Unit 2

Feature Engineering.

Q1) Define Blockchain.

→ • Blockchain technology is distributed, decentralized, immutable ledger that stores the record of ownership of digital assets in a business network.

• A blockchain is a distributed ledger / database that is shared among the nodes of a computer network.

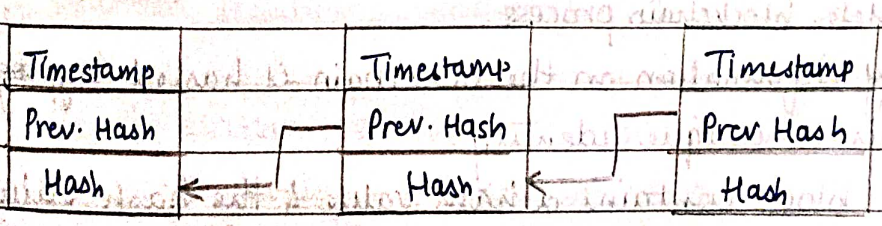
• It is a mechanism which enables secure transfer of assets without the need of intermediary.

• Anything from currencies to land titles to votes can be ~~took~~ tokenized, accumulated & exchanged on blockchain network.

• The majority participants verify every transaction in the system.

• The information is stored ~~in~~ together in blocks which are linked together.

• Every block contains the hash value of previous block.



Q2) What are the features of blockchain?

→ 1) Distributed

• For complete transparency, all network participants have a copy of the ledger.

• A public ledger supplies complete information about all the transactions & participants on the network.

- Tracking the events in ledger is easy as it changes propogate really fast.
- Every node on the blockchain network should participate in the validation.

2) Immutable.
- Immutability suggests that blockchain is an unalterable and permanent network.
- Once the transaction blocks is added on ledger, no one can go back & change it.
- Thus no user on the network can edit, update or delete it.

3) Decentralized
- In blockchain a single person or organization does not have control over the blockchain.
- Decentralization gives you the power to store your assets in a network without control of a single person or organization.
- Every node on the blockchain has the same copy of the ledger.

4) Secure
- All the records are individually encrypted in the blockchain
- use of encryption adds another layer of security to the complete blockchain process.
- Every information on the blockchain is hashed cryptographica & has a unique identity.
- Every block contains a hash value & the hash value of previous block

5) Consensus
- Every blockchain has a consensus to help the network to perform unbiased & quick decisions.
- Consensus is an decision making algorithm for the group of nodes active on the network to reach an agreement quick
- Nodes might not trust each other but they trust the algorithm that runs at the core of the network.

f) Unanimous.

- If node wants to add a block then it must get majority voting otherwise the block cannot be added to the network.
- A node cannot just add, update or delete information in the block chain.
- It is impossible to make changes without consent from majority ~~vote~~ of nodes in the network.

7)

Q3) Write a short note on History of Blockchain.

→ • Blockchain has a history that goes back to 1990s.

A) In 1991, Stuart Haber & W. Scott Sconetta presented a practical solution for time-stamping digital documents so that they could not be tampered.

- The concept of cryptographically secured block chain was used by them to design a system to store time-stamped docs.
- To create a secure chain of blocks, Merkle trees are used.

B) In 1998, a scientist, Nick Szabo worked on "Bit Gold" decentralized digital currency.

C) Blockchain technology is credited to satoshi Nakamoto as its creator.

- In 2008, Nakamoto created the first Blockchain from which the technology developed & found use in variety of applications outside cryptocurrencies.
- In 2009, Nakamoto published the first white paper on the subject.
- He explained in the whitepaper how the decentralized feature meant that nobody would be in control of anything & it suited to enhancing digital trust.
- Since then Nakamoto left the scene & gave control of the development of Blockchain to other core developers.

Q4. How does the Blockchain work?

