20IT702/PE4A

Hall Ticket Number:

IV/IV B.Tech (Regular) DEGREE EXAMINATION

January, 2025 — **Information Technology**

Seventh Semester — **Blockchain Technologies**

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

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

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

1	a)	Define Blockchain Technology. **Ans:** Blockchain is a decentralized digital ledger that securely stores records across a network of computers in a way that is transparent, immutable, and resistant to tampering.	1
	b)	Who invented bitcoin? Which year? **Ans**: bitcoin was invented by Satoshi Nakamoto. in 2008	1
	c)	Define CAP theorem. **Ans**: The CAP theorem is a theorem that describes the nature of blockchain. The CAP theorem states that it is impossible to satisfy the three properties of "Consistency," "Availability," and "Partition-tolerance" at the same time when operating a web service.	1
	d)	What is the role of nodes in the Bitcoin network? **Ans**: A node plays a vital role by validating transactions, maintaining the blockchain and keeping the network secure.	1
	e)	What is side chain? **Ans**: Sidechains are separate blockchain networks that connect to a parent blockchain, aiming to enhance its scalability and interoperability.	1
	f)	List out various security services provided by cryptography. **Ans**: data confidentiality, data integrity, data authentication, data authorization (or access control), and non-repudiation	1
	g)	What is ORACLE? How it is used in smart contract? **Ans**: It is a third-party service that provides trusted information to smart contracts from outside the blockchain. It allows contracts to access data from the real world.	1
	h)	Define avalanche affect. **Ans**: The avalanche effect means that a small change in the input of a cryptographic system causes a big and unpredictable change in the output.	1
	i)	What is CLARK. Where it is used? **Ans**: CLARK is a digital library that hosts diverse cybersecurity learning objects. It is used in creating of blocks.	1
	j)	What are the main properties of Storj? **Ans**: Main Properties includes, 1. Security 2. Token 3. Decentralized 4. Buy and sell	1
	k)	List the components of QUORUM block chain. **Ans**: 1. Permissions management 2. Private & public transactions 3. Constellation 4. Ethereum based distributed ledger system.	1
	l)	Define smart contract. **Ans**: A smart contract is a computer program or a transaction protocol that is intended to automatically execute, control or document events and actions.	1
	m)	What is the size of compressed and uncompressed public Keys. **Ans**: size of compressed public Keys is 33 bytes and uncompressed public Keys is 65 bytes.	1
	n)	What is Colored coin? **Ans:** This is a way to represent real-world assets or other virtual assets on a bitcoin blockchain.	1

UNIT -I

2 a) Write about decentralization using block chain. 7M

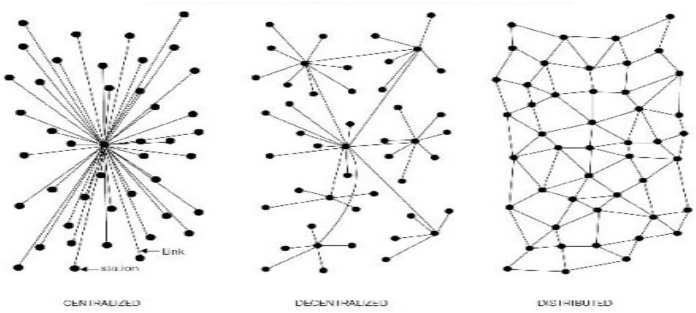
Ans: **Decentralization using blockchain**

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 provide 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.



Methods of decentralization

There are two methods: Disintermediation Example: Imagine you want to send money to your friend in another country. You go to a bank that will transfer your money to the bank in the country of your choice for a fee. In this case, the bank keeps a central database that is updated, confirming that you have sent the money. With blockchain technology, it is possible to send this money directly to your friend without the need for a bank. All you need

is the address of your friend on the blockchain. This way, the intermediary is no longer required and decentralization is achieved by disintermediation. It is debatable how practical decentralization is in the financial sector by disintermediation due to heavy regulatory and compliance requirements. Nevertheless, this model can be used not only in finance but also in many other different industries.

Through competition

In this method, a group of service providers compete with each other in order to be selected for the provision of services by the system. This does not achieve complete decentralization, but ensures that an intermediary or service provider is not monopolizing the service. Smart contracts can choose an external data provider from a large number of providers based on their reputation, previous score, reviews, and quality of service. This will not result in full decentralization. An environment of competition is among service providers, whereby they compete with each other to become the data provider of choice.

b) Write about different types of block chain. 7M

Ans: Types of blockchain

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.

