BLOCKCHAIN TECHNOLOGY

UNIT 1: Introduction and Basics of Distributed computing

I Need for Distributed Record Keeping

→ A distributed ledger can be described as a ledger of many transactions or contracts maintained in decentralised form across locations and people.

→ All info is encrypted and can be accessed using keys and cryptographic signatures

→ Any additions to the ledger must be reflected and copied to all participants.

→ Once info is stored, it becomes an immutable database, which the rules of the network govern, making the records resistant to malicious changes by a single party.

→ Digital records can be tampered with which makes them difficult to trust. There are many services that provide secure and verified document management but they are costly and 3rd party.

II Modelling Faults and Adversaries.

1) CRASH FAULT : Nodes could go permanently offline.

2) PASSIVE ADVERSARIES : They infringe on the privacy of the communicating parties by reading messages they weren't supposed to.

3) BYZANTINE/ACTIVE ADVERSARIES : The use the arbitrarily gathered information by sending false & conflicting messages.

BYZANTINE GENERALS PROBLEM

- Byzantine Generals Problem is an impossibility results which means the solution to this problem hasn't been found yet.
- It is basically a game theory problem that provides a description of the entent to which decentralized parties emperience difficulties in reaching consensus without any trusted central parties.

→ Byzantine army is divided into many batallions with each division led by a general.
→ The generals connect via messenger to agree to a joint plan of action in which all batallions coordinate and attack from all sides.
→ It is probable that traitors will try to sabotage their plan by intercepting or changing the messages.
→ As a result, the purpose of this challenge is for all of the faithful commanders to reach an agreement without the imposters tampering with their plans.

CONSENSUS ALGORITHMS AND THEIR SCALABILITY PROBLEMS.

A consensus algorithm is a procedure through which all the peers of the blockchain network reach a common agreement about the present state of the distributed ledger.

Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the blockchain.

Various Consensus Algorithms

1) Proof of Work (POW)
2) Proof of Stake (POS)
3) Proof of Authority (POA)
4) Proof of Activity (POA)
5) Proof of Capacity (POC)
6) Proof of Burn (POB)
7) Proof of Elapsed Time (PoET)
8) Proof of Identity (POI)
9) Delegated Byzantine Fault Tolerance (DBFT)
10) Delegated Proof of Stake (DPOS)

Ethereum changed from POW to POS in September 2022

PROOF OF WORK (POW)

- oldest mechanism. Also called mining where participating nodes are called miners.
- the central idea behind this algorithm is to solve a complex mathematical puzzle and easily give out a solution.
- this mathematical puzzle requires a lot of computational power and thus, the node who solves the puzzle as soon as possible gets to mine the next block

ISSUES :-

⇒ Becomes slower with increasing transactions
⇒ temp solution is to increase block size but as transactions increase exponentially, that won't last long.
⇒ Mining is time and energy consuming
⇒ 51% attack is possible

PROOF OF STAKE APPROACH (POS)

- It addresses the computing power need by introducing a mechanism where validation is done by random selection of node.
- chance of being selected ∝ stake amount
- stake acts as collateral incase node validates a false transaction

ISSUE :-

- Rich get richer
- compromises decentralization

PROOF OF AUTHORITY (POA)

- Modified version of POS in which the identities of validators in the network are at stake.
- Identity is validating by comparing validator's personal identification with their official documentation
- Validators put their reputation on the network

ISSUES :-

⇒ POA is not decentralized but an attempt to make centralized systems more efficient.

⇒ POA validator's identity are public. can lead to 3rd party manipulation.

PROOF OF ACTIVITY (POA) :

- It is a hybrid approach designed through the convergence of PoW and PoS blockchain consensus models.
- In POA, miners race to solve a cryptographic puzzle just like PoW. However, the blocks contain information about the block winner's identity. Here it becomes PoS.

PROOF OF CAPACITY :

- In this, validators are supposed to invest in hard drive space instead of expensive hardware or burning coins.
- The more hard drives the validators have, the better are their chances of getting selected to mine the next block.

PROOF OF BURN: (POB)

- In this, validators burn coins by sending them to an irretrievable address.
- Based on the coins burned, they are randomly selected.
- Can burn native currency or external
- No of coins burned ∝ chances of selection.

ISSUES :-

- Resources are wasted/burned
- Rich become richer.

PROOF OF ELAPSED TIME (POET):

- one of the fairest consensus algorithm
- widely used in permissioned blockchain networks
- Every validator makes their own block and adds proof of wait time. winner is the one with lowest time.
- checks in the algo to avoid same winner or generating lowest timer value.

PROOF OF IDENTITY (POI):

- used in permission-less blockchain
- Each individual receives one equal unit of voting power.

ISSUES :-

- too much storage
- can be thought of as centralized.

QUESTION BANK

Q1 Blockchain is disruptive technology. Justify.

ANS There are 2 types of innovation :-

- SUSTAINABLE which makes products & solutions better.
- DISRUPTIVE which 'relentlessly moves' within the market with the eventual goal of 'displacing established competitors'.
- Blockchain will be recognized as a disruptive innovation that threatens the market since its applications, which are only now being explored, have the potential to completely change existing industries and shatter the way bussinesses are managed.
- Financial institutions have the most to lose especially in terms of power but can save money also.

Q2 Components of Blockchain framework

ANS 1) NODE :→ Full node [Full copy of transactions ; miner]
→ Partial node [Headers only. Low power]

2) LEDGER : It is a digital database of information.
There are 3 types :-
→ Public ledger : Anyone in network can read/write
→ Distributed ledger : All nodes have a local copy of database. Group of nodes collectively execute jobs
→ Decentralized ledger : No central authority.

3) WALLET : Digital wallet that allows user to store crypto. Privacy is maintained using public & private keys.

4) NONCE : "Number only used once".
32-bit random number that assists to create a block or verify transaction. It is used to make the transaction more secure.

5) HASH: Maps block data to fixed size.
current hash ⇒ Previous hash.
Properties:-
→ collision resistant
→ Hiding
→ Puzzle friendliness

Q3 Structure of Block

ANS
- Block Height
- Block Reward
- Transaction count
- Transactions
- Block header :-
  → Timestamp
  → Version
  → Merkle Root
  → Difficulty
  → Nonce
  → Previous hash.

Q4 Why is blockchain growing and in-demand.

ANS
- Disruptive technology
- Secure / Trust
- Cryptocurrency
- Less transaction fees.
- Immutable.

Q5 Blockchain Applications in Healthcare

ANS
- Supply chain management
- Electric Health records
- Smart contract for insurance.

Q6 Proof of work.

