10/1/25

ASSIGNMENT 1

Unit - 1 Introduction to Blockchain

Q.1 Explain Blockchain in detail.

→ A Blockchain is a decentralized, distributed digital ledger that records transactions across multiple computers in such a way that the data cannot be altered later without the consensus of the network. It is the underlying technology for the cryptocurrencies, smart contracts, healthcare, finance, voting systems and also used for secure, transparent and immutable record-keeping in industries.

- Key Components of Blockchain :-

i) Block : A block is a container of data that consists of data (actual transmission), hash (unique identifier) and previous block's hash.

ii) Ledger : A digital record that keeps track of all the transactions. It is distributed across the network and is updated simultaneously on all participating nodes.

iii) Decentralization : No single central authority controls the blockchain. Instead, it operates on a peer-to-peer network.

iv) Consensus Mechanisms : Algorithms used to validate transactions and maintain

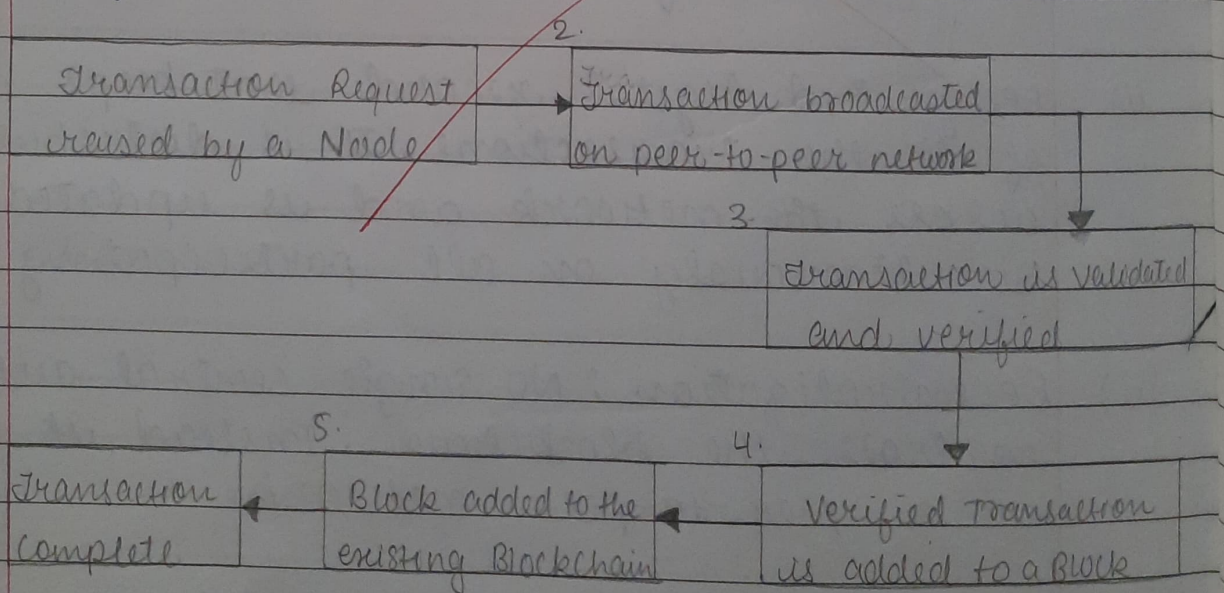
agreement across the network. Examples include Proof of Work (PoW) and Proof of Stake (PoS).

—4 There are four types of blockchain like ~~are~~ public, private, consortium and hybrid.

Advantages are enhanced security, greater transparency, faster transactions, and improved traceability. Disadvantages are scalability, energy consumption, complexity and initial setup cost.

Q.2 With diagram explain blockchain transactional flow.

—4 A Blockchain transaction flow represents the process by which a transaction is initiated, verified and recorded on the blockchain.



i) Transaction Initiation : A user initiates a transaction using their private key (a cryptographic signature), including details like sender's & receiver's address and amount. The transaction is then broadcast to the network.

ii) Transaction Validation : Nodes (computers) verify the transactions for authenticity by checking for sufficient funds in sender's account and valid cryptographic signatures.

iii) Transaction Pool : Verified transactions are added to the transaction pool (mempool) awaiting inclusion in a block.

iv) Block Creation (Mining/Validation) : Miners (PoW) or validators (PoS) select transactions from the pool to create a new block. In PoW, miners solve cryptographic puzzles, while PoS validators are chosen based on their stake.

v) Consensus Mechanism : The newly created block is broadcast to the network and nodes agree on its validity using the consensus ~~mechanism~~ algorithm (eg. PoW or PoS)

vi) Block Addition to the Blockchain : Once validated, the block is added to the blockchain, linking ~~to~~ it to the previous block through a cryptographic hash.

