Unit 3

CHAPTER 3

Blockchain Platforms and Consensus in Blockchain

University Prescribed Syllabus

Types of Blockchain Platforms: Public, Private and Consortium, Bitcoin, Ethereum, Hyperledger, IoTA, Corda, R3. Consensus in Blockchain: Consensus Approach, Consensus Elements, Consensus Algorithms, Proof of Work, Byzantine General problem, Proof of Stake, Proof of Elapsed Time, Proof of Activity, Proof of Burn.

3.1 TYPES OF BLOCKCHAIN PLATFORMS

GQ. Explain how public blockchains ensure the adherence of transaction and block-writing rules. **(6 Marks)**

GQ. Discuss the need for predefined mechanisms and rules to modify a public blockchain's protocols. **(6 Marks)**

GQ. Differentiate between a public/permissionless and a private/permissioned blockchain. **(4 Marks)**

GQ. List down advantages of a private/permissioned blockchain relative to a public/permissionless blockchain for enterprise usage. **(6 Marks)**

GQ. How Assest ownership use case can be implemented with private blockchain? **(6 Marks)**

GQ. Why hybrid blockchain is more suitable for medical application? **(6 Marks)**

GQ. What are the benefits of implementing banking applications with consortium approach? **(6 Marks)**

- Private and public blockchains are the two main types of blockchains. There are, however, a number of variants including Consortium and Hybrid blockchains.
- Let's first study what characteristics the various blockchain types have in common before going into the specifics of each type. A cluster of nodes operating on a peer-to-peer (P2P) network technology makes up every blockchain.
- Each node in a network maintains a copy of the shared ledger that is promptly updated. Each node has the ability to produce blocks, send or receive transactions, and verify transactions.

Now let's have a look in detail about the four types of blockchains that are possible.

3.1.1 Public Blockchain

GQ. Describe a public blockchain and mention its current applications. **(4 Marks)**

GQ. List down advantages and disadvantages of a public blockchain. **(4 Marks)**

- A distributed ledger system without constraints and permissions is known as a public blockchain. Anyone with internet connection may sign up on a blockchain platform to join the network as an authorised node and become a part of the blockchain.
- It is permitted for a node or user who is a member of the public blockchain to view recent and old data, confirm transactions or complete proof-of-work for an incoming block, and engage in mining.
- The mining and trading of cryptocurrencies is the most fundamental usage of public blockchains. As a result, Bitcoin and Litecoin blockchains are the most widely used public blockchains.

- If users adhere to security policies and procedures to the letter, public blockchains are generally secure. However, it is only risky when the participants don't really adhere to the security rules.

Example : Bitcoin, Ethereum, Litecoin

Advantages

(1) Public blockchains have the benefit of being fully independent of organisations; as long as there are computers still connecting to them, the public blockchain will continue to function even if the company that launched it goes out of business. Some blockchains incentivize users to devote computer power to securing the network by offering a reward."

(2) Public blockchains also offer the benefit of a transparent network. Public blockchains are generally safe as long as their users adhere strictly to security regulations and procedures.

Disadvantages

(1) The network may be slow, and companies cannot impose access or use restrictions. According to Godefroy, hackers may unilaterally change a public blockchain network if they control at least 51% of its computer power.

(2) Public blockchains also struggle with scalability. As more nodes join the network, it becomes slower.

Case studies

The mining and exchange of cryptocurrencies like Bitcoin is the most typical use case for public blockchains. It may also be used to electronically notary stamp affidavits and public documents of property ownership in order to create a permanent record with an auditable chain of custody.

For organisations that are based on transparency and trust, like social support networks or non-governmental organisations, this kind of blockchain is appropriate. Private enterprises will probably wish to stay away due to the network's open nature.

3.1.2 Private Blockchain

GQ. Describe a private blockchain and mention its current applications. **(4 Marks)**

GQ. List down advantages and disadvantages of a private/permissioned blockchain. **(4 Marks)**

- A private blockchain is an exclusive, permission-based blockchain that only functions in a closed network.
- Private blockchains are typically utilised inside of businesses or organisations where only a small group of people are allowed to participate in a blockchain network.
- The governing organisation controls the degree of security, authorizations, permissions, and accessibility.
- Therefore, private blockchains are used similarly to public blockchains but have a constrained and tiny network. Private blockchain networks are used for asset ownership, digital identity, supply chain management, voting, and other purposes.
- **Examples** of private blockchains are; Multichain and Hyperledger projects (Fabric, Sawtooth), Corda, etc.

Advantages

(1) Permission levels, security, authorizations, and accessibility are controlled by the governing organisation. For instance, the establishment of a private blockchain network allows an organisation to control which nodes may see, contribute, or modify data. It can also block third parties from accessing particular information.

(2) Public blockchains are more like the internet, whereas private blockchains are like the intranet.

(3) Private blockchains may execute transactions significantly more quickly than public blockchains because of their size restriction.

Disadvantages

(1) Private blockchains have drawbacks, including the contentious assertion that they aren't actual blockchains because decentralisation is the foundation of the technology. Since

centralised nodes decide what is genuine, it is also more challenging to fully create confidence in the information. Less security may also result from the small node count. The consensus process may be compromised if a few nodes act erratically.

(2) Furthermore, the source code from private blockchains is frequently closed-source and proprietary. It cannot be independently audited or verified by users, which may result in inferior security. On a private blockchain, there is no anonymity either.

Case studies

- Private blockchains are the best option when a blockchain has to be cryptographically secure but the governing entity doesn't want the data to be accessible to the general public due to their speed.
- For instance, businesses may decide to utilise blockchain technology without ceding their edge over rivals to outside parties. Private blockchains can be used for auditing and managing trade secrets.
- Other use cases for private blockchain include supply chain management, asset ownership and internal voting.

3.1.3 Consortium Blockchain

GQ. Describe a consortium blockchain and mention its current applications. **(4 Marks)**

GQ. List down advantages and disadvantages of a consortium blockchain. **(4 Marks)**

- A consortium blockchain is a semi-decentralized type in which a network of blockchains is controlled by many organisations.
- Contrary to what we saw with a private blockchain, which is controlled by only one company, this is not the case.
- In this kind of blockchain, many organisations may function as nodes, exchanging data or engaging in mining.
- The typical users of consortium blockchains include financial institutions, governmental bodies, etc.

Examples of consortium blockchain are; Energy Web Foundation, R3, etc.

☞ **Advantages**

(1) Compared to a public blockchain network, a consortium blockchain is typically more reliable, scalable, and effective.

(2) It enables access controls just as private and hybrid blockchain.

☞ **Disadvantages**

(1) Compared to public blockchain, consortium blockchain is less transparent.

(2) The network's operation may still be hampered by the blockchain's own rules if a member node is attacked.

☞ **Case studies**

There are two applications for this kind of blockchain: banking and payments. A consortium made up of many banks can decide which nodes will validate the transactions. Organizations who want to track food as well as research organisations can develop a similar methodology. It's perfect for supply chains, especially those involving food and medicine.

3.1.4 Hybrid Blockchain

GQ. Describe a hybrid blockchain and mention its current applications. **(4 Marks)**

GQ. List down advantages and disadvantages of a hybrid Blockchain. **(4 Marks)**

- A hybrid blockchain combines the features of public and private blockchains.
- It makes use of both the private permission-based system and the public permission-less system features of blockchains. Users may manage who has access to what data stored in the blockchain with the help of such a hybrid network.
- Only a certain subset of the blockchain's data or records may be made public, keeping the remainder secret and confidential.

- As a result of the hybrid blockchain's flexibility, users may quickly join a private blockchain that is connected to many public blockchains.
- A hybrid blockchain's private network is often used to verify a transaction. But users can also release it in the public blockchain to get verified.
- The public blockchains increase the hashing and involve more nodes for verification. This enhances the security and transparency of the blockchain network.

Example of a hybrid blockchain is Dragonchain.

☞ **Advantages**

(1) Because hybrid blockchain operates in a closed environment, one of its major benefits is that outside hackers are unable to launch a 51 percent attack on the network.

(2) Additionally, it safeguards privacy while allowing for third-party contact.

(3) Compared to a public blockchain network, it has higher scalability and delivers quick and inexpensive transactions.

☞ **Disadvantages**

(1) This kind of blockchain can have information hidden, so it's not entirely transparent.

