20CB604/20CS604/20DS604

Hall Ticket Number:

□□□□□□□□□

III/IV B.Tech (Regular) DEGREE EXAMINATION

July/August, 2023 **Common to CB,CS & DS Engineering**

Sixth Semester **Blockchain Technologies**

Time: Three Hours **Maximum:** 70 Marks

Answer question 1 compulsory. **(14X1 = 14Marks)**

Answer one question from each unit. **(4X14=56 Marks)**

			CO	BL	M
1	a)	Define Blockchain Technology.	CO1	L1	1
	b)	What is the purpose of a block header in a Blockchain?	CO1	L1	1
	c)	Define CAP theorem.	CO1	L1	1
	d)	What is the role of nodes in the Bitcoin network?	CO2	L1	1
	e)	Define mining in the context of Bitcoin.	CO2	L1	1
	f)	List out various security services provided by cryptography.	CO2	L1	1
	g)	What are the methods used to provide data origin authentication?	CO3	L1	1
	h)	Define avalanche affect.	CO3	L1	1
	i)	What is UTXO?	CO3	L1	1
	j)	What is genesis block?	CO4	L1	1
	k)	List the components of QUORUM block chain.	CO4	L1	1
	l)	Define smart contract.	CO4	L1	1
	m)	List three key features of a blockchain.	CO1	L1	1
	n)	What is the limit of total supply of Bitcoins.	CO2	L1	1

Unit-I

2	a)	Write about different types of block chain.	CO1	L2	7M
	b)	Write about decentralization using block chain.	CO1	L2	7M

(OR)

3	a)	Explain the key features of a Blockchain in detail.	CO1	L2	7M
	b)	Explain generic elements of block chain.	CO1	L4	7M

Unit-II

4	a)	Describe the process of a Bitcoin transaction in detail, and the role of each participant.	CO2	L2	7M
	b)	Explain in detail about asymmetric cryptography.	CO2	L4	7M

(OR)

5	a)	Write in detail about symmetric cryptography.	CO2	L2	7M
	b)	Explain about RSA algorithm.	CO2	L4	7M

Unit-III

6	a)	Explain the concept of extended protocols on top of the bitcoin.	CO3	L2	7M
	b)	Explain about ricardian contracts.	CO3	L2	7M

(OR)

7	a)	Analyse the key elements of the Ethereum blockchain	CO3	L4	7M
	b)	Explain the concept of development of alt coins.	CO3	L4	7M

Unit-IV

8	a)	Explain in detail about kadena block chain.	CO4	L4	7M
	b)	Explain the following i. Quorum ii. Storj	CO4	L4	7M

(OR)

9	a)	Explain in detail about ripple network.	CO4	L3	7M
	b)	Explain the following i. Stellar ii. Rootstock	CO4	L4	7M

1 a) Define Blockchain Technology.
Blockchain is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable, and updateable only via consensus or agreement among peers.

b) What is the purpose of a block header in a Blockchain?
A block header is used to identify a particular block on an entire blockchain and is hashed repeatedly to create proof of work for mining rewards.

c) Define CAP theorem.
The theorem states that any distributed system cannot have Consistency, Availability, and Partition tolerance simultaneously

d) What is the role of nodes in the Bitcoin network?
Verify transactions and maintain the ledger's accuracy

e) Define mining in the context of Bitcoin.
Mining is a resource-intensive process by which new blocks are added to the blockchain.

f) List out various security services provided by cryptography.
Confidentiality, Integrity, Authentication, Non-repudiation, Accountability

g) What are the methods used to provide data origin authentication?
Message Authentication Codes (MACs) and digital signatures

h) Define avalanche affect.
Avalanche effect specifies that a small change, even a single character change in the input text, will result in a totally different hash output.

i) What is UTXO?
Unspent Transaction Output (UTXO) is an unspent transaction output that can be spent as an input to a new transaction.

j) What is genesis block?
A genesis block is the first block in the blockchain that was hardcoded at the time the blockchain was started.

k) List the components of QUORUM block chain.
Transaction manager, Crypto Enclave, QuorumChain, Network manager

l) Define smart contract.
These are the programs run on top of the blockchain and encapsulate the business logic to be executed when certain conditions are met.

m) List three key features of a blockchain.
Distributed Consensus, Transaction Verification, Platforms for Smart Contracts, Transferring Value Between Peers, Smart Property.

n) What is the limit of total supply of Bitcoins.
21 million bitcoins

Unit-I

2 a) **Write about different types of block chain.**

Based on the way blockchain has evolved over the last few years, it can be divided into multiple types

Public blockchains: As the name suggests, these blockchains are open to the public and anyone can participate as a node in the decision-making process. Users may or may not be rewarded for their participation. These ledgers are not owned by anyone and are publicly open for anyone to participate in. All users maintain a copy of the ledger on their local nodes. They use a distributed consensus mechanism in order to reach a decision about the eventual state of the ledger. These blockchains are also known as permission-less ledgers.

Private blockchains: Private blockchains as the name implies are private and are open only to a consortium or group of individuals or organizations that has decided to share the ledger among themselves.

Semi-private blockchains: Here, part of the blockchain is private and part of it is public. The private part is controlled by a group of individuals whereas the public part is open for participation by anyone.

Sidechains: More precisely known as pegged (fixing/binding) sidechains, this is a concept whereby coins can be moved from one blockchain to another and back. Common uses include the creation of new altcoins (alternative cryptocurrencies) whereby coins are burnt as a proof of adequate stake.

There are two types of sidechain. 1) The example provided above for burning coins is applicable to a one-way pegged sidechain. 2) A two-way pegged sidechain, which allows the movement of coins from the main chain to the sidechain and back to the main chain when required.

Permissioned ledger: A permissioned ledger is a blockchain whereby the participants of the network are known and already trusted. Permissioned ledgers do not need to use a distributed consensus mechanism, instead an agreement protocol can be used to maintain a shared version of truth about the state of the records on the blockchain. There is also no requirement for a permissioned blockchain to be private as it can be a public blockchain but with regulated access control.

Distributed ledger: This ledger is distributed among its participants and spread across multiple sites or organizations. This type can either be private or public. The key idea is that, unlike many other blockchains, the records are stored contiguously instead of sorted into blocks. This concept is used in Ripple (currency exchange).

Shared ledger: This is generic term that is used to describe any application or database that is shared by the public or a consortium.

Fully private and proprietary blockchains: These blockchains perhaps have no mainstream application as they deviate from the core idea of decentralization in blockchain technology. In some cases within an organization there might be a need to share data and provide some level of guarantee of the authenticity of the data. These blockchains could be useful in that scenario. For example, for collaboration and sharing data between various government departments.

Tokenized blockchains: These blockchains are standard blockchains that generate cryptocurrency as a result of a consensus process via mining or via initial distribution.