Q7 Issues/Limitations in Blockchain

ANS
→ Too transperant
→ Scalability Issues
→ Computational Power
→ No regulation / central authority
→ Transaction speed
→ Complex to understand
→ 51% attack

Q8 Scope & Benefits of Blockchain

ANS
- Scope in all depts. especially finance.

Benefits :
- Secure
- Transperant
- Tracable
- Automation (smart contracts)
- No middleman (speed)

Q10 - 13 ANS

Types of Blockchain with adv & disadv

3 major types

1) PUBLIC BLOCKCHAIN :

- Anyone can join ~~or~~ and do transactions
- Requires peers to participate and do transactions or network becomes non-functional.

ADVANTAGES :-

→ Anyone can join
→ Everyone feels incentivized to work
→ Transperant
→ NO intermediaries

DISADVANTAGES :-

→ Transaction speed is less
→ cannot be scaled
→ uses consensus methods which can ~~be~~ take energy

2) PRIVATE BLOCKCHAIN

- Permissioned network
- Orgs can give roles

ADVANTAGES :-

→ Faster than public
→ More scalable

DISADVANTAGES :-

→ central authority
→ Security can be issue if one node is compromised

3) CONSORTIUM / FEDERATED BLOCKCHAIN

- Some aspects are public & some are private
- Multiple orgs manage
- Has validator nodes & member nodes

ADVANTAGES :-

- More customizability and control over resources
- More secure and efficient

DISADVANTAGES :-

- one bad fish can ...
- less transparent
- can be censored
- less anonymous

8/7 Delegated Proof of Stake (dPOS)

- users must stake their coins by voting/proxy vote for someone to be the "withness".
- "witnesses" with max vote gets to choose which transactions to mine
- Everything is on reputation and votes and the witness can be easily replaced by voting

ADVANTAGES :-

- More energy efficient that POW

DISADVANTAGE :-

- If there isn't much competition for withesses, can become centralized.

Delegated Byzantine Fault tolerance (dBFT)

- users are voted just like dPOS but they mine blocks / transaction following BFT.

ADVANTAGES :-

- Fast & efficient unlike POW

DISADVANTAGES :-

- Delegate's identities are not private.
- There is a big ↓ regulation / centralization.

JAGirkar →

Proof of Importance (POI)

- An upgraded version of POS
- Not only your stake but your reputation / ranking / importance score over past transactions also matter.

Proof of History (POH)

- Run hash a fixed number of times to get output.

Q.A What are target and difficulty level? How it plays to control bias mining

ANS
- Bitcoin algo adjusts difficulty with no. of active miners to ensure blocks are discovered at an early stage
- Mining difficulty is altered by adding or reducing zeros at the front of the target hash
- This prevents people with higher performance always win

Q21 New difficulty level in Bitcoin

ANS

$$\text{New mining difficulty} = \text{old difficulty} \times \frac{\text{Time to mine last 2016 blocks}}{20,160 \text{ minutes}}$$

Q22 What is Merkle tree? How is it used?

- Also called binary hash trees
- It's a mathematical data structure made up of hashes of various data blocks that summarize all the transactions in a block.
- It also enables quick and secure content verification across big datasets and verifies the consistency and content of the data.

WORKING:

→ Merkle trees are made by hashing pairs of nodes repeatedly until only one hash remains which is known as merkle root or root hash.

→ They are built from the bottom, using transaction ID's which are hashes of individual transaction

→ Each non-leaf node is a hash of its previous hash and every leaf node is a hash of transactional data.

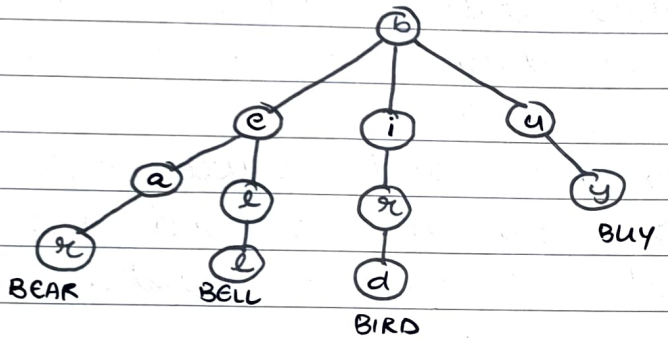
Q23 Types of nodes in blockchain:

- Full nodes / miners
- Light nodes
- Archival nodes [They validate blocks & maintain consensus]

Q24 Differentiate Patricia Trie and Merkle Tree

PATRICIA TREE:

- Patricia tree is also known as radix tree
- Used to store key-value pairs
- A node's position in the trie defines the key with which that node is associated unlike in BST, where a node stores key corresponding only to that node



Q25 EOA and CA

EOA	CA
• Controlled by humans	• Controlled by contract code
• Private key is required to access EOA	• No key required to access EOAs
• Created automatically on wallet creation	• CA requires EOAs to be activated
• Don't have their own associated code	• Have their own associated code
• No execution fee	• Has execution fee
• code hash is an empty string	• Code hash represents the code associated with the account

Q26 Gas Prices Pre and Post London

PRE-LONDON

Lets say A has to pay B 1 ETH. Gas limit = 21,000 units and gas price = 200 gwei

∴ Total fee = Gas units/limit * Gas price per unit
= 21,000 × 200
= 4,200,000 gwei
= 0.0042 ETH

∴ Deduction from A's account = 1.0042 ETH
B gets 1 ETH & miner gets 0.0042 ETH.

POST-LONDON

Ethereum network will decide a base transaction fees depending on the network's traffic.
Users can add tips on top ~~based on~~ to make their transactions be verified earlier.
Also block size was doubled.
To avoid the risk of miner collusion to artificially inflate the base fee for miner's benefit, only the miner's tip goes to the miner and the entire base fee is burned / destroyed.

Q27 What are the Ethereum data types

Solidity data types :-

1. BOOLEAN : T/F
2. INTEGER : signed (int) and unsigned (uint)
3. ADDRESS : 20 byte value. getBalance() or transfer()
4. BYTES AND STRINGS : Byte can store 1-32 bits.
   String has dynamic length
5. ENUMS : User defined data types to improve contract readability & efficiency

Q30 Key components of Ethereum.