(vii) Transaction Confirmation: The transaction is confirmed and becomes part of the immutable blockchain, visible through blockchain explorers (users can track).

Q.3 — 4 Explain different types of Blockchain.

Blockchain can be categorized into four main types based on access, governance and use-cases.

1. Public Blockchain

A decentralized blockchain open to anyone in the world. Any individual can participate in the network by reading, writing or validating transactions. It is fully decentralized, transparent and secure (due to PoW / PoS).

While they provide high transparency, trustlessness and censorship-resistance, they are often slower and consume more energy, especially in PoW.

Use cases are cryptocurrencies, decentralized applications (DApps).

2. Private Blockchain

A blockchain that is permissioned, where access is restricted to specific individuals or organizations. It is controlled by a single entity, it offers faster transactions and greater efficiency due to

fewer nodes.

While they provide privacy and confidentiality, they lack also higher efficiency & faster transaction times but they lack decentralization and limiting transparency.

Use cases are Record Management within organizations, Internal enterprise solutions (eg: supply chain management, finance).

3. Hybrid Blockchain

A blockchain that combines features of both public and private blockchains, offering flexibility in what data is made public and what is kept private. It is partially decentralized and sensitive information is kept private, while other data remains public.

They are highly flexible with greater security (selective transparency) and enables controlled access to sensitive data but can be complex to implement and may not fully achieve benefits of decentralizations.

Use cases are HealthCare, Real Estate (private property ownership records with public transaction history)

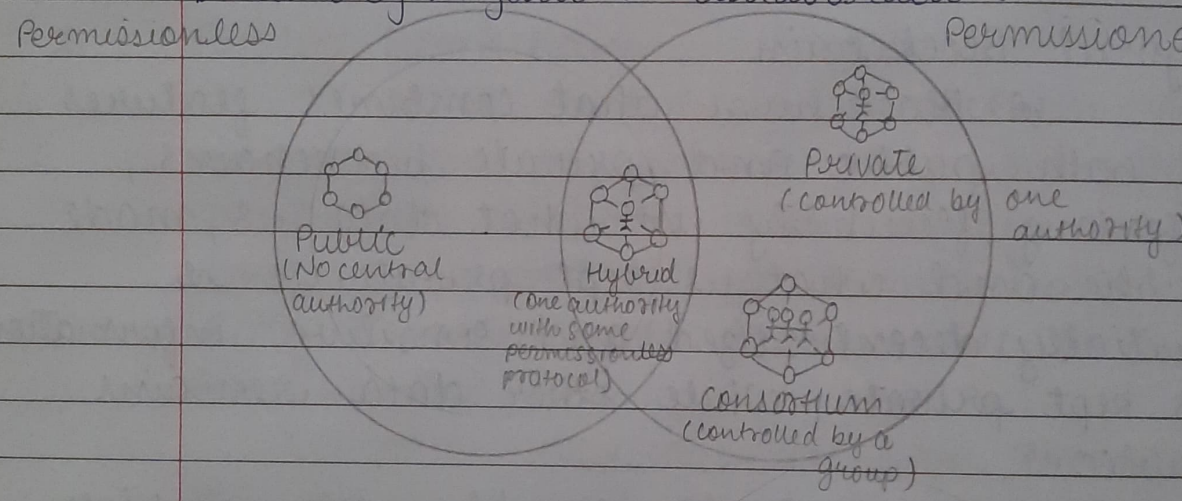
4. Consortium Blockchain

A semi-decentralized blockchain governed by a group of organizations instead of a single

entity. Access is restricted but shared among a trusted participants, offering collaborative control and decision-making. Also combines element of public and private blockchains

They offer higher security and scalability than public blockchains but have complex governance structure and requires trust among consortium members.

Use cases are Banking & Finance, Multi-organization collaboration.



Q.4 — Explain Merkle Trees with diagram.

A Merkle Tree (Binary Hash Tree) is a data structure used to efficiently and securely verify the integrity and consistency of large dataset. It organizes transactions in a hierarchical structure ~~where~~ where each node contains a cryptographic hash of its child nodes.

Structure of a Merkel Tree :-

(i) leaf Nodes: Represent individual transactions

hashes. Each transaction is hashed (eg. using SHA-256).

(ii) Non-leaf Nodes : Contain hashes derived from their child nodes. Each parent node hash is created by concatenating the hashes of its two child nodes and hashing the result.