Tokenless blockchains: These are probably not real blockchains because they lack the basic unit of transfer of value(token). Useful in situations where there is no need to transfer value between nodes and only sharing some data among various already trusted parties is required.

b) **Write about decentralization using block chain.**

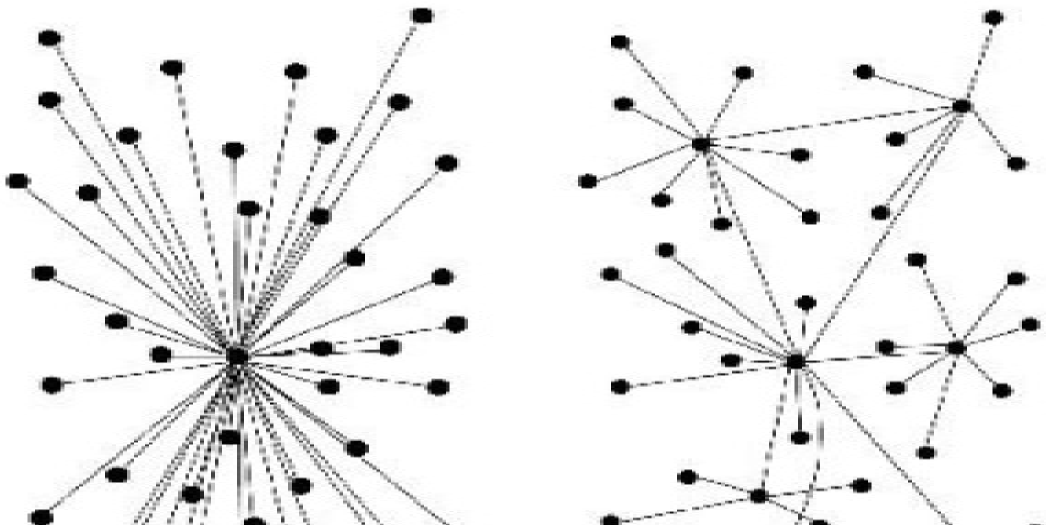
Decentralization is a core benefit and service provided by the blockchain technology. Blockchain by design is a perfect vehicle for providing a platform that does not need any intermediaries. It can function with many different leaders chosen via consensus mechanisms. This model allows anyone to compete to become the decision-making authority. This competition is governed by a consensus mechanism. Decentralization is applied in varying degrees from semi decentralized to fully decentralized depending on the requirements and circumstances. Decentralization can provides a way to remodel existing applications and paradigms or build new applications to give full control to users.

Information and communication technology (ICT)

Database or application servers are under the control of a central authority, such as a system administrator. With bitcoin and the advent of the blockchain technology, now the technology that allows anyone to start a decentralized system is available. It can either be run autonomously or by requiring some human intervention depending on the type and model of governance used in the decentralization. Different types of system that currently exist, that is, central, distributed, and decentralized. This concept was first published in 1964 in a paper by Paul Baran on distributed communication networks. All users of a central system are dependent on a single source of service. Online service providers, such as eBay, Google, Amazon, Apple's App Store, and the many other providers, use this common model of delivering services. On the other hand, in a distributed system, the data and computation are spread across multiple nodes in the network. Sometimes, this term is confused with parallel computing. In a parallel system, computation is performed by all nodes simultaneously in order to achieve a result. In a distributed system, computation may not happen in parallel and data is only replicated on multiple nodes that users view as a single coherent system. Both of these models are used with variations in order to achieve failure tolerance and speed. In this model, there is still a central authority that has control over all nodes and governs processing. This means that the system is still centralized in nature.

Different types of network/system

In a distributed system, there still exists a central authority that governs the entire system. In a decentralized system, no such authority exists. A decentralized system nodes are not dependent on a single master node; instead, control is distributed among many nodes. For example, each department in an organization has its own database server. Taking away the power from the central server and distributing it. A real innovation is decentralized consensus, which was introduced with bitcoin. A user to agree on something via a consensus algorithm without the need for a central trusted third party, intermediary, or service provider.



(OR)

3 a) **Explain the key features of a Blockchain in detail.**

A blockchain performs various functions. These are:

Distributed Consensus: This enables a blockchain to present a single version of truth that is agreed upon by all parties without the requirement of a central authority.

Transaction Verification: Any transactions posted from nodes on the blockchain are verified based on a predetermined set of rules and only valid transactions are selected for inclusion in a block.

Platforms For Smart Contracts: A blockchain is a platform where programs can run that execute business logic on behalf of the users, now a very desirable feature.

Transferring Value Between Peers: Blockchain enables the transfer of value between its users via tokens. Tokens can be thought of as a carrier of value.

Generating Cryptocurrency: This is an optional feature depending on the type of blockchain used. A blockchain can generate cryptocurrency as an incentive to its miners who validate the transactions and spend resources in order to secure the blockchain.

Smart Property: For the first time it is possible to link a digital or physical asset to the blockchain in an irrevocable manner. It cannot be claimed by anyone else; you are in full control of your asset and it cannot be double spent or double owned. Compare it with a digital music file, which can be copied many times without any control; On a blockchain, if you own it no one else can claim it unless you decide to transfer it to someone. This feature has far-reaching implications especially in Digital Rights Management (DRM) and electronic cash systems where double spend detection is a key requirement. The double spend problem was first solved in bitcoin.

Provider Of Security: Blockchain is based on proven cryptographic technology that ensures the integrity and availability of data. Generally, confidentiality is not provided due to the requirements of transparency. This has become a main barrier for its adaptability by financial institutions and other industries that need privacy and confidentiality of transactions. It could be argued that in many situations confidentiality is not really needed and transparency is preferred instead. In bitcoin confidentiality is not really required;Major progress has been made towards providing confidentiality and privacy on blockchain. A more recent example is Zcash (another cryptocurrency. Other security services such as nonrepudiation (can't deny the fact) and authentication are also provided by blockchain. All actions are secured by using private keys and digital signatures.

Immutability: This is another key feature of blockchain: records once added onto the blockchain are immutable. There is the possibility of rolling back the changes, it will require an unaffordable amount of computing resources. This difficulty makes the records on a blockchain practically immutable.

Uniqueness: This feature of blockchain ensures that every transaction is unique and has not been spent already. Detection and avoidance of double spending are a key requirement.

Smart Contracts: Blockchain provides a platform to run smart contracts. These are automated autonomous programs that reside on the blockchain. They encapsulate business logic and code in order to execute a required function when certain conditions are met. This is indeed a revolutionary feature of blockchain as it allows flexibility, programmability, and much desirable control of actions that users of blockchain need to perform according to their specific business requirements.

b) **Explain generic elements of block chain.**

Addresses: Addresses are unique identifiers that are used in a transaction on the blockchain to denote senders and recipients. An address is usually a public key or derived from a public key. While addresses can be reused by the same user, addresses themselves are unique. In practice, however, a single user may not use the same address again and generate a new one for each transaction. This newly generated address will be unique. Bitcoin is in fact a pseudonymous(under false name) system. End users are usually not directly identifiable but some research in de-anonymizing bitcoin users have shown that users can be identified successfully. As a good practice it is suggested that users generate a new address for each transaction in order to avoid linking transactions to the common owner, thus avoiding identification.

