BLOCKCHAIN (UE20CS335)

Name: Adithya M	
SRN: PES1UG20CS621	
ASSIGNMENT 2	
S. NO.	Question
1	The RSA Algorithm: Given p=13, q= 31, d = 7, What should be the value of e?
Ans	e*d= 1 (mod phi(n)) n= pq phi= (p-1)x(q-1). n= 13x31 = 403 phi= (13-1) * (31-1) = 360 7e = 1%360 =103
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.
Ans	q = 17, root = 5, a = 4, b = 6. A = 5^4 % 17 = 4 B = 5^6 % 17 = 2 B^a % q = A^b % q 2^4 % 17 = 4^6 % 17 = 16
3	What is distributed consensus? How that can be guaranteed in blockchain?
Ans	Distributed consensus is the process by which a group of computers agree on a common state of data, even if some of the computers fail or behave maliciously. • In blockchain, distributed consensus is achieved through a consensus algorithm that ensures all nodes in the network agree on the validity of transactions and the current state of the blockchain. • This is typically achieved through a process called mining, where nodes compete to solve a complex mathematical puzzle, with the winner being allowed to add a new block of transactions to the chain.

	• Once a block is added, all nodes in the network must agree to update their copy of the blockchain to reflect the new state.
4	What are the advantages and disadvantages of using PoS over PoW
Ans	Advantages: • It is energy efficient and does not burn electricity when mining • It can be more expensive to attack than PoW- hackers need to purchase a large percentage of the native cryptocurrency • It scales easily to handle transaction load and size Disadvantages: • PoS can be vulnerable to a "nothing at stake" problem, where validators may be incentivized to validate multiple competing blocks at the same height, which can lead to blockchain forks and reduced security. • PoS can be susceptible to centralization and censorship, as wealthy individuals or organizations may hold a majority of the coins and have a disproportionate influence on the network.
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.
Ans	PoS is a better choice compared to PoW due to the following reasons: • Energy efficiency: PoS requires significantly less energy than PoW, as it does not require large amounts of computational power to solve complex mathematical puzzles. This makes it a more environmentally-friendly alternative to PoW. • Decentralization: PoS allows for a more decentralized network, as it does not require expensive mining equipment to participate in the consensus process. This can lead to a more diverse set of validators and reduce the risk of centralization. • Security: While PoW is generally considered to be more secure than PoS, PoS has its own security mechanisms in place, such as slashing penalties for validators who behave maliciously. Additionally, some argue that PoS can be more resilient to 51% attacks than PoW.
6	What is the role of SGX technology in proof of elapsed time?
Ans	SGX allows for the creation of a trusted execution environments (TEE) to provide a verifiable delay function that serves as a replacement for the energy-intensive computations required by PoW. This ensures that the computation is performed securely and cannot be tampered with. This is important because the VDF is used to determine the consensus in PoET, and any attempt to manipulate it could compromise the security of the entire blockchain network.
7	Can Proof of authority be used in public blockchain setup? Justify.

Ans	PoA although best suited for private, permissioned Blockchain can be used with public blockchains where the trust is distributed. There are a few limitations wrt to being vulnerable to DDoS attacks and as addresses are unknown, it is difficult to remove the malicious nodes from the network.
8	Why is it difficult to become a validator in Proof of authority? What are the requirements for becoming a validator node?
Ans	• It's difficult to become a validator in PoA as validators are required to be able to handle a DDoS attack (systems must be well equipped). • In some cases, validators may be required to stake or lock up a certain amount of cryptocurrency or other assets as collateral. • Validators are typically required to have a good reputation or be a trusted entity within the network
9	In hashing, what is the difference between strong and weak collision?
Ans	Weak collision can be found with relatively low computational effort, as they are not intentionally designed to be difficult to find, whereas finding a strong collision is much more difficult than finding a weak collision, as it requires effort to craft the inputs in a way that produces the same hash value. Weak collision is a natural occurrence, whereas strong collisions are typically used in attacks against hashing algorithms, where an attacker tries to generate inputs that produce the same hash value as a target input.
10	What has happened in "The DAO story"? Which type of forking took place to make the system correct?
Ans	The DAO was a decentralized investment fund on the Ethereum platform that was hacked on June 17, 2016. Initially, a soft fork upgrade was carried out step by step but it was discovered that it would cause the entire Ethereum network to collapse if any transaction related to TheDAO and Child DAO was invalidated. As a result, a hard fork was executed which put Ethereum's network history back in place as it was before the DAO attack and allowed investors to withdraw their funds.
11	Proof of Space is used by SpaceMint. True /false? If true, how are they using Proof of space in their setup?
Ans	True

	• In SpaceMint, proof of space is used to enable mining. • Miners dedicate disk space to store data and are rewarded for doing so. • This allows for more distributed participation as smaller miners are rewarded fairly according to their contribution to the network. SpaceMint's design solves or alleviates several of Bitcoin's issues: its large energy consumption.
12	Paxos and RAFT gives assurance of liveness or safety. Comment
Ans	Paxos guarantees safety by ensuring that a proposed value is eventually selected by the group of participants. Raft on the other hand has more guarantees of liveness
13	It is given in literature that in blockchain setup, it is better to use PBFT than BFT. Why?
Ans	• PBFT can run over an asynchronous network. • PBFT deals with byzantine failures by dealing with arbitrary node behaviour. • PBFT guarantees privacy by providing tamper proof messaging and authentication
14	What is the difference between Pre-prepare, Prepare and Commit stage of PBFT?
Ans	• In the Pre-Prepare phase, the primary node is responsible for verifying requests and generating corresponding pre-prepare messages. Then, it broadcasts these messages to all replica nodes. • In the Prepare phase, each replica node verifies that it has received a pre-prepare message from the primary node with a valid sequence number. If so, it multicasts a prepare message to all other replicas. • In the Commit phase, each replica node waits until it has received 2f+1 prepare messages from different replicas that match its pre-prepare message (where f is the maximum number of faulty nodes). Once this condition is met, it multicasts a commit message to all other replicas.
15	Can two consensuses be merged? Give an example to justify.
Ans	Yes. Hybrid consensus algorithm can use PoS and PoW. Ethereum network makes use of Ethash which is a hybrid PoW/PoS algorithm which involves using the existing Ethash algorithm for a certain number of blocks, and then switching to a new algorithm for the next set of blocks. This would make it more difficult for any single miner or mining pool to dominate the network, as they would need to have significant resources dedicated to both mining algorithms