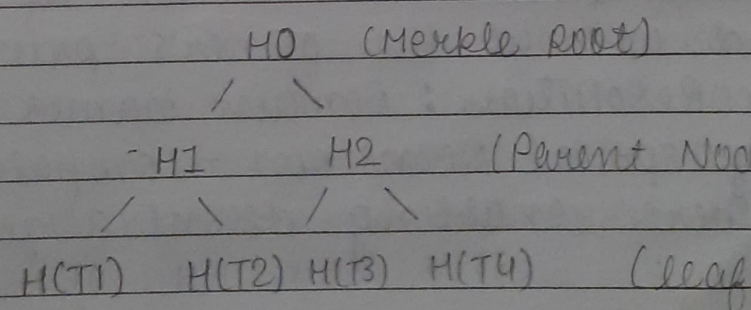
(iii) Root Node (Merkle Root) : The single hash at the top of the tree. It uniquely represents all the transactions in the tree.

-4 Working of Merkle Tree :-

i) Transaction Hashing : All transactions are hashed individually to form the leaf nodes.

ii) Pairwise Hashing : Hashes of two child nodes are combined and hashed to form their parent node.

iii) Repeat Until Root : This process continues iteratively until a single hash, the Merkle Root, is generated.



Q.5 Explain Namecoin.

-4 Namecoin, launched in 2011, is a decentralized

open-source platform built on Bitcoin's ~~database~~ code. It is primarily used to manage a censorship-resistant, decentralized DNS for websites, offering an alternative to traditional, centralized DNS.

Key features include secure, immutable data storage and the use of the .bit top-level domain. It ensures censorship resistance, preventing domain seizures by centralized entities and allowing users to prove ownership without relying on central authorities.

- Working of a Namecoin :-

i) Domain Registration : Users pay Namecoin to register a domain name (example.bit)

ii) Transaction on Blockchain : The domain registration is recorded as a transaction on the Namecoin blockchain.

iii) Ownership of domain : It is linked to the user's wallet and the blockchain ensures it cannot be altered without the owner's private key.

iv) Name Resolution : Domain names are resolved using special Namecoin-compatible DNS resolvers, enabling decentralized browsing.

- Use cases are Censorship-Resistant website, secure file verification, decentralized identity.

Q.6 Explain Ripple.

—↓ Ripple is a blockchain-based digital payment protocol and cryptocurrency (XRP) designed for fast, low-cost and secure cross-border transactions. Founded in 2012, it aims to improve global payments for banks, financial institutions and payment providers.

Key features include real-time settlement of transactions in 3-5 seconds, low transaction fees (often under $0.01) and scalability, processing up to 1500 transactions per second. XRP helps facilitate instant currency conversions, reducing the need for pre-funded accounts across borders.

- Working of Ripple :-

i) Transaction Initiation : A user initiates a payment on the Ripple network.

ii) RippleNet : The payment is processed on RippleNet, which connects a network of financial institutions and payment providers.

iii) XRP as Bridge Currency : If the sender & receiver use different currencies, XRP can be used as a bridge to facilitate the exchange, converting from one currency to another.

iv) Settlement : The transaction is settled in seconds and funds are transferred to recipient.

v) Consensus Mechanism : Ripple uses a unique consensus algorithm where independent

validators agree on the transaction's validity, ensuring fast and reliable processing.

-4 Use cases are Cross-Border Payments, liquidity Management, Payment Gateways, smart contracts.

Q.7 -4 Explain Ethereum.

Ethereum is an open-source, decentralized blockchain platform that enables developers to build and deploy smart contracts and decentralized applications (DApps). Launched in 2015 by ~~Vat~~ Vitalik Buterin, Ethereum is the second most popular blockchain after Bitcoin.

Key features ~~are~~ include smart contracts, which are self-executing agreements coded directly into the blockchain. Ethereum uses the Ethereum Virtual Machine (EVM) to execute code in a secure, platform-independent environment. The network is decentralized, maintained by thousands of nodes for security and transparency. Also, it requires gas, a fee to compensate miners or validators.

- Working of Ethereum :-

i) Transaction Creation : A user sends a transaction or initiates a smart contract on Ethereum.

ii) Gas Fees : To execute a transaction or smart contract, users need to pay a small fee in ETH, called "gas".

iii) Validation : Validators (under POS) check if the transaction is legitimate and include it in a block.

iv) Block Creation : Validated transactions are grouped into blocks and added to the blockchain.

v) Execution : Smart contracts are triggered and executed based on predefined conditions.