(2) There is little incentive for users to take part in or contribute to the network, and upgrading can be difficult.

☞ **Case studies**

- Real estate is one of the many interesting use cases for hybrid blockchain technology. A hybrid blockchain can be used by businesses to run systems securely while displaying some information, like listings, to the general public. Hybrid blockchain may be used to simplify procedures in the retail sector as well as in highly regulated industries like the banking sector.
- A hybrid blockchain may be used to store medical records. Users may access their information using a smart contract, but random third parties cannot see the data. Governments might also utilise it to securely communicate and keep citizen data among various entities.

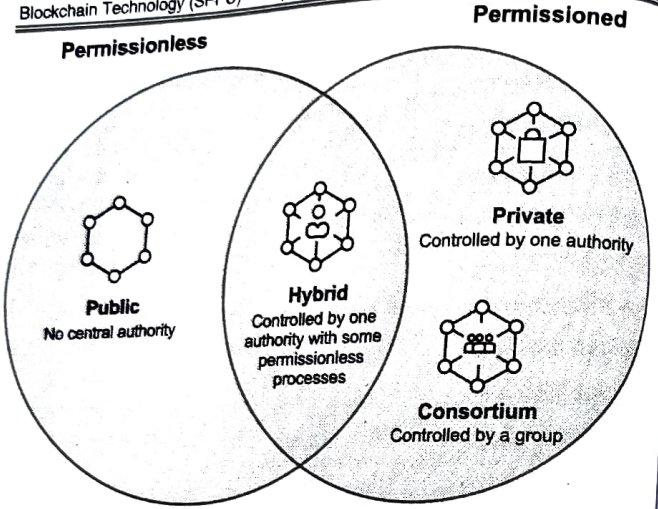

Fig. 3.1.1 : Types of blockchain

☞ **4 main types of blockchain technology**

	Public (permissionless)	Private (permissioned)	Hybrid	Consortium
Advantages	(1) Independence (2) Transparency (3) Trust	(1)Access control (2) Performance	(1) Access control (2) Performance	(1) Access control (2) Scalability (3) Security
Disadvantages	(1) Performance (2) Scalability (3) Security	(1) Trust	(1) Transparency (2) Upgarading	(1) Transparency
Use cases	(1) Cryptocurrency (2) Document validation	(1) Supply chain (2) Asset ownership	(1) Medical records (2) Real estate	(1) Banking (2) Research (3) Supply chain

Fig. 3.1.1 : Comparing different types of blockchains

3.2 BITCOIN

GQ. Write about emergence of bitcoin. **(2 Marks)**

GQ. How Bitcoin is different from fiat currency? **(2 Marks)**

- A virtual currency called Bitcoin was created to serve as money and a means of payment independent of any one person, organisation, or entity, eliminating the need for third parties to be involved in financial transactions.
- It is available for purchase on numerous platforms and is given to blockchain miners as reward for their efforts in verifying transactions.

Fig. 3.2.1 : Bitcoin image

- In August 2008, the domain name Bitcoin.org was registered.
- In 2009, a developer or group of developers going by the pseudonym Satoshi Nakamoto released Bitcoin to the general world.
- Since then, it has grown to be the most well-known cryptocurrency worldwide. Many additional cryptocurrencies have been created as a result of its success.
- Block 0 the very first Bitcoin block was mined on January 3, 2009. This is also referred to as the "genesis block" and contains the text: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks," which may serve as both pertinent political commentary and as evidence that the block was mined on or after that date.

- Bitcoin rewards are halved every 210,000 blocks. For instance, in 2009, the block reward was 50 brand-new bitcoins. The third halving took place on May 11, 2020, reducing the reward for finding a block to 6.25 bitcoins.
- The smallest unit of a bitcoin, which is divisible to eight decimal places (100 millionths of a bitcoin), is known as a satoshi.
- If necessary, and if the participating miners accept the change, Bitcoin could eventually be made divisible to even more decimal places.
- Bitcoin, as a form of currency, isn't too complicated to understand. For example, if you own a bitcoin, you can use your cryptocurrency wallet to send smaller portions of that bitcoin as payment for goods or services. However, it becomes very complex when you try to understand how it works.

3.2.1 Blockchain Technology for Bitcoin

- A blockchain and the network needed to power it include cryptocurrency. A distributed ledger, or blockchain, is a shared database that stores data. The blockchain uses encryption to protect the data inside.
- On the blockchain, when a transaction occurs, data from the previous block is transferred to a new block with the new data, encrypted, and the transaction is validated by validators, or miners, in the network.
- A new block is created and a new bitcoin is created and provided as a reward to the miner(s) that validated the data in the block once a transaction has been confirmed, and they are then free to use, hold, or sell the new Bitcoin.
- Bitcoin uses the SHA-256 hashing algorithm to encrypt the data stored in the blocks on the blockchain. Simply explained, a 256-bit hexadecimal integer is used to encrypt transaction data that is stored in a block. That number contains all of the transaction data and information linked to the blocks before that block.
- Transactions are queued up to be verified by network miners. In the Bitcoin blockchain network, many miners simultaneously attempt to validate the same transaction.
- The nonce, a four-byte number contained in the block header that miners are attempting to solve, is worked on by the mining software and hardware.
- The block header is hashed, or randomly regenerated by a miner repeatedly until it meets a target number specified by the blockchain. The block header is "solved," and a new block is created for more transactions to be encrypted and verified.

3.2.2 Security of Bitcoins

- The US National Security Agency's SHA-256 algorithm provides a framework for the cryptography used by bitcoin.
- It is very difficult to crack this since there are 2256 times as many potential private keys as there are atoms in the universe (estimated to be somewhere between 1078 to 1082).
- Although there have been a number of high-profile instances of bitcoin exchanges being hacked and having money stolen, these firms almost always kept the digital currency for the benefit of their users. In these instances, the website rather than the bitcoin network was compromised.
- Theoretically, an attacker could incorporate a consensus that they controlled all bitcoin into the blockchain if they had control over more than half of the bitcoin nodes now in use. However, this becomes less feasible as the number of nodes increases.
- The fact that bitcoin has no centralised control is a genuine issue. Anyone making a mistake with a transaction on their wallet is therefore helpless.
- There is no one to turn to if you unintentionally transmit bitcoins to the wrong person or forget your password.

3.2.3 Mining for Bitcoin

GQ. How mining process is carried out in Bitcoin? (4 Marks)

- The process of mining is what keeps the bitcoin network running and creates new currency.
- Every transaction is broadcast openly on the network, and miners group sizable groups of transactions together into blocks by performing a cryptographic computation that is exceedingly difficult to produce but very straightforward to verify.

- The blockchain is updated when the first miner to solve the subsequent block broadcasts it to the network and is confirmed to be accurate. A quantity of freshly produced bitcoin is subsequently given to the miner as reward.
- The software for bitcoin has a hard limit of 21 million coins. There will never be anything more than that. By the year 2140, all of the coins will be in use. By lowering the size of the rewards, the programme roughly doubles the difficulty of mining bitcoin every four years.
- When bitcoin was originally introduced, even a simple computer could practically instantly mine a coin. Now that it demands rooms full of sophisticated hardware, including highest graphics cards that are skilled at doing the computations, mining can occasionally become more expensive than it is worth due to a fluctuating bitcoin price.
- Fees of varied amounts are added by the sender as an incentive for miners, who also decide which transactions to group into a block.
- These fees will remain as a motivator for mining after all coins have been created. Due to the fact that it supports the Bitcoin network's architecture, this is necessary.

3.2.4 Drawbacks with Bitcoin

GQ. What are the drawbacks of Bitcoin? **(2 Marks)**

- A number of things have been said against bitcoin, including how energy-intensive the mining process is.
- Energy use at the University of Cambridge is tracked by an online calculator, and by the start of 2021, it was projected to use more than 100 terawatt hours year. To put things in context, the UK consumed 304 terawatt hours overall in 2016.
- Critics have pointed out that cryptocurrencies are an ideal tool for conducting black market transactions, and this has led to links between cryptocurrencies and criminal activity.
- In actuality, money has served this purpose for ages, and bitcoin's open ledger may serve as a tool for law enforcement.

