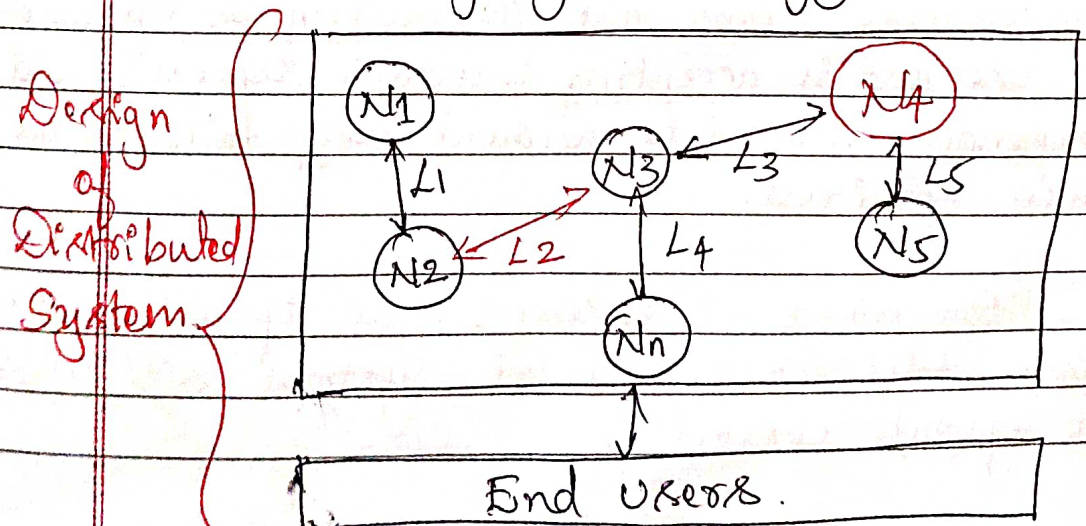
Blockchain Technology

Module - 1

⇒ DISTRIBUTED SYSTEMS

* Distributed systems are computing paradigm, where two or more nodes work each other in a coordinated fashion in order to achieve a common outcome, but the end user see it as a single logical platform. Eg: Google Search engine.
* A node can be defined as an individual player in a distributed system.
* All nodes are capable of sending and receiving messages to and from each other.
* nodes can be
  - → honest
  - → faulty
  - → malicious
  - → have own memory and Processor.
* A node that can exhibit arbitrary behavior is also known as a "Byzantine node".
* Arbitrary behavior can be intentionally malicious which is detrimental to the operation of the network.
* "Any unexpected behavior of a node on the network can be categorized as Byzantine.



* The distributed system has six nodes out of which N4 is Byzantine node leading to possible data inconsistency. L2 is a link that is broken or slow this can lead to partion in the network.

* The main challenge in distributed system design is co-ordination b/w the nodes and fault tolerance. Even if some of the nodes become fault & network links break, the distributed system should tolerate this and should continue to work flawlessly inorder to achieve the desired Result.

Explain the Concept of CAP theorem in blockchain

CAP theorem (10 marks)

* This is also known as Brewer's theorem, introduced by Eric Brewer in 1998.

* The theorem states that any Distributed System cannot have Consistency, Availability and partition tolerance simultaneously:

- **Consistency:** is a property that ensures all the nodes in a distributed system have a single latest copy of data.

- **Availability:** means that the system is up, accessible for use and is accepting incoming requests and responding with data without any failures as & when required.

- **Partition tolerance:** ensures that if a group of nodes fails the distributed system still continues to operate correctly.

* it has been prooven that distributed system cannot have all the mentioned 3 properties at the same time.

* To achieve fault tolerance, replication is used.
To achieve consistency, consensus algorithms used to ensure all nodes have same copy of data. This is known as state machine replication.