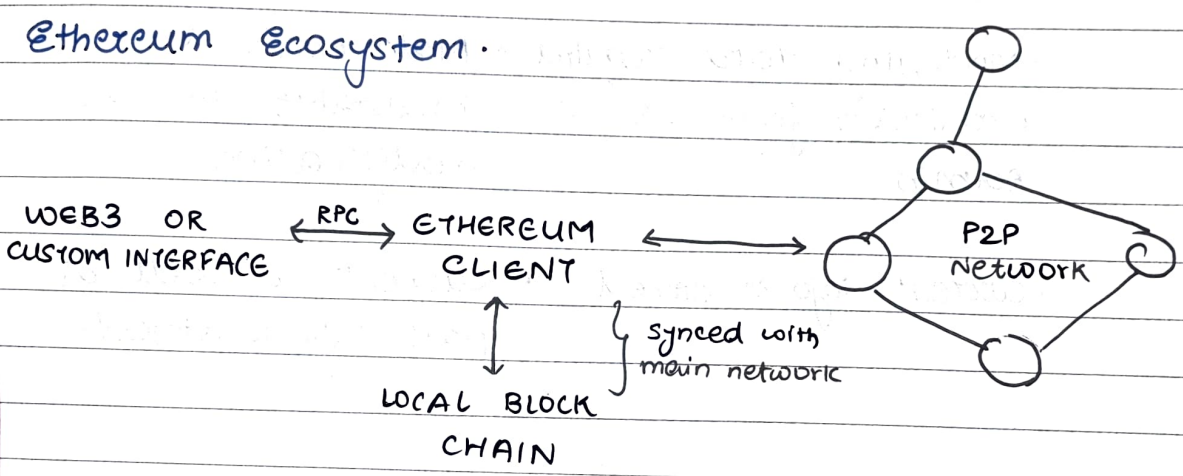
1. NODES → Mining node
   → Ethereum Virtual Machine node
2. ETHER
3. GAS
4. Ethereum Account → EOA
   → CA
5. Nonce
6. Storage Root [Merkle root]
7. Algorithm.

Q31 ~~a] Merkle Patricia Trie~~

Q27 Ethereum Data types

- Permanent data e.g. transaction
- Ephemeral data e.g. account balance

Q29 Ethereum Ecosystem.



An Ethereum client provides all blockchain components to maintain world state and state ~~transactio~~ transitions in the BC network, including the following :-

→ Managing transactions & state transitions with the ethereum blockchain
→ Maintaining world state and account state
→ Managing P2P communication block finalization with mining
→ Managing transaction pool.
→ Managing cryptoassets, gas, ether & tokens

Q 33 DB vs Blockchain ledgers

DB	BLOCKCHAIN
• Centralized	• Decentralized
• DBMS Admin is required	• NO Admin
• Modifying data requires permission from DB Admin	• Main chain is irresistable to data modification
• Current info is stored	• Current as well as past info is stored.

Q 35 Double Spending

- You've sent 1 BTC to 2 addresses
- Transactions are in unconfirmed pool.
- 1st transaction gets verified and 2nd rejected
- If both are taken simultaneously then the one with higher no. of confirmations is selected.
- many merchants wait for atleast 6 confirmations of transaction i.e. 6 blocks have been further added.

Q36 Ethereum Smart Contract vs traditional contract

SMART CONTRACT	TRADITIONAL CONTRACT
• Fast & Efficient	• Time consuming
• Immutable	• can be changed
• No 3rd party authority	• Needs a 3rd party authority
• Cost effective	• Expensive
• Automatic Payment	• Manual Payment
• Virtual presence (Digital sign)	• Physical presence
• Pseudonymous	• Legal Identity

Q37 Life cycle of Ethereum Smart Contract

4 Phases → Create smart contract
→ Freeze smart contract
→ Execute Smart Contract
→ Finalize Smart Contract

CREATION : Tasks done :-
a) Negotiation between the parties
b) Smart contract's design, implementation & validation.

FREEZING : a) Smart contracts are stored on the blockchain
b) Freezing of digital assets of involved parties

EXECUTION : a) Execution of smart contract condition
b) Auto-execute smart contract statement triggered

FINALIZE : a) State updating & digital assets allocated.
b) Unfreezing of digital assets received from the first party.

Q 38 Why smart contract execution has a cost

- Code takes memory space and there is a cost per byte of memory used.
- Miners need to be incentivized to mine it
- Transactions need fees.

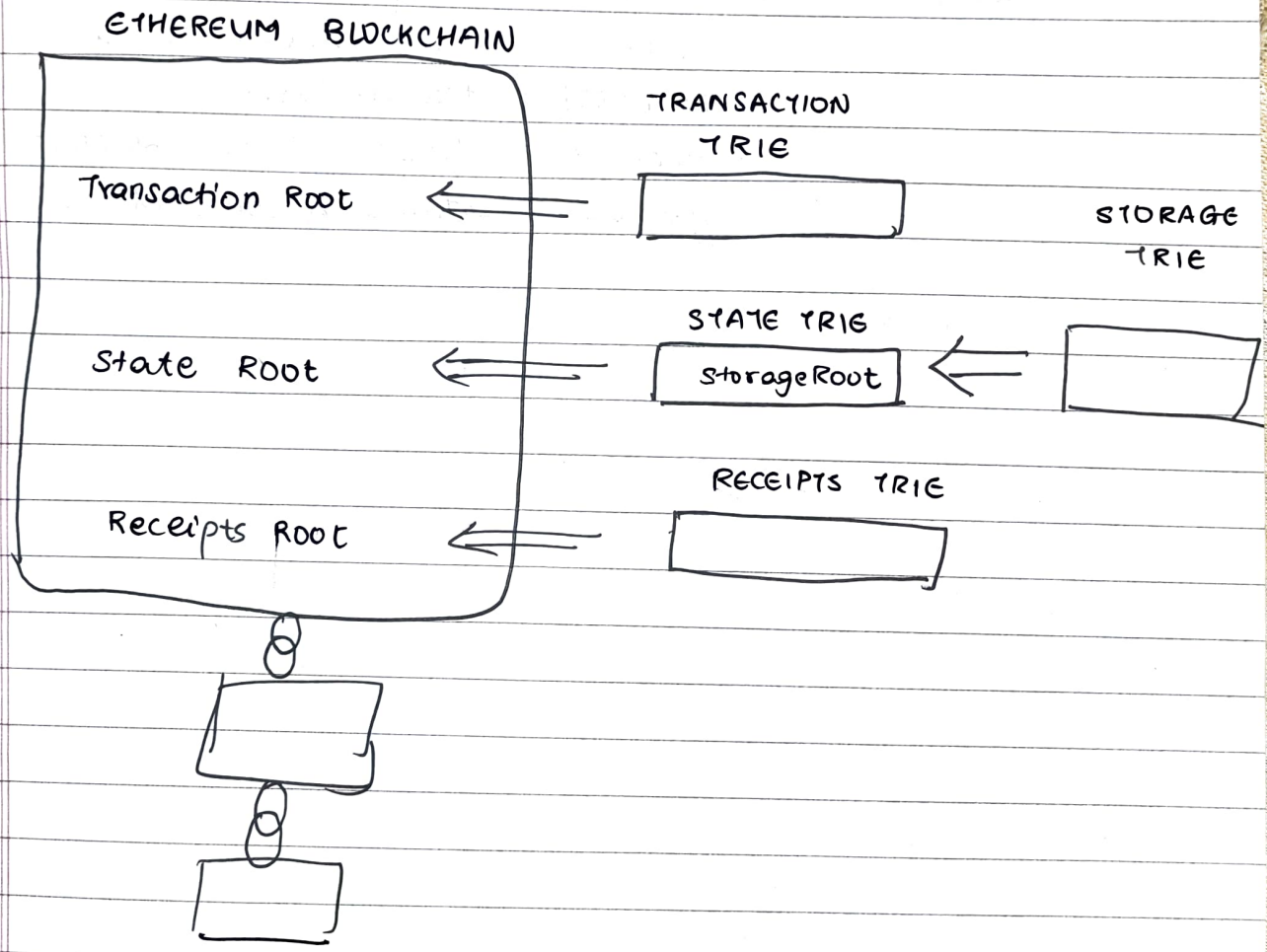
Q 40 Bitcoin vs Ethereum.