→ Use cases are Decentralized Finance (DeFi), Non-Fungible Tokens (NFTs), Gaming & Entertainment, supply chain management.

→ Ethereum is undergoing ~~to~~ a significant upgrade called Ethereum 2.0 (Eth2) to improve scalability, security and sustainability.

Q.8 Differentiate between Bitcoin and Ethereum.

→

Bitcoin	Ethereum
> Primarily a digital currencys for peer-to-peer transactions	A decentralized platform for smart contracts and dApps.
> Launched on January 2009	Launched on July 2015
> Creator is Satoshi Nakamoto	Creator is Vitalik Buterin and Others.

> Fixed supply of 21 million BTC	No fixed supply; ETH issuance rate controlled by network protocol.
> Bitcoin network has transaction fees based on demand.	Ethereum uses "gas" fees, which are variable based on computational complexity.
> No formal governance structure	Ethereum improvement Proposals (EIPs) for protocol changes.
> Miners validate transactions using PoW	Validators (under PoS) validate transactions and block.

Q.9 Explain Blockchain implementations for Bitcoin.

→ The Bitcoin Blockchain is the first and most well-known blockchain implementation. It serves as the public ledger that records all Bitcoin transactions in a chain of blocks. It is decentralized, secure and transparent peer-to-peer transactions.

- Bitcoin Blockchain Process :-

i) Transaction Initiation : A user initiates a

Bitcoin transaction, specifying the recipient's address and the amount of Bitcoin to transfer.

iii) Broadcasting to Network: The transaction is broadcast to the Bitcoin network, where nodes pick it up for validation.

iii) Transaction Validation: Nodes verify the sender has sufficient funds and that the transaction structure is correct.

iv) Mining / Proof of Work: Miners compete to add the next block of the blockchain by solving a complex mathematical puzzle (PoW) that requires significant computational resources. The first to solve it gets to add the validated block to the blockchain.

v) Block Addition: Once a miner solves the puzzle, the block is added to the blockchain, linking it to the previous block. (with a reference)

vi) Confirmation: The transaction is confirmed as the block is added, with subsequent blocks providing additional ~~info~~ confirmation.

Q.10 Describe Blockchain Gambling and Betting.

—↓

Blockchain gambling and betting refer to the use of blockchain technology to enhance transparency, security and fairness in online

gambling platforms. By leveraging blockchain's decentralized and immutable nature, gambling platforms can offer provably fair games, secure transactions and a more transparent betting environment.

- Working of Blockchain Gambling :-

i) Decentralized Platforms : Gambling platforms are built on blockchain, removing the need for a central authority.

ii) Cryptocurrency Betting : Players deposit cryptocurrencies into a smart contract to place bets.

iii) Smart contracts for Betting : Smart contracts automatically execute bets, ensuring rules and payouts are followed.

iv) Provably Fair Mechanism : Games use blockchain for provably fair results, allowing players to verify outcomes.

v) Transaction Verification : Every bet and outcome is recorded on the blockchain for easy verification.

—4 Use cases are online casinos, sports betting, lottery systems, eSports Betting, Tokenized Gambling.

Q.11 Describe any one of the Blockchain collaborative implementations :

1. Hyperledger

→ Hyperledger is an open-source project under the linux foundation, designed to create enterprise-grade, permissioned blockchain frameworks and tools for business application. It aims to drive cross-industry collaboration and innovation by offering flexible solutions for various industries.

Key features include permissioned blockchains, where network access is controlled for privacy and security. Its modular architecture allows for customized blockchain solutions tailored to specific business needs. Focused on industries like finance, supply chain and healthcare. It also enables smart contracts to automate business processes across organizations.

- Hyperledger Projects :-

i) Hyperledger Fabric : A modular blockchain for smart contracts, private channels and flexible consensus.

ii) Hyperledger Sawtooth : A scalable framework using Proof of Elapsed Time (PoET) for consensus.

iii) Hyperledger Iroha : Simplifies building permissioned blockchains with an easy-to-use system.

iv) Hyperledger Indy : Focuses on decentralized identity management and secure data sharing.

2. Corda

-> Corda is a distributed ledger platform developed by R3, a consortium of over 200 financial institutions, aimed at enabling secure and efficient transactions between regulated entities. It focuses on privacy and direct transactions between parties.

It ensures privacy by restricting transaction visibility to involved parties and supports smart contracts for automating transactions. It integrates with legacy systems and uses a notary service for transaction validation, rather than traditional blocks and chains.