* In general there are 2 types of fault that a node can experience:
  - where faulty node has simply crashed and
  - where the faulty node can exhibit malicious or inconsistent behavior

Byzantine Generals Problem

* In septmber 1962, Paul Baran introduced the idea of cryptographic signatures with his peper on distributed communications networks.

Describe the various Consensus mechanism in Block Chain (10 marks)

⇒ Consensus

* Consensus is a process of agreement between distrusting nodes on a final state of data. Inorder to achieve consensus different algorithms can be used.

* It is easy to reach agreement between two nodes but when multiple nodes are participating, they need to agree on single value it becomes very difficult to achieve consensus.

* The concept of achieving consensus between multiple nodes is known as distributed consensus.

* Consensus Mechanisms

* A consensus mechanism is a set of steps that are taken by all or most of the nodes inorder to agree on a proposed state or value.

* following are the requirements must be met inorder to provide the desired results in a consensus mechanism.

Agreement: All honest nodes decide on the same value.

Termination: All honest nodes terminate execution of the consensus process and eventually reach a decision.

Validity: The value agreed upon by all honest nodes must be the same as the initial value proposed by at least one honest node.

Fault tolerant: The consensus algorithm should be able to run in the presence of faulty or malicious nodes.

Integrity: This is a requirement where by no node makes the decision more than once. nodes makes decision only once in a single consensus cycle.

* Types of consensus mechanism

* There are various types of consensus mechanism

Byzantine fault tolerance based:
With no compute intensive operations such as partial hash inversion, this method relies on a simple scheme of nodes that are publishing signed messages.

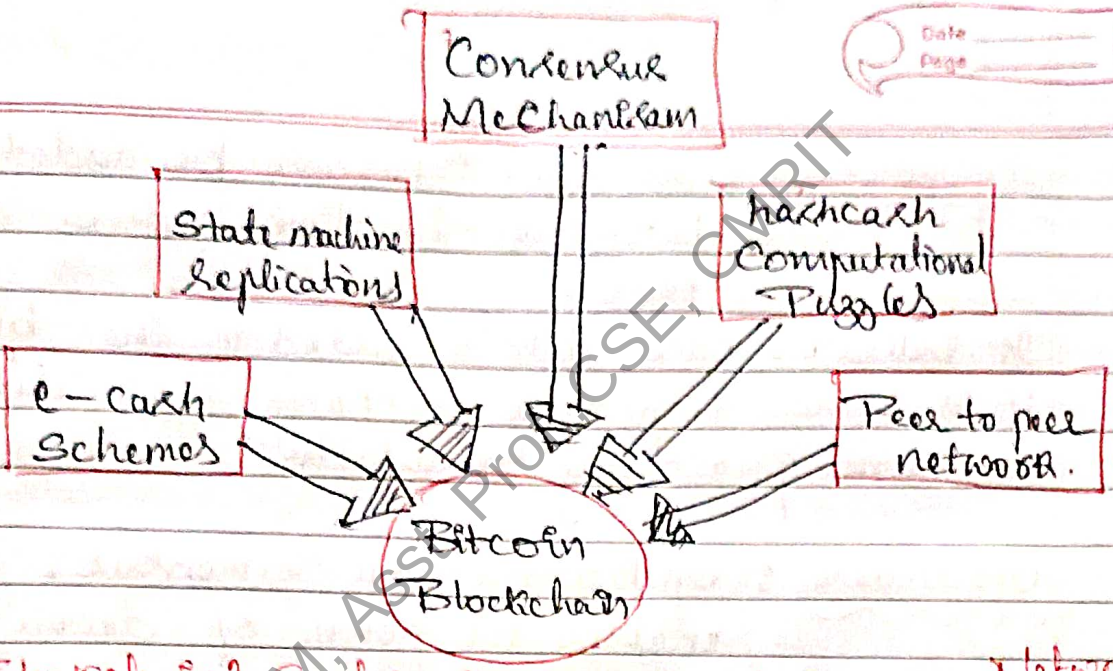
Leader based consensus mechanisms: This type of mechanism requires nodes to compete for the leader-election lottery and the node that wins it proposes a final value.

