Unit - 1

Introduction to Blockchain

1.1 Introduction to Blockchain

A blockchain is a type of data structure where data or information is stored in blocks of chain. Each block contains some information with hash value of previous block. The hash is unique mathematical code which shows the specific block in blockchain.

Block chain ensures the transparency, security as well as decentralization. A blockchain is a one type of digital ledger of transaction where each transaction is duplicated and distributed across the entire network of computer system.

As each block contains number of transaction and any new transaction occur on blockchain then it is known to every other participant's ledger.

This block of chain is managed by multiple participants with the help of decentralized database this technology is referred as Distributed Ledger Technology (DLT).

The blockchain technology is used in Digital Crypto Currency Bitcoin.

Why blockchain is trustable:

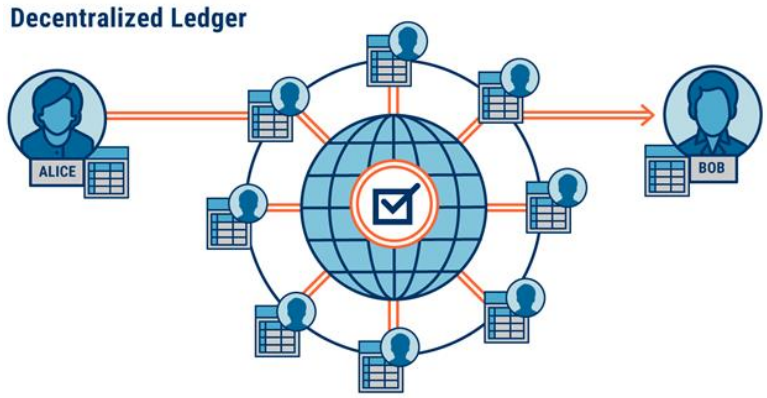
- The blockchain is trustable on various reasons.
- It is an open source in nature that why it is used in business applications.
- It is compatible in business applications.
- It is used in online transaction because of high security.
- In business the developers always pay for security.
- The business does not matter in any situation, the blockchain is considered easily.

Benefits of Blockchain Technology:

- The process is faster and cheaper because of no central authority for verification.
- There are no expenses added in the blockchain technology.
- It gives tighter security over blockchain where no other person can modify the data.
- The blockchain enhanced the security.
- The blockchain provides the greatest transparency where blockchain provides the distributed ledger, transactions and data are recorded in multiple locations identically.
- Blockchain creates audit trail which documents the provenance of an asset at every stop on its journey.
- The blockchain increases the efficiency and speed.
- The reconcile multiple ledgers are not needed so clearing and settlement can be much faster in blockchain.
- The transactions are automated using smart contracts which increase the speed of process.
- Business spend lot of money on managing their current system that why the blockchain is used to reduce cost and divert money into improving the process.

1.2 Digital Money to Distributed Ledgers

- ✓ The distributed ledger is a technological infrastructure and protocols which grants the access to the multiple users, verification and modification of records.
- ✓ This work can be done on multiple locations or entities over computer network.
- ✓ The distributed ledger is also called as shared ledger or distributed ledger technology.
- ✓ Blockchain is best example of distributed ledger technology.
- ✓ DLT uses the cryptographic technology to make it secure for storing data with cryptographic signature and key to access only authorized participant.
- ✓ DLT creates its own database where once the data is stored it cannot be deleted and updates will be permanently recorded for posterity.
- ✓ DLT gives the transparency, high security.
- ✓ The distributed ledger is a consensus of replicated, shared and synchronized digital data.
- ✓ The hardware of DLT ecosystem is comprised of large number of nodes where each node could either be a computer, server or storage device.



Following figure 1.1 shows the digital ledger working.

Following are some examples of Digital ledgers:

i. Blockchain
ii. Tangle
iii. Corda
iv. Ethereum
v. Hyperledger fabric

Properties of Distributed Ledger Technology:

The blockchain is the one type of distributed ledger where transactions are recorded in immutable cryptographic signature called as hash.

The decentralized database manages all the multiple participants is known as distributed ledger technology (DLT).

Following are the properties of DLT.

1. Programmable:
    - The blockchain is programmable.
    - The transactions are recorded as smart contract.
2. Secure:
    - All records are individually encrypted.

3. Distributed:
    - The records are stored in distributed database.
    - All network participant has a copy of ledger for complete transparency.

