BLOCKCHAIN (UE20CS335)

Name: P K Navin Shrinivas	
SRN: PES2UG20CS237	
ASSIGNMENT 1	
1.	**The RSA Algorithm: Given p=13, q= 31, d = 7, What should be the value of e?**
Answer	> We first find the eulers toient and then find the mdular multiplcative invser of d over the euler toient. (p-1)*(q-1) = 360 = phi(n). ed=1 mod phi Hence e is the modular multiplicative inverse of d in phi(n). Hence e = (1/d) mod 360 = 103 mod 360 = 103 Hence value of e = 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**.
	- the values 17 and 5 are shared before hand. - Alice decides a random number(a) and does : `A = 5^4 % 17 = 3` => `A = p^a % q`. Bob also decides a random number and does the following : 'B = b^p %q' => 'B = 5^6 % 17 = 12'. - Number A and B are shared to each other - A does the following : `N = 12^4 % 17 = 13` and B does `3^6 % 17 = 13`. - Hence both A and B end up with a common number.
3.	**What is distributed consensus? How that can be guaranteed in blockchain?**
	A process in which a group of nodes in a network agree on a single value or state. With respect to blockchain, this is the validation of block and keeping a single source of truth for the chain in an completely distributed and

	trustless network. Algorithms/protocols such as BFT, PoW, PoS help in maintaining the guarantee in a blockchain network. Often time its the compute or stake that the nodes advertise to prove their validity. In addition to consensus algorithms, blockchain networks also use cryptographic techniques such as digital signatures and hash functions to ensure the integrity and security of the blockchain.
4.	**What are the advantages and disadvantages of using PoS over PoW.**
	PoS stand for proof os stake and PoW stands for proof of Work, Both are consensus algorithm used in an trustless blockchain network. Here are some of the davantages of PoS over PoW : - Energy efficieny : PoS is much more efficient than PoW as the nodes do not have to solve a difficult problem to get reward, they only need to stake they coins and validat blocks created by other nodes. - Decentralistion : PoS can achieve higher degree of Decentralistion than PoW. - Security : Unlike in PoW, 51% attacks are much harder in a PoS protocol and a single entity needs to have more than 51% of the currency/tokens to skew the results in their favour. A 51% compute power is easier to achieve than 51% of tokens.
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.**
	I'd choose to support PoS, for the following reasons : - A green alternative/solution to the new age of truless networking/financial banking. I simply do not see the

	need to spend enourmous energy mining and solving hard cryptographic problems to only validate your block. - Higher degree of Decentralistion, this can lead for much more powefull network validating transactions, this can in turn improve quality of blockchain based finanaces. - Security : It is inhertitly harder to get 51% of the token in a network, this is the 51% attack alternative in PoS making it much more secure.
6.	**What is the role of SGX technology in proof of elapsed time?**
	SGX is a hardware based security solution built into the CPU, it allows the system to create a isolated execution environment that is hidden from the rest of the system. Here we a random wait time decided by the PoET protocol, SGX ensures the nodes wait for a given time before validating the block. SGX makes sure no entity in the system can modify the wait time.
7.	**Can Proof of authority be used in public blockchain setup? Justify.**
	In a technical perspective, yes it can be used in a public blockchain. But doing so leads to the following issues : - Much less decentralised that PoS or PoA making it harder to exploit. This is because of the small set of pre-approves validators. - If a signifcant number of validators are compromised the entier network can be considered compromised. Hence leading to a notion of centralisation. - Hence, using PoA in a pulbic blockchain renders the advantages of blockchain nil.
8.	**Why is it difficult to become a validator in Proof of authority? What are the requirements for becoming a validator node?**

	Entity gain reward by being a validator in a PoA network, one becomes a validator under the following conditions : - Identitfication (By a cental authority). - Token ownership (Should contain some amount of networks tokens) - Reputation - Participartion in the consensus protocol. > Often times any of the above are kept in stake to become a validator of the network.
9.	**In hashing, what is the difference between strong and weak collision?**
	A collision in hasing is the case where 2 different inputs lead to the same has output. The two types of hash collisions are : - Strong collision : Probablity that 2 random inputs hash to the same output. - Weak collision : Given one input and its hash, what the probablity of finding another number that hashes to the same output.
10.	**What has happened in “The DAO story”? Which type of forking took place to make the system correct?**
	DAO is a smart contract on the eth blockchain, it allowed members of the eth network to get "DAOs" in exchange for ether. Later on a vunerability was discovered in DAOs code base which lead to a theft of 50million dallars with in ether. The reason as to why this happened split the community into 2. One community considered the modification of blockchain to be a fault and the other considered it to be viable fault. This lead to the hard forking of the ther chain into two, both of which still maintains the confidence in ethereum networks.

11.	**Proof of Space is used by SpaceMint. True /false? If true, how are they using Proof of space in their setup?**
	Answer : True, Proof of Space is used by SpaceMint. In SpaceMint, the process of generating a new block triggers challenge where the network asks the nodes to present a proof of space. Nodes respond by providing a set of pre-computed values that prove that they have stored in the space of they memory. This is then validated ans used a proof for validity of a block.
12.	**Paxos and RAFT gives assurance of liveness or safety. Comment.**
	- liveness is the property of the network that states that each node tries to find and become the single source of truth rather than trying to find the right node with truth. There exists no situation that a given node can no longer participate in the node. - safety is the property where a given node can be told to have a consistent state given it's actively part of the protocol. Paxos guarantees safety by doing round trips across the network to ensure a common value is agreed upon, where as RAFT uses a commited log as the single source of truth. Paxos doesn't guarentee liveness by default as there exists conditions where 2 nodes confict with each other an can no longer take part in the protocol Paxos has to use timeouts to guarentee liveness. Raft ensure liveness by letting anyone be the leader but also uses random timers to let the network move forward even on leader failures.

13.	**It is given in literature that in blockchain setup, it is better to use PBFT than BFT. Why?**
	pBFTs are preffered over BFTs for the following reasons : - Lower latency : pBFTs allow us to achieve consensus in lower number of rounds. - Higher throughput - Finality of transactions : A commited transaction cannot be reverted. - Robustness to BFT : This is crucial in a trustless network.
14.	**What is the difference between Pre-prepare, Prepare and Commit stage of PBFT?**
	- Pre-prepare : A block is proposed to the network indicating it needs to be included in the network. It also indicates a new term/round in the network. - Prepare : Each node verfies the block and further advertises the block along with its ID and senquence number, Once reply is recived from quorum of nodes it moves on to commit stage. - Commit : Each node broadcasts a commit message to the network, once a quorum of commit messages are observed by a node, it add it to the blockchain.
15.	**Can two consensuses be merged? Give an example to justify.**
	It is not possible to merge two two consensus protocols as each have their set of rules and assumptiions. property of one protocol cannot be guarenteed by another making this exlcusive of each other. But it is possible to have a single blochain use multiple consensus on topo of each other as a way of verification. Hence 2 consensus protocols can only work together in a complementary way.