Transaction: A transaction is the fundamental unit of a blockchain. A transaction represents a transfer of value from one address to another.

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

Peer-To-Peer Network: This is a network topology whereby all peers can communicate with each other and send and receive messages.

Scripting Or Programming Language: This element performs various operations on a transaction. Transaction scripts are predefined sets of commands for nodes to transfer tokens from one address to another and perform various other functions. Turing complete programming language is a desirable feature of blockchains.

Virtual Machine: A virtual machine allows Turing complete code to be run on a blockchain. Virtual machines are not available on all blockchains. Various blockchains use virtual machines to run programs, for example Ethereum Virtual Machine (EVM) and Chain Virtual Machine (CVM).

State Machine: A blockchain can be viewed as a state transition mechanism. A state is modified from its initial form to the next and eventually to a final form as a result of a transaction execution and validation process by nodes.

Nodes: A node in a blockchain network performs various functions depending on the role it takes. A node can propose and validate transactions and perform mining to facilitate consensus and secure the blockchain. This is done by following a consensus protocol. (Most commonly this is PoW.) Nodes can also perform other functions such as: simple payment verification (lightweight nodes), validators, many others functions depending on the type of the blockchain used and the role assigned to the node.

Smart Contracts: These programs run on top of the blockchain and encapsulate the business logic to be executed when certain conditions are met. The smart contract feature is not available in all blockchains. It is now becoming a very desirable feature due to the flexibility and power it provides to the blockchain applications.

Unit-II

4 a) **Describe the process of a Bitcoin transaction in detail.**

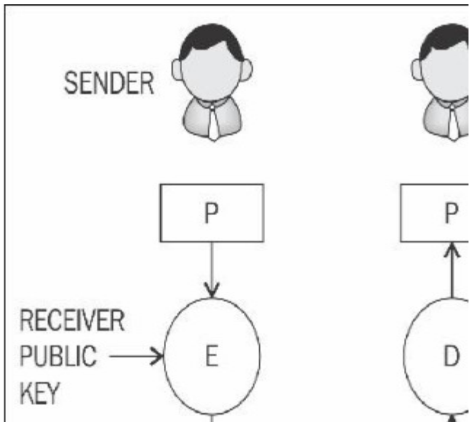
Transactions are at the core of the bitcoin ecosystem. Transactions can be as simple as just sending some bitcoins to a bitcoin address, or it can be quite complex depending on the requirements. Each transaction is composed of at least one input and output. Inputs can be thought of as coins being spent that have been created in a previous transaction and outputs as coins being created. If a transaction is minting new coins, then there is no input and therefore no signature is needed. If a transaction is to send coins to some other user (a bitcoin address), then it needs to be signed by the sender with their private key and a reference is also required to the previous transaction in order to show the origin of the coins. Coins are, in fact, unspent transaction outputs represented in Satoshis. Transactions are not encrypted and are publicly visible in the blockchain. Blocks are made up of transactions and these can be viewed using any online blockchain explorer.

The transaction life cycle

1. A user/sender sends a transaction using wallet software or some other interface.
2. The wallet software signs the transaction using the sender's private key.
3. The transaction is broadcasted to the Bitcoin network using a flooding algorithm.
4. Mining nodes include this transaction in the next block to be mined.
5. Mining starts once a miner who solves the Proof of Work problem broadcasts the newly mined block to the network.
6. The nodes verify the block and propagate the block further, and confirmation starts to generate.
7. Finally, the confirmations start to appear in the receiver's wallet and after approximately six confirmations, the transaction is considered finalized and confirmed.
8. However, six is just a recommended number; the transaction can be considered final even after the first confirmation.
9. The key idea behind waiting for six confirmations is that the probability of double spending is virtually eliminated after six confirmations.

b) **Explain in detail about asymmetric cryptography.**

The key that is used to encrypt the data is different from the key that is used to decrypt the data. Also known as public key cryptography, it uses public and private keys in order to encrypt and decrypt data, respectively. Various asymmetric cryptography schemes are in use, such as RSA, DSA, and El-Gammal. The diagram explains how a sender encrypts the data using a recipient's public key and is then transmitted over the network to the receiver. Once it reaches the receiver, it can be decrypted using the receiver's private key. This way, the private key remains on the receiver's side and there is no need to share keys in order to perform encryption and decryption, which is the case with symmetric encryption.



Security mechanisms offered by public key cryptosystem include key establishment, digital signatures, identification, encryption, and decryption. Key establishment mechanisms are concerned with the design of protocols that allow setting up of keys over an insecure channel. Non-repudiation service, a very desirable property in many scenarios, can be provided using digital signatures. Sometimes, it is important to not only authenticate a user, but to also identify the entity involved in a transaction; this can also be achieved by a combination of digital signatures and challenge-response protocols. Finally, the encryption mechanism to provide confidentiality can also be realized using public key cryptosystems, such as RSA, ECC, or El-Gammal. Public key algorithms are slower in computation as compared to symmetric key algorithms. Therefore, they are not commonly used in the encryption of large files or the actual data that needs encryption. They are usually used to exchange keys for symmetric algorithms and once the keys are established securely, symmetric key algorithms can be used to encrypt the data. Public key cryptography algorithms are based on various underlying mathematical problems.

Public and private keys

In order to understand public key cryptography, the first concept that needs to be looked at is the idea of public and private keys. A private key, as the names suggests, is basically a randomly generated number that is kept secret and held privately by the users. Private key needs to be protected and no unauthorized access should be granted to that key; otherwise, the whole scheme of public key cryptography will be jeopardized as this is the key that is used to decrypt messages. Private keys can be of various lengths depending upon the type and class of algorithms used. For example, in RSA, typically, a key of 1024-bit or 2048-bits is used. 1024-bit key size is no longer considered secure and at least 2048 bit is recommended to be used in practice. A public key is the public part of the private-public key pair. A public key is available publicly and published by the private key owner. Anyone who would then like to send the publisher of the public key an encrypted message can do so by encrypting the message using the published public key and sending it to the holder of the private key. No one else would be able to decrypt the message because the corresponding private key is held securely by the intended recipient. Once the public key encrypted message is received, the recipient can decrypt the message using the private key.

(OR)

5 a) **Write in detail about symmetric cryptography.**

Symmetric cryptography refers to a type of cryptography whereby the key that is used to encrypt the data is the same for decrypting the data, and thus it is also known as a shared key cryptography. The key must be established or agreed on before the data exchange between the communicating parties. This is the reason it is also called secret key cryptography.

There are two types of symmetric ciphers, stream ciphers and block ciphers.