BITCOIN	ETHEREUM
• Satoshi Nakamoto in 2008	• Vitalik Buterin in 2013
• Purpose is to use as currency	• currency as well as to store code
• Doesn't have smart contracts	• Has smart contracts
• BC data is transactions	• BC data can be transactions or code
• SHA-256 algorithm.	• Keccak-256 algorithm
• POW consensus	• POW until sep'22. POS now
• Block time is 10 minutes	• Block time is 14-15s.
• Most popular digital currency	• 2nd most popular.

Q3) Etherium Tries

4 types of state tries :-

1) World state & Account state
2) Transaction
3) Receipt
4) Account storage Trie



WORLD STATE TRIE :
- Mapping between address & A/c states
- Constantly updated
- All info about accounts
- has storageRoot field that points to root in A/c storage trie

ACCOUNT STORAGE TRIE : · Stores data associated with account

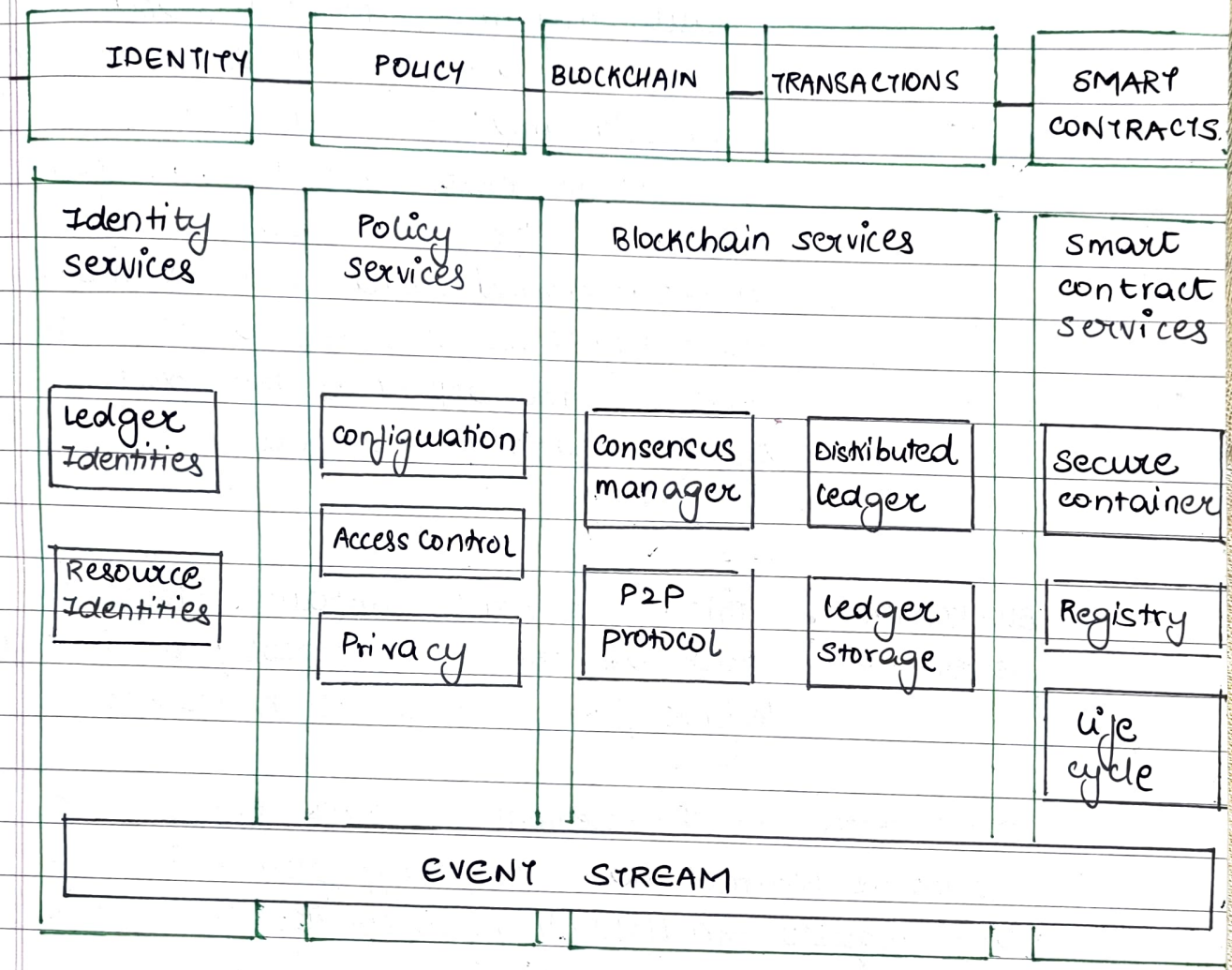
TRANSACTION TRIE : · Records transactions
• Transaction are imp as they change state.
• Transactions are immutable

RECEIPT TRIE : - Records receipts of transactions
- Receipt is the result of a successful transaction
- Receipt includes hash, block no, gas used, address of contract, etc.

BC TT2 QUESTION BANK

Q1 Explain Hyperledger services : Identity, policy, Blockchain, Transaction, smart contract.

ANS



Hyperledger services.

IDENTITY SERVICES : This component matches the IDs of all network objects (such as blockchain network participants, smart contracts, and verification nodes used for consensus).

POLICY SERVICES : This component manages policies. It provides access control and authority management, and manages areas such as participant privacy and consensus rules.

At its most basic level, a policy is a function which accepts as input a set of signed data and evaluates successfully, or returns an error because some aspect of the data did not satisfy the policy.