→ • A Blockchain is a peer-to-peer, distributed database that hosts a constantly growing number of transactions.
• Each transaction is refered to as a "block".
• The block is secured through timestamping cryptography & is validated by all authorised members/nodes by using consensus algorithm.
• A particular transaction not validated by nodes ~~to~~ is not added to the database.
• Every transaction is connected to the previous transaction in a sequential ~~man~~ order forming a chain of transactions.
• A transaction cannot be edited, deleted.
• A transaction can only be altered by adding another transaction to the chain.
• Transactions are fixed together in an irreversible chain known as block chain.
• Each added block in the chain makes the verification of previous block stronger & thus the entire blockchain.
• This makes the blockchain tamper-evident.
• This removes the possibility of tampering by a bad intentioned actor.
• For eg. X wants to send money to ~~per~~ Y for paying an outstanding invoice related to purchase of software.
- X inserts the transaction in the database, thus creating a block.
- The block is broadcasted to every authorized member of the network.
- After validation of the transaction from all the members a block is added to chain or transactions.
- The money is then transferred from X to Y & Transaction is finished.

Q5. What does centralization mean?

→. Centralized systems are IT systems in which central authority is in control of functions & data for the platform which is in use.

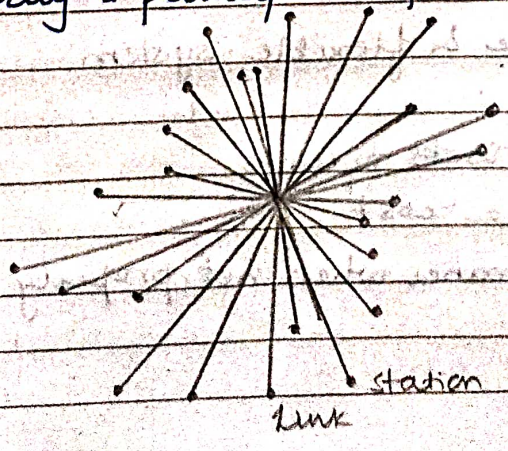
- The central authority is entirely in charged of all operations on the system.
- All users rely on a single source of service.
- A centralized authority controls majority of service providers like Google, Amazon, Ebay, Facebook, Youtube etc.
- All users in a centralised system are linked to a single server that controls the whole network.
- Both user information & data that may be accessed by other users are stored by the central owner.
- A centralised system is quickly constructed & simple to set up.
- This technique has a significant setback. if the server is down, users are unable to access the data.
- Pros

1) Simple deployment
2) Can be developed quickly
3) Affordable to maintain
4) Practical when data needs to be controlled centrally.

- Cons.

1) Prone to failures.
2) Higher security & privacy risks for users.

Q6)



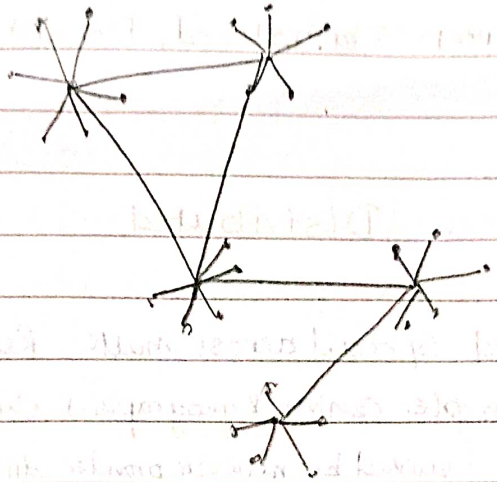
Q6. What is decentralization?

→ • A decentralized system is a type of network in which nodes are not dependent on a single master node.
• Control is distributed among many nodes.
• They use a number of central owners, each of whom keep a copy of these resources that users may access.
• Decentralized systems experience crashes as frequently as centralized ones.
• But decentralized systems are more fault tolerant by design.
• Even if one or two central owners servers fail, others can still access the data.
• This implies that system administrators fix broken servers & take care of other issue while system continues to function properly.
• This approach has benefit of quicker data access.
• Decentralized systems expose users to same security & privacy dangers as centralized ones.
• Although they can tolerate more errors, cost of maintainence is high.

