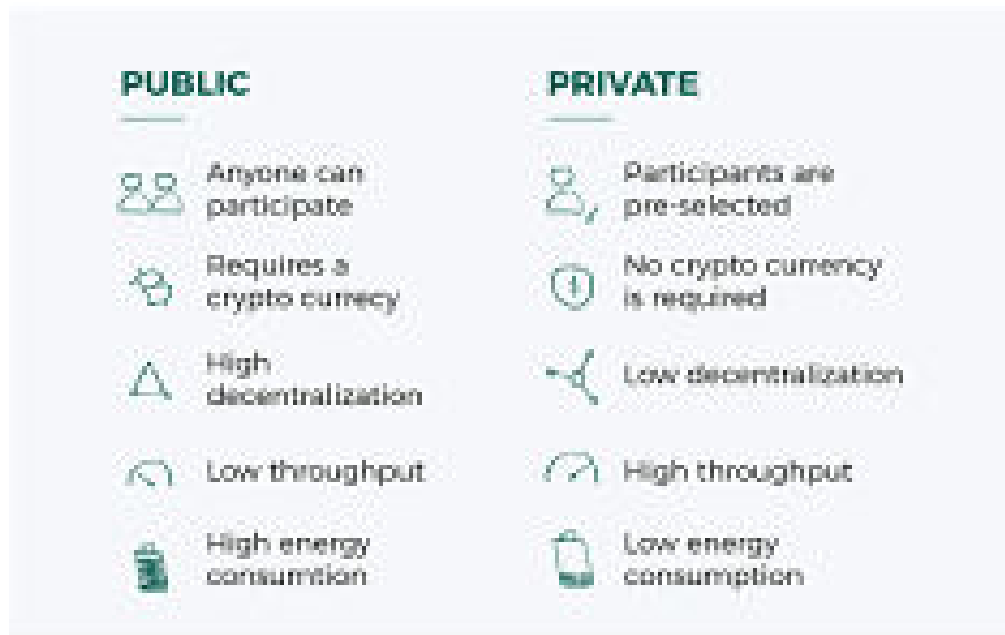


(source: masterthecrypto.com)

➔ A few companies that use Private Blockchain

- Walmart is based on Hyperledger Fabric
- Comcast uses Blockgraph
- BurstIQ
- Spotify

➔ Differences between Public and Private Blockchain



(source: e-ziguurat.com)

Consortium Blockchain

- Also named Federated blockchains
- Permissioned Blockchain
- Governed by a group of organizations
- Example: Ripple, IBM Food Trust

➔ Advantages of Consortium Blockchain

- Saves cost
- Risk sharing
- Gradual mass adoption

➔ Differences between Public, Private and Consortium Blockchain

Characteristics	Public Blockchain	Private Blockchain	Consortium Blockchain
Permission Read	Public Class	Could be public or restricted	May be public or restricted
Determination of Consensus	All miners	Only one organization	Designated set of nodes
Efficiency	Low	High	High
Immutability	Impossible to tamper	Could be tampered	Could be tampered
Centralized	No	Yes	Partial
Consensus	Permissionless	Permissioned	Permissioned

(source: researchgate.net)

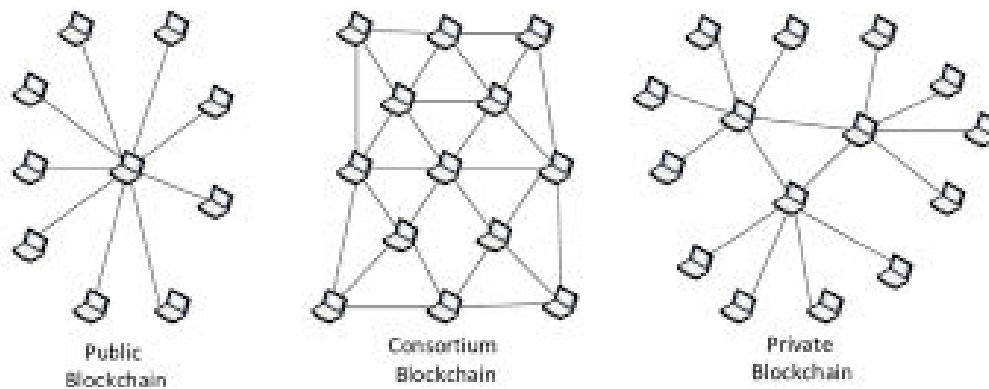
Hybrid Blockchain

- Blend of public and private blockchain
- Provides controlled access and freedom at the same time
- Use cases- Supply chain, Banking industry, Government process
- Example- Dragonchain

➔ Advantages of Hybrid Blockchain

- Offers privacy
- Good scalability
- Rule modification allowed

Summary



(source: researchgate.net)

	Public (permissionless)	Private (permissioned)	Hybrid	Consortium
ADVANTAGES	<ul style="list-style-type: none"> + Independence + Transparency + Trust 	<ul style="list-style-type: none"> + Access control + Performance 	<ul style="list-style-type: none"> + Access control + Performance + Scalability 	<ul style="list-style-type: none"> + Access control + Scalability + Security
DISADVANTAGES	<ul style="list-style-type: none"> - Performance - Scalability - Security 	<ul style="list-style-type: none"> - Trust - Auditability 	<ul style="list-style-type: none"> - Transparency - Upgrading 	<ul style="list-style-type: none"> - Transparency
USE CASES	<ul style="list-style-type: none"> ■ Cryptocurrency ■ Document validation 	<ul style="list-style-type: none"> ■ Supply chain ■ Asset ownership 	<ul style="list-style-type: none"> ■ Medical records ■ Real estate 	<ul style="list-style-type: none"> ■ Banking ■ Research ■ Supply chain

