BLOCKCHAIN (UE20CS335)

Name: Vishwa Mehul Mehta	
SRN: PES2UG20CS389	
ASSIGNMENT 1	
S. NO.1	**The RSA Algorithm: Given p=13, q= 31, d = 7, What should be the value of e?**
Answer	e = 103
S. NO.2	**The Diffie Hellman algorithm: Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged? Explain.**
Answer	In this instance, the generator is 5 and the prime number is 17. Alice: She calculates her public key, which is, and picks her private key as 4, which 5^4 mod (17) = 7 Bob: He calculates his public key using 6 as his private key. 5^6 mod (17) = 2 They now exchange public keys. Likewise, determine the shared secret key. Alice, 24 mod (17) equals 16. Bob, 76 mod (17) equals 16. Their shared secret key is the same number **16**, which they both exchanged.
S. NO.3	**What is distributed consensus? How that can be guaranteed in blockchain?**

Answer	Distributed consensus is the process of achieving agreement among a group of distributed nodes in a network, even if some of those nodes are unreliable, malicious, or fail to respond. In the context of blockchain, distributed consensus is the mechanism by which transactions are verified and added to the blockchain ledger. In a blockchain network, nodes work together to verify new transactions and reach consensus on the state of the ledger. This is achieved through a consensus algorithm that ensures that all nodes agree on the order of transactions and the state of the ledger. One common consensus algorithm used in blockchain networks is the Proof-of-Work (PoW) algorithm, used in the Bitcoin network, where nodes compete to solve a complex mathematical puzzle, with the first node to solve the puzzle adding a new block to the blockchain and receiving a reward.
S. NO.4	**What are the advantages and disadvantages of using PoS over PoW.**
Answer	Advantages: Efficiency in terms of energy use: In contrast to PoW, which depends on mining nodes to solve challenging mathematical puzzles, PoS does not require significant energy to secure the network. Decentralization: PoS can be more decentralised than PoW due to its greater accessibility to ordinary users and lack of need for specialist hardware to participate in the consensus process. Security: PoS can offer greater security than PoW since successful attacks require a majority of the cryptocurrency supply, which is more difficult and

	expensive to obtain than the majority of the mining power needed in PoW. Less centralised power: Because big mining pools can't control the consensus process, PoS can help the network become less centralised. Disadvantages: PoS mandates the initial distribution of bitcoin to participants, which could result in a concentration of power within a select group of affluent people. PoS has the potential to provide people with more bitcoin more voting power, which could result in a concentration of authority. Risks to long-term security: Because PoS is founded on the idea that users will act in the network's best interest, it may be subject to long-term security problems. This presumption might not always be accurate, and some users might behave deliberately or selfishly, thereby jeopardising the network's security.
S. NO.5	**If you have to choose, which society do you support: The PoW or The PoS? Please give a clear reason to justify your thoughts.**
Answer	PoS would be the choice here as it consumes less energy and is efficient since no high computation is required. It also provides fast and inexpensive transaction processing. Has a much smaller environmental impact Gives an economic incentive to approve valid blocks.
S. NO.6	**What is the role of SGX technology in proof of elapsed time?**
Answer	In PoET a special verification is required from a node when it tries to join the network. This verification is

	achieved using Intel's Software Guard Extension (SGX) technology which was first introduced in 2015. It creates an attestation for a piece of code and protects the code from external access.
S. NO.7	**Can Proof of authority be used in public blockchain setup? Justify.**
Answer	No, proof of authority cannot be used in a public blockchain as it causes centralization and requires the identity of the nodes to be known in order to work correctly. It is best suited for private, permissioned Blockchain.
S. NO.8	**Why is it difficult to become a validator in Proof of authority? What are the requirements for becoming a validator node?**
Answer	It is difficult to become a validator in Proof of authority as the node must put their identity at stake. A tough process reduces the risks of selecting questionable validators and incentivize a long-term commitment. The following are the requirements: • Verified, valid, and trustworthy network identity • No criminal record • Good moral standards • Stay committed to the network • Willing to put reputation at stake
S. NO.9	**In hashing, what is the difference between strong and weak collision?**
Answer	Weak collision: given an input X and a hashing function H(), it is very difficult to find another input X' on which H(X) = H(X') Strong collision: given a hashing function H() and two arbitrary inputs X and Y, there exists an absolute minimum chance of H(X) being equal to H(Y).
S. NO.10	**What has happened in "The DAO story"? Which type of forking took place to make the system correct?**

Answer	A hacker found a loophole in the coding that allowed him to drain funds from The DAO. This happened because of the fact that when the DAO smart contract was created the coders did not take into account the possibility of a recursive call and the fact that the smart contract first sent the ETH funds and then updated the internal token balance. To fix this Ethereum hard forked the chain to send the hacked funds to an account available to the original owners.
S. NO.11	**Proof of Space isused by SpaceMint. True /false? If true, how are they using Proof of space in their setup?**
Answer	Proof of space is used in SpaceMint. In this the miners are rewarded for dedicating disk space instead of using computational power and dedicating more disk space yields a proportionally higher expectation of successfully mining a block. The Interactivity problem is solved by SpaceMint creating a third interaction by using the Fiat-Shamir paradigm, which is a method of using a hash of a previous message to replace a public-coin challenge on the SpaceMint platform.
S. NO.12	**Paxos and RAFT gives assurance of liveness or safety. Comment.**
Answer	Paxos: In order to guarantee safety (also called "consistency"), Paxos defines three properties and ensures the first two are always held, regardless of the pattern of failures: Validity (or non-triviality) - Only proposed values can be chosen and learned. Agreement (or consistency, or safety) - No two distinct learners can learn different values (or there can't be more than one decided value) Raft: The combination of leader election and log replication

	commitment rules provide Raft's safety guarantees: Correctness and availability of the system remains guaranteed as long as a majority of the servers remain up. For each term, every server gives out one and only one vote and, consequently, two different candidates can never accumulate majorities within the same term. This vote needs to be reliably persisted on disk, in order to account for the possibility of servers failing and recovering within the same term.
S. NO.13	**It is given in literature that in blockchain setup, it is better to use PBFT than BFT. Why?**
Answer	It is better to use PBFT than BFT as it provides safety over an asynchronous network, which is not there in BFT. It also has a low overhead and is fast compared to BFT. In PBFT let total number of replicas be 3f+1 then it can handle 1/3N of faulty nodes which is more compared to BFT where 1/4 N of faulty node is tolerated.
S. NO.14	**What is the difference between Pre-prepare, Prepare and Commit stage of PBFT?**
Answer	PBFT has views where one view is primary and other are secondary. Once Client requests Primary view , Primary view asks all secondary views to prepare for the change by sending transaction and sequence number . That is pre – prepare stage. Once all the secondary views/nodes receive the command they check for its valdidity and if it is valid they send response to primary view saying that they are ready to prepare if more than 2/3rd of Secondary view(SV) agrees. That is Prepare stage. After receiving the response from more than 2/3rd of node, primary View(PV) ask them to commit the change and they eventually do it . This is the Commit stage.

S. NO.15	**Can two consensuses be merged? Give an example to justify.**
Answer	It is possible to merge two consensuses but it might be difficult. Since Proof of work (PoW) does not support green mining but is easy to verify and computation is less in Proof of Stake(PoS) we can merge the two consensuses where Proof of work(PoW) can be used for block validation and Proof of Stake (PoS) for block finality. It will ensure both security and decentralization