Stream Ciphers

These ciphers are encryption algorithms that apply encryption algorithms on a bit-by-bit basis to plain text using a key stream. There are two types of stream ciphers: synchronous and asynchronous. Synchronous stream ciphers are ones where key stream is dependent only on the key, whereas Asynchronous stream ciphers have a key stream that is also dependent on the encrypted data. In stream ciphers, encryption and decryption are basically the same function because they are simple modulo 2 additions or XOR operation. The key requirement in stream ciphers is the security and randomness of key streams. Various techniques have been developed to generate random numbers, and it's vital that all key generators be cryptographically secure: Operation of a stream cipher.

Block Ciphers

These are encryption algorithms that break up plain text into blocks of fixed length and apply encryption block by block. Block ciphers are usually built using a design strategy known as Fiestel cipher. Recent block ciphers, such as AES (Rijndael) have been built using substitution-permutation network (SPN).

Fiestel ciphers are based on the Fiestel network, which is a structure developed by Horst Fiestel. This structure is based on the idea of combining multiple rounds of repeated operations to achieve desirable cryptographic properties known as confusion and diffusion. Fiestel networks operate by dividing data into two blocks (left and right) and process these blocks via keyed round functions.

Data Encryption Standard (DES)

DES was introduced by the US National Institute of Standards and Technology (NIST) as a standard algorithm for encryption. In main use during 1980s and 1990s, but it has been not proven to be very resistant against brute force attacks, due to advances in technology and cryptography research. Especially in July 1998, Electronic Frontier Foundation (EFF) broke DES using a special purpose machine. DES uses a key of only 56 bits, which has raised some concerns. Problem solved using Triple DES (3DES), which proposed the usage of a 168-bit key using three 56-bit keys. But other limitations, such as slow performance and 64-bit block size, are not desirable.

Advanced Encryption Standard (AES)

In 2001, after an open competition, an encryption algorithm named Rijndael that was invented by cryptographers Joan Daemen and Vincent Rijmen was standardized as AES with minor modifications by NIST in 2001. So far, no attack has been found against AES that is better than the brute force method. Original Rijndael allows different key and block sizes of 128-bit, 192-bit, and 256-bits, but in the AES standard, only a 128-bit block size is allowed. However, key sizes of 128-bit, 192- bit, and 256-bit are allowed.

AES steps

During the AES Algorithm processing, a 4 by 4 array of bytes knows as state is modified using multiple rounds. Full encryption requires 10 to 14 rounds depending on the size of the key.

1. In the AddRoundKey step, the state array is XORed with a subkey, which is derived from the master key.
2. This is the substitution step where a lookup table (S-box) is used to replace all bytes of the state array.
3. This step is used to shift each row except the first one in the state array to the left in a cyclic and incremental manner.
4. Finally, all bytes are mixed in this step in a linear fashion column-wise.

The preceding steps describe one round of AES. In the final round (either 10, 12, or 14 depending on the key size), stage 4 is replaced with Addroundkey to ensure that the first three steps cannot be simply inverted back.

b) **Explain about RSA algorithm.**

A description of RSA is discussed here. RSA was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adelman, hence the name RSA. This is based on the integer factorization problem, where the multiplication of two large prime numbers is easy but difficult to factor it back to the two original numbers. The crux of the work in the RSA algorithm is during the key generation process.

An RSA key pair is generated by performing the steps described here.

Modulus generation: Select p and q very large primes Multiply p and q, n=p.q to generate modulus n

Generate co-prime: Assume a number called e. It should satisfy certain conditions, that is, it should be greater than 1 and less than (p-1) (q-1). In other words, e must be such a number that no number other than 1 can be divided into e and (p-1) (q-1). This is called co-prime, that is, e is the co-prime of (p-1)(q-1).

Generate public key: Modulus generated in step 1 and e generated in step 2 is pair that, together, is a public key. Modulus n, e are the public part that can be shared with anyone; however, p and q need to be kept secret.

Generate private key: Private key called d here and is calculated from p, q and e. Private key is basically the inverse of e modulo (p-1)(q-1). In the equation form, it is this: ed = 1 mod(p-1)(q-1). Usually, an extended Euclidean algorithm is used to calculate d; this algorithm takes p, q and e and calculates d. The key idea in this scheme is that anyone who knows p and q can calculate private key d easily, by applying the extended Euclidean algorithm, but someone who doesn't know the value of p and q cannot generate d. This also implies that p and q should be large enough for the modulus n to become very difficult (computationally infeasible) to factor.

Encryption and Decryption using RSA:
RSA uses the following equation to produce cipher text: C = Pe mod n
This means that plain text P is raised to e number of times and then reduced to modulo n.
Decryption in RSA is given by the following equation: P = Cd mod n
This means that the receiver who has a public key pair (n, e) can decipher the data by raising C to the value of the private key d and reducing to modulo n.

Unit-III

6 a) **Explain the concept of extended protocols on top of the bitcoin.**

Colored coins

Colored coins is a set of methods that have been developed to represent digital assets on the bitcoin blockchain. Coloring a bitcoin refers colloquially to updating it with some metadata representing a digital asset (smart property). The coin still works and operates as a bitcoin but additionally carries some metadata that represents some assets. This mechanism allows issuing and tracking specific bitcoins. Metadata can be recorded using the bitcoins OP_RETURN opcode or optionally in multi-signature addresses.

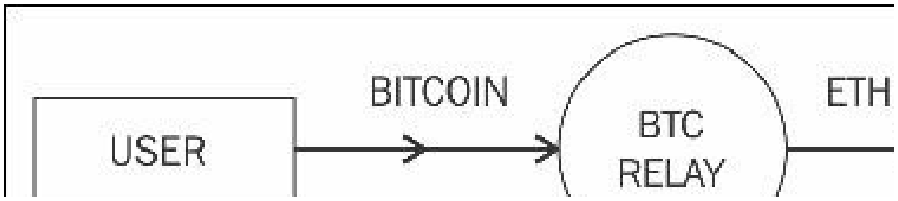
This metadata can also be encrypted if required to address any privacy concerns.Colored coins can be used to represent a multitude of assets including but not limited to commodities, certificates, shares, bonds, and voting. In order to work with colored coins, a wallet that interprets colored coins is necessary and normal bitcoin wallets will not work.Colored coin wallets can be set up online using a service available at https://www.coinprism.com/. Using this service, any type of digital asset can be created and issued via a colored coin.The idea of colored coins is very appealing as it does not require any modification to the existing bitcoin protocol and can make use of the already existing secure bitcoin network.

In addition to the traditional representation of digital assets, there is also the possibility of creating smart assets that behave according to the parameters and conditions defined for them. These parameters includes time validation, restrictions on transferability, and fees. This opens the possibility of creating smart contracts. A major use case can be the issuance of financial instruments on the blockchain. Advantages: This will ensure low transaction fees, valid and mathematically secure proof of ownership, fast transferability without requiring an intermediary, and instant dividend pay outs to the investors.

