**Frequently Asked Questions (Week-1)**

1. **Difference between distributed and decentralized systems and whether blockchain is one of them or not.**

A distributed system is one that has multiple interacting components or microservices. These components may be owned and managed by different entities or a single entity. When they are managed by a single entity, it would be a distributed system that is centralized in ownership/control (e.g, Google search, facebook are distributed systems that are centrally owned). Of course, a centralized system may have just one component, in which case it won’t be a distributed system.

When a distributed system is owned and controlled by different entities, it is also referred to as a decentralized system. All or many of the nodes in the system partake in the decision making process. So, by definition, all decentralized systems are distributed systems. A good example is BitTorrent. A blockchain is also a decentralized system.

1. **Which is better between distributed and decentralized systems?**

In any practical system, the term 'better' can be used if it suits the requirement in a better way. Moreover, any decentralized system is a distributed system. For example, if we want to create a very basic swarm architecture, then decentralizing may be enough. But if we want something like a cryptocurrency based transaction system, we may need to implement a full-fledged distributed ledger. So, the “betterness” depends on your objective.

1. **Why all the transactions are visible to all the nodes in the blockchain?**

In case of blockchain there are no central systems like banks which list all the transactions in their ledgers in a centralized manner, instead here there is a decentralized (or distributed) system which involves all the nodes. So if you have to store/track/validate a transaction that should be through all these nodes only. Therefore, everyone should have the complete knowledge of the system. Or in other words, the system needs to be transparent enough, so that everyone can see what is happening and can differentiate between the “Good” and the “Bad”.

1. **How the privacy and security are maintained if all the transactions can be viewed by everyone?**

In blockchain, the transactions won't involve the names of the users directly. Instead, there will be encoded id(s) representing them. Hence even though the transaction details would be there still no one will be able to figure out the parties involved. A single physical person can have more than one ids as well. So, individual user privacy is always maintained. On top of this, all these records are tamper proof hence is highly secure.   
Even if you compare the system with our normal monitory system, this level of information is still available to everyone. The distribution of wealth is always public, you know how many percentage of people in a state has what percentage of wealth; but you do not know what is the amount of wealth available to Mr. XYZ. The same thing is ensured in Bitcoin. You can see that an id “1BoatSLRHtKNngkdXEeobR76b53LETtpyT” has 20 BTC, but you really cant figure out whether this id belongs to Mr. XYZ or Mrs. UVW.

1. **How longest chains are determined in Bitcoin?**

Longest chains are not determined by the maximum number of blocks in the chain. It is determined by the total work done (in terms of Proof of Work mining) for mining all the blocks in the chain. Note that the work done is a function of the mining difficulty. The intuition behind selecting the chain with the maximum work is that such a chain will be more difficult to tamper as you have to do more work.

1. **What are orphaned blocks and how to remove them?**

The block from one of the miners (who will pass the difficulty posed by the network) will be the part of the longest chain, others will be marked as orphaned block and will not be used. Moreover, If there is a transaction inside an orphan block, then it should also be there in one of the valid block. The miners look whether the broadcasted transactions have been included in one of the valid blocks (nor the orphaned blocks); if not, they include them in the next mined block. The orphaned blocks can be removed afterwards.

1. **Who are the miners and who selects them?**

No one selects miners. If you are a normal Bitcoin user (have a Bitcoin wallet), you can join as a miner as well. Miners are simply the nodes with sufficient computation resources so that they can perform the mining process. As a miner, its task is just to propose a new block with a proof that the other nodes can verify.

1. **Who validates the transactions?**

Every full node in the blockchain network, including the miners validate the transactions. Note the term “full node” here. A full node is a node that implements full blockchain functionalities (<https://bitcoin.org/en/full-node>) in Bitcoin. A full node Bitcoin wallet is more secure than a client node wallet that implements partial blockchain functionalies. A client node wallet with partial implementation just creates the public-private key and initiates the transactions; if they observe the transaction in a valid block, they commit it. However such nodes are less secure, typically they rely on the more than 50% honest mining power or one or more *remote servers* to protect them from double-spends and other network attacks (<https://en.bitcoin.it/wiki/Clients>). Bitcoin always suggests for a full node implementation.