4. Anonymous:
    - All the participant of the network is authorized by the DLT.
    - The identity of the participant is either anonymous or pseudonymous.

5. Unanimous:
    - All the records can be change by all the participant of network.
    - As the record are validated by participant before adding into the network.
    - All network participant agrees to the validity of each of the records.

6. Tim stamped:
    - The records are added in the network by participant with time stamp as blockchain provides the transparency.
    - A transaction should have a time stamp on block.

7. Immutable:
    - All the records are irreversible and not changeable by any of the user after adding the record.
    - Any validated records are irreversible and cannot changed.

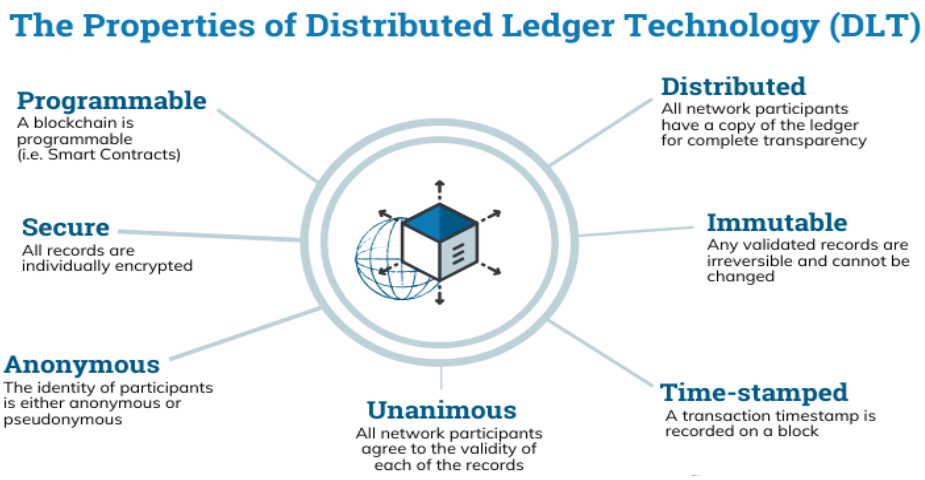


Figure 1.2 Represents the properties of the digital ledger.

Classification of DLT

There are three types of distributed ledger technology as follows:

1. Permission less DLT
2. Permissioned DLT
3. Hybrid DLT

Permission less DLT

- The permission less DLT is open source of DLT.
- Any participant can validate the records without permission from any authority.
- The user can operate and maintain the distributed ledger technology.
- It is free to download.

Permissioned DLT

- The permissioned DLT is opposite to the permission less DLT.
- The participant requires the permission.
- Users validating the block must be authorized in permissioned DLT.
- The transactions can be restricted for read and to write access for the user in permissioned DLT.

Hybrid DLT

- It is the combination of permissioned and permission less DLT.
- The benefits of permissioned DLT such as security and transparency are combined with benefits of permission less DLT.
- The hybrid DLT gives the flexibility to the developers as which data they want to make public and transparent and which data they want to keep private.

1.3 Design Primitives: Protocols, Security, Consensus, Permissions, Privacy

1.3.1 Protocols

Following are five major protocols used to build blockchain.

1. Hyper ledger

- It is an open source project used to create suite of tools for blockchain technologies quickly and effectively.
- This protocol is useful because it has its libraries which helps in developing of blockchain.

2. Multichain

- The multichain protocol is used in private blockchain to facilitate more efficient transactions.

- This protocol gives the profit in corporation.
- It also offers an API to accelerate deployment and development of blockchain.

3. Enterprise Ethereum

- This protocol is used to increase the use cases of blockchain software development.
- This protocol helps to grow business rapidly on large scale with exchange values.

4. Corda

- Corda offers protocol design for enterprises same as multichain.
- This protocol is used in the sector of finance and banking.

5. Quorum

- Quorum protocol is most significantly leading protocol in finance sector because it has strong backing from financial community.
- This protocol is used to build a blockchain software development project. As above protocols are highly complex and usually used to work with customized blockchain development services.