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.

Consensus is the backbone of a blockchain and provides decentralization of control as a result through an optional process known as mining.

The choice of consensus algorithm is also governed by the type of blockchain in use.

(OR)

3 a) Explain The Key Features of a Blockchain in Detail. 7M

Ans**: Features of A Blockchain**

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.

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.

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.

b) Explain generic elements of block chain. 7M

Ans: Generic elements of a blockchain

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.

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.

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, and the role of each participant. 7M

Ans**: Bitcoin**

In 2008, a paper on bitcoin, *Bitcoin: A Peer-to-Peer Electronic Cash System* was written by *Satoshi Nakamoto*.

The first key idea introduced in the paper was that purely peer-to-peer electronic cash that does need an intermediary bank to transfer payments between peers. Bitcoin is built on decades of cryptographic research such as the research in Merkle trees, hash functions, public key cryptography, and digital signatures. Moreover, ideas such as BitGold, b-money, hashcash, and cryptographic time stamping provided the foundations for bitcoin invention. All these technologies are cleverly combined in bitcoin to create the world's first decentralized currency. The key issue that has been addressed in bitcoin is an elegant solution to the Byzantine Generals problem along with a practical solution of the double-spend problem. The value of bitcoin has increased significantly since 2011. The regulation of bitcoin is a controversial subject and as much as it is a libertarian's dream, law enforcement agencies and governments are proposing various regulations to control it, such as BitLicense issued by New York's state department of financial services. This is a license issued to businesses that perform activities related to virtual currencies. The growth of Bitcoin is also due to so-called *Network Effect*. Also called demand-side economies of scale, it is a concept that basically means more users who use the network, the more valuable it becomes.

Bitcoin definition

Bitcoin can be defined in various ways;

It's a protocol, a digital currency, and a platform.

It is a combination of peer-to-peer network, protocols, and software that facilitate the creation and usage of the digital currency named bitcoin.

Note that Bitcoin with a capital *B* is used to refer to the Bitcoin protocol, whereas bitcoin with a lowercase *b* is used to refer to bitcoin, the currency.

KEYS AND ADDRESSES

Elliptic curve cryptography is used to generate public and private key pairs in the Bitcoin network. The bitcoin address is created by taking the corresponding public key of a private key and hashing it twice, first with the SHA256 algorithm and then with RIPEMD160.

The resultant 160-bit hash is then prefixed with a version number and finally encoded with a Base58Check encoding scheme. The bitcoin addresses are 26-35 characters long and begin with

digit 1 or 3. A typical bitcoin address looks like a string shown here: 1ANAguGG8bikEv2fYsTBnRUmx7QUcK58wt This is also commonly encoded in a QR code for easy sharing.

PUBLIC KEYS IN BITCOIN

In public key cryptography, public keys are generated from private keys.

Bitcoin uses ECC based on the SECP256K1 standard. A private key is randomly selected and is 256-bit in length. Public keys can be presented in an uncompressed or compressed format.

Public keys are basically *x* and *y* coordinates on an elliptic curve and in an uncompressed format and are presented with a prefix of 04 in a hexadecimal format. *X* and *Y* coordinates are both 32-bit in length. In total, the compressed public key is 33 bytes long as compared to 65 bytes in the uncompressed format.

PRIVATE KEYS IN BITCOIN

Private keys are basically 256-bit numbers chosen in the range specified by the SECP256K1 ECDSA recommendation.

Any randomly chosen 256-bit number from 0x1 to 0xFFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFE BAAE DCE6 AF48 A03B BFD2 5E8C D036 4140 is a valid private key.

Private keys are usually encoded using Wallet Import Format (WIF) in order to make them easier to copy and use. WIF can be converted into private key and vice versa. The steps are described here.

Transactions

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 Satoshi's. 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.

b) Explain in detail about asymmetric cryptography. 7M

Ans: Asymmetric cryptography

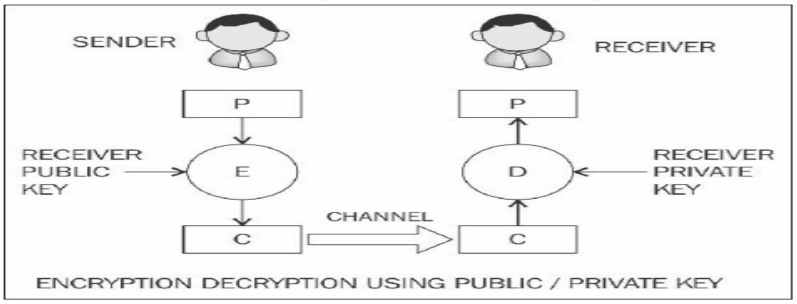
The key that is used to encrypt the data is different from the key that is used to decrypt the data.