3.3 ETHEREUM

GQ. Compare Bitcoin and Ethereum. **(4 Marks)**
GQ. How Ethereum development took place? **(4 Marks)**
GQ. Write a short note on DeFi. **(2 Marks)**
GQ. What is Non fungible tokens? What are its applications? Explain with example. **(4 Marks)**

- Ethereum is a platform that enables the creation of decentralised apps and organizations as well as asset keeping, trading, and communication.
- You retain control over your own data and what is shared, so using Ethereum doesn't need you to give up all of your personal information.
- Ether, an Ethereum-specific cryptocurrency, is used to pay for some services on the Ethereum network.
- 2013 have seen the creation of Ethereum by programmer VitalikButerin.
- Gavin Wood, Charles Hoskinson, Anthony Di Iorio, and Joseph Lubin were other Ethereum founders.
- Crowdfunding for development work started in 2014, and on July 30, 2015, the network launched. Anyone may publish permanent and unchangeable decentralised applications on Ethereum, allowing users to communicate with them.
- Ethereum is a decentralised blockchain platform that creates a peer-to-peer network for safely executing and validating smart contract application code. Participants can do business with one another using smart contracts without the need for a reliable central authority.

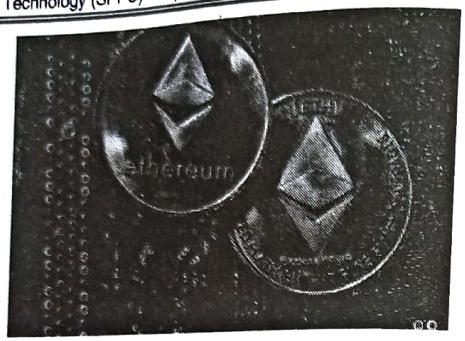

Fig. 3.3.1 : Ethereum

- Participants have complete ownership and visibility over transaction data since transaction records are immutable, verifiable, and securely disseminated across the network.
- Ethereum accounts that users have created both send and receive transactions. As part of the cost of completing transactions on the network, a sender must sign transactions and spend Ether.
- The native Solidity programming language and Ethereum Virtual Machine provide an incredibly versatile platform on which to construct decentralised apps.
- Developers of decentralised applications that use Ethereum to create smart contracts get access to a large ecosystem of developer tools and well-established best practises.
- With wallets like MetaMask, Argent, Rainbow, and others offering simple and direct user interfaces through which to interact with the Ethereum blockchain and the smart contracts deployed there, this maturity also extends to the quality of the user-experience for the average user of Ethereum applications.
- The vast user base of Ethereum encourages programmers to release new apps on the network, thus solidifying Ethereum as the go-to platform for decentralised applications like DeFi and NFTs.

- Future decentralised applications that need higher transaction throughput can be built on a more scalable network using the backwards-compatible Ethereum 2.0 protocol, which is presently being developed.

Decentralized Finance (DeFi)

- Developed on top of blockchain networks, DeFi is a network of financial apps. Because it is open and programmable, runs without a centralised authority, and lets developers to create new models for payments, investing, lending, and trading, it differs from conventional financial networks.
- Customers may quickly create safe decentralised financial apps by utilising distributed networks and smart contracts. DeFi companies, for instance, currently provide goods that make it possible to trade on decentralised exchanges, earn interest on bitcoin holdings, and conduct peer-to-peer lending and borrowing. Compound, Aave, UniSwap, and MakerDAO are a few of the well-known DeFi systems.

Non-Fungible Tokens (NFTs)

- NFTs are one-of-a-kind, indivisible digital tokens that may be used to demonstrate the origin of valuable assets, whether they be digital or physical. NFTs, for instance, can be used by an artist to tokenize their creations and guarantee that they are original and theirs.
- The blockchain network stores and updates the ownership information. Because they enable interoperability between gaming platforms, NFTs are likewise becoming more and more popular in the gaming sector.
- For instance, CryptoKitties, the first NFT project on Ethereum, allowed users to acquire digital cat collectibles backed by NFTs.

Fig. 3.3.2 : Non fungible tokens

- A card game called Gods Unchained uses NFTs to provide players complete ownership of all of their in-game possessions.
- NFTs are gaining popularity as more companies look to tokenize assets and provide users with tamper-proof lineage information about their assets.

3.3.1 Bitcoin Vs Ethereum

Table 3.3.1 : Comparison of Bitcoin and Ethereum

	Bitcoin	Ethereum
Founded	2009	2015
Market dominance	42%	18%
Consensus mechanism	Proof of work	Proof of stake
Block time	10 minutes	12-14 seconds
Max supply	21 million	Unlimited

3.4 HYPERLEDGER

GQ. What type of blockchain is Hyperledger? (2 Marks)
GQ. What are different features of Hyperledger? (4 Marks)
GQ. Justify how and why Hyperledger is more suitable for enterprise grade applications. (4 Marks)
GQ. Compare Hyperledger with Ethereum. (4 Marks)

- Providing the necessary framework, rules, guidelines, and tools to construct open-source blockchains and related applications for usage across several sectors, Hyperledger is a global enterprise blockchain initiative.
- Projects from Hyperledger include a range of permissioned blockchain systems that are enterprise, where network users are familiar with one another and have an inherent incentive in taking part in consensus-making.

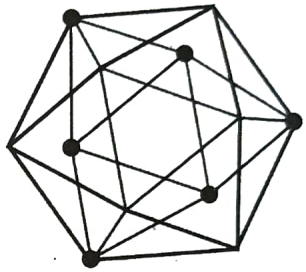

Fig. 3.4.1 : Hyperledger

- A company may implement multiple modular blockchain solutions and services using the parts that are offered under the Hyperledger umbrella to dramatically increase the effectiveness of their operations and business processes.
- The Linux Foundation, which has its headquarters in San Francisco, California, launched the Hyperledger project in December 2015.
- Today, there are more than 120 member companies, up from its initial 30 member companies.
- In order to improve the efficiency, performance, and transactions of different business processes, Hyperledger was established with the goal of speeding up industry-wide collaboration for the development of high-performance and dependable blockchain and distributed ledger-based technological framework.
- Leading companies from the financial, banking, Internet of Things (IoT), supply chain management, manufacturing and production, and technology sectors are part of the global collaboration known as Hyperledger. Big brands like Bosch, Daimler, IBM, Samsung, Microsoft, and Hitachi American

Express, JP Morgan, and Visa, in addition to a host of blockchain-based startups like Blockforce and ConsenSys are among them.

3.4.1 Hyperledger's Organizational Structure

GQ. Draw and explain various components of Hyperledger green house. **(4 Marks)**

In essence, Hyperledger is neither a company nor a network of cryptocurrencies nor a blockchain system. Although it does not support a cryptocurrency like bitcoin, it functions by offering the required standards and infrastructure for the creation of a variety of blockchain-based systems and applications for use in the industrial sector. Imagine Hyperledger as a hub, where numerous independent blockchain-based projects and tools that follow its specified design philosophies operate under its umbrella.

The several initiatives contain the following :

- Hyperledger Fabric is a framework for creating different blockchain-based products, services, and software programmes for commercial usage.
- Fabric has now incorporated Hyperledger Composer, a defunct layer, as well.
- Hyperledger Cello offers an on-demand "as-a-service" deployment mechanism for using blockchain (Blockchain-as-a-Service).
- Hyperledger Explorer is a dashboard utility that allows for the monitoring, searching, and maintenance of blockchain developments and related data.
- Hyperledger Burrow is a permissioned Ethereum smart-contract blockchain node that handles transactions and executes smart contract code on the Ethereum Virtual Machine (EVM).
- Hyperledger Sawtooth is an enterprise-level, permissioned, modular blockchain platform that uses an innovative Proof of Elapsed Time consensus algorithm.

- Hyperledger Caliper is a blockchain benchmark tool that is used to evaluate the performance of a specific blockchain implementation.