1.3.2 Security

- Blockchain uses the cryptography technology to ensure trust in transactions. The blockchain is based on principle of decentralization and consensus.
- As blockchain is type of data structure where each block contains transactions or bundle of transactions. Each new block connects with other blocks of chain it goes in cryptographic chain in such a way that it's impossible to modify the data.
- All transactions are validated by consensus mechanism to correct and ensure the transactions. Blockchain is based on decentralization where participants are across the distributed network.
- There is no single point of failure and single user cannot change the records of transactions. However, the blockchain technology differs in some critical security aspects.

1.3.3 Consensus

- As the blockchain technology ensure privacy, security, transparency and immutability. There is no central authority is present to verify the transactions therefore the blockchain considered as completely secure and verified. This is all because of consensus protocols present in blockchain technology.
- The consensus mechanism is core part of blockchain. The consensus protocol ensures that every block which is going to added in blockchain should be only the truth that is agreed by all the nodes in blockchain. Consensus mechanism provides the reliability in

blockchain where trust is in between the unknown peers established in distributed network. Consensus is basically a common agreement works in entire network.

Following are various consensus algorithms used in blockchain.

- ✓ Proof Of Work (Pow)
- ✓ Practical Byzantine Fault Tolerance(Pbft)
- ✓ Proof Of Stake (Pos)
- ✓ Proof Of Burn (Pob)
- ✓ Proof Of Capacity
- ✓ Proof Of Elapsed Time

1.3.4 Permission

- The blockchain needs permission to participate in network and interact with it. In public blockchain anyone can participate as open source clients and attach to the network.
- Once the necessary synchronization done with rest of the network then it gives the copy of ledgers. The permissioned blockchain works differently where participant needs permission to join the network.
- This permission is granted by the rest of the participants of network where they compare the signer's identity against permissioning policy. This permissioning policy applies on both peer to peer networking. It is used to propagate transactions as well as blocks with other functional messages.
- The permissioning policy can be locally maintained by each of the operator or administrator. The administrator will decide who will interact with the network. The permission can be maintained as network-wide consistent policy which is a smart contract.

1.3.5 Privacy

- The blockchain gives the privacy to the participants of network.
- This privacy includes two concepts as confidentiality and anonymity.
- Confidentiality is needed to conceal the transaction details.
- Anonymity refers to concealing the parties of transaction.

1.4 Blockchain Architecture and Design

The blockchain is the one type of transactional data structure which is authorized and authenticated. The structure of blockchain is represented as list of blocks with transactions order. The pointer and linked list data structures are used by blockchain architecture.

The blockchain is open for every financial ledger. There are many nodes (blocks) in the blockchain. The blockchain is the decentralized network where numbers of computers are connected. The ledgers are connected through distributed database in blockchain where each

node is playing important role as administrator in the blockchain. The ledgers can join the network voluntarily.

Since the blockchain does not having third party in the network therefore there is no chance to hack the network (As blockchain is decentralized network). The blocks in the blockchain are known as growing list of ordered records in the blockchain architecture.

Each block includes timestamp and link to the previous block. In blockchain architecture each participant can main, approve and update new transactions.

The system of blockchain is maintained by every participants of network where each participant ensures that all records or procedure are in order that gives data security and validity.

The blockchain architecture is used mostly in financial industries to create crypto currencies, keeping records, digital notary and smart contracts.

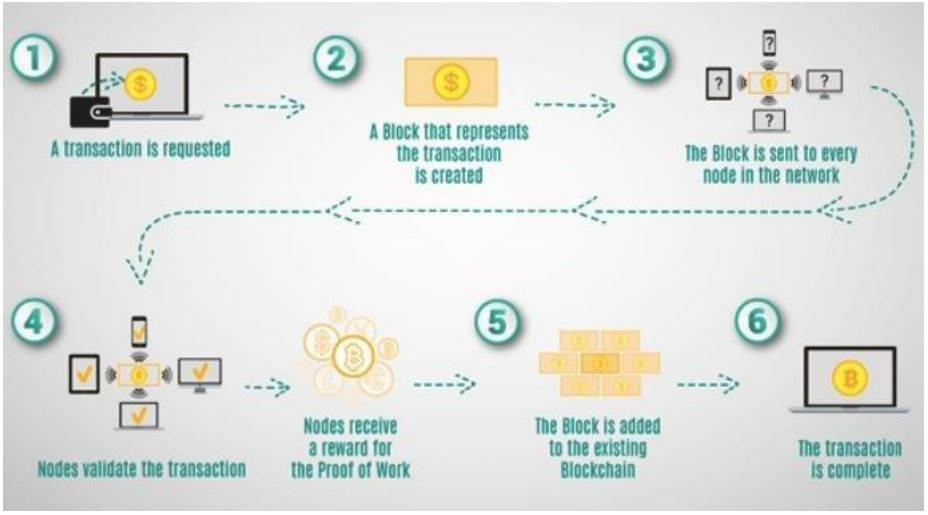


Figure 1.3 Depicts the blockchain working.