⇒ The history of Blockchain

* Blockchain was introduced with the invention of bitcoin in 2008 and practical implementation in 2009.

Electronic cash

* The ~~The~~ first successful application of blockchain is bitcoin ~~is~~ broadly cryptocurrencies.
* Electronic cash is nothing but digital currency.
* Fundamental issues that need to be addressed in e-cash systems are accountability and anonymity.
* David Chaum addressed both of these issues through blind Signature and Secret Sharing.
* After this other protocols emerged such as Chaum, Fiat and Naor (CFN), e-cash schemes that introduced anonymity and double spending detection.
* Later hashcash was introduced by Adam Back in 1997.
* In 1998 b-money was introduced, creating money via solving computational puzzles such as hashcash
* Another similar idea called BitGold was introduced in 2005 and also proposed solving computational puzzles to mint digital currency
* In 2009, the first practical implementation of a cryptocurrency named bitcoin was introduced, it slove the problem of distributed consensus in trustless network.



Define Blockchain? Explain the growth of BC with network view diagram

Introduction to blockchain: (peer to peer)

* Blockchain at its core is Distributed ledger (peer to peer) that is cryptographically secure, append-only immutable and updatable only via consensus or agreement among peers.

Peer to peer: This means that there is no central controller in the network and all the participants talk to each other directly.

* This property allows for cash transactions to be exchanged directly among the peers without a third-party involvement such as a bank.

Distributed ledger: meaning that a ledger is spread across the network among all peers in the network. and each peer holds the copy of the ledger.

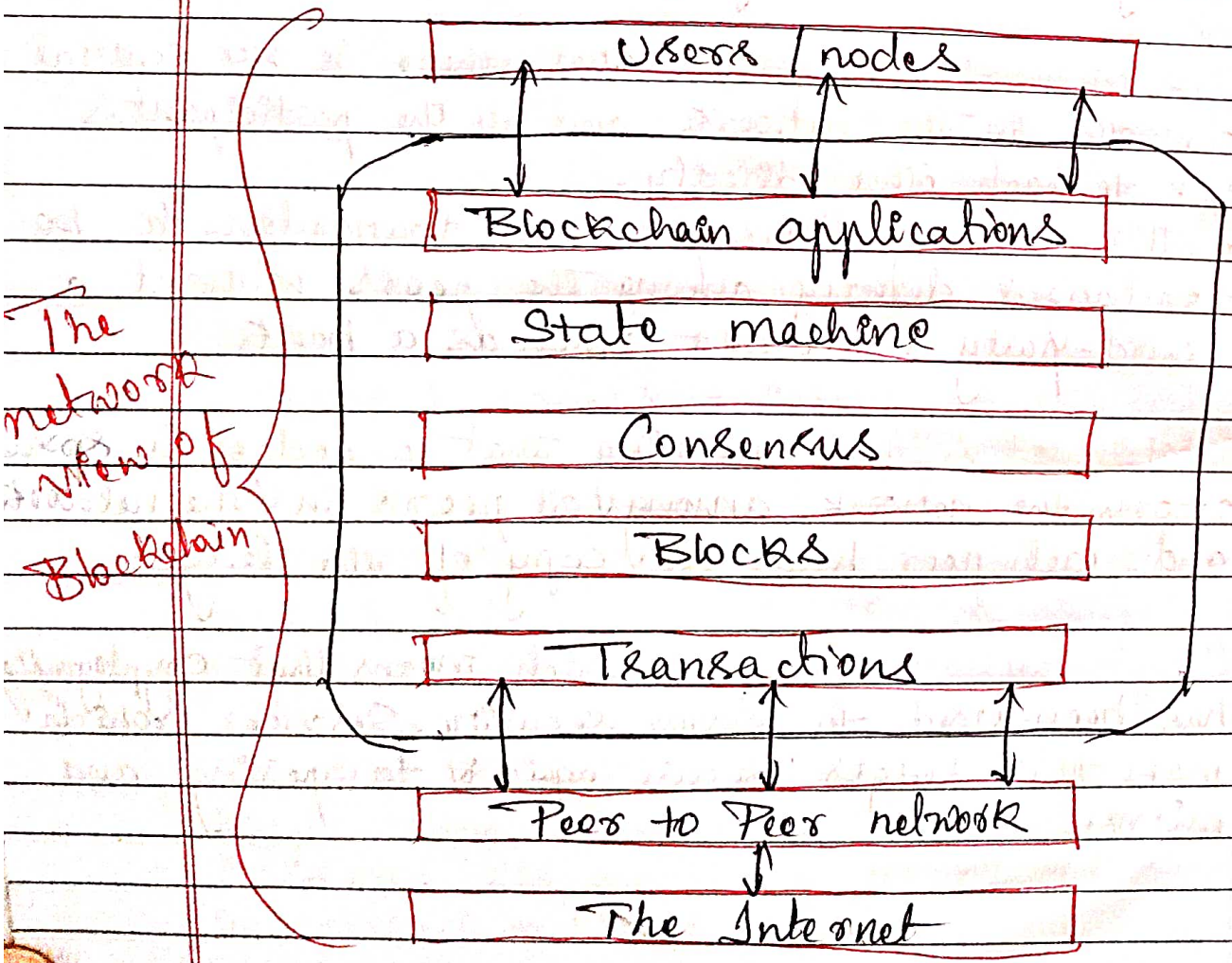
Cryptographically-Secure: which means that cryptography has been used to provide security services which make this ledger secure against tampering and misuse