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.

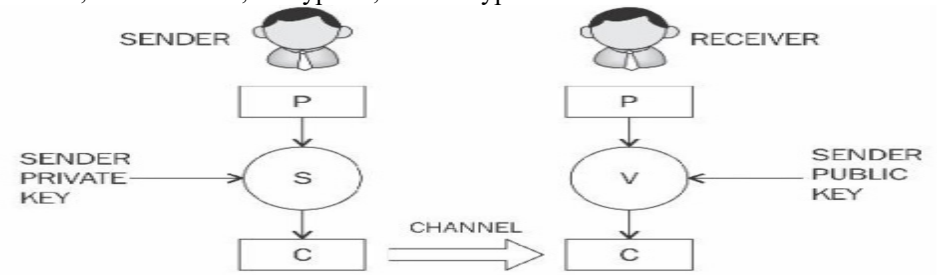
The diagram explains how a sender encrypts the data using a recipient's public key and is then transmitted over the network to the receiver.

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.

Another diagram shows how public key cryptography can be used to verify the integrity of the received message by the receiver.
In this model, the sender signs the data using their private key and transmits the message across to the receiver.
Once the message is received on the receiver's side, it can be verified for its integrity by the sender's public key.
Note that there is no encryption being performed in this model. This model is only used for message authentication and validation purposes:
Security mechanisms offered by public key cryptosystem include key establishment, digital signatures, identification, encryption, and decryption

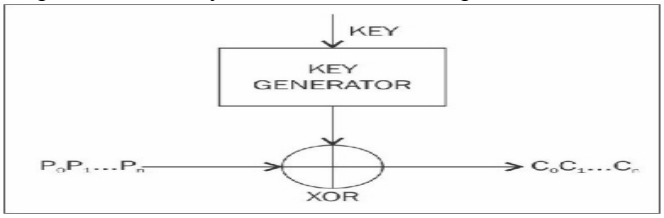


Key establishment mechanisms are concerned with the design of protocols that allow setting up of keys over an insecure channel.
Non-repudiation service, a very desirable property in many scenarios, can be provided using digital signatures.
Sometimes, it is important to not only authenticate a user, but 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.

5 a) Write in detail about symmetric cryptography. 7M

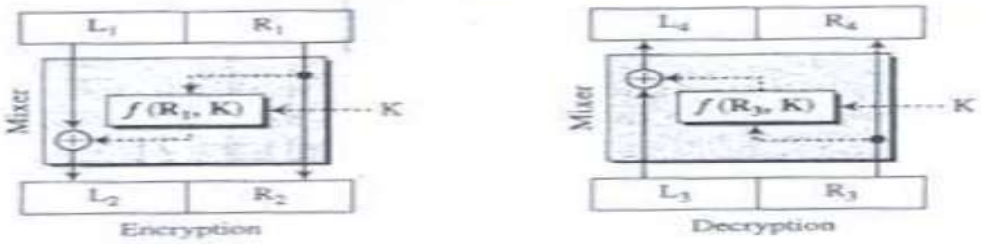
Ans: **Symmetric cryptography**

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.
Data Encryption Standard
DES, Advanced Encryption Standard (AES) are common examples of block ciphers, whereas RC4 and A5 are commonly used stream 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
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.
Confusion makes the relationship between the encrypted text and plaintext complex.
This is achieved by substitution in practice. For example, 'A' in plain text is replaced by 'X' in encrypted text.
In modern cryptographic algorithms, substitution is performed using lookup tables called S-boxes.