The Hyperledger Greenhouse

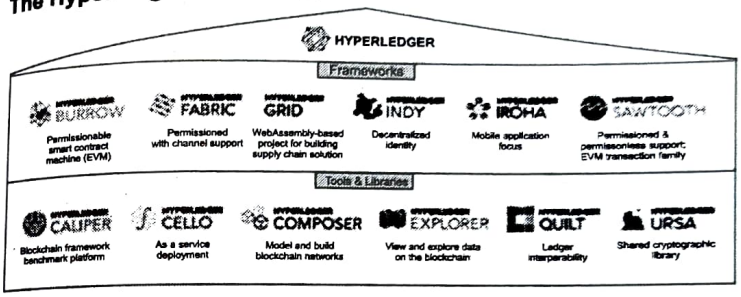

Fig. 3.4.2 : Hyperledger greenhouse

- All such projects under the Hyperledger umbrella follow the design methodology that supports a modular and extensible approach, interoperability, and security features. The projects remain agnostic to a particular token or cryptocurrency, though a user can create one as required.

3.4.2 Hyperledger Technology Layers

GQ. What are the layers in Hyperledger architecture? **(4 Marks)**

- The primary business elements used by Hyperledger in its architecture are as follows:
- The consensus layer is in charge of establishing an understanding of the sequence and validating the accuracy of the collection of transactions that make up a block.
- Processing transaction requests and approving only legitimate transactions are the responsibilities of the smart contract layer.

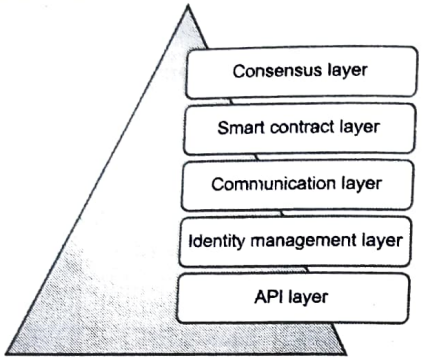

Fig. 3.4.3 : Hyperledger layers

- The transfer of messages between peers is handled by the communication layer. In order to preserve and validate users' and systems' identities and build trust on the blockchain, identity management services are a must.
- Applications and clients from outside sources can connect to the blockchain using the API, or application programming interface.

Table 3.4.1 : Comparison of Ethereum and Hyperledger

	Ethereum	Hyperledger Fabric
Public vs. Private	Public	Private
Permissions	Permissionless	Permissioned
Governance	Decentralized	Federated
Consenus Mechanism	Proof-of-Work	Pluggable BFT
Smart Contract Languages	Solidity, Vyper	Go, Java, Javascript (Node.js)
Private Transactions	No	Yes
Ideal Use Cases	Tokenization (stablecoins, NFTs), DeFi, public transaction settlement	B2B data exchange, transaction settlement, and non-repudiation

3.5 IOTA

GQ. Write a short note on IOTA. **(4 Marks)**

GQ. State about various issues in current system and how IOTA addresses them? **(4 Marks)**

- IOTA (MIOTA) is a distributed ledger designed to record and execute transactions between machines and devices in the Internet of Things (IoT) ecosystem.
- The ledger uses a cryptocurrency called MIOTA to account for transactions in its network.
- IOTA's key innovation is Tangle, a system of nodes used for confirming transactions. IOTA claims that Tangle is faster and more efficient than typical blockchains used in cryptocurrencies.
- The IOTA Foundation, the nonprofit foundation responsible for the ledger, has inked agreements with prominent companies, such as Bosch and Volkswagen, to extend the platform's utility among connected devices.

3.5.1 Understanding IOTA

- Billions of devices were connected to the Internet by 2020. Within this Internet of Things (IoT) ecosystem, devices can exchange data and payment information with multiple other devices in transactions conducted throughout the day.
- IOTA wants to replace existing device transaction methods with its own.
- The ledger, according to its creators, serves as a "public permission-less backbone for the Internet of Things that facilitates interoperability between various devices."
- Simply put, this implies that anybody will be able to access it and that it will facilitate transactions between linked devices.
- IOTA's creators assert that it addresses a number of issues that are present in cryptocurrencies created on conventional blockchains.
- These issues include scalability, network speed issues, and the concentration of mining power in the hands of a small number of people.

- Scalability in the context of cryptocurrencies refers to the challenge of increasing the volume of transactions that a blockchain can handle without affecting other metrics.
- Those problems are primarily caused due to a backlog of transactions on Bitcoin's blockchain.
- The backlog itself is due to a variety of reasons, from small block sizes to the difficulty of puzzles that miners must solve to earn the cryptocurrency as a reward.
- IOTA solves these problems by reconfiguring the blockchain architecture into Tangle, a new way of organizing data and confirming transactions.

3.5.2 History of IOTA

GQ. Write about history of IOTA? **(4 Marks)**

- Sergey Ivancheglo, Serguei Popov, David Sønstebø, and Dominik Schiener, who joined later, together co-founded IOTA.
- The project was announced in October 2015 through a post announcing a token sale in an online bitcoin forum.
- IOTA has its origins in the Jinn project. The goal of the project was to create general-purpose processors, or ternary hardware, which is low-cost and energy-efficient technology, for usage in the IoT ecosystem. In September 2014, Jinn performed a crowd sale for its tokens. During the crowd sale, almost 100,000 tokens were sold, bringing in a total of $250,000.
- Because they were advertised as profit-sharing tokens, which may be considered security tokens, the Jinn tokens quickly got into trouble. Initial coin offers (ICOs) were still developing at the time, and it was unclear how regulated they were. A new token sale was performed in 2015, and Jinn was rebranded as IOTA.
- This time, the tokens were advertised as utility tokens. Holders of Jinn tokens might trade them for equivalent tokens under the new system. David Snsteb claimed that because of the Jinn project, IOTA was "spawned," hence introducing IOTA first and Jinn afterwards made sense.
- IOTA's founding transaction was a balance transfer to an address that included all of the MIOTA, the cryptocurrency it uses, that would ever be mined.

- However, according to sources, a screenshot of the genesis transaction has not yet been discovered online.
- Other "founder" addresses received these tokens in distribution. There are 27 quadrillion MIOTAs expected to exist in all.
- The creators of IOTA claim that the total number of MIOTAs "nicely" corresponds to the largest integer value that can be used in JavaScript. During the 2016–2017 bull market, MIOTA attained a high valuation of $14.5 billion three months after making its debut on cryptocurrency exchanges.
- However, like the majority of other cryptocurrencies, its value eventually fell.

3.5.3 Concerns About IOTA

GQ. What are the drawbacks of IOTA ? **(4 Marks)**

- IOTA has primarily been criticised for its technological flaws. Similar to the majority of cryptocurrencies, IOTA's mechanism is new and untested.
- A phishing assault on its network led to the $3.94 million loss of MIOTA. The IOTA development team published a blog post in reaction to the hack that outlined how to create a secure seed when utilising its cryptocurrency.

Fig. 3.5.1 : IOTA

- The creators of IOTA are rumoured to have "rolled" their cryptocurrency. In other words, they didn't employ the popular SHA-256 hash function that is used in Bitcoin, instead designing their own encryption technique from scratch. IOTA's Curl hash function has been revealed to have significant vulnerabilities by the researchers at MIT's Digital Currency Initiative.

- When given two alternative inputs, the function yielded the same result. Collision is a characteristic that indicates a malfunctioning hash function.
- The MIT team said that a malicious party may have used their method to damage or steal user cash from Tangle in their investigation of the issue. The flaw has been fixed by the IOTA team.
- There may be flaws with IOTA's claims that the usage of Decentralized Acyclic Graph (DAGs)would solve the scaling challenges that plague blockchains.
- The co-founder of Ethereum, VitalikButerin, has questioned whether hashgraphs, which serve as the foundation for DAG, can address scalability problems. According to him, the problem of a blockchain's dependence on computer memory and processing power is not resolved by the existing iterations of hashgraphs. Hashgraph systems are nevertheless limited in their ability to scale by the power and speed of the individual machines that make up their network.
- In order to guarantee transaction security as of 2020, IOTA's network utilised a central server called a Coordinator. Due to the Coordinator's implementation, a single point of failure has been introduced, undermining the system's claims to be decentralised. It has also slowed down the network's pace because parallel processing does not occur in a Coordinator-based system.
- The IOTA Foundation, however, envisioned a future removal strategy for the Coordinator known as "The Coordicide."