Counterparty

This is another service that can be used to create custom tokens that act as a cryptocurrency and can be used for various purposes such as issuing digital assets on top of bitcoin blockchain. This is quite a powerful platform and runs on bitcoin blockchains at their core but has developed its own client and other components to support issuing digital assets. The architecture consists of a counterparty server, counterblock, counter wallet, and armory_utxsvr. Counterparty works based on the same idea as colored coins by embedding data into regular bitcoin transactions. Provides a much richer library and set of powerful tools to support the handling of digital assets.

This embedding is also called embedded consensus because the counterparty transactions are embedded within bitcoin transactions. The method of embedding the data is by using OP_RETURN opcode in bitcoin. The currency produced and used by counterparty is known as XCP and is used by smart contracts as the fee for running the contract. At the time of writing its price is 2.78 USD. Counterparty allows the development of smart contracts on Ethereum using solidity language and allows interaction with bitcoin blockchain. In order to achieve this, BTC Relay is used as a means to provide interoperability between Ethereum and bitcoin. This is a clever concept where Ethereum contracts can talk to bitcoin blockchain and transactions through BTC Relay. The relayers (nodes that are running BTC Relay) fetch the bitcoin block headers and relay them to a smart contract on the Ethereum network that verifies the PoW. This process verifies that a transaction has occurred on the bitcoin network. This is available at http://btcrelay.org/. Technically, this is basically an Ethereum contract that is capable of storing and verifying bitcoin block headers just like bitcoin simple payment verification lightweight clients do by using bloom filters.



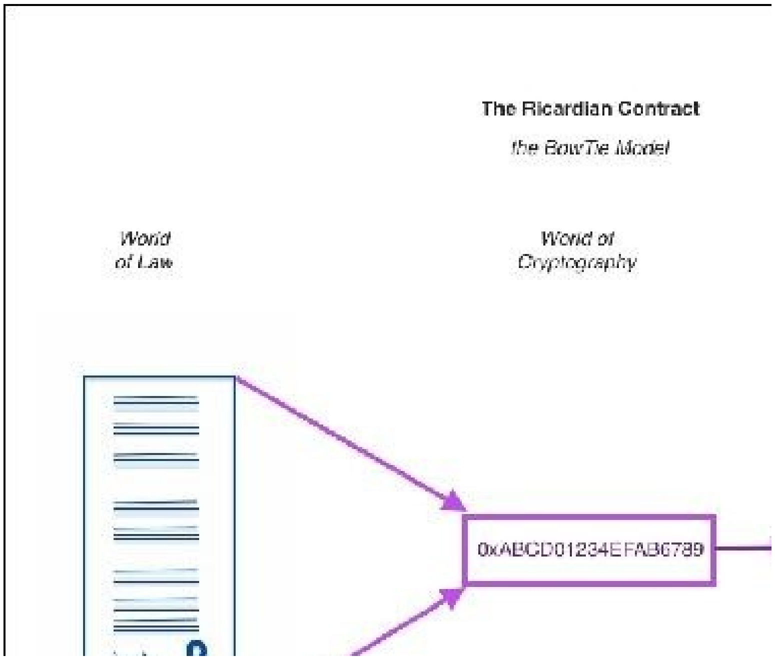
b) **Explain about Ricardian contracts.**

Ricardian contracts were originally proposed in the Financial Cryptography in 7 Layers paper by Ian Grigg in late 1990s. These contracts were used initially in a bond trading and payment system called Ricardo. The key idea is to write a document which is understandable and acceptable by both a court of law and computer software. They address the challenge of issuance of value over the Internet. It identifies the issuer and captures all the terms and clauses of the contract in a document in order to make it acceptable as a legally binding contract.

Based on the original definition by Ian Grigg, a Ricardian contract is a document that has several of the following properties:

- A contract offered by an issuer to holders
- A valuable right held by holders, and managed by the issuer
- Easily readable by people (like a contract on paper)
- Readable by programs (parseable, like a database)
- Digitally signed
- Carries the keys and server information
- Allied with a unique and secure identifier

The contracts are implemented by producing a single document that contains the terms of the contract in legal prose and the required machine-readable tags. This document is digitally signed by the issuer using their private key. This document is then hashed using a message digest function to produce a hash by which the document can be identified. This hash is then further used and signed by parties during the performance of the contract in order to link each transaction, with the identifier hash thus serving as evidence of intent. This is depicted in the diagram called a bowtie model. The diagram below shows the World of Law on the left hand side, origin. It is then hashed and the resultant message digest is used as an identifier throughout the World of Accountancy.



The World of Accountancy can basically represent any or multiple accounting, trading and information systems that are being used in a business to perform various business operations. The idea behind this flow is that the message digest generated by hashing the document is first used in a so called genesis transaction, or first transaction, and then used in every transaction as an identifier throughout the operational execution of the contract.This way, a secure link is created between the original written contract and every transaction in the World of Accounting.A Ricardian contract is different from a smart contract in the sense that a smart contract does not include any contractual document and is focused purely on the execution of the contract. A Ricardian contract, on the other hand, is more concerned with the semantic richness and production of a document that contains contractual legal prose.

The semantics of a contract can be divided into two types: operational semantics and denotational semantics. The first type defines the actual execution, correctness and safety of the contract, and the latter is concerned with the real-world meaning of the full contract. Some researchers have differentiated between smart contract code and smart legal contracts where a smart contract is only concerned with the execution of the contract and the second type encompasses both the denotational and operational semantics of a legal agreement. It makes sense to perhaps categorize smart contracts based on the difference between semantics, but it is better to consider smart contracts as a standalone entity that is capable of encoding legal prose and code (business logic) in it.

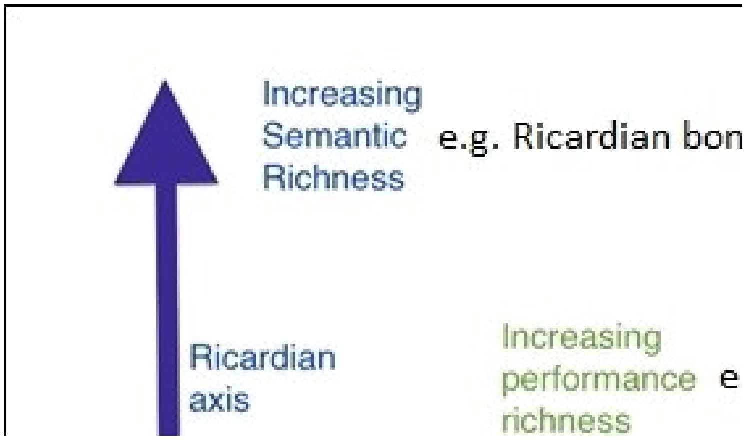


Diagram explaining performance v. semantics are orthogonal issues as described by Ian Grigg; slightly modified to show examples of different types of contracts on both axis. A smart contract is made up to have both of these elements (performance and semantics) embedded together, which completes an ideal model of a smart contract. A Ricardian contract can be represented as a tuple of three objects, namely Prose, parameters and code. Prose represents the legal contract in regular language; code represents the program that is a computer understandable representation of legal prose; and parameters join the appropriate parts of the legal contract to the equivalent code.