The diffusion property spreads the plain text statistically over the encrypted data.
It ensures that even if a single bit is changed in the input text, it results in changing at least half (on average) of the bits in the cipher text.
Confusion is required to make finding the encryption key very difficult even if many encrypted and decrypted data pairs are created using the same key.
In practice, this is achieved by transposition or permutation.
A key advantage of using Fiestel cipher is that encryption and decryption operations are almost identical and only require a reversal of the encryption process in order to achieve decryption.

b) Explain about RSA algorithm. 7M
Ans: **RSA**

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: $ed = 1 \bmod (p-1)(q-1)$
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: $C = P^e \ mod \ n$
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: $P = C^d \ mod \ n$
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. 7M

Ans: **Extended protocols on top of bitcoin**

For various other purposes instead of just as a virtual currency.
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 include 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, counter block, 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.

b) Analyse the key elements of the Ethereum blockchain 7M

Ans: Ethereum is a decentralized global software platform powered by blockchain technology. It is most commonly known by investors for its native cryptocurrency, ether (ETH), and by developers for its use in blockchain and decentralized finance application development.
Anyone can use Ethereum—it's designed to be scalable, programmable, secure, and decentralized to create any secured digital technology. Its token is designed to pay for work done supporting the blockchain, but participants can also use it to pay for tangible goods and services if accepted.

Ethereum uses a blockchain, which is a distributed ledger (like a database). Information is stored in blocks, each containing encoded data from the block before it and the new information. This creates an encoded chain of information that cannot be changed. Throughout the blockchain network, an identical copy of the blockchain is distributed. Each cell, or block, is created with new ether tokens awarded to the validator for the work required to validate the information in one block and propose a new one. The ether is assigned to the validator's address. Once a new block is proposed, it is validated by a network of automated programs that reach a consensus on the validity of transaction information. On the Ethereum blockchain, consensus is reached after the data and hash are passed between the consensus layer and the execution layer. Enough validators must demonstrate that they all had the same comparative results, and the block becomes finalized.

Proof-of-Stake Validation Process

Proof-of-stake differs from proof-of-work in that it doesn't require the energy-intensive computing referred to as mining to validate blocks. It uses a finalization protocol called Casper-FFG and the algorithm LMD Ghost, combined into a consensus mechanism called Gasper. Gasper monitors consensus and defines how validators receive rewards for work or are punished for dishonesty or lack of activity. Ethereum. Solo validators must stake 32 ETH to activate their validation ability. Individuals can stake smaller amounts of ETH, but they are required to join a validation pool and share any rewards. A validator creates a new block and attests that the information is valid in a process called attestation. The block is broadcast to other validators called a committee, which verifies it and votes for its validity. Validators who act dishonestly are punished under proof-of-stake. Those who attempt to attack the network are identified by Gasper, which flags the blocks to accept and reject based on the validators' votes. Dishonest validators are punished by having their staked ETH burned and removed from the network. "Burning" is the term for sending crypto to a wallet without private keys, effectively taking it out of circulation.

Ethereum's transition to the proof-of-stake protocol, which enabled users to validate transactions and mint new ETH based on their ether holdings, was part of a significant upgrade to the Ethereum platform. However, Ethereum now has two layers. The first layer is the execution layer, where transactions and validations occur. The second layer is the consensus layer, where attestations and the consensus chain are maintained. The upgrade added capacity to the Ethereum network to support its growth, which will eventually help to address chronic network congestion problems that have driven up gas fees

7 a) Explain about Ricardian contracts. 7M

Ans: **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

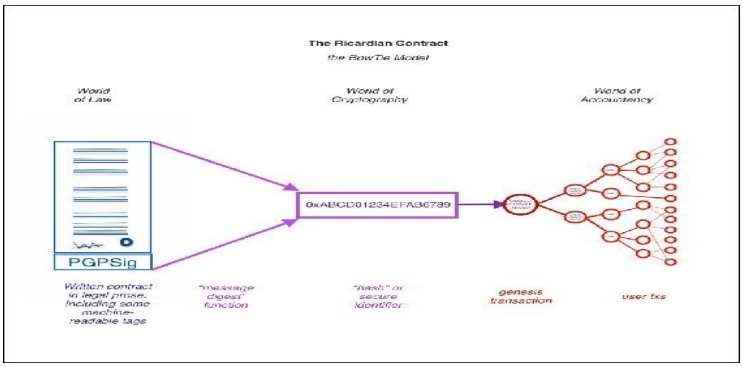
Carries the keys and server information

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 below, usually called a *bowtie* model.