3.5.4 Future of IOTA

- Even while IOTA's market value was still significantly lower than it was in 2017, towards the end of 2020, things appeared to be looking up for this cryptocurrency.
- As of December 19, 2020, it has a market valuation of more over $900 million, up from $446 million at the beginning of 2020.
- That is a gain of more than 100%, but it wasn't an easy route. IOTA stands out from other cryptocurrencies and draws interest from investors because to its ongoing partnerships with major organisations and concentration on the expanding

Internet of Things (IoT). IOTA has a market worth of almost $3.2 billion as of September 28, 2021, so it must be functioning.

3.5.5 How Is IOTA Different From Bitcoin ?

GQ. Compare IOTA with Bitcoin. **(4 Marks)**

- Several fundamental ideas and topological limitations of a blockchain are eliminated in IOTA as a remedy to Bitcoin's issues.
- The cryptocurrency used by IOTA, MIOTA, is premined, and consensus of transactions happens otherwise than it does on a blockchain. A brand-new data structure called Tangle has been suggested by IOTA developers as a mechanism to arrange numerical representations in a computer's memory.
- Tangle is a nonsequential network of nodes known as a Decentralized Acyclic Graph (DAG). As a result, each node in a Tangle can connect to several other nodes.
- However, they are only linked in one way, therefore a node cannot refer to itself. Because a normal blockchain is a sequential linked set, it is also a DAG.
- However, IOTA's Tangle is a parallel architecture that allows transactions to be handled concurrently rather than sequentially. The Tangle becomes more secure and effective at processing transactions as more systems are connected to it.
- For confirmations and consensus in Bitcoin, a network of computers running full nodes, which store the complete history of transactions for a ledger, is necessary. This method uses a lot of compute and energy.
- In Tangle, full node miners are not necessary. The amount of time and memory required to validate a transaction is decreased by using references to two prior transactions to confirm each new transaction.
- As a last stage, the Proof of Work (PoW) challenge is added to the transaction, which is simple and quick to solve. The two selected transactions are referred to as tips.
- The transaction is approved by the IOTA system using a tip selection mechanism using "confidence" as a parameter. Let's say a deal has already received 97 approvals.

- There is then a 97 95 % confidence that a node will eventually accept it.
- The idea of "confidence" is connected to a transaction's weight. The weight of a transaction increases as it passes through Tangle. The more approvals a deal receives, the more weight it carries.
- A transaction is published to the whole network once it has been confirmed. Once that transaction has been confirmed, another unconfirmed one may select it as one of its tips to confirm itself.
- This method of confirming a transaction results in no fees and low power consumption, enabling MIOTA to be used across a wide variety of devices and machines with different power requirements.

3.6 R3 CORDA

GQ. Enlist and explain essential features of R3 Corda? **(6 Marks)**

- On September 15, 2015, the top financial companies in the world formed the R3 consortium. The consortium has evolved into an ecosystem with more than 300 members now that actively contribute to the field of distributed ledger and blockchain technology.

r3.corda

Fig. 3.6.1 : R3 Corda

- R3 made the decision to use blockchain technology to address actual business issues in areas that are both complex and heavily regulated. R3 created a custom blockchain framework they called "Corda" after realising there wasn't one already on the market that could fulfil their needs.
- Corda is an open-source blockchain project that was created with business in mind.

- It lets you create interoperable blockchain networks that carry out transactions in complete secrecy. Smart contract technology from Corda enables direct, valuable commercial transactions.

3.6.1 Differentiating Factors of Corda from Blockchain Framework

Privacy

- Any system using distributed ledger technology must prioritise privacy. It's because your data will inevitably be spread over several nodes and servers that belong to various commercial firms. The only persons with access to a transaction's information in R3's Corda are those participating in the transaction and those who need to confirm the transaction's origin.
- It indicates that two or more people can conduct business together while only disclosing information that is essential.
- This stands in sharp contrast to public blockchain frameworks or certain limited private blockchain frameworks, which broadcast the transaction or its information throughout the whole network.

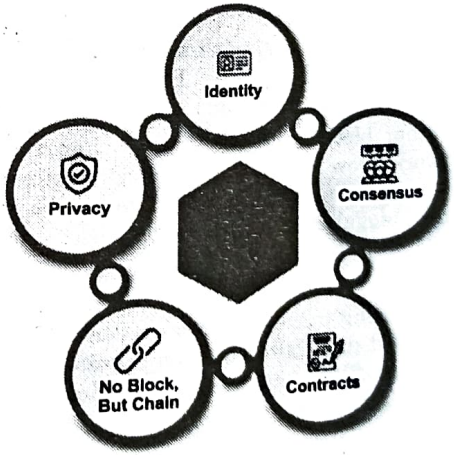

Fig. 3.6.2 : Identity

- Enterprises and corporations would prefer the Corda blockchain framework's privacy feature.Like other comrade frameworks, Corda does not include any gossip protocols which broadcasts all transactions to the network.
- The essential need for creating a closed network of the system among known participants becomes the identification of various parties in the DLT system through a permissioned blockchain.
- Parties can be sure of the members of the blockchain network's identification using R3 Corda. A key component of a global decentralised ledger where you are blind to other players is identity.
- The ability of Corda to assign a single user profile to any legal entity, be it a company or an individual, is made feasible by the KYC requirements of all network members.

Consensus

- Through the use of consensus, organisations on a distributed and decentralised network can come to some agreement about the transactions taking place between them.
- It is critical to know this idea in order to spot fraud and uphold the integrity of any blockchain network, whether it is public or private.
- Through a process of consensus and the use of a variety of algorithms, such as Byzantine Fault Tolerant algorithms, transactions in Corda are confirmed.
- Like any other blockchain, the special characteristics of the Corda network allow for the implementation of several distinct consensus pools employing various algorithms, providing its users with a pluggable consensus model based on their needs.

Contracts

- Any company being managed across several companies over a blockchain-based distributed system requires smart contracts and programme files encoding the business logic and rules validation.
- To process transactions in R3's Corda, all participants must deterministically execute the same code in order to validate the proposed ledger revisions.

- The available languages are high-level and productive, rather than arcane ones like Solidity, just like Ethereum. Examples include Java and Kotlin.
- Only the validation chain of each related transaction is required for the validation function of the CorDapp (Corda Distributed Applications) contract code.

No Block, But Chain

- The UTXO input/output model, which is the foundation of Corda's functionality, is remarkably similar to the transaction structure used in conventional blockchains like Bitcoin.
- However, unlike other commercial blockchain frameworks, such as Hyperledger Fabric, which groups together a number of transactions between "n" participants across the channel into a block based on various criteria, the storage and verification do not result in a chain of blocks.
- In a cryptographically linked (chained) chain, Corda binds each transaction to the transactions it depends on rather than to a prior block comprising a different set of transactions.
- Contrary to other business blockchain solutions described above, Corda does not batch together transactions based on certain criteria on a regular basis and wait for confirmation into a block before confirming them all at once. Instead, each transaction is instantly confirmed by R3's Corda.
- There is no need to wait for a "block interval" or for a lot of additional transactions to follow. As we progress, every transaction is confirmed.
- Corda provides several notaries on the same network, greatly enhancing privacy and facilitating quicker and more efficient transactions.
- An enterprise architecture called Corda has a comprehensive understanding of the blockchain and distributed ledger technologies.
- It is a perfect blockchain platform since it lacks chains or cryptographic blocks. and is versatile enough to fit into a number of business use cases.

3.7 CONSENSUS IN BLOCKCHAIN

GQ. What is Consensus mechanism in blockchain? Enlist different algorithms of consensus. (4 Marks)

GQ. What is the need of consensus in blockchain? (4 Marks)

GQ. What are the goals of consensus mechanism? (2 Marks)

- We see new developments in blockchain technology every day. No matter how hard we work to understand the most recent technologies, there is always something new to learn.
- Have you ever wondered where all these blockchain technology came from? Well, the fundamental building block of this ground-breaking technology is consensus algorithms.
- The blockchain consensus algorithms are what distinguish one blockchain consensus sequence from the others.
- The blockchain network allows infinite numbers of individuals to coexist in the same space.
- Why then do they never conflict with one another or coexist? The answer is in the architecture of the blockchain network.
- The architecture is cleverly designed, and consensus algorithms are at the core of this architecture.