- **Append-only**: the data can only be added to the blockchain in time-ordered sequential order.

It indicates once data is added to the blockchain it is almost impossible to change that data and considered practically immutable.

Updateable: Updateable via consensus. which enables the power of decentralization.

* Here no central authority is in control of updating the ledger. Instead any update made to blockchain is validated against strict criteria defined by the blockchain protocol and added to the blockchain only after a consensus reached among all participating nodes.



- Blockchain can be thought of as a layer of a distributed peer-to-peer network running on top of the internet, as seen in the provided diagram.

* At the bottom layer, there is the internet, which provides a basic communication layer for any n/w.

* Here a peer-to-peer network runs on top of the internet, which hosts the another layer of Blockchain. This layer contains transactions, blocks, consensus mechanism, state machines and blockchain smart contracts.

* All of these components are shown as a single logical entity in a box, representing blockchain above the peer-to-peer network.

* Finally at the top, there are users or nodes that connect to the blockchain and perform various operations.

* A blockchain can be defined as a platform where peers can exchange valid / electronic cash using transactions without the need for a centrally trusted arbitrator.

* A block is merely a selection of transaction bundled together and organized logically.

* A transaction is a record of an event. for example transferring amount from a sender's account to beneficiary account.

* A block is made up of Transactions and its size varies depending on the type and design of the blockchain in use.