Each block contain some other informational fields such as:

1. Certain data
2. Hash of the block
3. Hash from previous block

The data stored inside the block is depends on the type of blockchain.

In bitcoin blockchain, the block includes the data about receiver, sender and amount of coins. The hash value is used as fingerprint of blockchain where long records consist with some digits and letters.

Each block hash is generated by cryptographic hash algorithm SHA 256. The hash value is used to identify each block in blockchain easily. The block is created with the hash value whenever the block is changed it changes with the hash value too.

The hash value attached with block automatically. The hash value is used as identification of any changes made in blocks in blockchain. The final element is hash from the previous block in block. The hash from previous block is the main element for security of the blockchain which creates the blocks in blockchain.

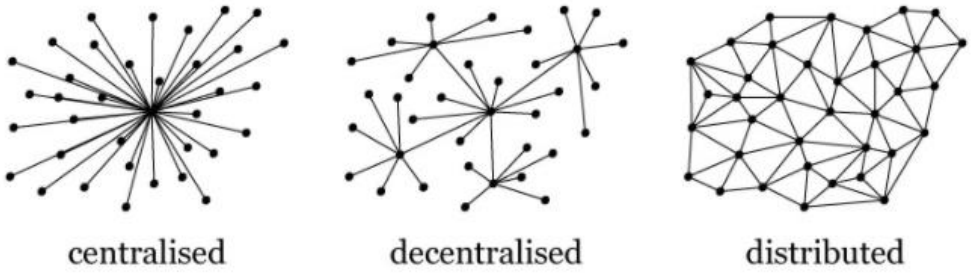


Figure 1.4 Shows some types of structures that represents the blockchain architecture.

1.4.1 Components of blockchain architecture

Following are the various components present in the blockchain architecture:

Block: it is an encapsulated structure which contains

1. Hash code to identify the block
2. Hash code of previous connected block
3. Set of time stamped transactions

Transaction: it is a data record which is verified by all the participants which serves almost immutable confirmation of authenticity of financial transaction or contract.

Node: it is a connected computer in the blockchain architecture.

Miners: it is a node which validate the blocks before adding it to the blockchain structure

Chain: it is a sequence of blocks.

Consensus: it is a protocol having set of rules and agreements for performing blockchain operations.

1.4.2 Types of blockchain architecture

There are three types of blockchain architecture as follows:

1. **Public Blockchain Architecture**

- The proof of work (PoW) consensus and appropriate protocols are used to build public blockchain architecture.
- It is an open blockchain source as it does not require any permission.
- Here participant can create new block with their existing state as it is an open source.

- The participant can check the transactions also can download it through network.
- Following are public blockchains:

  Bitcoin

  Ethereum

  Litecoin

2. Private Blockchain Architecture

- This blockchain allows only certain group of participants or organizations to access the information.
- This blockchain is built to increase benefits or efficiency of organization.
- In this blockchain the proof of Stake (Pos) and Byzantine fault tolerance (BFT) consensus algorithms are used.
- This blockchain opens with some programmable transaction area which is called as smart contract layer or online market.

3. Consortium Blockchain Architecture

- It also known as public permissioned blockchain architecture.
- In this chain anyone can connect and view the blockchain, but participant need permission to add information and connect to the node of other participant.
- This type of blockchain are used to build trust in customers. Consumers or society of organization.
- The proof of stake (PoS) and Byzantine fault tolerance (BFT) consensus algorithms are used to build consortium blockchain architecture.

Characteristics of blockchain architecture:

The blockchain has various benefits for business. Following are some of the characteristics of blockchain architecture.

Cryptography

The blockchain are validated and trustworthy due to cryptographic proof among involved parties.

Immutability

The records of blockchain cannot be changed and deleted by user after validating it.

Provenance

The origin of the record is identified by the provenance inside blockchain ledger.

Decentralization

The blockchain is based on distributed database which keeps transparency.