3.7.1 Introduction to Consensus Algorithms

The technical definition would be :

- Consensus algorithms are methods for collective decision-making in which members of the group create and support the decision that will benefit the group as a whole.
- People are required to support the majority decision in this type of resolution, whether they agree with it or not.
- Simply said, it's a way for a group to make decisions. Consider an example to help. Consider a group of 10 individuals who wish to decide on a project that will benefit them all.
- While everyone of them is free to make a suggestion, the one that will best benefit them will likely receive the most support. Whether or not they agreed with the decision, others had to deal with it.

- Now imagine the same thing with thousands of people. Wouldn't that drastically make it way more difficult?
- Consensus algorithms don't only concur with the majority votes, they also agree with one that is advantageous to everyone. Thus, the network constantly benefits.
- Blockchain consensus models are tools for promoting fairness and equality online. A consensus theorem is the name given to the consensus mechanisms that were employed for this agreement. These blockchain consensus models have certain specific goals, like:

(1) **Reaching a consensus** : The method collects as many agreements from the group as it can.

(2) **Collaboration** : Each group strives to reach a deeper understanding that benefits the interests of the group as a whole.

(3) **Cooperation** : Everyone will set aside their personal interests to operate as a team.

(4) **Equal Rights** : Each voter's vote is equally important. This implies that every voter's vote counts.

(5) **Participation :** Every member of the network must take part in the voting process. Nobody will be excluded or able to do so without a vote.

(6) **Activity** : Each group member participates actively. Nobody in the group is more accountable than the others.

- Now that we have a better understanding of the entire network, let's explore into the blockchain technology.
  - It's a novel method of database organisation.
  - can keep track of everything that changes based on the network.
  - The information is organised into blocks of information.
- Therefore, blockchain technology will not implement the decentralisation process; it will simply let you establish a new organised database. Because of this, the blockchain is regarded as the foundation of the whole decentralised network.
- The process is actually fairly easy. The only way to get to an agreement is through these Blockchain consensus models. However, without standard consensus techniques, there cannot be any decentralised system.

- Even whether the nodes trust one another or not won't matter. They will be required to adhere to specific standards and come to a consensus. You must examine each Consensus method to do this.

3.7.2 Different Types of Consensus Algorithms

- Proof-of-Work
- Proof-of-Stake
- Delegated Proof-of-Stake
- Leased Proof-Of-Stake
- Proof of Elapsed Time
- Practical Byzantine Fault Tolerance
- Simplified Byzantine Fault Tolerance
- Delegated Byzantine Fault Tolerance
- Directed Acyclic Graphs
- Proof-of-Activity
- Proof-of-Importance
- Proof-of-Capacity
- Proof-of-Burn
- Proof-of-Weight

Let's explore some of them in detail.

Proof of Work

GQ. Which consensus mechanism is used by Bitcoin and How?

GQ. Describe the process of PoW. **(4 Marks)**

GQ. What are the drawbacks of PoW? **(4 Marks)**

GQ. Explain whether the electrical energy and equipment costs required by PoW are justified. **(4 Marks)**

GQ. Explain what is likely to happen to the PoW mining industry after the most recent halving of bitcoin. **(4 Marks)**

GQ. What is Byzantine Generals problem? How PoW solves it? **(4 Marks)**

GQ. How Bitcoin provides the solution to Byzantine Generals problem? **(4 Marks)**

- The first and original Blockchain algorithm presented to the

blockchain network is proof of work. The algorithm adds a new block to the chain and confirms the transaction.

- In this method, minors (a group of individuals) compete with one another to complete the network transaction. Mining is the process of competing with one another.
- He is rewarded as soon as miners have successfully produced a valid block. Bitcoin is the most well-known application of Proof of Work (PoW). This blockchain consensus mechanism is used by several blockchain technologies to validate all of their transactions and add appropriate blocks to the network chain.
- All of the information pertaining to the blocks is gathered via the decentralised ledger system. However, each transaction block needs to be treated with careful attention.

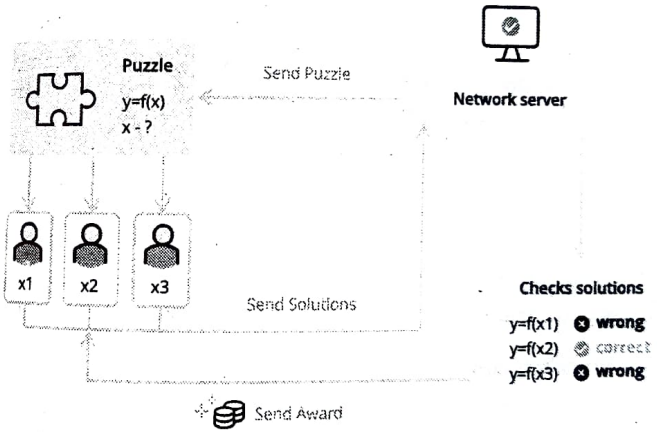

Fig. 3.7.1 : Proof of Work

- Producing proof of work can be a random process with low probability. In this, a lot of **trial and error** is required before a valid proof of work is generated.
- The main idea behind this technology is to readily provide solutions to challenging mathematical problems.
- To begin with, these mathematical problems demand a lot of computational power. For instance, understanding the Hash Function or how to determine the output without knowing the input. Another is integer factorization, which also applies to

crossword puzzles.

- This occurs when the server suspects a DDoS attack, and the consensus mechanisms need a lot of computation to confirm it. The miners are helpful in this situation. The hash is the solution to the entire mathematical equation problem.
- Proof of work, however, has some limitations. The network appears to be expanding rapidly, requiring a lot of processing power. The system's overall sensitivity is rising as a result of this process.

Why Has the System Developed Such Sensitivity?

- Most of the time, the blockchain consensus sequence depends on reliable data and information. But the system's speed is seriously lacking. It takes a long time to produce a block when a problem is very complex.
- The transaction is delayed, and the workflow as a whole is stopped. Block generation will turn into a miracle if the problem can't be solved in a specific amount of time.
- The system would be vulnerable to DDoS attacks if it can solve that problem too easily. Additionally, because not all nodes can check for potential problems, the solution needs to be further examined accurately.
- If they could, the network would be lacking of its most crucial component: transparency.

Proof of Work Implementation Process

- The miners will first work out all of the riddles before creating new blocks and confirming transactions. It's impossible to predict how difficult a problem could be.
- The maximum number of users, the lowest current power, and the network's total load all play a significant role.
- Each new block has a hash function that also contains the hash function from the preceding block. The network therefore offers an additional layer of security and stops any breaches. When a miner completes the problem, a new block is generated and the transaction is confirmed.

Where Exactly Is the Blockchain Proof of Work Consensus Algorithm Used?

- Bitcoin is the most popular one. This particular blockchain consensus algorithm was first introduced by Bitcoin. Based on the total network power, the Blockchain consensus models allowed for any change in the puzzle's level of difficulty.
- The time it takes to make a new block is roughly ten minutes. The same mechanism is also offered by other cryptocurrencies, including Litecoin as a consensus example.
- Ethereum, a platform that uses blockchain technology, employed proof of work in about three to four significant applications. Ethereum, however, has shifted to Proof of stake.
- **Blockchain Technology :** Use Proof of Work because PoW provides DDoS protection and reduces mining stake overall. The blockchain algorithms present a good amount of challenge for hackers. The system requires a lot of computational power and effort.
- This is why it is possible for hackers to break the Blockchain consensus models, although doing so would be expensive and time-consuming.
- On the other hand, since network-wide decisions are made independently of financial considerations, no miners are able to influence them. Whether you can create new blocks depends on how much computing power you have.

Primary issues with PoW

- Not every consensus algorithm is flawless, and proof of work isn't much different either. It has many benefits, but it also has many drawbacks. Let's examine the system's primary flaws.
- Greater Energy Consumption The blockchain network is made up of millions and millions of specially built microchips that continually hash data.
- Currently, Bitcoin delivers 20 billion hashes per second. The network's miners hash data using a special type of microprocessor.
- This process gives the network an additional layer of defence against botnet attacks.
- The proof-of-work-based blockchain network's high degree of security consumes a lot of energy. In a world where energy is getting scarcer, the increased consumption is becoming an

issue. Miners on the system must pay a significant amount of money owing to power use. The best solution to this problem would be a cheap source of energy.