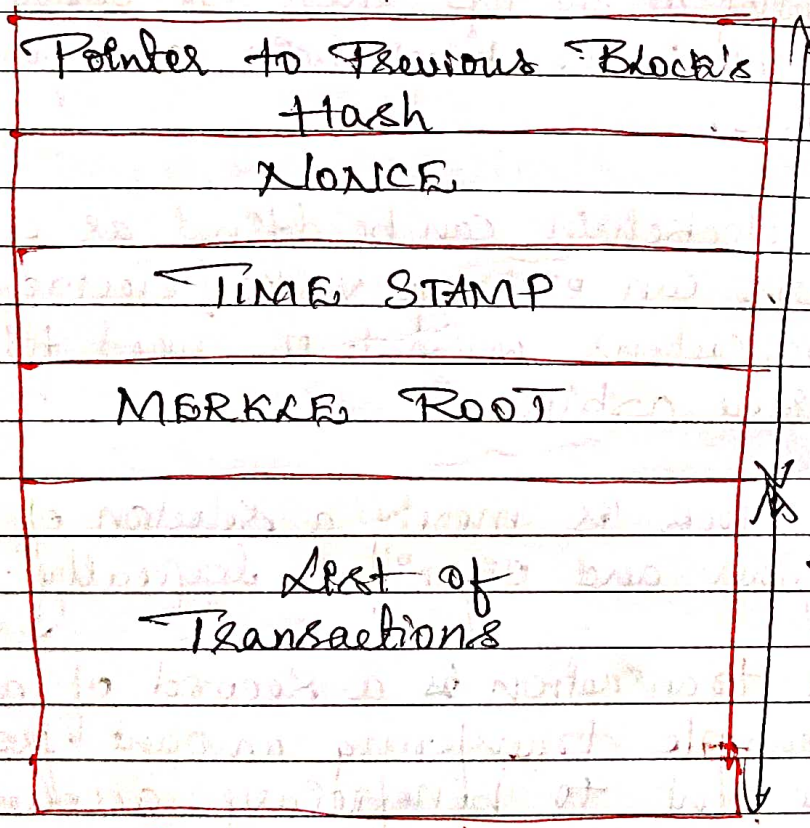
* A reference to a previous block is also included in the block, unless it is a genesis block.

* A Genesis block is the first block in the blockchain that is hardcoded at the time the blockchain was first started.

Define a Block? Explain the Generic Structure of a block

* Structure of the Block.

* The block consist of block header, which is composed of pointer to previous block, timestamp, nonce, Merkle root and the block body that contains transactions.



Generic Structure of a block.

* A nonce is a number that is generated and used only once. A nonce is used extensively in many cryptographic operations to provide replay protection, authentication and encryption.

* In blockchain, it is used in PoW consensus algorithms and for transaction replay protection.

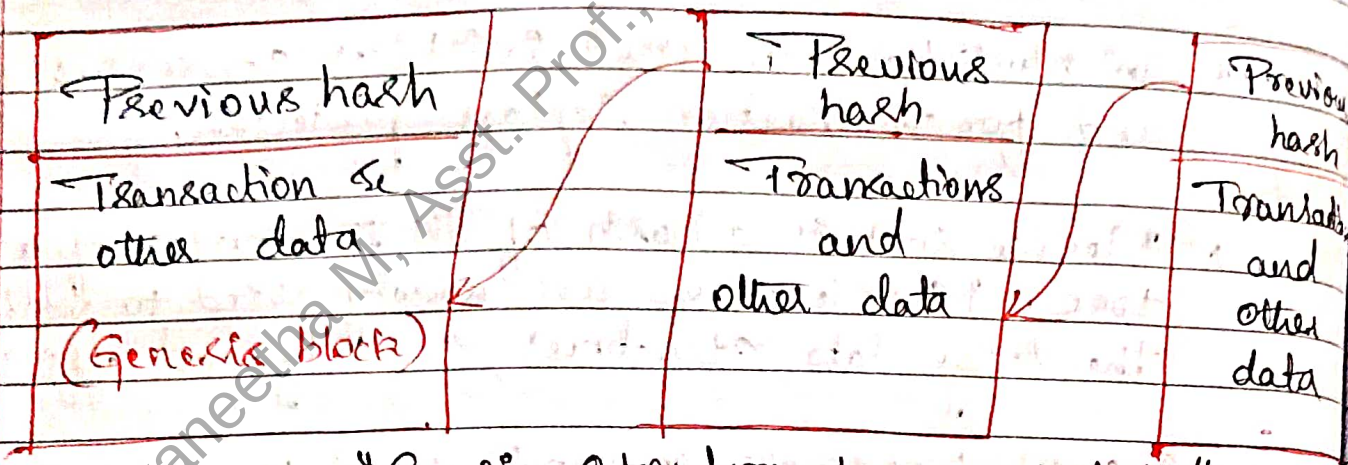
* Merkle root is a hash of all the nodes of a Merkle tree. Merkle trees are widely used to validate the large data structures securely and efficiently.

