BLOCKCHAIN (UE20CS335)

Name: Vishwa Mehul Mehta	
SRN: PES2UG20CS389	
ASSIGNMENT 1	
S. NO.1	**Can blockchain be applied to any application? Give an example to support your answer.**
Answer	Blockchain cannot be applied to any application. It does not work in isolation, and cannot be applied to applications that require constant modification.
S. NO.2	**Why do we say that public blockchain is prone to 51% attack?**
Answer	A 51% attack is an attack on a cryptocurrency blockchain by a group of miners who control more than 50% of the network's mining hash rate. Owning 51% of the nodes that is the majority of nodes on the network gives the controlling parties the power to alter the blockchain. When it comes to blockchains that use proof of work , 51% of attacks involve the attacker being able to gain control of more than 50 per cent of the hashing power. By doing so, he or she is able to manipulate the data in the blockchain.
S. NO.3	**What is the disadvantage of Consortium blockchain? In what type of systems, would you prefer consortium blockchain over private or hybrid blockchain?**
Answer	The disadvantages include: Centralization Limited accessibility Complexity Limited flexibility It can be used when creating a shared supply chain management system or a decentralized digital identity

	system. Mostly within an enterprise or a group of organisations when there is a common goal or set of goals. Enables development of shared platforms for various industries and organizations to work together to find solutions and reduce the time and expenses of development.
S. NO.4	**How much time would it require for a miner to mine a block?**
Answer	It takes roughly 10 minutes to mine a Bitcoin. This varies for different chains and depends on its difficulty.
S. NO.5	**Why DES is not a good idea to be used in blockchain setup?**
Answer	It is easy to derive the key from the encrypted data and key distribution is a problem. Here, the number of keys between parties will also increase very quickly, some what in quadratic speed.
S. NO.6	**What are the different fields present in a block header of bitcoin and Ethereum?**
Answer	Bitcoin header: Version Previous block header hash Merkle Root Hash Time Nonce Ethereum header: Parent Hash State Root Transaction Root Reciepts Root
S. NO.7	**Consider two friends Alice and Bob. Bob wants to send a message m that is digitally signed to Alice. Let the pair of private and public keys for Alice and Bob be denoted represent the operation of encrypting m**

	with a key Kx and H(m) represent the message digest. How the message will be transmitted from Bob to Alice.
Answer	The message m is encrypted by Bob using his public key Kx i.e. E(M, Kx) and the hash of the message H(m) is transmitted along with the encrypted message to allow non-repudiation and authentication.
S. NO.8	**How does blockchain contribute to the development of digital identity and personal data management?**
Answer	Blockchain enables more secure management and storage of digital identities by providing unified, interoperable, and tamper-proof infrastructure with key benefits to enterprises, users, and IoT management systems. Individuals would use their self-sovereign ID to verify their identity, removing the need for passwords. Backed by blockchain innovation, the solution gives individuals total privacy and control of their personal information, while making data shareable on a trusted network, and ensuring security of identity transactions. Anonymous authentication is also established.
S. NO.9	**Compare and contrast blockchain with other emerging technologies such as artificial intelligence and the Internet of Things.**
Answer	AI uses machine learning to promote data performance, efficiency, and accuracy. Whereas, blockchain looks for power and energy to execute and run a network of computers. AI and machine learning aim at carrying out tasks that include learning, adapting, performing, processing information, and speech recognition similar to humans. But, information technology systems are based on evaluating, storing, capturing, and analyzing data. IoT devices track the state of safety for critical machines and their

	maintenance. From engines to elevators, blockchain provides for a tamper-free ledger of operational data and the resulting maintenance.
S. NO.10	**Given a message of 748 bits. How many padded bits are required for SHA 256?**
Answer	(748 - 10- 1) mod 256 = 225 bits. The number of padded bits is 225.
S. NO.11	**What is the future of blockchain-based finance?**
Answer	Blockchain technology is revolutionizing finance as we know it. Its ability to create a secure and transparent ledger of transactions has made it a promising solution for a wide range of financial applications. Blockchain technology can be used to record transactions between two parties in a verifiable and permanent way. The immutability of a blockchain allows for verification and finalization of transactions along with eradication of invalid and faulty transactions, making the process of exchange of value easier.
S. NO.12	**How has the evolution of mining hardware and software impacted the competitiveness and efficiency of blockchain mining, and what are some of the latest trends and innovations in this field?**
Answer	What makes blockchain technology so revolutionary is that anything of value can be tracked and traded on its network, reducing risk and cutting costs for all involved. As the mining hardware and software evolve and become better with time, the competitiveness and efficiency in the process increases. Hardware advancements will also likely have a significant impact on the future of crypto mining. This will allow miners to earn more rewards while using less energy. Furthermore, the development of new technologies, such as quantum computing, could completely change (or render useless) how crypto currencies are mined.

S. NO.13	**How is difficulty playing an important role in mining process?**
Answer	Every blockchain has a mining process by which miners can generate fresh coins. An algorithm regulates how difficult it is for the miners to mine a certain block. This difficulty is known as mining difficulty. For mining a block, a miner must solve complex mathematical problems by finding a valid hash. As the process progresses, the network adjusts the rate so miners can find valid hashes. The higher the mining difficulty of a cryptocurrency, the more energy you'll need to have a chance at mining a block.
S. NO.14	**What is the difference between gas fee, gas price, transaction fee, block fee, uncle fee, burnt fee in Ethereum? Out of these, which are not present in bitcoin?**
Answer	Gas fees are paid in Ethereum's native currency, ether (ETH). Gas prices are denoted in gwei, which itself is a denomination of ETH. Ethereum Transaction Fee measures the fee in USD when an Ethereum transaction is processed by a miner and confirmed. The block fee is calculated by a formula that compares the size of the previous block (the amount of gas used for all the transactions) with the target size. The uncle fee is the one that's given to those miners whose blocks are not accepted in the blockchain. The amount of transaction fee reduced in every transaction to lower the rate of ethereum issuance. Out of these the "uncle fee" is not present in bitcoin.
S. NO.15	**It is said that the contents on blockchain are immutable. If any change is made at a node X, everyone in the network sees it and X's ledger is**

	updated to its previous state to maintain the consistency. Now consider that Digilocker application is launched on a blockchain platform. In this application, if a person's address has to be updated on his Aadhaar document. Does the blockchain allow this change? Ideally No because of the immutable property. But in a situation like this, it should be allowed as the address of a person can change. In a scenario like, how blockchain will perform such a change?
Answer	In this case, once the change has been made by a node, the other nodes must mine all the blocks that follow the updated block again in order to validate the change on the blockchain and confirming the update as valid. This is a very memory intensive task.