Page No.
Date

Assignment No. 1.

Q1. Explain DLT in detail with its benefits and differentiate between DLT Vs Blockchain.

Ans→ - DLT stands for distributed Ledger Technology, which is decentralized system for recording transaction and managing data in secure
  - transparent
  - tamper-proof way.

- DLT is underlying technology behind popular crypto-currencies like Bitcoin and Etheram.
- DLT works by creating a distributed network of nodes that all have taken place.
- Each transaction is validated by network, and once it is verified, it is added to ledger.
- Because the ledger is distributed accross many nodes, it is very difficult for any one person or group to alter or manipulate the ledger.
- Benefits of DLT :-
  - high level of security and transparency, as all transacⁿ are validated and recorded on ledger.
  - It eliminates the need for intermediaries like banks, which can reduce transaction fees and increase efficiency
  - It enables faster and more secure cross-border transacⁿ as there is no need to go through multiple intermediaries
  - It can be used in wide range of industries beyond just finance, such as supply chain management and healthcare.

Page No.
Date

Types of Distributed ledger technology

The distributed ledger can be categorizes into three categories
- Permissioned DLT
- Permissionless DLT
- Hybrid DLT

1) Permissioned DLT → nodes have to take permission from central authority to access or makes any changes in network.
→ mostly these types of permissions include identify verification.

2) Permissionless DLT → There is no central authority to validate transactions, rather existing nodes are collectively responsible for validating the transactions.
→ various consensus meehanism are used to validate transaction based on predefined algorithm.

3) Hybrid DLT → It is combined with both permissionless and permissioned DLTS and can benefit from both of them.

	DLT	Blockchain
1.	In Distributed ledger, the blocks can be organized in different form	In blockchain, blocks are added in form of chain.
2.	It is more scalable because it does not need power of work consensus mechanism for validation of each transaction.	It is subset of DLT, power of work consensus mechnism adds more functionalities and security.
3.	It does not require any tokens or digital currency	In blockchain, tokens must be considered while working with blockchain
4.	It doesn't require any specific sequence of data	All blocks are arranged in particular series.
5.	Trust among these participating nodes is high	Trust among participating nodes is less than DLT. Decision making power can be on one hand.

Page No.
Date

Q2. Short note on - i) Consensus mechanism
ii) The genesis block.

i) Consensus Mechanism.
- Consensus mechanism is fault tolerance mechanism.
- It is used in computer and blockchain system to achieve necessary agreement on single state of network among multiple nodes.
- It is useful in record keeping.

Types of mechanism:-
- proof of work. (POW)
- proof of stake (POS)
- proof of capacity (POC)
- proof elapsed time [POET)

1) Proof of work :- Required as stakeholder node to prove that work is done
- submit by them
- certified by them
- to receive, rights to add new transaction in blockchain.

2) Proof of stake
- It is most common algorithm/ mechanism
- It is low cost and low energy consuming.
- It is an alternative of proof of work.

3) Proof of capacity - allows sharing of memory space of all nodes in blockchain network.

Page No.
Date

4) Proof of elapsed Time [POET] → It encrypts the passage of time cryptographically to reach an agreement without spending many resources.

ii) The genesis block.

→ A Genesis block refers to first block in blockchain and is usually hardcoded into its application's s/w.

→ A blockchain contains growing lists of "blocks" securely linked together by cryptography thus forming chain of block.

→ Each block of crypto asset contains referential data from previous one and derives its value from its predecessor.

→ The genesis block, thus, refers to first block (block 0 or 1) of new blockchain, to which all of the subsequent blocks are attached.

→ It has special significance, as they form the very foundation of blockchain and often contain interesing stories or hidden meaning.

→ It is unique as it is the only block in blockchain that does not reference of predecessor block, and in almost all cases, the first mining rewards it unlocks are unspendable.

Page No
Date

Q3 Explain bitcoin keys in details.

There are mainly two types of keys in bitcoin.