BLOCKCHAIN SERVICES : This component contains elements such as the P2P protocol, distributed ledger, and consensus manager.

⇒ P2P PROTOCOL – This element provides P2P functions such as bidirectional streaming, flow control, and request multiplexing. It works in coordination with existing networks

⇒ DISTRIBUTED LEDGER – This element manages the blockchain and status

⇒ CONSENSUS MANAGER – This element provides the interfaces for plug-in consensus algorithms such as the PBFT interface.

SMART CONTRACT SERVICES : This component provides the means for executing smart contracts on verification nodes. It contains a secure execution environment and smart contract life cycle (deploy - update - terminate) management functions.

EVENT STREAM : This element provides pub / sub event management functions. For eg., it enables outside systems to detect distributed ledger events.

API : This element provides the API for the component elements above. It also contains open source APIs

Q2 Discuss Hyperledger fabric : Design - goals

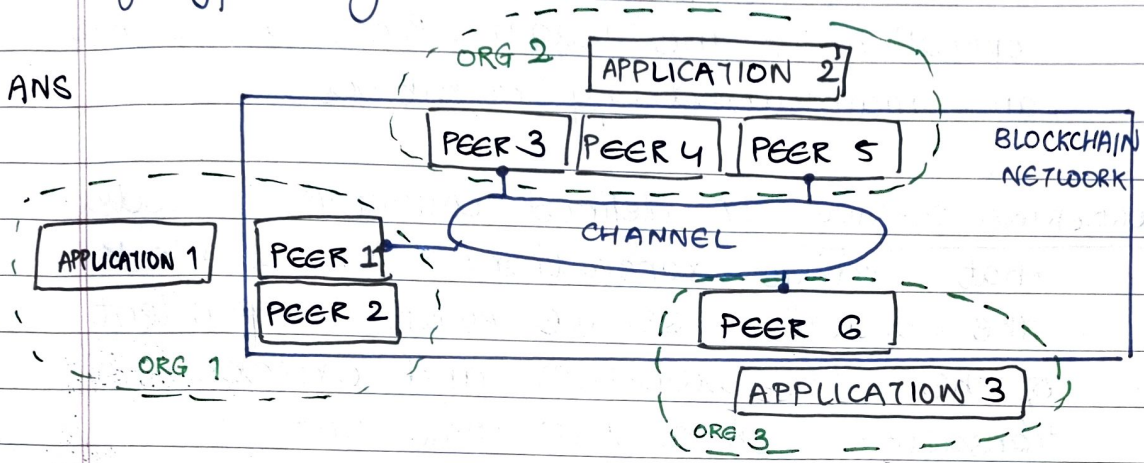
ANS
- Hyperledger fabric is open-source, private, permissioned blockchain
- Allows components, such as consensus and membership services, to be plug-and-play.
- First distributed ledger platform to support smart contracts authored in general-purpose programming languages.
- Supports pluggable consensus protocols.

DESIGN GOALS

1. Modular Approach [Plug and Play]
2. Scalability.
3. Privacy and confidentiality [Tx visible to those with access]
4. Deterministic Tx [same everywhere]
5. Identity [Flexible PKI, handling Access control]
6. Auditability [Immutable audit trail]
7. Interoperability [Blockchains intercommunication]
8. Portability [Run across multiple platform]
9. Rich data queries [Must query using traditional lang on ledger]

Q3 Draw and discuss High level architecture of Hyperledger Fabric / Explain various components of Hyperledger Fabric Network

ANS



1 LEDGER : A ledger consists of two distinct, though related, parts — a "blockchain" and the "state database", also known as "world state". unlike other ledgers, blockchains are immutable — that is, once a block has been added to the chain, it cannot be changed.

2 MEMBERSHIP SERVICE PROVIDER (MSP) : The Membership Service Provider (MSP) refers to an abstract component of the system that provides credentials to clients, and peers for them to participate in a Hyperledger Fabric network.

3 SMART CONTRACT : A smart contract is code — invoked by a client application external to the blockchain network — that manages access and modifications to a set of key-value pairs in the world state.

4. PEERS : A network entity that maintains a ledger and runs chaincode containers in order to perform read/write operations to the ledger. Peers are owned and maintained by members.

5. ORDERING SERVICE : A defined collective of nodes that orders transactions into a block. The ordering service exists independent of the peer processes and orders transactions on a first-come-first-serve basis for all channels on the network.

6. CHANNEL : A channel is a private blockchain overlay which allows for isolation and confidentiality. A channel-specific ledger is shared across the peers in the channel, and transacting parties must be properly authenticated to a channel in order to interact with it.

7. CERTIFICATE AUTHORITY : Hyperledger Fabric CA is the default certificate authority component, which issues PKI-based certificates to a network member organization & their users.

8. ORGANIZATIONS : Also known as "members", organizations are invited to join the blockchain network by a blockchain service provider. An org is joined to a network by adding its Membership service Provider to the network.

Q4 What is the role of "chaincode" in hyperledger fabric. Explain ordering, system and core chaincodes.

ANS A chaincode (or smart contract) is an application that runs on top of the underlying architecture to enforce business rules and maintain the state. This application can define its own data structures, or use the types of services enposed by other chain codes running in parallel on the same peer node.

- The node that participates in the consensus protocol validates blocks and distributes them to other peers. Each node has access to all information required for this task and runs an internal chaincode that enforces business rules.
- Chaincode is the program that is running on a peer node.
- There are many chaincodes out there and they all run the same way, enforcing business rules on transactions.
- Chaincode can be written in any language supported by the underlying platform.

ORDERER CHAINCODE

This type of chaincode is executed by an orderer node (a peer with special tagging configured in the network identity). The orderer executes this chaincode for each transaction and subsequently enforces the business logic associated with this transaction by representing it as an "order" object. The order is then sent

to the participants in the P2P network and they are responsible for processing it.
This type of chaincode is executed by an orderer node.

The orderer executes this chaincode for each transaction and subsequently enforces the business logic associated with this transaction by representing it as an "order" object. The order is then sent to the participants in the P2P ("Peer") and they are responsible for processing it.

SYSTEM CHAINCODE

A system chaincode is a set of functions that provides the blockchain runtime with information about the status of a transaction, while still allowing the transaction to execute. It can be used to validate or reject transactions, or to obtain additional information about Blockchain interactions.

In Hyperledger Fabric, system chaincodes are usually written in a programming language based on JS and run in a container as an isolated process

CORE CHAINCODE

This type of chaincode is executed by a core node (a peer that runs multiple chaincodes). The core node has special tagging configured in the network identity. The core node executes this chaincode for each transaction but represents it as a new message that is sent using the

Messaging service. chaincode will run on peer nodes in hyperledger fabric network. while running a chaincode, there are several things that will be enforced on transactions by chaincode. A peer group is a cluster of peer connected to each other through a leader. Each peer in this group will be running the chaincode of the same type.