Centralization of Miners

- With the energy shortage, the focus will shift to less expensive electricity-related solutions. However, if a bitcoin miner-manufacturer rises, it would be the biggest issue.
- The manufacturer has a certain amount of time before becoming more power-hungry and attempting to introduce additional rules into the mining system.
- The decentralised network will become centralised as a result of this circumstance. This makes it yet another significant issue that these Blockchain algorithms are confronting.
- The 51% Attack
- This attack might result in the majority of users being under control and the majority of the mining power being captured.
- In this case, the attackers would have complete control over the network. They can stop other people from generating new blocks. Attackers can also receive rewards based on their tactics.
- Imagine that X is using the blockchain network to transfer Y some bitcoin. Y is not a part of the attack, but X is.
- The transaction is completed, but the attackers prevent any currency from being transmitted by forking the chain.
- In other cases, the miners will join in a particular branch. On certain blocks, they will have the highest processing power combined.
- Other blocks with a shorter life are thus excluded. Therefore, Y won't get the money.
- This isn't a profitable solution, though. After the incident is widely publicised, a lot of mining power will be consumed, people will start to leave the network, and gradually the cost of trade will decrease.

The Byzantine Generals Problem

- Game theory's "Byzantine Generals Problem" identifies the

challenges decentralised parties have in reaching consensus without the help of a reliable central authority.

- How can members of a network agree on a certain truth when no member has access to other members' identities?
- The Byzantine Generals analogue in game theory . The problem is that Byzantium city is under attack by multiple generals.
- They have encircled the city, but they must determine when to launch an attack as a group.
- They will succeed if every general launches an attack at once, but they will fail if each general launches an attack independently.
- The generals are unable to communicate securely with one another since Byzantium's defenders might intercept or falsifiably broadcast any signals they send or receive. How can the generals organize to attack at the same time?

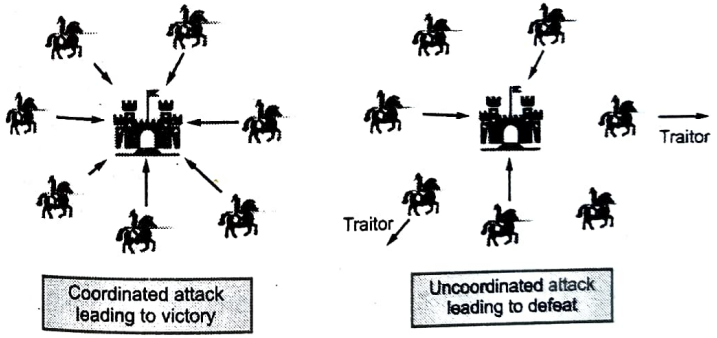

Fig. 3.7.2

- Only decentralised systems are prone to the Byzantine Generals problem because they lack a reliable information source and a mechanism to validate the data they gather from other members of the network.
- In centralised systems, it is assumed that a central authority would publish accurate information and guard against the network's spread of incorrect or fraudulent information.
- For instance, in the conventional financial system, banks are relied upon to accurately report to customers their balances and transaction histories. A central bank or government is

trusted to restore trust if a bank does seek to lie to or cheat its consumers.

- The Byzantine Generals problem, which demands that truth be verified in an unreliable manner, cannot be solved by centralised systems.
- Instead, they decide not to face the issue at all and sacrifice efficiency for trustlessness. The central government may corrupt centralised systems, though.

The Problem of the Byzantine Generals and Money

- A great example of the Byzantine Generals Problem is money. How can a community create a kind of payment that all members can rely on and accept? For a considerable part of history, communities have chosen to use uncommon items like shells or glass beads or precious metals as currency.
- Gold provided a partial solution to the Byzantine Generals Problem because it was respected and trusted in decentralised systems like international trade.
- Its weight and purity, however, continued to be questionable, and they still are. Gold's partial inability to resolve the Byzantine Generals Problem led to the formation and issue of money being taken over by reliable central parties, typically governments. Governments established monopolies over mints to promote confidence in the currency's purity and weight.
- The Byzantine Generals Problem was plainly not resolved by centralised systems. Governments, the apparently reliable central authorities for money, have betrayed that confidence by seizing, devaluing, or altering the currency.
- A money would need to be verifiable, untraceable, and counterfeit-resistant in order to solve the Byzantine Generals Problem. This accomplishment was not made until the creation of Bitcoin.

How Bitcoin Solves the Byzantine Generals Problem?

- Bitcoin was the first realized solution to the Byzantine Generals Problem with respect to money.
- Prior to Bitcoin, a number of initiatives and programmes that aimed to produce money independent of the government all ended in failure.

Blockchain Addresses the Issue of Double Spend

- Bitcoin required a mechanism to control ownership and avoid double spending in order to function as a currency. Bitcoin employs a blockchain, a public, distributed ledger that records a history of all transactions.
- The blockchain is the truth that all parties must agree upon in the Byzantine Generals analogy.
- They might construct a working, trustless currency without a centralised authority if all nodes, or participants of the Bitcoin network, could agree on which transactions took place and in what sequence.

Proof-of-Work Solves the Byzantine Generals Problem

- By employing a Proof-of-Work method to provide a clear, objective set of rules for the blockchain, Bitcoin was able to resolve the Byzantine Generals Problem.
- A network participant who wants to contribute data—known as blocks—to the blockchain must provide proof that they put a lot of work into making the block.
- Since the developer of this work incurs high expenditures, they are encouraged to share reliable information.
- There can be no dispute or tampering with the information on the Bitcoin network since the rules are fair.
- The method for deciding who may create new bitcoins is also objective, as are the rulesets dictating which transactions are acceptable and which are invalid.
- The past of Bitcoin is immutable because it is very difficult to remove a block after it has been added to the network.
- Members of the Bitcoin network may therefore always agree on the blockchain's current status and all of its transactions. Each node independently confirms the validity of blocks based on the Proof-of-Work requirement and transactions depending on additional criteria.
- All nodes on the network will instantly identify fraudulent information as objectively incorrect and ignore it if any member of the network tries to broadcast it.
- Bitcoin is a trustless system because each node can independently validate all data on the network, eliminating the need to rely on other users.

☞ **Proof of Stake**

GQ. How Proof of Stake algorithm works? **(4 Marks)**
GQ. Q. What is the need of PoS? **(4 Marks)**
GQ. How PoS overcomes the drawbacks of PoW? **(4 Marks)**
GQ. How PoS addresses 51% attack issue? **(4 Marks)**
GQ. What are the drawbacks of PoS? **(4 Marks)**
GQ. Enlist and explain benefits of PoS. **(4 Marks)**
GQ. What is Delegated PoS? **(4 Marks)**
GQ. Discuss whether business owners are likely to be comfortable with a Proof-of-Stake (PoS) blockchain. **(6 Marks)**

- A consensus algorithm called proof of stake addresses the key problems with the proof-of-work algorithm.
- This one requires each block to be validated before the network can add it to the blockchain ledger.
- This one has a small amount of Twist. Miners may participate in the mining process by staking their currency.
- A novel idea called proof of stake allows each participant to mine or even validate brand-new blocks solely based on their currency holdings. Therefore, in this case, having more coins increases your chances.
- The minors in this consensus process are preselected.
- Even if the process is completely random, not all minors are allowed to take part in the staking.
- The network's miners are all selected at random. You will be eligible to join the network as a node if you have a certain number of coins already held in your wallet.
- You must deposit a particular quantity of currency after becoming a node in order to be eligible to become a miner.
- The validators will then be chosen via a vote mechanism. At the conclusion of the process, the miners will stake the minimum amount needed for the unique wallet staking.
- Actually, the procedure is fairly easy. According to the wallet, new blocks will be generated in direct proportion to the quantity of currencies. For instance, if you own 10% of the coins, you may mine 10% of the new blocks.
- A number of proof of stake consensus algorithms are used by

various blockchain technologies.

- However, all algorithms function identically while mining new blocks. Each miner will get a share of the transaction fees in addition to the block reward.

