Q.1 What do you understand by Bitcoin Wallet? Discuss different types.

Ans.
1 A Bitcoin wallet is a digital wallet that can hold Bitcoin as well as other cryptocurrencies, like Ethereum or XRP.
2 A Bitcoin wallet (and any crypto wallet, for that matter) is a digital wallet storing the encryption material giving access to a Bitcoin public address and enabling transactions.

3 Bitcoin wallets not only hold your digital coins, but they also secure them with a unique private key that ensures that only you, and anyone you give the code to, can open your Bitcoin wallet. Think of it like a password on an online bank account.

4 With a crypto wallet, you can store, send and receive different coins and tokens. Some just support basic transactions while others include additional features, like built-in access to blockchain-based decentralized applications commonly known as dapps.

5 Among other things, these may allow you to loan out your cryptocurrency to earn interest on your holdings.

<u>Types of Bitcoin Wallets</u>

•As with physical wallets, Bitcoin wallets come in a range of styles, each offering a tradeoff between convenient access and security against theft.

Mobile

Mobile wallets, like WazirX multi-cryptocurrency wallet and Exodus bitcoin wallet are those that run as apps on phones, tablets and other mobile devices.

Web

Web-based wallets, like Guarda Bitcoin Wallet, store your coins through an online third party. You can gain access to your coins and make transactions through any device that lets you connect to the internet. These web-based wallets are frequently associated with crypto exchanges that allow you to trade and store crypto all in one place.

Desktop

Desktop wallets, like Guarda and Exodus, are programs you can download onto a computer to store coins on your hard drive. This adds an extra layer of security versus web and mobile apps because you aren’t relying on third-party services to hold your coins. Still, hacks are possible because your computer is connected to the internet.

Hardware
Hardware wallets are physical devices, like a USB drive, that are not connected to the web. These include Ledger Nano X Bitcoin Wallet and Trezor Model T Bitcoin Wallet available in India.

To make transactions, you first need to connect the hardware wallet to the internet, either through the wallet itself or through another device with internet connectivity. There is typically another password involved to make the connection, which increases security but also raises the risk you may lock yourself out of your crypto if you lose the password.

Hardware-based crypto wallets are also known as cold storage or cold wallets. (Wallets connected to the internet, in contrast, are called "hot wallets.")

Paper Wallets
In a paper wallet, you print off your key, typically a QR code, on a paper document. This makes it impossible for a hacker to access and steal the password online, but then you need to protect the physical document.

Q.2 Discuss in brief about Hardness of Bitcoin Mining.

Ans.
In order to ensure bitcoin blocks are discovered roughly every 10 minutes, an automatic system is in place that adjusts the difficulty depending on how many miners are competing to discover blocks at any given time.

As the name implies, bitcoin mining difficulty refers to the degree of difficulty involved in discovering new bitcoin blocks through mining.

Because the Bitcoin network is completely decentralized and not run by any single overarching authority, an algorithm hard-coded into the source code by Bitcoin's creator(s) Satoshi Nakamoto is used.

This algorithm constantly readjusts the difficulty of the mining process in line with how many miners are operating in the network to ensure that blocks are discovered at a steady pace.

Q.3 Discuss about the advantages and disadvantages of bitcoin.

Ans.

Q.4 How does Double Spending Happen? What are its type?

Ans.
Double spending can never arise physically. It can happen in online transactions. This mostly occurs when there is no authority to verify the transaction. It can also happen if the user’s wallet is not secured.

Suppose a user wants to avail of services from Merchant ‘A’ and Merchant ‘B’.
The user first made a digital transaction with Merchant ‘A’. The copy of the cryptocurrency is stored on the user’s computer. So the user uses the same cryptocurrency to pay Merchant ‘B’ .
Now both the merchants have the illusion that the money has been credited
since the transactions were not confirmed by the miners.

Types Of Double Spending Attacks
There are different types of Double Spending attacks:

Finney Attack: Finney Attack is a type of Double spending Attack. In this, a merchant accepts an unauthorized transaction. The original block is

eclipsed by the hacker using an eclipse attack. The transaction is performed
on an unauthorized one. After that, the real block shows up and again the transaction is done automatically for the real block. Thus the merchant loses money two times.

Race attack: is an attack in which there is a ‘race’ between two transactions. The attacker sends the same money using different machines to two different merchants. The merchants send their goods but
transactions get invalid.

51% Attack: This type of attack is prevalent in small blockchains. Hackers
usually take over 51% of the mining power of blockchain and therefore can do anything of their own will.

Q.5 Write short notes on POW and POS.

Ans.

Proof of Work (PoW)

•Proof of Work consensus is the mechanism of choice for the majority of cryptocurrencies currently in circulation. The algorithm is used to verify the transaction and create a new block in the blockchain. Proof of Work(PoW) is the original consensus algorithm in a blockchain network. The algorithm is used to confirm the transaction and creates a new block to the chain. In this algorithm, minors (a group of people) compete against each other to complete the transaction on the network. •The process of competing against each other is called mining. As soon as miners successfully created a valid block, he gets rewarded. The most famous application of Proof of Work(PoW) is Bitcoin.
•Producing proof of work can be a random process with low probability.
In this, a lot of trial and error is required before a valid proof of work is
generated.
•The main working principle of proof of work is a mathematical puzzle
which can easily prove the solution. Proof of work can be implemented
in a blockchain by the Hashcash proof of work system.