Anonymity

Each block has generated address not user identity which keeps the user's anonymity.

Transparency

The blockchain cannot be corrupted. The data can be retrieved by the distributed database network.

1.5 Basic Crypto Primitives: Hash, Signature, Hashchain to Blockchain, Basic Consensus Mechanisms

1.5.1 Hash

- The cryptographic hash function is used for security purpose in blockchain.
- The hash is the backbone of crypto security.
- It hash function converts random input data into string of fixed length and structure.
- The hash value in the blockchain used as an identifier which identify the transaction on the blockchain.

1.5.2 Signature

- The digital signature is an authentication of message used as public key primitive.
- It is a technique to bind person into the digital data.
- The digital signature is a cryptographic value which is calculated by data and secret key that is only known by signer.

1.5.3 Hash chain to Blockchain

- It is a repeated application of a cryptographic hash function to a given data asset.
- The hash chain is like the blockchain. The hash chain is used in various cryptographic security setups.
- It is a successive secure chain which impossible to hijack a data asset through applying a single input.
- In the hash chain the participant first supplies an individual input on the first interaction or session then it adds authenticating data on the next session.
- Over the set of sessions, the individual hash inputs create a hash chain. This hash chain authenticates single user input in a more profound way.
- The hash chain having more relevant features than blockchain hence it makes gold standard for ledger transparency in the global finance.
- The hash chain also used in bit coin and other crypto currency like blockchain.

1.5.4 Basic consensus mechanisms

- The blockchain is a distributed and decentralized network which provides privacy, immutability, transparency and security.
- There is no central authorization in blockchain therefore it is completely secure and verified structure.
- This is possible only because of consensus protocol. Consensus protocols are the core part of blockchain network.
- The consensus algorithm is a procedure through which all the participants of the blockchain network reach a common agreement about present state of distributed ledger.
- The consensus algorithm gives the reliability to the blockchain.
- Following are the various consensus algorithms used by blockchain network.

  - ✓ Proof of work
  - ✓ Practical byzantine fault tolerance
  - ✓ Proof of stake
  - ✓ Proof of burn
  - ✓ Proof of capacity
  - ✓ Proof of elapsed time

Proof of work

- This consensus algorithm is used to solve complex mathematical puzzles.
- The mathematical puzzles require lot of computational power and then node who solves the puzzle soon that gets the mine to the next block.
- The bitcoin uses the Proof of Work consensus algorithm.
- In this consensus the miner is selected for next block generation.

Practical byzantine fault tolerance (PBFT)

- The PBFT consensus algorithm is used in asynchronous system where no upper bound on when the response to the request will be received.
- This consensus algorithm is used on low overhead time.
- Practical byzantine fault tolerance selves the many problems regarding to byzantine fault tolerance solution which is available.
- BFT is the consensus used when some of the nodes in the network fail to respond or respond incorrect information.
- This algorithm is used in blockchain and distributed computing.

Proof of stake (PoS)

- It is alternative of proof of work (Pow). The PoS used by Ethereum which is shifted from PoW consensus.
- In this consensus algorithm the validators invest on the coin of the system by locking up some of their coins as stake.

- Instead of investing on expensive hardware to solve complex puzzles validators invest on locking up coins as stake.
- After that all the validators start validating the blocks.
- Validators placed bet on the block that they want to be added if the block is discovered the block is added into the chain.
- As the block gets added by validators, they win reward according to their bets and their stakes get increase respectively.
- At the end, a validator is chosen to generate a new block based on their economic stake in the network.
- Hence PoS encourages validators through an incentive mechanism to reach an agreement.

Proof of burn (PoB)

- The validators in the PoB invest on 'burn' coins by sending it to address from where the loss is irretrievable.
- The validators do not invest on expensive hardware equipment.
- The validators commit the coins to unreachable address to achieve privilege to mine on the system based on random selection process.
- Hence the burning means the validators committing the long-term investment on their short-term loss.
- The PoB implemented will cause the native currency to be burn by validators in bitcoins.
- The more coins the validator burn, better are their chances of being selected to mine the next block.

Proof of capacity (PoC)

- In the proof of capacity consensus algorithm, the validators invest on the hard drive space.
- The validators do not invest on the expensive hardware or burning coins.
- As validator gets more hard drive spaces, they can get chance to mine for next block and can earn block reward.