(OR)

7 a) **Analyse the key elements of the Ethereum blockchain.**

Ethereum is a decentralized blockchain platform that introduced the concept of smart contracts and decentralized applications (DApps). It was proposed by Vitalik Buterin in late 2013 and development began in early 2014, with the network going live on July 30, 2015. Ethereum's blockchain has several key elements that make it unique and powerful:

Decentralized Smart Contracts: Ethereum's most notable innovation is its ability to support smart contracts. These are self-executing contracts with the terms of the agreement directly written into code. Smart contracts allow for automated and trustless execution of agreements, reducing the need for intermediaries and potentially enabling a wide range of applications across industries.

Ether (ETH): Ether is Ethereum's native cryptocurrency. It serves as both a digital currency and a fuel for executing transactions and running smart contracts on the Ethereum network. Ether is also used to incentivize miners who secure the network and validate transactions.

EVM (Ethereum Virtual Machine): The Ethereum Virtual Machine is a runtime environment that executes smart contracts on the Ethereum network. It allows developers to write code in various programming languages and deploy it on the blockchain. The EVM abstracts the underlying complexities of the blockchain, making it easier for developers to create DApps.

Gas: Gas is a measure of computational effort required to execute operations or perform transactions on the Ethereum network. Each operation within a smart contract consumes a certain amount of gas, and users need to pay gas fees in Ether to cover these computational costs. Gas fees prevent network abuse and ensure that resources are used efficiently.

Decentralized Applications (DApps): DApps are applications built on top of the Ethereum blockchain that utilize smart contracts for their functionality. These applications can range from financial services and gaming to supply chain management and decentralized finance (DeFi) protocols.

Decentralized Autonomous Organizations (DAOs): DAOs are organizations that are governed by code and smart contracts on the Ethereum blockchain. They allow for decentralized decision-making and management, potentially eliminating the need for traditional hierarchical structures.

Immutable Blockchain: Like other blockchains, Ethereum's ledger is immutable, meaning that once data is recorded on the blockchain, it cannot be altered or deleted. This feature ensures data integrity and builds trust among participants.

Proof of Stake (PoS) Transition: Ethereum is in the process of transitioning from a Proof of Work (PoW) consensus mechanism to a Proof of Stake (PoS) mechanism. This change, known as Ethereum 2.0 or ETH 2.0, aims to improve scalability, reduce energy consumption, and make the network more environmentally friendly.

Interoperability: Ethereum has played a significant role in driving interoperability among various blockchain platforms. Initiatives like the Ethereum Name Service (ENS) and cross-chain solutions enable easier communication and data sharing between different blockchains.

Development Community: Ethereum has a large and active development community that continuously works on improving the platform, proposing and implementing upgrades, and building new applications. This community-driven approach contributes to the platform's evolution and innovation.

These key elements collectively contribute to Ethereum's position as a pioneering blockchain platform that has had a profound impact on the world of decentralized technologies and applications.

b) **Explain the concept of development of alt coins.**

Altcoin projects can be started very easily by simply forking the bitcoin or another coin's source code but this probably is not enough. When a new coin project is started, there are several things that need to be considered in order to ensure a successful launch and the coin's longevity. Usually, the code base is written in C++ as was the case with bitcoin but almost any language can be used to develop coin projects, for example Golang or Rust. Writing code or forking the code for an existing coin is the trivial part, the challenging issue is how to start a new currency so that new investors and users can be attracted to it. Generally, the following steps are taken in order to start a new coin project. From a technical point of view, in the case of forking the code of another coin, for example bitcoin, there are various parameters that can be changed to effectively create a new coin. These parameters are required to be tweaked(modified) or introduced in order to create a new coin.

These parameters can include but are not limited to the following.

Consensus Algorithms: There is a choice of consensus algorithm: Proof of Work (PoW) as used in bitcoin or Proof of Stake (PoS), as in Peercoin.

Hashing Algorithms: This is either SHA256, Scrypt, X11, X13, X15, or any other hashing algorithm that is adequate for use as a consensus algorithm.

Difficulty Adjustment Algorithms: Various options are available in this category to provide difficulty retargeting mechanisms. The most prominent examples are KGW, DGW, Nite's Gravity Wave, and DigiShield. Also all these algorithms can be tweaked based on requirements to produce different results; therefore many variants are possible.

Inter-Block Time: This is the time elapsed between the generation of each block. For bitcoin the blocks are generated every 10 minutes, for litecoin it's 2.5 minutes. Any value can be used but an appropriate value is usually between a few minutes; if the generation time is too fast it might destabilize the blockchain, if it's too slow it may not attract many users.

Block Rewards: A block reward is for the miner who solves the mining puzzle and is allowed to have a Coinbase transaction that contains the reward. This used to be 50 coins in bitcoin initially and now many altcoins set this parameter to a very high number; for example in Dogecoin it is 10,000, currently.

Reward Halving Rate: This is another important factor; in bitcoin it is halved every 4 years and now is set to 12.5 bitcoins. It’s a variable number that can be set to any time period or none at all depending on the requirements.

Block Size And Transaction Size: This is another important factor that determines how high or low the transaction rate can be on the network. Block sizes in bitcoin are limited to 1 MB but in altcoins it can vary depending on the requirements.

Interest Rate: This property applies only to PoS systems where the owner of the coins can earn interest at a rate defined by the network in return for the amount of coins that are held on the network as a PoS to protect the network.

Coin Age: This parameter defines how long the coin has to remain unspent in order for it to become eligible to be considered stake worthy.

Total Supply of Coins: This number sets the total limit of the coins that can ever be generated. For example in bitcoin the limit is 21 million, whereas in Dogecoin it's unlimited. This limit is fixed by the block reward and halving schedule discussed above. There are two options to create your own virtual currency: forking existing established cryptocurrency source code or writing a new one from scratch. The latter option is less popular but the first option is easier and has allowed the creation of many virtual currencies over the last few years. Fundamentally, the idea is that first a cryptocurrency source code is forked and then appropriate changes are made at different strategic locations in the source code to effectively create a new currency.