* Merkle trees are commonly used to allow efficient verification of transactions and it will be present in the block header section, which is the hash value of all transactions in a block.

* This means that verifying only the Merkle root is required to verify all transactions present in the Merkle tree.

Define a Blockchain? Explain the Generic elements of a Blockchain with diagram.

Generic elements of a Blockchain



"Generic Structure of a Blockchain"

* Elements of a generic blockchain are described here one by one.

(1) **Address:** Addresses are unique identifiers used in a blockchain transaction to denote sender and recipients. An address is usually a public key or is derived from a public key. While addresses can be owned by the same user, addresses themselves are unique.

A good practice is for users to generate a new address for each transaction in order to avoid linking transactions to the common owner

(2) **Transactions:**

A Transaction is the fundamental unit of a block chain. It represents a transfer of value from one address to another

(3) Block: A block is composed of multiple transactions and other elements, such as the previous block hash (hash pointer), timestamp & nonce.

(4) Peer-to-Peer network: is a network topology wherein all peers can communicate with each other and send and receive messages.

(5) Scripting or programming language: Scripts or programs perform various operations on a transaction in order to facilitate various functions.

For example:

In Bitcoin, transaction scripts are predefined in a language called Script, which consist of set of commands that allow nodes to transfer tokens from one address to another.

Script is a limited language, i.e it only allows essential operations that are necessary for executing transactions, but it does not allow any arbitrary program development

Bitcoin script language cannot be called Turing complete. Turing complete language means that it can perform any computation.

(6) Virtual machine: This is an extension of the transaction script introduced earlier.

A virtual machine allows turing complete code to be run on a blockchain. but virtual machines are not available on all blockchain

EVM - Ethereum Virtual machine (EVM)

CVM - chain virtual machine (CVM)

(7) State machine: A blockchain can be viewed as a state transition mechanism where by a state is modified from its initial form to the next one and eventually to a final form by nodes on the block-chain network as a result of a transaction execution, validation and finalization process.

(8) Node: A node in a blockchain network performs various functions depending on the role that it takes on.

* a node can propose and validate transactions and perform mining to facilitate consensus and secure the blockchain
* nodes can also perform simple payment verification validation etc.

(9) Smart contract: These programs run on the top of the blockchain and encapsulate the business logic to be executed when certain conditions are met.

Explain - How blockchain validates transaction and How Blockchain works? creates and adds the blocks?

* Nodes are either miners who create new blocks, mint cryptocurrency (coins) or block signers who validates and digitally sign the transactions.

* The critical decision that every blockchain network has to figure out that which node will append the next block to the blockchain.

This decision is made using a consensus mechanism.

How a blockchain validates transactions and creates and adds blocks to grow the blockchain

* This scheme is presented here to give you a general idea of how blocks are generated and what the relationship is between transactions and blocks.

1. A node start a transaction by first creating and then digitally signing it with its private key.

A transaction can represent various action in a blockchain. Most commonly this is a data structure that represents transfer of value between users on the blockchain network

2. A transaction is propagated (flooded) by using flooding protocol called Gossip protocol, to peers that validate the transaction.

3. Once the transaction is validated, it is included in a block, which is then propagated onto the network. At this point, the transaction is considered Confirmed.

4. The newly-created block now becomes part of the ledger and the next block links itself cryptographically back to this block.

This link is a hash pointer. At this stage, the transaction gets it second confirmation and the block gets its first confirmation.

5. Transactions are then reconfirmed every time a new block is created. Usually six confirmations in the Bitcoin network are required to consider the transaction final.

Explain Benefits and Disa

* The notable benefits of b are as follows:

1. Decentralization:

* It is a core concept and There is no need for a intermediary to validate Consensus mechanism is