- Public key
- Private key

Bitcoin keys are digital codes that are used to access and manage Bitcoin funds. There are two types of Bitcoin keys

1) Public keys → String of alphanumeric characters that are used to receive Bitcoin funds.
   - → Anyone can send Bitcoin to public key, and it can be shared with others without any risk of theft.
   - → Public keys are generated from mathematical algorithm known as eliptic curve multiplication.

2) Private keys → String of alphanumeric characters that are used to access and manage bitcoin funds.
   - → private keys are secret and should never be shared with anyone.
   - → They are used to digitally sign transactions which are then broadcast to the bitcoin network for verification.
   - → private keys are generated from corresponding public key using a process called cryptographic hashing.
   - → It is important to keep private keys secure as anyone who has access to private keys can spend the bitcoin associated with it.

Page No.
Date

Q 4 How bitcoin mining works and Explain different types of wallets.

→ Bitcoin mining.

Bitcoin mining is reffered to as method of verifying bitcoin transaction on blockchain and generating new bitcoin just like central bank printing new fiat currency.

→ Process of bitcoin mining.

- The node uses computational power of CPU to process the transaction
- It initiates transaction by providing detailed list of
  - no of bitcoin sent
  - address
  - private key – generated digitial sign.

  is present to miner in network
- Miner verifies the transaction checks sufficient balance carried out transaction.
- Faster the CPU greater the chances miner get rewarded.
- Miner's main role is to provide CPU
- transaction will be verified. After verification no. of transaction broadcasted to network to copy or download block.
- Block saved to form sequential blockchain.
- Then miner must have updated copy blockchain ledger to earn bitcoin.

Page No.
Date

→ Different types of wallet (bitcoin wallet)

Bitcoin wallets are digital wallets that store your private keys and allow you to interact with the bitcoin network

There are serveral types of bitcoin wallets mainly

- software bitcoin wallet
- hardware bitcoin wallet.

Hardware wallets
- most secure type bitcoin wallet
- private keys are stored on physical device and theoritically cannot accessed by computer or from internet
- When person wishes to make transaction without compromising the private keys
- The disadvantage of H/w wallets are
  - cost
  - availability of devices
- ledger and Trezor are well known hardware wallets.

Software wallets
- It exists of computing devices
- Since computing devices run many programs and application, they are susceptible to viruses, malware and phishing schemes, making all software wallet vulnerable to some degree

Page No.
Date

Q5. What is smart contract and explain its use cases.

→ Smart contract are self executing digital contracts
→ These contracts are programmed to automatically enforce the rules and regulations of an agreement between two or more parties.
→ Smart contracts runs on top of blockchain technology
→ allows them to decentralize
  - transparent and
  - tamper-proof

→ usecases of smart contract includes:-
  - Supply chain management
  - Real estate transactions
  - identity verifications.

1) Supply chain management → smart contracts can be used to automate and streamline supply chain management processes such as → tracking inventory
  - verifying product auth.

2) Real estate transactions – It is used for → property transfer
  - Ease agreements
  - Rental payments

3. Identify verification - smart contracts can be used to verify and manage digital identities.

Page No.
Date

Q6. Short note of EVM.

→ - EVM stands for Ethereum Virtual machine.
- It is runtime enviroment for executing smart contracts on etherum blockchain
- It is virtual machine that enables developers to write and deploy decentralized application on ethereum network.
- EVM s/w runs on each node of ethereum network and executes bytecode of smart contracts
- It is designed to be sandboxed enviroment that ensures safety and security of smart contracts.
- The EVM is responsible for managing the gas fee required for executing smart contracts and transactions.
- One of key feature of EVM is its ability to support turing-complete smart contracts meaning that they can perform any computation that can be done by computer.
- This allows for wide range of application to be built on etherum network including
  - decentralized exchanges
  - predictions markets
  - governance system.
- EVM is crucial component of ethereum ecosystem and has been instrumental in growth of decentralized finance (Defi) industry.
- Its flexibility and power have enabled developers to create innovative DApps that provide new solutions to traditional finance problems.