Permissioned Blockchain

- Distributed ledger that is not publicly accessible
- It is a closed eco-systems that can only be accessed by those who are allowed access.
- Example- Ripple, Hyperledger, Quoruma

Permission-less Blockchain

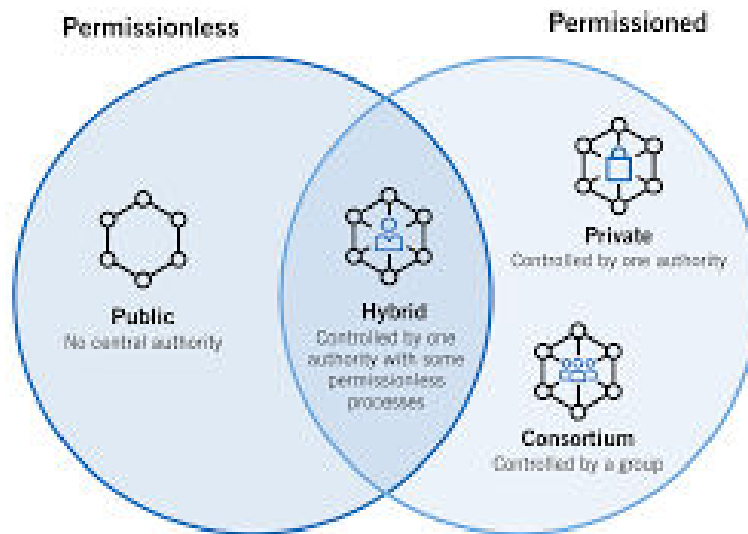
- It is an open environment and works over a large network of participants
- Users do not reveal their identity to others
- It is a tamper proof network – it is “extremely hard” to make a change in the blockchain
- Transactions are sent to public key addresses which ensures security
- The longest chain is the accepted main blockchain
- Orphaned Blocks (the blocks which are not part of the longest chain) are eliminated.
- Example- banking using cryptocurrency

→ Differences

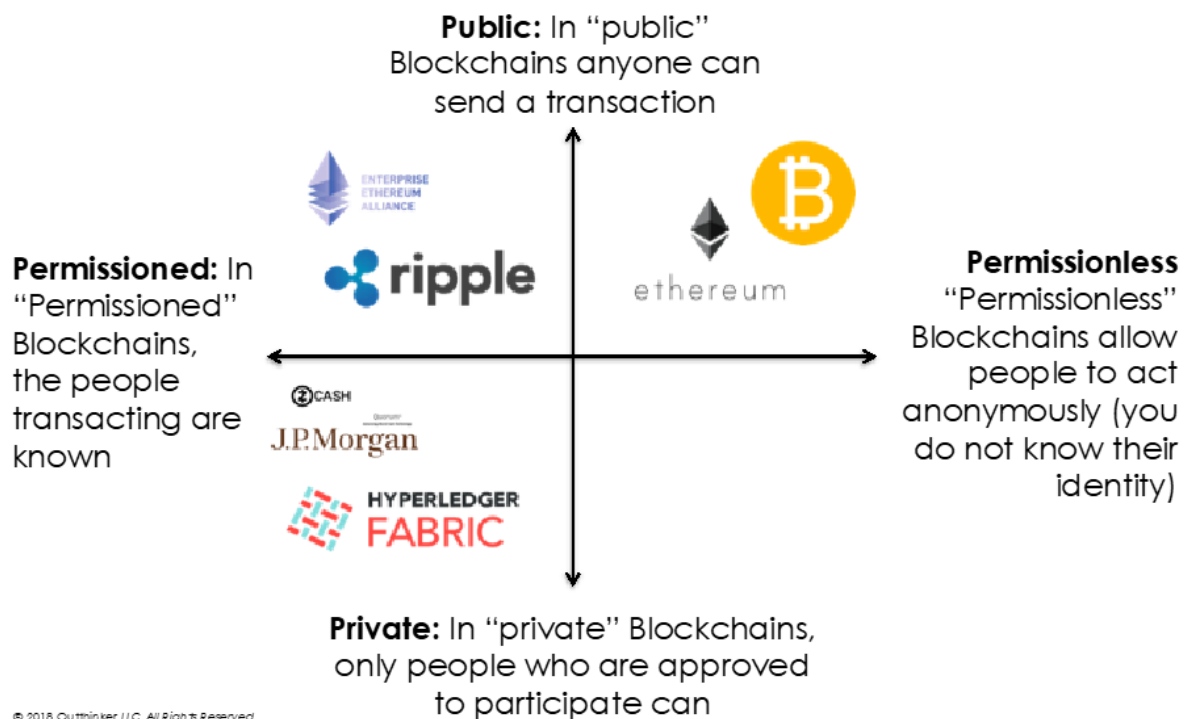
Permissioned Blockchain vs Permissionless Blockchain		
Category	Permissioned	Permissionless
Speed	Faster	Slower
Privacy	Private membership	Transparent and open - anyone can become a member
Legitimacy	Legal	Illegal
Ownership	Managed by a group of nodes pre-defined	Public ownership - no one owns the network
Decentralization	Partially decentralized	Truly decentralized
Cost	Cost-effective	Not so cost-effective
Security	Less secure	More secure

(source:101blockchains.com)

Summary



(source:foley.com)



(source:kaihan.net)