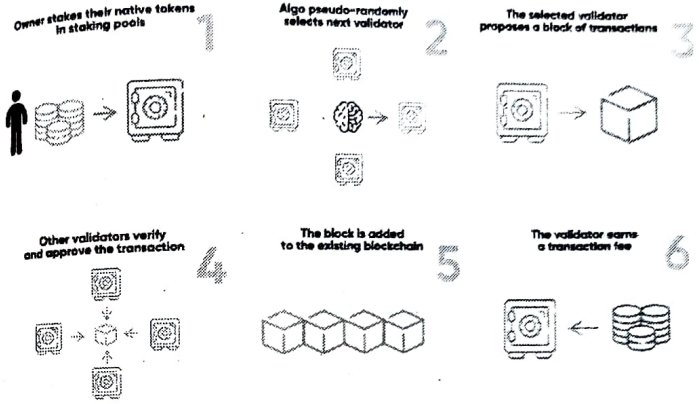

Fig. 3.7.3 : Proof of Stake

How Does The Proof of Stake Pooling Work?

- There are many methods to participate in stacking. You can join a pool and make profit there if the stake amount is too high. Two methods exist for doing it.
- You can first loan your currency to another user who will join the pool and share the profits with you. To stake with, you'll need to try and locate a trustworthy partner.
- Joining the pool is another option. By doing this, the profit from that particular pool will be divided among all participants according to the amount staked.

Benefits as Proof of Stake

- First off, these consensus methods don't need a lot of powerful hardware support. All you need is a working computer and a steady internet connection. Transactions may be confirmed by anybody with sufficient coins on the network.
- A network investment won't lose value over time as other investments do. Only changes in pricing will have an impact on the profit. The blockchain's proof of stake consensus process

uses substantially less energy than proof of work. It doesn't even require a lot of electricity.

Additionally, it lessens the risk of a 51% attack.

- Even while proof of stake appears to be more profitable than proof of work, there is still a substantial drawback. The system's primary flaw is that complete decentralisation will never be achievable.
- This is due to the fact that only a small number of nodes are allowed to take part in network staking. The majority of the system will eventually be under the hands of those with the most coins.

Delegated Proof-of-Stake Consensus for Blockchain

- It is variant of the standard proof of stake in which users still stake their cryptocurrency coins. However, rather than becoming responsible for validating the block themselves, users (or stakeholders) stake their coins to delegate the work by voting on the node that would validate the block on their behalf.
- Thus the consensus mechanism got its name "Delegated Proof of Stake". Once the nodes have been elected, they're responsible for reaching a consensus between themselves to validate transactions and add blocks to the Blockchain.
- The technology is highly reliable and gives the entire process an additional level of flexibility.
- Delegated Proof of Stake is the ideal option if you want quick, effective, decentralised consensus mechanisms.
- Here, the stakeholders' problem is entirely resolved in a democratic manner. Every element in the network has the ability to act as a delegate.
- Here, the nodes are referred to as delegates rather than miners or validators.
- This technology can complete a transaction in less than one second by working out block production! Additionally, this system was created to guarantee the highest level of protection against regulatory issues.

☞ Proof of Elapsed Time (PoET)

GQ. What is proof of elapsed time? How it works ? **(6 Marks)**

GQ. What Blockchains use proof of elapsed time? **(2 Marks)**

GQ. What is an advantage of using consensus algorithm proof of elapsed time PoET instead of proof PoW? **(4 Marks)**

- One of the top consensus algorithms is PoET. This specific technique is mostly utilised in permissioned blockchain networks, where access to the network requires authorization. These permissions networks must choose voting or mining rights policies.
- The PoET algorithms employ a specific strategy for ensuring network transparency to ensure everything goes well. Since the network requires identity before allowing a user to join the miners, the Consensus methods also guarantee a safe entrance into the system.
- Naturally, employing only fair methods to select the winners is possible with this consensus process.
- Let's examine the key tactic behind this amazing consensus sequence.
- Every user on the network needs to wait for a certain duration of time, but this time limitation is pretty arbitrary.
- The participant who has completed their fair share of waiting time will be allowed to add a new block to the ledger.
- The programme must take into account two things in order to defend these cases.
  - Whether the winner made the random number selection initially?
- He or she might pick an arbitrary little period and win the game first.
  - Did the person actually wait the allotted amount of time?
- PoET is dependent on a unique CPU requirement. It is referred to as the Intel Software Guard Extension. This Software Guard Extension supports the network's use of unique codes.
- PoET uses this system and makes sure the winning is purely fair.

☞ Proof-of-Activity

GQ. What is Proof of Activity? How it functions? **(4 Marks)**

GQ. How PoA deals with 51% Attack issue? **(4 Marks)**

GQ. What are the drawbacks of PoA? **(4 Marks)**

- The Litecoin founder and three other authors had a wonderful idea while people were arguing the issue of Proof-of-Work vs. Proof-of-Stake.
- They posed a straightforward query to the world: Why can't the PoW and PoS be combined rather than opposed against one another?
- As a result, the interesting hybrid concept known as Proof-of-Activity was born. It combines the finest two qualities, making it less power-hungry and more secure against attacks.

The Function of Proof-of-Activity

- The mining process begins with the Proof-of-Activity blockchain consensus mechanism in the same way as it does with the PoW algorithm. For a prize, the miners must solve a complicated puzzle.
- So where is PoW's main difference? In a PoW network, miners create blocks with a completed transaction.
- Miners only mine the block templates in Proof-of-Activity. These templates contain two elements: the header data and the reward address for the miners.
- When these block templates are mined by the miners, the system switches to the Proof-of-Stakes algorithm.
- A block's header information identifies a random stakeholder. The pre-mined blocks are then validated by these parties.
- A validator's probability to confirm a block rises with the amount of stack they currently possess. That specific block enters the blockchain only after being validated.
- The best of the two consensus algorithms is utilised in this manner by Proof-of-Activity to validate and add a block to the blockchain. Additionally, the network shares the transaction fees fairly across the validators and miners.
- Thus the system acts against the "tragedy of the commons" and creates a better solution for block validation.

The Effects of Proof of Activity

- The 51 % attack is one of the main challenges a blockchain must deal with. The likelihood of the 51 percent attack is nil according to the consensus theory.
- It occurs because neither the miners nor the validators can command a majority since adding a block to the network requires an equal contribution from both groups.
- The Proof-of-Activity blockchain consensus mechanism, however, is said to have serious faults by some critics.
- The mining function will result in a significant increase in energy usage like the first one.
- Second, there is no way to prevent the validators from signing their own work twice using Proof-of-Activity. The consensus theorem is somewhat put on the back foot as a result of these two key shortcomings.
- Two popular blockchains adopt the Proof-of-Activity – Decred and Espers. Still, they have some variations. In reality, Decred is getting considered as the more popular one than the Espers consensus theorem.

☞ Proof-of-Burn

GQ. Write a shot note on Proof of Burn. **(4 Marks)**

GQ. What is Eater address in Proof of Burn? **(2 Marks)**

GQ. What are the pros and cons of Proof of Burn? **(4 Marks)**

- Impressively, this consensus sequence is pretty good. Some of the coins will be burned to protect the PoW cryptocurrency! A few coins are sent to a "Eater Address" by the miners, which triggers the process.
- These coins cannot be used in any way by the Eater Addresses. Since the burned coins are recorded in a ledger, they are actually unusable as currency. Additionally, the person who burned the money will receive a reward.
- The burning is indeed a loss. However, the harm is just momentary because the procedure will eventually protect the coins against hackers and their cyber-attacks.
- Additionally, the process of burning raises the stakes of the substitute coins.
- In such a case, a user is more likely to mine the future block

and will receive more rewards in the future. Burning may therefore be utilised as a mining privilege.

- A cryptocurrency that makes use of this blockchain consensus protocol is the counterparty, which is a great example of consensus.

The Eater Address

- Users transfer bitcoin to the Eater Addresses to burn them. A private key is not associated with an Eater Address.
- Therefore, no user will ever be able to access these addresses to use the coins stored there. Additionally, these addresses are created randomly.
- Although these coins are unavailable or "gone forever (!)," they are nonetheless included as part of the supply and given the burned label. The Advantages and Disadvantages of Proof-of-Burn Algorithm
- The main intent for burning the coins is to increase stability. We are aware that long-term gamers frequently keep coins for a very long period in order to benefit.
- By providing more stable currency and long-term commitment, the system benefits those long-term investors. Additionally, this improves decentralisation and develops a more evenly distributed network.
- But no matter how you look at the situation, burning coins is wasteful! Even some eater addresses contain Bitcoins worth more over $100,000. There is no way to get the money back; they lose everything.

Chapter Ends...

❑❑❑