1. **Why does every node need to validate the transactions?**

Blockchain works in this principle - our objective is to ensure that the valid, legitimate and non-malicious nodes should be able to differentiate between the right / wrong, and should be able to include only the valid blocks with valid transactions in the local copy of the blockchain. We do not care about the blockchain stored at malicious nodes, but we care about the activities of the malicious nodes.

This is the task of the miner - to generate a "proof" for the valid blocks with valid transactions. Some of the nodes can bypass validation of transactions (as long as a majority of the nodes are validating them), it does not hamper the safety of the Blockchain operations. With a valid block, the "proof" (target hash with the nonce) is there to verify the validity. So, if a malicious miner creates a invalid block, others will be able to discard it.

**Then, Why do we ask all the non-malicious nodes to validate the transactions?**

This is to ensure the liveness of the system by blocking propagation of invalid blocks any further. If we do not do so, an adversary may launch a DoS attack by propagating large number of invalid blocks in the network, and all the nodes will be busy to broadcast those invalid blocks. Just to prevent this type of DoS attacks, we ask the valid nodes not to propagate any invalid transaction any further.

Safety of the system is ensured as long as a majority of the nodes are validating transactions and are discarding blocks with invalid transactions. This is explained further in Q11.

1. **Can a miner propose an invalid block?**

The miners are normal nodes, so it is highly possible that a miner is an adversary and it proposes an invalid block (a block with invalid transactions).

1. **What if a miner proposes an invalid block?**

The invalid block gets propagated to the network. Whenever a node receives a new block, it does the followings before including it in the Blockchain - (a) validate all the transactions in the block, (b) ensure that the block does not have any double-spend transactions, (c) check the block is not a replay and is signed by the originator, (d) check the hash and the nonce of the block (verify the proof). So, if a block contains an invalid transaction or a double-spend transaction, then the block is simply discarded. [Again, this is the reason that you need sufficient transparency - you need to store the old transactions in your local machine].

1. **How does the first node in the blockchain get created?**

It has been created manually, called the genesis block - <https://www.investopedia.com/terms/g/genesis-block.asp>

1. **How is it possible to have the copy of Public Ledger ( which is increasing day by day) for every client? [Similar question: If the size of the Blockchain is few hundred GBs, then how do everyone store the blockchain in local machines?]**

For reducing the size of the block, several compaction techniques are used. One such technique is called “Sharding". Check this - <https://medium.com/edchain/what-is-sharding-in-blockchain-8afd9ed4cff0>

1. **Can the attacker tamper the last block?**

The hypothesis is as follows. Mining requires some time. Say the last block has been propagated in the network. When the miners observe a new block, they start working on the next block to be mined. So, by the time the attacker makes an alternation in the last block and propagate an altered copy of that block, a correct new block has been mined and added to the blockchain with the correct last block. So, the adversary has to change this new block as well, and the procedure goes on. Therefore, it would be extremely difficult (although, theoretically, not impossible) for an attacker to make a change even in the last block.

1. **How is the difficulty determined in bitcoin?**

In every 2016 blocks, the elapsed time between the first and last block is computed. Ideally, the value is nearly 2 weeks. If the actual value is less than 2 weeks, then the difficulty is increased at most 300%. If the actual value is greater than 2 weeks, then the difficulty is reduced by at most 75%.

1. **How is the mining incentive provided to the miners?**

All the miners who have solved the puzzle receive the equal incentive as in case of a single miner solve the puzzle. However, in every case, that incentive amount cannot be used for at least 100 blocks for confirming that the block is not an orphan block. The miners of an orphan block do not get any incentive.

1. **How is the Merkle tree root computed for the non-even transactions?**

The last transaction id is concatenated with a copy of itself and performed the hash. For example, the transaction ids are 1,2 and 3. Then the combined hash will be formed as {1, 2}, and {3, 3}.

1. **What is the difference between transaction fees and block reward? Which one of them goes to the miner?**

Transaction fees are the amount that the spenders provide for the transaction. The block reward is the combination of the transaction fees and the block subsidy. The block subsidy is the incentive for creating the new block. Total block reward goes to the miner.

However, as the block reward gets reduced gradually, the transaction fees can be increased to provide equal incentives to the miners all the time. We’ll discuss later about how this block reward changes with time.