Q7. ~~what are the advantages & disadvantages~~

* Pros
1) Less likely to fail than centralized system
2) Better performance
3) Allows more diverse & flexible system.

* Cons
1) Security & privacy risks to users
2) Higher maintenance cost
3) Inconsistent performance when not properly optimized.



Decentralized

Q7. What are distributed systems?

→ • Users in a distributed system enable user rights as required, but all users in the system have equal rights & access to the data.
• The internet is a great example of distributed systems.
• Shared ownership of data is made possible by distributed system.
• Users are also given equal access to hardware & software resources
• A distributed system is protected from the simultaneous failure of many components which increases uptime.
• The shortcomings of centralized & decentralized systems led to the development of distributed systems.

* Pros.
1) Fault tolerant
2) Transparent & secure
3) Promotes resource sharing
4) Extremely scalable

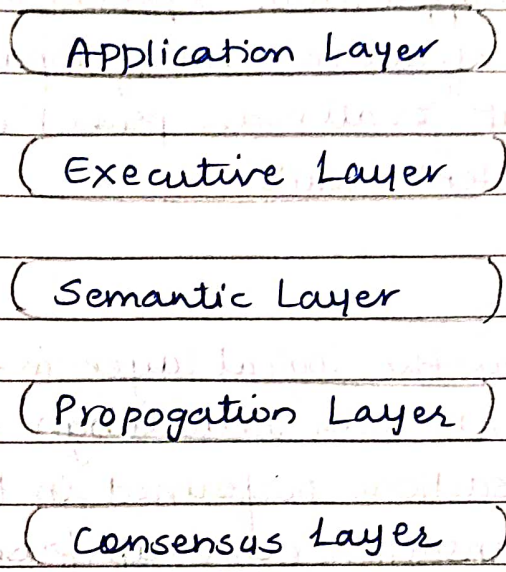
* Cons
1) More difficult to deploy
2) Higher maintainenance cost.

Q8. State difference between Centralized, Decentralized & Distributed Systems.

	Centralized	Distributed	Decentralized
Network Resources	Maintained & controlled by a single entity in centralized location.	Spread across multiple centres & geographies owned by network provider	Resources are owned & shared by network owners difficult to maintain as no one owns it.
Solution Components	Maintained & controlled by central entity.	Maintained & controlled by solution provider	Maintains. Each member has same copy of the ledger
Data	Maintained & controlled by central entity	Typically owned by customer	Added through group consensus.
Control	Controlled by central entity	Shared responsibility bet^n network provider, sol^n provider & customer	No one owns the data & everyone owns the data.
Fault tolerance	Low	High	Extremely high
Security	maintained by central entity.	shared bet^n network provider, sol^n provider & customer.	Increases as no. of network members increase
Performance	Maintained & controlled by central entity	Increases as hardware/ network resources ↑.	Decreases as no. of members increase
Example	ERP system	Cloud computing	Blockchain

Q9. Explain Layered architecture of Blockchain.

→ • The blockchain technology is based on a layered approach.
• Following are the layers of blockchain technology.



A) Application Layer
• Multiple applications can be built on a blockchain technology.
• Application layer contains the applications that are used by end users to interact with the blockchain network.
• Some applications built in the application layer can interface with other layers.
• Therefore application layer is on the top.
• The application layer is the layer where users can code the desired functionality & build the application.
• The application needs to be installed on each node as block-chain technology is decentralized technology.
• It neither has a client-server model, nor shared server & this is exactly how Bitcoin works.

B) Execution layer.
• This layer operates the executions of all the instructions that are performed at the application layer.

- This layer has the actual code & rules that are executed
- Simple or many instructions might be included in the set of instructions.
- Code is then performed individually on every node in the network if one application is present on all of them.
- The execution of code on a set of inputs should always result in same output for all nodes present on the blockchain to prevent inconsistent results.

c) Semantic layer.