Unit-IV

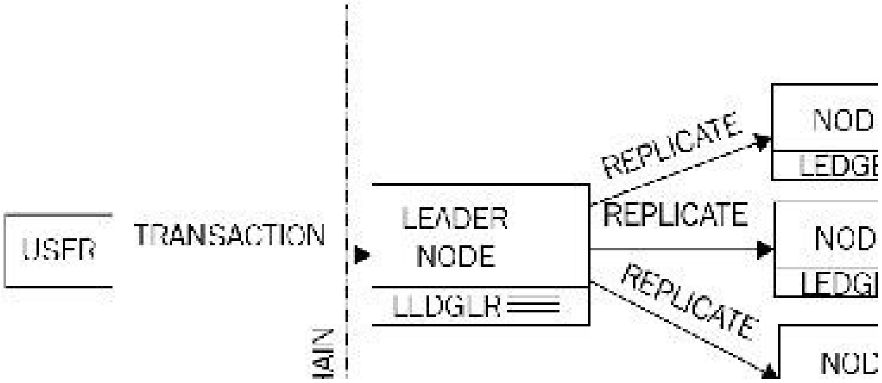
8 a) **Explain in detail about kadena block chain.**

Kadena is a recently-introduced private blockchain that has successfully addressed scalability and privacy issues in blockchain systems. A new Turing incomplete language called Pact has also been introduced with Kadena that allows the development of smart contracts. A key innovation in Kadena is its Scalable BFT consensus algorithm, which has the potential to scale to thousands of nodes without performance degradation. Scalable BFT is based on the original Raft algorithm and is a successor of Tangaroa and Juno. Tangaroa, which is a name given to an implementation of Raft with fault tolerance (a BFT Raft), was developed to address the availability and safety issues that arose from the behavior of byzantine nodes in the Raft algorithm. Juno was a fork of Tangaroa that was developed by JPMorgan. Both of these proposals have a fundamental limitation - they cannot scale while maintaining a high level of high performance. Private blockchains have the more desirable property of maintaining high performance as the number of nodes increase, but the aforementioned proposals lack this feature. Kadena solves this issue with its proprietary Scalable BFT algorithm, which is expected to scale up to thousands of nodes without any performance degradation.

Moreover, confidentiality is another important aspect of Kadena that enables privacy of transactions on the blockchain. This is achieved by using a combination of key rotation, symmetric on-chain encryption, incremental hashing, and Double Ratchet protocol. Key rotation is used as a standard mechanism to ensure security of the private blockchain. It is used as a best practice to thwart any attacks if the keys have been compromised, by periodically changing the encryption keys. Symmetric on chain encryption allows encryption of transaction data on the blockchain. These transactions can be automatically decrypted by the participants of a particular private transaction. Double Ratchet protocol is used to provide key management and encryption functions. Scalable BFT consensus protocol ensures that adequate replication and consensus has been achieved before smart contract execution.

Consensus is achieved by following the process described below:

- First, a new transaction is signed by the user and broadcasted over the blockchain network, which is picked up by a leader node that adds it to its immutable log.
- At this point, an incremental hash is also calculated for the log.
- Incremental hash is a type of hash function that basically allows computation of hash messages in the scenario where, if a previous original message which is already hashed is slightly changed, then the new hash message is computed from the already existing hash.
- This scheme is quicker and less resource intensive compared to a conventional hash function where an altogether new hash message is required to be generated even if the original message has only changed very slightly.
- Once the transaction is written to the log by the leader node, it signs the replication and incremental hash and broadcasts it to other nodes.
- Other nodes, after receiving the transaction, verify the signature of the leader node, add the transaction into their own logs, and broadcast their own calculated incremental hashes (quorum proofs) to other nodes.
- Finally, the transaction is committed into the ledger permanently after an adequate number of proofs are received from other nodes.



Once the consensus is achieved, smart contract execution can start and takes a number of steps, as follows:

1. First, the signature of the message is verified.
2. Pact smart contract layer takes over.
3. Pact code is compiled.
4. The transaction is initiated and executes any business logic embedded within smart contract. In case of any failures, an immediate rollback is initiated that reverts that state back to what it was before the execution started.
5. Finally, the transaction completes and relevant logs are updated.

b) **Explain the following**

i. Quorum ii. Storj

i. Quorum

This is a blockchain solution built by enhancing the existing Ethereum blockchain. There are several enhancements such as transaction privacy and a new consensus mechanism that has been introduced in Quorum. Quorum has introduced a new consensus model known as QuorumChain, which is based on a majority voting and time based mechanism. Another feature called Constellation is also introduced which is a general purpose mechanism for submitting information and allows encrypted communication between peers. Furthermore, permissioning at node level is governed by smart contracts. It also provides a higher level of performance compared to public Ethereum blockchains.

Several components make up the Quorum blockchain ecosystem.

Transaction manager

This component enables access to encrypted transaction data. It also manages local storage and communication with other Transaction managers on the network.

Crypto Enclave

As the name suggests, this component is responsible for providing cryptographic services to ensure transaction privacy. It is also responsible for performing key management functions.

QuorumChain

This is the key innovation in Quorum. It is a Byzantine Fault-tolerant consensus mechanism which allows verification and circulation of votes via transactions on the blockchain network. In this scheme, a smart contract is used to manage the consensus process and nodes can be given voting rights to vote on which new block should be accepted. Once an appropriate number of votes is received by the voters, the block is considered valid. Nodes can have two roles, namely Voter or Maker. The Voter node is allowed to vote, whereas the Maker node is the one that creates a new block. A node can have either rights, none or only one.

Network manager

This component provides an access control layer for the permissioned network. A node in the quorum network can take several roles, for example, a Maker node that is allowed to create new blocks. Transaction privacy is provided using cryptography and the concept that certain transactions are meant to be viewable only by their relevant participants. As it allows both public and private transactions on the blockchain, the state database has been divided into two databases representing private and public transactions. As such, there are two separate Patricia-Merkle trees that represent the private and public state of the network.

ii. Storj

Existing models for cloud-based storage are all centralized solutions, which may or may not be as secure as users expect them to be. There is a need to have a cloud storage system that is secure, highly available, and above all decentralized. Storj aims to provide blockchain based, decentralized, and distributed storage. It is a cloud shared by the community instead of a central organization. It allows execution of storage contracts between nodes that act as autonomous agents. These agents (nodes) execute various functions such as data transfer, validation, and perform data integrity checks.

The core concept is based on Distributed Hash Tables (DHT) -Kademlia, however this protocol has been enhanced by adding new message types and functionalities in Storj. It also implements a peer to peer publish/subscribe (pub/sub) mechanism known as Quasar, which ensures that messages successfully reach the nodes that are interested in storage contracts. This is achieved via a bloom filter-based storage contract parameters selection mechanism called topics. Storj stores files in an encrypted format spread across the network. Before the file is stored on the network, it is encrypted using AES-256-CTR symmetric encryption and is then stored piece by piece in a distributed manner on the network. This process of dissecting the file into pieces is called sharding and results in increased availability, security, performance, and privacy of the network. Also if a node fails the shard is still available because by default a single shard is stored at three different locations on the network. It maintains a blockchain, which serves as a shared ledger and implements standard security features such as public/private key cryptography and hash functions similar to any other blockchain. As the system is based on hard drive sharing between peers, anyone can contribute by sharing their extra space on the drive and get paid with Storj's own cryptocurrency called Storjcoinx (SJCX).