Q5 Explain steps involved in hyperledger transaction.

ANS
- client initiating a transaction
- validation of transaction
- simulating of transaction
- verifying proposal response
- Broadcast transaction to the orderer
- order Tx and create a block
- Peers validate each Tx in the block
- committing to the ledger.

Q6 Explain various types of nodes in hyperledger fabric.

ANS CLIENT : A user who sends a transaction invoice to the register and publishes transaction requirements to the scheduling server is known as a client.

PEER : Node that processes transactions & keeps track of data as well as a duplicate of the ledger.

ORDERER : Node that performs interaction services with a delivery guarantee, such as instantaneous or complete order dissemination.

Q6 Various nodes in hyperledger fabric?

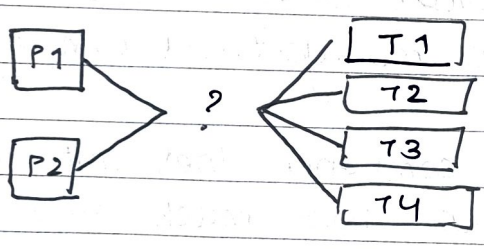
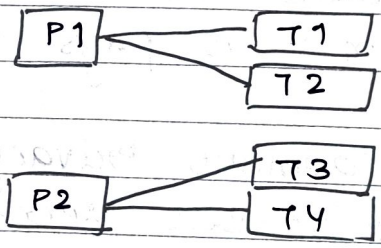
ANS COMMITTING PEER : Maintains ledger and state. Commits transactions. May hold smart contract / chaincode

ENDORSING - PEER : Specialized committing peer that receives a transaction proposal for endorsement, responds granting or denying endorsement. Must hold smart contract.

ORDERING NODE : Approves the inclusion of transaction blocks into the ledger and communicates with committing and endorsing peer nodes. Does not hold smart contract or ledger.

Q8 Differentiate anonymity and pseudonymity with examples

ANS

ANONYMITY	PSEUDONYMITY
• It means that the identity of a person is unknown.	• Pseudonymity, is a much weaker form. It means that a person's identity is unknown.
• It is not possible to track the actions of anyone.	• It is possible to assign actions to some person.
• 	• 
• E.g. Zcash	• E.g. Bitcoin & Ethereum.

Q9 Explain need for privacy in blockchain with e.g?

ANS Data privacy, sometimes referred to as information privacy, deals with proper handling of sensitive data including personal data. Data privacy has regulated the manner in which personal data is collected, processed & stored.

DATA PRIVACY IMPORTANCE:

Data is the most important asset in the business. We live in an era where companies find value in collecting and sharing data.

* The business has to meet legal responsibilities about the collection, storage, and process of personal data.

EXAMPLES:

1. Supply chain privacy: car company (Hyundai) does not want to reveal secret about how much it pays to tyre manufacturer company (Apollo)

2. Payment - Privacy: A company does not want to reveal secret about how much they pay to the employees.

3. Privacy for rent, privacy for donations, privacy for purchases.

Q.10 What is Zcash? What are the various transactions supported in Zcash

ANS
- Zcash is a cryptocurrency that offers anonymity and privacy. All the information transmitted between two parties using zcash is encrypted & secure.
- Appealed in 2016. Bitcoin was forked into Zcash. Initially was called zerocoin protocol then zerocash system and then Zcash.
- It verifies ownership of coins and transactions more anonymously than bitcoin, thus providing more security for users.
- Shielded Zcash ensures transactions remain confidential while allowing people to selectively share address and transaction information for auditing or regulatory compliance.
- zcash addresses are either private (z-address) or transparent (t-addresses).

TRANSACTION TYPES:

1) Private [z to z]
2) Deshielding [z to t]
3) Shielding [t to z]
4) Public [t to t]

Q11 Discuss core features and capabilities in Zcash?

ANS 1) Low-fee transactions : Fast transactions @ 0.0001 Zcash

2) Supported on large number of top wallets

3) Address and transaction privacy.

4) Encrypted memos : sent relevent info encrypted.

5) Viewing keys : with keys, owner has option to show incoming transactions & memo.

6) Payment disclosure : Receiver can disclose all transaction details except sender's address.

7) Transaction expiration : A transaction is expired if its not mined in 50 minutes or 40 blocks.

8) Multisignature transaction : Transaction may require 2 or more signs. These are transpeiant only.

Q12 Explain key terms in "zero-knowledge succint non-interactive argument of knowledge"

ANS
- zero knowledge allows one party to prove to another that a statement is true, without revealing any additional info beyond the validity of the statement itself. For eg: Given hash of a random no, the prover can convince the verifier that there exits a number with this hash value without revealing the number.

- Succint zero-knowledge proofs can be verified within a few milliseconds with short proof lengths even for large statements.

Q13 How Zk-snarks are constructed in Zcash?

ANS A zero knowledge proof is a cryptographic protocol that allows for information to be accurately verified without having to expose the underlying information itself to the entity doing the verifying.

Zcash uses zero-knowledge proofs. Zcash developers built their own technology called zk-snarks allowing users to opt for privacy while transacting with the crypto.

↳ address types : 'z' and 't'

↳ transaction types : - Private - Public
- Shielding - Deshielding

Q14 Explain attacks on blockchain

i) 51% attack

This attack is possible when a miner or a group of miners controls 51% or more of the mining power of the blockchain network.

Higher possibility in smaller networks. Once a group has majority control over transactions on a blockchain network, it can prevent specific transactions or even reverse old transactions.

ii) Eclipse attack

A node will depend upon "n" number of nodes selected using peer strategy selection to have its view of the distributed ledger. But if an attacker can manage to make the node to choose all the "n" number of nodes from its malicious nodes alone, then he can eclipse the original ledger's view and present his own manipulated ledger to the node.

iii) Sybil Attack

While the eclipse attack is about eclipsing a user's view of the true ledger, the sybil attack targets the whole network. In a sybil attack, an attacker will flood the network with large number of nodes with pseudonymous identity and try to influence the network. These nodes, although

appearing like unrelated individuals, are operated by a single person at the back. In this case, the objective is not to target one user, but a number of nodes or network as whole, and generate a fork in the ledger if possible, allowing the attacker to make double spending and other attacks.

iv) Timejack attack.

