Name- Piyusha Rajendra Supe
Roll No- 23CO315 [BE- Computer B]

Blockchain Technology Assignment

Attempt Q1 or Q2.

Q1] (a). Discuss the following consensus algorithms used in Blockchain
i) Proof of work.
ii) Proof of activity.
iii) Proof of Burn.
iv) Proof of Stake.

→ i) Proof of work (PoW) -

- PoW requires miners to solve complex cryptographic puzzles (hashing problems). The first miner to solve the puzzle gets the right to add a new block to the blockchain.
- Miners compete to find a nonce that when hashed with the block data produces a hash below a target difficulty.
- The winning miner broadcasts the block and other nodes validate it.

ii) Proof of Activity (PoA) -

- A hybrid of PoW and PoS, designed to combine the strengths of both.
- Mining starts similar to PoW where miners try to solve puzzles.
- Once a block is mined, a group of validators (chosen based on their stake) signs on block
- Only after enough validators sign, the block becomes part of chain.

(iii) Proof of Burn (PoB) -

In PoB, participants burn, destroy a portion of cryptocurrency by sending it to an unusable address. This destruction demonstrates long term commitment and grants the participant the right to mine or validate.

(iv) Proof of stake (PoS) -

Instead of using computational power like (PoW), PoS selects Validators based on the number of coins they 'stake' (lock up as collateral). The more coins staked, the higher the chance of being chosen to validate a block.

- Validators lock their coins in a stalking wallet.
- The algorithm pseudo randomly selects one validator to propose the next block.
- Other validators confirm the block.

Q1 b) Explain in detail - i) Bitcoin ii) Ethereum iii) Hyperledger.

i) Bitcoin -

- First decentralized cryptocurrency (2008, Satoshi Nakamoto)
- Uses proof of Work for consensus
- Based on UTXO model (Unspent Transaction Outputs)
- Miners solve puzzles, validate transactions, and add blocks.
- Supply capped at 21 million BTC with halving events.
- Strengths - secure, decentralized, censorship resistant.
- limitations - : slow (~10 min / block), energy, intensive, limited throughput.

ii) Ethereum -

- launched in 2015 (Vitalik Buterin).
- General purpose blockchain for smart contracts via Ethereum Virtual Machine.
- Uses account model (externally owned accounts + contract accounts.)
- Transactions require gas; fees adjust with demand (EIP)
- Moved from PoW to PoS in the Merge.
- Strengths - flexible, supports DeFi, NFTs, DAOs
- Limitations - high gas fees, scalability issues contact security risks.

iii) Hyperledger -

- open source blockchain project under Linux foundation.
- permission system (participants are known).
- Key framework - Hyperledger Fabric (modular, supports chainnode, channels, private data).
- No native cryptocurreny required.
- Strengths - privacy, scalability, customizable consensus
- Use cases - supply chain, trade finance, healthcare, identity.

Q1c) Concept of Bitcoin in Blockchain Technology.

→ • Bitcoin is the first and most popular cryptocurrency introduced by Satoshi Nakamoto in 2008.

- It is built on Blockchain Technology which is distributed, immutable and transperent ledger that records all transactions in a secure and verifiable way.
- Transactions are grouped into blocks and each block is linked to previous one, forming a chain.

- Consensus Mechanism - Bitcoin uses PoW where miners solve cryptographic puzzles. The winner adds a new block and earns block rewards plus transaction fees.
- UTXO Model - Balances are managed through unspent transactions outputs, ensuring accuracy and preventing double spending.
- Supply Cap - Only 21 million Bitcoins will ever exist; new bitcoins are issued through block rewards, halved approximately every four years (halving).
- Key features - decentralized no central authority.
  - Secure via cryptography and PoW
  - Transperent (public ledger)
  - Immutable (once recorded, transactions cannot be changed.

Attempt Q3 or Q4.

Q4 a) Compare and contrast coinbase and Binance -

→

	Coinbase	Binance.
1.	Founded in 2012, USA	1. Founded in 2017, China.
2.	Beginner friendly exchange.	2. Advanced global trading platform.
3.	Heavily regulated, strong compliance.	3. Faced regulatory issues. stronger outside US.
4.	Higher fees. (1.5%, spreads)	4. Low fees. (0.1%, discounts with BNB).

Coinbase	Binance.
5. Offers coinbase wallet (self custody + exchange).	5. Built in wallet + Trust wallet support.
6. Strong security (insurance, 2FA)	6. 2FA, SAFU fund, but past hacks.
7. Popular among retailers. esp. U.S.	7. Preferred by global and professional traders.
8. Supports 200+ tokens.	8. Supports 600 + coins including many altcoins.
9. Simple ~~by~~ buy/sell, staking, learning rewards	9. Spot margin, futures, staking, launchpad, NFTs.

Q4 b) Differentiate between Metamask and Coinbase wallet.

→

Metamask	Coinbase.
1. Non custodial crypto wallet and browser extension.	1. Non custodial crypto wallet (separate from Coinbase exchange account)
2. Developed by consensys (Ethereum focused)	2. Developed by Coinbase (integrated with coinbase ecosystem)

Metamask	Coinbase.
3. Primarily ethereum and EVM compatible blockchains (Polygon, BSC, Avalanche, etc)	3. Supports ethereum, EVM chains, and some other networks (also connects easily with coinbase exchange).
4. Browser extension + mobile app, (heavily used for DeFi and Web3 apps.	4. Mobile app + browser extension, user friendly integrates with coinbase.
5. Strong DApp browser integration, default choice for many DeFi users	5. Has DApp browser but more streamlined toward Coinbase services.
6. User controls private Keys (12- word seed phraase)	6. User contols private keys (12 - word recovery phase).
7. Popular among developers DeFi, NFT users, requires crypto knowledge	7. Gaining popularity due to ease of use.

Piyusha Supe
2360315.