(OR)

9 a) **Explain in detail about ripple network.**

Introduced in 2012, Ripple is a currency exchange and real-time gross settlement system. In Ripple, the payments are settled without any waiting as opposed to traditional settlement networks, where it can take days for settlement. It has a native currency called Ripples (XRP). It also supports non-XRP payments. This system is considered similar to an old traditional money transfer mechanism known as Hawala. This system works by making use of agents who take the money and a password from the sender, then contact the payee's agent and instruct them to release funds to the person who can provide the password. The payee then contacts the local agent, tells them the password and collects the funds. An analogy to the agent is Gateway in Ripple.

The Ripple network is composed of various nodes that can perform different functions based on their type.

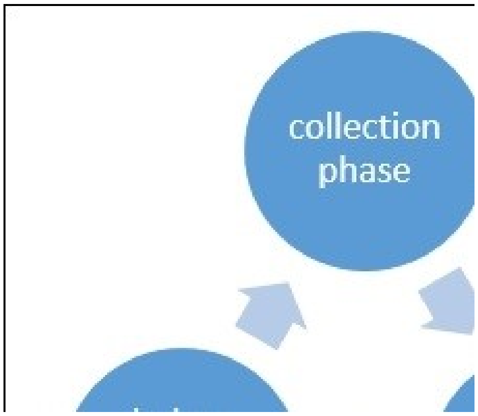
- First, user nodes: these use in payment transactions and can pay or receive payments.
- Second, validator nodes: these participate in the consensus mechanism. Each server maintains a set of unique nodes, which it needs to query while achieving consensus.
- Nodes in the unique node List (UNL) are trusted by the server involved in the consensus mechanism and will accept votes only from this list of unique nodes.

Ripple is sometimes not considered truly decentralized as there are network operators and regulators involved. However it can be considered decentralized due to the fact that anyone can become part of the network by running a validator node. Moreover, the consensus process is also decentralized because any changes proposed to made on the ledger have to be decided by following a scheme of super majority voting. Ripple maintains a global distributed ledger of all transactions that is governed by a novel low-latency consensus algorithm called Ripple Protocol Consensus Algorithm (RPCA). The consensus process works by achieving an agreement on the state of an open ledger containing transactions by seeking verification and acceptance from validating servers in an iterative manner until an adequate number of votes are achieved. Once enough votes are received (super majority, initially 50% and gradually increasing with each iteration up to at least 80%) the changes are validated and the ledger is closed. At this point, an alert is sent to the whole network indicating that the ledger is closed.

In summary, the consensus protocol is a three-phase process.

- First, the collection phase, where validating nodes gather all transactions broadcasted on the network by account owners and validate them.
- Transactions, once accepted, are called candidate transactions and can be accepted or rejected based on the validation criteria.
- Then the consensus process starts, and after achieving it the ledger is closed.
- This process runs asynchronously every few seconds in rounds and, as result, the ledger is

opened and closed (updated) accordingly.



In a Ripple network there are a number of components that work together in order to achieve consensus and form a payment network.
These components are discussed individually below:
Server: This component serves as a participant in the consensus protocol. Ripple server software is required in order to be able to participate in consensus protocol.
Ledger: This is a main record of balances of all accounts on the network. A ledger contains various elements such as ledger number, account settings, transactions, timestamp, and a flag that indicates validity of the ledger.
Last closed ledger: A ledger is closed once consensus is achieved by validating nodes.
Open ledger: This is a ledger that has not been validated yet and no consensus has been reached about its state. Each node has its own open ledger, which contains proposed transactions.
Unique node list: This is a list of unique trusted nodes that a validating server uses in order to seek votes and subsequent consensus.
Proposer: As the name suggests, this component proposes new transactions to be included in the consensus process. It is usually a subset of nodes (UNL defined above) that can propose transactions to the validating server.

b) **Explain the following**

i. Stellar ii. Rootstock

i. Stellar

Stellar is a payment network based on blockchain technology and a novel consensus model called Federated Byzantine Agreement (FBA). FBA works by creating quorums of trusted parties. Stellar Consensus Protocol (SCP) is an implementation of FBA. Key issues identified in the Stellar whitepaper are the cost and complexity of current financial infrastructure. This limitation warrants the need for a global financial network that addresses these issues without compromising the integrity and security of the financial transaction. This requirement has resulted in the invention of Stellar Consensus Protocol (SCP) which is a provably safe consensus mechanism.
It has four main properties:

- *decentralized control*, which allows participation by anyone without any central party;
- *low latency*, which addresses the much desired requirement of fast transaction processing;
- *flexible trust*, which allows users to choose which parties they trust for a specific purpose.
- finally, *asymptotic security*, which makes use of digital signatures and hash functions for providing the required level of security on the network.

The Stellar network allows transfer and representation of the value of an asset by its native digital currency, called Lumens, abbreviated as XLM. Lumens are consumed when a transaction is broadcasted on the network, which also serves as a deterrent against **Denial of Service** (**DOS**) attacks. At its core, the Stellar network maintains a distributed ledger that records every transaction and is replicated on each Stellar server. The consensus is achieved by verifying transactions between servers and updating the ledger with updates. The Stellar ledger can also act as a distributed exchange order book by allowing users to store their offers to buy or sell currencies.

ii. Rootstock

Before discussing Rootstock in detail, it's important to define and introduce some concepts that are fundamental to the design of Rootstock. These concepts include sidechains, drivechains, and two-way pegging. The concept of the sidechain was originally developed by Blockstream. Two way pegging is a mechanism by which value (coins) can transfer between one blockchain to another and vice versa. There is no real transfer of coin between chains. The idea revolves around the concept of locking the same amount and value of coins in a bitcoin blockchain (main chain) and unlocking the equivalent amount of tokens in the secondary chain.

Sidechain

This is a blockchain that runs in parallel with a main blockchain and allows transfer of value between them. This means that tokens from one blockchain can be used in the sidechain and vice versa. This is also called a pegged sidechain because it supports two-way pegged assets.

Drivechain

This is a relatively new concept, where control on unlocking the locked bitcoins (in mainchain) is given to the miners who can vote when to unlock them. This is in contrast to sidechains, where consensus is validated though Simple payment verification mechanism in order to transfer the coins back to the mainchain.

Rootstock is a smart contract platform which has a two-way peg into bitcoin blockchain. The core idea is to increase the scalability and performance of the bitcoin system and enable it to work with smart contracts. Rootstock runs a Turing complete deterministic virtual machine called Rootstock Virtual Machine (RVM). It is also compatible with the Ethereum virtual machine and allows solidity-compiled contracts to run on Rootstock. Smart contracts can also run under the time-a tested security of bitcoin blockchain. The Rootstock blockchain works by merge mining with bitcoins. This allows RSK blockchain to achieve the same security level as bitcoin. This is especially true for preventing double spends and achieving settlement finality. It allows scalability, up to 100 transactions per second.