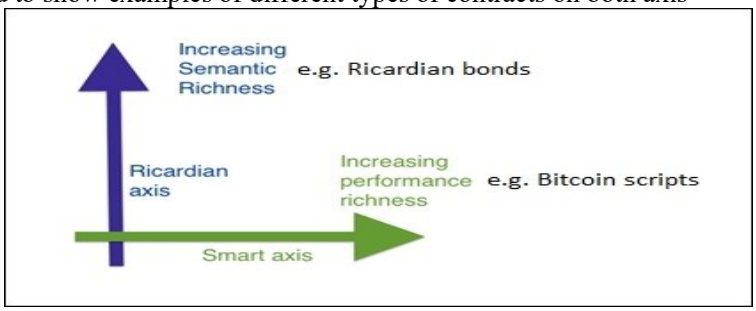
The diagram below shows the World of Law on the left-hand side, origin.

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.
At bitcoin, a very simple implementation of a smart contract can be observed which is fully oriented towards the execution of the contract, whereas a Ricardian contract is more geared towards producing a document that is understandable by humans, with some parts that a computer program can understand.
This can be viewed as legal semantics vs operational performance (semantics vs performance) as shown in the following diagram.
This was originally proposed by *Ian Grigg* in his paper *On the intersection of Ricardian and smart contracts*.
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



b) Explain the history and definition of smart contracts? 7M
Ans: **History**

Smart contracts were first theorized by *Nick Szabo* in the late 1990s, but it was almost 20 years before the true potential and benefits of them were truly appreciated.
Smart contracts are described by *Szabo* as follows:
"A smart contract is a computerized transaction protocol that executes the terms of a contract". The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both

malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs."
This idea of smart contracts was implemented in a limited fashion in bitcoin in 2009, over a peer-to-peer network where users do not necessarily trust each other and there is no need for a trusted intermediary.

Definition

There is no consensus on a standard definition of smart contracts.
It is essential to define what a smart contract is, and the following is the author's attempt to provide a generalized definition of a smart contract.
A smart contract is a secure and unstoppable computer program representing an agreement that is automatically executable and enforceable. Smart contract is in fact a computer program that is written in a language that a computer or target machine can understand. Also, it encompasses agreements between parties in the form of business logic. Another key idea is that smart contracts are automatically executed when certain conditions are met. They are enforceable, which means that all contractual terms are executed as defined and expected, even in the presence of adversaries. It is possible to execute contract terms without requiring any mediation. It should be noted that true smart contracts should not rely on traditional methods of enforcement. Instead, they should work on the principle that "*code is law".* Meaning that there is no need for an arbitrator or a third party to control or influence the execution of the smart contract.

Smart contracts are self-enforcing as opposed to legally enforceable. This might be regarded as a libertarian's dream, but it is entirely possible, and is in line with the true spirit of smart contracts. They are secure and unstoppable. Means that these computer programmers are required to be designed in such a fashion that they are fault tolerant and executable in reasonable amount of time. These programmers should be able to execute and maintain a healthy internal state, even if external factors are unfavourable. For example, imagine a normal computer programmed which is encoded with some logic and executes according to the instruction coded within it, but if the environment it is running in or external factors it relies on deviate from the normal or expected state, the programmer may react arbitrarily or simply abort. It is important that smart contracts are immune to external factors. Smart contracts usually operate by managing their internal state using a state machine model. This allows development of an effective framework for programming smart contracts, where the state of a contract is advanced further based on some predefined criteria and conditions. There is also on-going debate on the question of whether code is acceptable as a contract in a court of law. This is totally different in presentation from traditional legal prose, albeit they do represent and enforce all contractual clauses but a court of law does not understand code. This raises several questions around how a smart contract can be legally binding. Smart contracts are inherently required to be deterministic in nature. This property will allow a smart contract to be run by any node on a network and achieve the same result. If the result differs even slightly between nodes, consensus cannot be achieved and the paradigm of distributed consensus on blockchain can fail. It is also desirable that the contract language itself is deterministic thus ensuring the integrity and stability of the smart contracts. Should not produce varied results on different nodes.

UNIT-IV

8 a) Explain in detail about kadena block chain. 7M

Ans: Kadena

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.

b) Explain in detail about ripple network. 7M

Ans: RIPPLE

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.

9 Explain the following
i. Stellar ii. Rootstock iii. Quorum iv. Storj 14M

Ans: 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, drive chains, and two-way pegging. The concept of the sidechain was originally developed by Block stream. 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 number 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. Drive chain 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.

III. 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, per missioning 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 right, none or only one.

IV. 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).

Prepared By, HOD, IT
Dr. P. Sreedhar, Asst. Prof
K. Sai Prasanth, Asst. Prof