Proof of Stake (PoS)

•Proof of Stake (PoS) is a type of algorithm which aims to achieve distributed consensus in a Blockchain.
•A stake is value/money we bet on a certain outcome. The process is called staking.
•Proof-of-Work is quite energy intensive. So, a proof-of-work based
consensus mechanism increases an entity’s chances of mining a new
block if it has more computation resources.

A typical PoS based mechanism workflow:

•Nodes make transactions. The PoS algorithm puts all these transactions in a pool. All the nodes contending to become validator for the next block raise a stake. This stake is combined with other factors like ‘coin-age’ or ‘randomized block selection’ to select the validator.
•The validator verifies all the transactions and publishes the block. His stake still remains locked and the forging reward is also not granted yet. This is so that the nodes on the network can ‘OK’ the new block.
If the block is ‘OK’-ed, the validator gets the stake back and the reward too. If the algorithm is using a coin-age based mechanism to select validators, the validator for the current block’s has its coin-age reset to 0. This puts him in a low-priority for the next validator election.
•If the block is not verified by other nodes on the network, the validator loses its stake and is marked as ‘bad’ by the algorithm. The process again starts from step 1 to forge the new block.

Q.6 Discuss about pros and cons in case of EVM.

Ans.

Benefits of EVM

Execute untrusted code without risking data:
•One can execute untrusted code without putting the data at risk. EVM guarantees that its computations will not interfere with anything else happening in the system or with the personal files.

Can run complex smart contracts:
• One can run complex smart contracts in EVM without worrying about how they interact with each other. One can write them once and then run them on multiple platforms, which allows for the creation of a single contract that runs on multiple computing environments.

Deterministic processing:
• Smart contracts written on EVM have access to all of Ethereum’s states at any given time, allowing for processing to happen in a deterministic way and giving more guarantees about their correctness.

Distributed consensus:
•One of the potential applications of Ethereum is to allow for distributed consensus where everyone is running the same program but from their own computers.

Robust against failure:

•This is a complex process because the network needs to be able to come to a consensus at any given time. This way, the system becomes more robust against failures of individual nodes and you can update several nodes simultaneously without worrying that they might end up disagreeing with each other because of how code was written.

Disadvantages of EVM

High cost of storing data:
•First is gas, which is what you need to use in order to pay the fee to run a smart contract, and the other is the high cost of storing data on the blockchain, which could take up more than 3TB.

High gas cost:
• In Ethereum, all transactions require a fee to execute. These fees are called “gas”, and are paid in ETH tokens. Gas is priced at the moment of execution, and depends on the complexity of executing a transaction. The more difficult the computation for a transaction, the higher its gas cost will be.

High gas price during network congestion: •During times when there is high network congestion due to many transactions being pushed onto the blockchain, gas prices rise because there are fewer transactions that can go through (the same amount of computational power has to service more transactions).

Technical expertise required:
•Writing smart contracts and using EVM requires technical expertise. It’s a Turing-complete system, which allows programmers to write scripts in any programming language they wish. This can be excellent or disastrous, depending on the intention behind the code being written.
•The downside of this technology is that it could create a lot of complicated problems because with more power comes more responsibility for the writer of code.

Q.7 What are smart contracts on blockchain?

Ans.

•A Smart Contract (or cryptocontract) is a computer program that directly and automatically controls the transfer of digital assets between the parties under certain conditions.
•A smart contract works in the same way as a traditional contract while also automatically enforcing the contract. Smart contracts are programs that execute exactly as they are set up(coded, programmed) by their creators. Just like a traditional contract is enforceable by law, smart contracts are enforceable by code.

•The bitcoin network was the first to use some sort of smart contract by using them to transfer value from one person to another.

•The smart contract involved employs basic conditions like checking if the amount of value to transfer is actually available in the sender account.

•There are some common smart contract platforms like Ethereum, Solana, Polkadot, Hyperledger fabric, etc.

Q.8 Write short notes on Ethereum Solidity.

Ans.

Solidity is a brand-new programming language created by Ethereum which is the second-largest market of cryptocurrency by capitalization, released in the year 2015 and led by Christian Reitwiessner.
Some key features of solidity are listed below:

Solidity is a high-level programming language designed for implementing smart contracts.

It is a statically typed object-oriented (contract-oriented) language.

Solidity is highly influenced by Python, c++, and JavaScript which run on the Ethereum Virtual Machine(EVM).

Solidity is the primary language for blockchains running platforms.

Solidity can be used to create contracts like voting, blind auctions, crowdfunding, multi-signature wallets, etc.

Q.9 What do you understand by Ethereum Virtual Machine (EVM)? How Does EVM Works?

Ans.

The **Ethereum Virtual Machine** or EVM is a piece of software that executes smart contracts and computes the state of the Ethereum network after each new block is added to the chain.

The EVM sits on top of Ethereum's hardware and node network layer. Its main purpose is to compute the network's state and to run and compile various types of smart contract code into a readable format called 'Bytecode.'

Working of EVM

In Ethereum, there is something called a smart contract. These contracts have some computer code which facilitates the exchange of money and information**.**

These contracts are predefined by the creator of the smart contract, in order to ensure that a certain outcome will happen based on either what happens or doesn’t happen.

Ethereum Virtual Machine provides Turing complete environment for execution of scripts and smart contracts. This means that anything that can be implemented with a computer can be run on EVM.

Ethereum Virtual Machine ensures that all transactions and smart contracts made on the Ethereum blockchain are executed in correct and expected manner as desired by the smart contract code.