BLOCKCHAIN (UE20CS335)

Name: Adithya M	
SRN: PES1UG20CS621	
ASSIGNMENT 1	
1	Can blockchain be applied to any application? Give an example to support your answer
Answer	Blockchain can be applied to any application, but is not necessarily the best solution. It is effective when there's a need for security, transparency and decentralisation. Example for when blockchain is useful: Supply chain management, where it can be used to track the movement of the package from the manufacturer to the end consumer and ensures that the product is tamper proof.
2	Why do we say that public blockchain is prone to 51% attack?
Answer	Public blockchains are prone to 51% attack because they rely on a decentralized network of users. Anyone with enough computing power can participate in maintaining the blockchain, and if a single user or group of users control over 50% of the computing power, they can manipulate transactions on the blockchain. This is more likely to happen with blockchains that use proof of work consensus algorithms.
3	What is the disadvantage of Consortium blockchain? In what type of systems, would you prefer consortium blockchain over private or hybrid blockchain?
Answer	Consortium blockchain relies on a high level of trust among the participating entities and leads to slower decision-making processes and require more resources to maintain the network and requires consensus among the parties on how the network is managed A consortium blockchain can be used to manage the settlement of

	cross-border payments between multiple banks. By using a shared ledger that records all transactions and enables real-time settlement, the need for intermediaries and corresponding bank accounts can be reduced, which can result in lower costs and faster transaction times.
4	How much time would it require for a miner to mine a block?
Answer	The time required for a miner to mine a block varies depending on the difficulty level and the hash rate and block size and is largely determined by the consensus mechanism of the blockchain. BTC ~10mins
5	Why DES is not a good idea to be used in blockchain setup?
Answer	• DES uses a small key size of 56bits which makes it vulnerable to brute-force attacks and can be cracked in a reasonable amount of time. • DES is a symmetric encryption algorithm, which makes the network less secure as leakage of one of the keys compromises the data generated using that key and an attacker can easily decrypt the message.
6	What are the different fields present in a block header of bitcoin and Ethereum?
Answer	BTC: • Version • Merkle Root Hash • Previous Block Hash • Timestamp • Difficulty • Nonce ETH: • Parent Block Hash • Transaction Hash Root • Receipt Root Hash • State Root Hash

<table>
<tr><td></td><td>

Timestamp
Difficulty
Nonce
Gas Limit
Gas Used

</td></tr>
<tr><td>7</td><td>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</td></tr>
<tr><td>Answer</td><td>

Bob signs the message with his private key Kb and generate a signature S
Bob sends the message m along with his signature S
Alice upon receiving the message m calculates the message digest of the message m using a hash function H(m) and generates a hash h.
Alice decrypts the signature using Bob’s public key Pb to obtain original hash h’. If the process is successful, it implies that the signature has not been tampered with.
Alice compares the calculated hash h against the original hash value h’. If they match, then the message was not tampered with.
If the hashes do not match then, it implies that the message was tampered with/got corrupted before arrival.

</td></tr>
<tr><td>8</td><td>How does blockchain contribute to the development of digital identity and personal data management?</td></tr>
<tr><td>Answer</td><td></td></tr>
<tr><td>9</td><td>Compare and contrast blockchain with other emerging technologies such as artificial intelligence and the Internet of Things</td></tr>
<tr><td>Answer</td><td>
<table>
<tr><td>Blockchain</td><td>AI, IoT</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td colspan="2"><table>
<tr><td>Blockchain is a decentralized and secure database that enables tamper-proof and transparent records of digital transactions.</td><td>AI is the ability of machines to learn, reason, and make decisions like humans.
IoT is a network of connected devices and machines that can communicate and exchange data with each other.</td></tr>
<tr><td>Blockchain offers immutability, transparency, decentralization, security, and anonymity, and can be used for cryptocurrency, supply chain management, digital identity, etc.</td><td>AI is used for natural language processing, image recognition, speech recognition.</td></tr>
<tr><td>Main challenges with blockchain are with respect to scalability, compliance to regulations, user adoption.</td><td>Challenges with AI and IoT include ethical concerns, privacy, data management, security, bias, etc.</td></tr>
<tr><td colspan="2">Despite challenges, these technologies are proving to be effective in fields of digital transactions and personalised experiences.</td></tr>
</table></td></tr>
<tr><td>10</td><td colspan="2">Given a message of 748 bits. How many padded bits are required for SHA 256?</td></tr>
<tr><td>Answer</td><td colspan="2">813+k=512n
K=512n-813
n=2
k=211
211 zeros + 1 one=212 bits</td></tr>
<tr><td>11</td><td colspan="2">What is the future of blockchain-based finance?</td></tr>
<tr><td>Answer</td><td colspan="2">The future of blockchains in finance industry is promising as they offer tamper-proof, transparent, and secure transfer of funds.

Decentralised Finance is getting increasingly popular as new applications are being built on the ETH and Solana blockchains. This is largely due to the fact that these applications are not managed</td></tr>
</table>

	by a single institution and are open source and decentralised. This makes them more resistant to fraud and allows to offer new kinds of financial products and services
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	• Machines that maintain the Bitcoin network have undergone rapid technological development. • The introduction of ASICs has made mining more competitive, as it requires a significant investment in hardware to be competitive in the mining ecosystem. • These devices are designed specifically to mine bitcoin. All hardware and software components of these ASIC devices came pre-designed and optimized to compute strictly those calculations necessary to create new bitcoin blocks. • Some of the latest trends and innovations in the field of blockchain mining include the development of alternative consensus mechanisms, such as Proof-of-Stake (PoS), which is designed to be less energy-intensive than Proof-of-Work (PoW) mining used by Bitcoin and other cryptocurrencies. • Usage of renewable energy sources for mining reduce the carbon footprint and is leading to widespread adoption of the technology.
13	How is difficulty playing an important role in mining process?
Answer	Difficulty is important in the mining process because it helps to regulate the rate at which new blocks are added to the blockchain. When more miners join the network, the target difficulty level is increased to maintain a consistent block time. Conversely, when miners leave the network, the target difficulty level is decreased to maintain a consistent block time. If the difficulty level is too low, new blocks will be added to the blockchain too quickly, which can lead to network congestion and

	potentially compromise the security of the network. On the other hand, if the difficulty level is too high, it can make mining unprofitable and can lead to a reduction in the number of miners.
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 fee is the fee paid in Ether for the amount of computational power (gas) needed to execute a transaction or a contract on the Ethereum blockchain. Gas price is the amount of Ether paid per unit of gas, and it determines the priority of the transaction in the mining process. Block fee, also known as block reward, is the amount of Ether paid to the miner who successfully mines a new block. Uncle fee is the amount paid to the miner who includes a new uncle block, which is a block that is not part of the main blockchain but is still valid and contains valid transactions. Burnt fee is the minimum fee required for a transaction to be included in a block. Bitcoin doesn't have gas fees and burnt fees.
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	To allow for such an update on the network, a new transaction can be made such that it references to the original document and the changes such as address, phone number etc can be added as the data of the new block and committed to the original blockchain ledger. This creates another version of the document with the updated info. This ensures that the immutability property of the blockchain is not compromised.