Nodes in certain blockchain networks like Bitcoin depend on internal timing derived from median time reported by its peer nodes. The first step to this attack can be an eclipse attack on the target node. Once this attack is complete on a target node, then the target node will not accept blocks from the actual network as the timestamp of the blocks will not be in line with its timestamp. This provides an opportunity for the attacker to be double spending or do transactions with the targeted node as these transactions can't be submitted to the actual blockchain network.

v) Selfish mining attack

Many blockchains consider the longest chain to be the true latest version of the ledger. So a selfish miner can try to keep building blocks in ~~stelth~~ stealth mode on top of the existing chain, and when he can build a lead of greater than two blocks or more than the current chain in the network, he can publish his private fork, which will be accepted as a

new truth as it is the longest chain. He can do transactions in the public network just before publishing his longer stealth chain to reverse the transaction he just did.

vi) Finney attack

If you can mine a block with one of your transactions in it and keep it in stealth, there is an opportunity for you to double spend the money. If a merchant accepts the unconfirmed transaction, you can transfer him the earlier transacted currency. Next you publish the earlier mined block, which was kept in stealth, before your new transaction is confirmed on network.

vii) Race attack.

Minor variant of the finney attack. The difference is that the attacker need not pre-mine the block with its transaction, which he intends to double spend. During the attack, the attacker submits an unconfirmed transaction to a merchant and simultaneously does another transaction which he broadcasts to the network. This would give the merchant an illusion that his transaction is the first, but that is never submitted to the blockchain network by the attacker.

Q15 List some general measures to prevent these attacks?

ANS
- Improve mining pool monitoring
- Make certain that the hash rate is higher.
- Avoid POW consensus to avoid 51% attack.
- Monitor other node's behavior and check for the nodes that are only forwarding blocks from one user.
- smart contracts need to be thoroughly vetted for any bugs before implementation
- use secure routing protocols to avoid routing attacks.

Q16 Role of quantum computing in crypto ecosystem?

ANS
- Quantum computers are powerful machines that can solve complex equations much more quickly than regular computer.
- Qubits can hold 0, 1, and both states.
- Experts say 15 years away.
- We should be ready with safe tech like quantum resistant ledger (QSL)
- Bitcoin's SHA-256 is safe
- If more than one miner has QC, we are safe

JAG

Q.19 Explain key ingredients of DeFi

ANS
- Decentralized Finance [DeFi] is an emerging finance technology that challenges the current centralized banking system.
- DeFi eliminates the fees that banks and other financial companies charge for using their services and promotes the use of P2P transactions

- Its OPEN, PSEDONYMOUS, FLEXIBLE, FAST

Components of DeFi Ecosystem
→ open ledger protocols
→ stablecoins
→ Decentralized Exchange - Platforms
→ Platforms for managing Insurance Investment.

Advantages:
→ No permissions required
→ No dependency on banks
→ Improved open access with trust
→ Flexible earning opportunities
→ More opportunities for Innovation
→ Customers are in control.

NOT IN TT QUESTIONS.

UNIT 1

(1) Why Nakamoto came up with Blockchain based currency.

ANS Satoshi explicity said that the reason for creating this digital cash system is to remove the third party intermediaries that are traditionally required to conduct digital monetary transfers.

Third party incur significant costs to conduct these services which are passed on to the end user. costs include :-

- Recovering back office expenses
- Take appropriate security measures
- Accounting for fraudulent activity (Refunds)

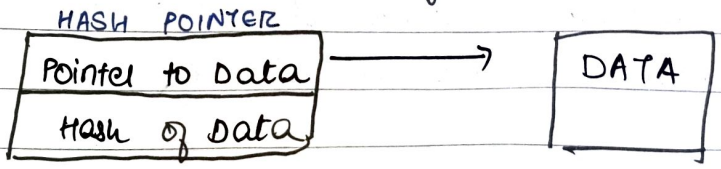
⇒ Another point mentioned by Nakamoto is that the root problem with conventional currency is that it requires trust in banks to hold money and transfer accordingly but history has shown banks cant be trusted.

(2) Hash Pointers

ANS Data Structure comprised of 2 parts :-

- Pointer to where some information is stored
- Cryptographic hash of that system.

The pointer can be used to get the information and the hash can be used to verify that information hasn't been changed.



*Blockchain & Merkle tree use hash pointers

(3) Digital cash

ANS Electronic cash is a digital currency technique from which transactions can be achieved anywhere through the internet.

Easier form of ~~buy~~ payment based on principles of blockchain technology among the P2P network.

All transactions are stored.

Features : — Decentralized
— Transperant

Advantages : — Higher flexibility and ability
— High security
— Time Efficient
— No hard copy needed.

Disadvantages : — cyber attacks
— Tech infrastructure needed
— Network issues.

(4) Atomic Broadcast

ANS In fault-tolerant distributed computing, an atomic broadcast is a broadcast where all correct processes in a system of multiple processes receive the same set of messages in same order.

Called atomic because either all receive in same order or all get aborted.

PROPERTIES:

- If one participant broadcasts, all will receive it.
- If one receives, all will receive
- one message is received only once
- sequence should be same.

(;

classmate
Date
Page

UNIT 2

2.1 Hash functions

ANS A hash function is a mathematical function that takes an input string of any length and converts it into a fixed-length output string called hash value.

PROPERTIES :

- Collision Resistant : 2 messages cant have same hash value
- Preimage Resistance : cant find message from hash
- Second preimage resistance : Given m1, can't find m2 having same hash

Uses of hash functions in Blockchain :

- Merkle Tree
- Digital signatures
- Pow consensus
- Chain of blocks

2.2 Puzzle Friendly hash

ANS Even if you have majority of input value (200 out of 256 bits), and ~~ba~~ output of hash function, you still can't get the tiny part of input value (56 bits) in a feasible time

2.3 Verifiable random function

ANS A VRF is a public-key pseudorandom function that provides proofs that its outputs were calculated correctly.

Owner uses secret key & input to compute the output as well as the proof.

Everyone can use public key to check if calculations are correct but can't see input value.

2.4 Bitcoin Scripting Language

ANS
- Simple programming language used to interact with Bitcoin software
- Stack - based. LIFO
- Written in Go
- Script gives instructions to Bitcoin - software on how coins in a UTXO (unspent Transaction output) can be spent.
- Postfix notation
- Turing incomplete. No loops
- Has 186 opcodes to conduct operations

UNIT 3

3.1 Turing Completeness of Smart Contract languages

ANS
- A language is said to be turing complete if it can be used to simulate a turing machine, which means that an appropriately designed program can solve any program that a universal turing machine (UTM) can solve.

- Basically refers to the idea that given infinite time, a program in one language can be written (maybe inefficiently) in another.
- Program must be free from restrictions such as halting & infinite loops

- Blockchain used to be but now isn't.
- Ethereum is turing complete.

⇒ No benefits in blockchain for tuling completeness
⇒ some turing incomplete are more secure.