- Architecture of Corda :-

i) Corda Nodes : Participants (banks, businesses) run nodes with their own ledger storing relevant transactions.

ii) Corda Contract : Defines the rules and conditions for executing transactions.

iii) Corda States : Represents data at a specific point in time.

iv) Corda Notary Service : Validates transactions, preventing double-spending and ensuring consistency with system rules.

-> Use cases are Supply chain, trade finance, Finance & Banking.

Q.12 Explain Blockchain in the Financial Technology Space

-> Blockchain technology is revolutionizing the Financial Technology (FinTech) industry by offering secure, transparent, decentralized and efficient solutions to traditional financial systems. In the FinTech Space, blockchain enables faster, cheaper, and more secure financial transactions including payments, lending, insurances and trading.

- How Blockchain Transforms FinTech :-

i) Security and Transparency : Blockchain creates immutable transaction records, enhancing fraud prevention and transparency, with everyone having an auditable copy.

ii) Decentralization : It eliminates intermediaries, reducing costs and improving efficiency. Peer-to-peer transactions enable faster transfers and better financial inclusion

iii) Reduced Transaction Cost : Blockchain lowers transaction fees, especially for cross-border payments, by removing intermediaries.

iv) Faster Transactions : Real-time transactions are enabled, speeding up cross-border payments compared to traditional systems.

v) Smart Contract and Automation : Smart contract automate financial agreements, reducing reliance on intermediaries, speeding up execution and minimizing errors.

—ν Use cases are Cross Border Payments & Remittances, Decentralized Finance (DeFi), Digital asset Tokenization, Insurance, Digital identity & KYC

Q.13 Describe Blockchain and Real Estate

—ν Blockchain technology is transforming the real estate industry by providing secure, transparent and efficient solutions for managing property transactions, ownership records and related processes.

• working of Blockchain in Real Estate :-

i) Property Ownership Records : It stores secure, immutable ownership records, reducing fraud and speeding up verification.

ii) Smart contracts : Automates property transfers and escrow services, cutting out intermediaries and reducing costs.

iii) Tokenization : Enables fractional ownership of real estate, allowing smaller investments in high-value properties.

iv) CrowdFunding : Decentralized platforms let investors pool funds, with profits distributed automatically via smart contracts.

v) Supply Chain Transparency : Tracks all stages of the real estate process, ensuring transparency and reducing fraud in construction.

-v Use cases are Property Title & Ownership Tracking, real estate tokenization, smart contracts in transactions, real estate crowdfunding.

Q.14 Describe Blockchain and Cloud Computing.

-v Blockchain in cloud computing combines the decentralized nature of blockchain with the scalability and flexibility of cloud services to enhance security, transparency and efficiency. By integrating it, cloud systems can securely store data, ensure trust between parties and automate processes through smart contracts.

- Working of Blockchain in Cloud Computing :-

i) Enhanced Security : It encrypts and timestamps cloud data, ensuring immutability and protection.

ii) Decentralized ~~ation~~ ed Storage : It enables secure, distributed cloud storage across multiple nodes.

iii) Improved Data Integrity : It maintains audit trails, ensuring only authorized changes are made, critical for regulated industries.

iv) Transparency and Auditability : It provides real-time transaction tracking, offering transparent, auditable records for cloud services.

v) Enhanced Security : Cryptographic ~~signatures~~ techniques like zero-knowledge proofs ensure data privacy while validating information.

—4 Use cases are Data Sharing & Marketplace, Supply Chain & logistics, decentralized cloud Storage, Healthcare Data Management.

Q.15 Describe Decentralized Autonomous Organization.

—4 A Decentralized Autonomous Organization (DAO) is a blockchain-based entity governed by smart contracts, operating without centralized control or intermediaries. DAOs are decentralized, with decisions made by a distributed network of participants rather than a central authority.

Key features include decentralized governance, where members vote using tokens representing their influence. They are autonomous, with operations handled by smart contracts and open to participation, allowing anyone to join by acquiring tokens, making them inclusive and decentralized.

- Working of DAOs :-

i) Smart Contracts and Governance : DAOs uses smart contracts on public blockchains (Ethereum), to define rules and automate actions

ii) Token-Based Voting : Members vote using governance tokens; more tokens = more voting power.

iii) Transparency and ~~Auditability~~ Accountability : All transactions are recorded on the blockchain, ensuring

Transparency and trust.

iii) Autonomous Execution : Once a proposal is approved, smart contracts automatically execute the decision without intermediaries.

→ There are various types of DAOs like Protocol, Investment, Social, Charity and service DAOs.

→ Use cases are MakerDAO, Uniswap, MetaCartel Ventures, The DAO (2016).

Done