- It is known as the logical layer in the blockchain.
- This layer deals with validation of the blocks as well as the transactions performed in the blockchain
- When the transaction comes up from a node, the set of instructions are executed in the execution layer & are validated by the semantic layer
- Semantic layer is also in charge of linking of blocks created in the network.
- With the exception of the genesis block, each block on the blockchain contains the hash of the one before it.
- On this layer, this block linkage must be defined.

d) Propogation layer.

- The propogation layer handles the peer-to-peer communication between nodes.
- It allows them to discover each other & get synced with some other node in the network.
- When a transaction takes place, it gets broadcasted to all the other nodes in the network.
- Also, when a node proposes a block, it will immediately get broadcast so that other nodes in the network can use this

newly created block & work upon it.

- This layer ensures the spread of transactions / blocks in the network which ensures the entire network's stability.
- Depending upon the network bandwidth or network capacity sometimes propogation could occur immediately or it may take longer.

e) Consensus Layer.

- This layer is the foundation layer for most of the blockchain systems.
- The main aim of this layer is to make sure that all the nodes must agree on a common state of the shared ledger.
- This layer also deals with security & safety of the blockchain.
- Once the block is proposed & grown by all the nodes, it is checked whether it is a valid block with legal transactions & the PoW problem has been solved correctly.
- There are many kinds of consensus algorithms like Proof of Stake (POS), Delegated PoS (DPoS) etc.

Q10. What are the limitations of Blockchain Technology?

→ i) Low scalability.

- The more people or nodes are involved, the slower the pace is.
- The problem is related to scalability issues with blockchain networks.
- The more people join the network, the chances of slowing down are more.

Eg - Centralized payment systems can process tens of thousands of transactions per second, while Bitcoin can only manage seven.

2) Lack of Awareness.

People do not know about blockchain & how they could implement it on different platforms.

3) Limited availability of technical talent
In Blockchain technology, there are not so many developers available who have special expertise in blockchain.
Hence, the lack of developers is a problem.

4) Implementation ~~probt~~ challenge
Its all about initial financial investments.
For some businesses, implementation may turn out overwhelmin

5) Immutable
- In immutable, we cannot make any changes to any of the record
- It is very helpful if you want to maintain integrity but it can be a drawback

6) High Energy Consumption.
- Most blockchain based solutions like bitcoin use a proof of work consensus algo. ~~obt~~ for validating transactions which utilizes excessive computing power comparable to yearly electricity consumption of a country.

7) Private key issues.
- In decentralized environment, private keys may become weak spot
- If someone loses the private key, wallet access is gone forever.

8 II) Elaborate the importance of blockchain.

→ 1) Immutability.
- Blockchain cannot be ~~chained~~ changed.
- This creates several chances for platforms that require immutable characteristics to improve the functionality of their system.
- Take the example of supply chain. Immutability enables businesses to guarantee that the packages are not harmed while in transit.
- The package information cannot be changed in any manner since

blockchain is immutable.

2) Transparency
- Due to its nature, public blockchain offers transparency.
- It serves many purposes in our society including voting.

3) Digital freedom
- Consider the bank as an example.
- If considered appropriate, it has the power to halt your transac or sieze your account
Some banks take action even though account holders haven't broken any laws.
- If you bring blockchain into account, we will have no centralized authority & you are your own bank.
- It provides digital independence.

4) Truly Decentralized Services
- Our advanced civilization is built on decentralized services.
- The music industry, for eg, can benefit from decentralized services where both creator & consumer can participate without need for approval from a big ~~co~~ centralized corporation.

5) Outstanding use-cases
- Blockchain is not restricted to a single use-case.
Nearly every industry ~~use~~ including banking, government, educatio healthcare, oil industry may utilise it.

6) Inexpensive
- As compared to other technologies, blockchain is less costly.
- The buffer of centralised authority is removed.
- Cost-effectiveness increased as there is no need to pay a middleman when there is no centralisation.
- It also reduces paperwork.