3.2 Bitcoin Scripting vs Ethereum Smart Contract

ANS

BITCOIN SCRIPTING	ETHEREUM SMART CONTRACT
• Turing Incomplete	• Turing complete
• No loops	• Has loops
• Doesn't have a state. All required info needed is contained in the locking and unlocking scripts.	• Has a contract storage that can influence behaviour of the program.
• Programs are part of transaction. If transaction is pruned, program is gone.	• Smart contract code is persistant in state & is gone only if its self-distructed via opcode

UNIT 4

4.1 Hyperledger Fabric on Microsoft Azure

ANS

- Hyperledger Fabric on Azure Kubernetes Service (AKS)
- Template has various configurable params for production-grade deployment of Hyperledger Fabric network
- Supports Fabric CA
- Supports levelDB & CouchDB
- Scalable

UNIT 5

5.1 Advent of Algorand

ANS

- Algorand is a POS BC cryptocurrency protocol
- Negligible energy consumption per transaction and is carbon-negetive.
- Intended to solve "blockchain trilemma" — scalability, security, decentralization
- 3 steps - propose, soft vote & certify vote
- works on everyday workstations.
- Participants of a group are regularly shuffled.
- Ethereum alternative for DApps due to rising gas-fees

5.2 Sharding based consensus Algorithms.

ANS
- Sharding involves splitting a blockchain into smaller, more agile blockchains so that it can handle more transactions.
- Ethereum plans to shift to shading based consensus in 2023.
- Scalability.

Ethereum 2.0
- One central "Beacon chain"
- Multiple shards
- 1% attack vulnerability
- Nodes in shards will be switched randomly

UNIT 6

6.1 Applications in Healthcare

ANS
- Patient-centric Electronic health records
- Smart contracts for insurance settlements
- Supply chain transparency
- Medical staff credential validation
- Protection of healthcare data
- Integration with wearable IoT devices

6.2 Application in Automotive

ANS
- Secure payment
- Supply Chain Management
- Sensor data management
- Insurance claims
- Eliminate counterfeit parts
- Leasing & Financing
- Pay tolls

Q.3 Applications in Government

ANS
- Record keeping
- Government smart contracts
- Foreign Aid money delivery
- Dubai's judicial system
- Law enforcement
- Taxation system
- Supply chain
- Voting
- Pension Administration

Q.4 Applications in Insurance

ANS
- Reinsurance practices
- Claims handling
- Record keeping
- Smart contract triggers
- New type of insurance [code Insurance]

Q.5 Applications in Media & Entertainment

ANS
- Streamline royalty payments
- Ads management & tracking
- Micro-payments according to usage
- P2P content distribution

6.6 Estonian Blockchain

ANS
- Even before 2008, Estonia was testing with BC tech with the name "hash-linked time stamping".
- Since 2012, BC is in production use in Estonia to protect national data, e-services and smart devices both in public & private sector.

- Estonian Information systems Authority (RIA) guarantees access to state Agencies via x-road infrastructure
- Selected state registries backed by BC tech are:-
  - Healthcare registry
  - Property
  - succession
  - state Gazette.
  - Digital court system
  - surveillance / tracking system
  - official state Announcements

* Estonia makes use of KSI Blockchain by Guardtime.

- KSI have published the blockchain in physical media like the Financial Times newspaper.
- If someone wants to manipulate KSI Blockchain, not only do they have to deal with "digital defence dust" in the electronic form but also replace 1000's of newspapers in world's libraries.

- Data doesn't leave the system. only has is stored on the BC making it light & scalable.
- Taxes can be filed in 5 mins
- E-voting is done

E-ID: Electronic Identity Document
X-Road: open-source data exchange layer.
KSI Blockchain: Timestamp system used to preserve doc integrity.

6.7 Distributed Ledger Technology

* GOVERNANCE AND REGULATION

→ Permissioned DLT networks for corporates require the creation of rules & governance over who can do what.
→ Building a viable DLT networks for a community of cooperating but competitive orgs requires a common set of standards & practices.
→ Important to establish who is accountable in case of any crashes or failures.
→ New business workflows are emerging that enable transactional exchanges of assets and payments to be recorded, linked and traced through their entire lifecycle.
→ Info about an asset, its ownership, payments and transfers are recorded in a shared distributed ledger
→ DLT has eliminated traditional "data silos" of each party.
→ Purpose of DLT is to buid a system once, share data across a community with tremendous efficiencies and eliminate different schemes, constructs & individual interpretation of rules.

→ A DLT governance operating model should include administrative tools to react to idiosyncratic events, transparently & accountably modify state of ledger in case of errors.

* Key Ingredients of DeFi

ANS
- Emerging Finance technology that challenges the current centralized banking system.
- DeFi eliminates the fees that banks and other financial companies charge for using their services and promotes the use of P2P transactions.
- open, Pseudonymous, Flexible, Fast.

INGREDIENTS

* LENDING AND BORROWING : With DeFi lending, investors deposit crypto through a decentralized application, and someone can then borrow the crypto through the network, paying interest on the loan.

* STABLE COINS : Crypto that has its value pegged to another asset like fiat money, exchange-traded commodity, etc.

* DECENTRALIZED EXCHANGES : Connect buyers and sellers and allows users to make transactions via P2P network.

* DERIVATIVES : Contracts whose values are derived from the performance of an underlying financial asset

* CRYPTO MARGIN TRADING : Utilizing borrowed funds to increase a position in a certain asset.

* DEFI INSURANCE : Ensures guarantees of compensation in exchange for payment of a premium.

* Key terms in ZK SNARKS

ANS Zero-Knowledge Succint Non-Interactive Argument of Knowledge

Zero-knowledge allows one party to prove to another that a statement is true without revealing any additional info beyond its validity.

Succint means proofs should be verified within a few milliseconds with short proof lengths even for large statements

Non-Interactive means the proof consists of a single message sent from prover to verifier.

Argument-of-knowledge means the prover can convince the verifier not only that the number exists but they in fact know such a number without revealing any information about the number.

* Zk snarks working :

At high-level, Zk-SNARKs work by first turning what you want to prove into an equivalent form about knowing a solution to some algebraic equations.

COMPUTATION ⟶ Arithmatic Circuit ⟶ R1CS ⟶ QAP ⟶ ZkSNARK

The first step in turning our transaction validity function into a mathematical representation is to break down the logical steps into the smallest possible operations, creating an "arithmatic circuit".

Next step is to build a Rank-1 Constraint System (R1CS) to check the values are travelling correctly

To "bundle" all these constraints into one", this method uses a representation of the circuit called a Quadratic Arithmatic Program.

Zk-Snark is constructed.