**BCT Sessional QB – Answers**

|  |
| --- |
| **1. a) What is Blockchain? What are its key elements of blockchain?** |
| **Ans 1. a)**  **Blockchain**   * **Blockchain is a type of shared database that differs from a typical database in the way that it stores information; blockchains store data in blocks that are then linked together via cryptography.** * **As new data comes in, it is entered into a fresh block. Once the block is filled with data, it is chained onto the previous block, which makes the data chained together in chronological order.** * **Different types of information can be stored on a blockchain, but the most common use so far has been as a ledger for transactions.** * **In Bitcoin’s case, blockchain is used in a decentralized way so that no single person or group has control—rather, all users collectively retain control.** * **Decentralized blockchains are immutable, which means that the data entered is irreversible. For Bitcoin, this means that transactions are permanently recorded and viewable to anyone.**   **Key elements of a blockchain:**   1. **Distributed ledger technology**   **All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that’s typical of traditional business networks.**   1. **Immutable records**   **No participant can change or tamper with a transaction after it’s been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.**   1. **Smart contracts**   **To speed transactions, a set of rules — called a smart contract — is stored on the blockchain and executed automatically. A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more.** |
| **1. b) Explain the Core Components of Blockchain Architecture.** |
| **Ans 1. b)**  **Blockchain Architecture**  **Blockchain is a technology where multiple parties involved in communication can perform different transactions without third-party intervention. Verification and validation of these transactions are carried out by special kinds of nodes.**     * **Header: It is used to identify the particular block in the entire blockchain. It handles all blocks in the blockchain. A block header is hashed periodically by miners by changing the nonce value as part of normal mining activity, also Three sets of block metadata are contained in the block header.** * **Previous Block Address/ Hash: It is used to connect the i+1th block to the ith block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.** * **Timestamp: It is a system verify the data into the block and assigns a time or date of creation for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.** * **Nonce: A nonce number which uses only once. It is a central part of the proof of work in the block. It is compared to the live target if it is smaller or equal to the current target. People who mine, test, and eliminate many Nonce per second until they find that Valuable Nonce is valid.** * **Merkel Root: It is a type of data structure frame of different blocks of data. A merkel tree stores all the transactions in a block by producing a digital fingerprint of the entire transaction. It allows the users to verify whether a transaction can be included in a block or not.** |
| **2. a) Discuss about the advantages and disadvantages of blockchain.** |
| **Ans 2. a)**  **Advantages of Blockchain Technology:**   1. **Open: One of the major advantages of blockchain technology is that it is accessible to all means anyone can become a participant in the contribution to blockchain technology, one does not require any permission from anybody to join the distributed network.** 2. **Verifiable: Blockchain technology is used to store information in a decentralized manner so everyone can verify the correctness of the information by using zero-knowledge proof through which one party proves the correctness of data to another party without revealing anything about data.** 3. **Permanent: Records or information which is stored using blockchain technology is permanent means one needs not worry about losing the data because duplicate copies are stored at each local node as it is a decentralized network that has a number of trustworthy nodes.** 4. **Free from Censorship: Blockchain technology is considered free from censorship as it does not have control of any single party rather it has the concept of trustworthy nodes for validation and consensus protocols that approve transactions by using smart contracts.** 5. **Tighter Security: Blockchain uses hashing techniques to store each transaction on a block that is connected to each other so it has tighter security. It uses SHA 256 hashing technique for storing transactions.** 6. **Immutability: Data cannot be tampered with in blockchain technology due to its decentralized structure so any change will be reflected in all the nodes so one cannot do fraud here, hence it can be claimed that transactions are tamper-proof.** 7. **Transparency: It makes histories of transactions transparent everywhere all the nodes in the network have a copy of the transaction in the network. If any changes occur in the transaction it is visible to the other nodes.** 8. **Efficiency: Blockchain removes any third-party intervention between transactions and removes the mistake making the system efficient and faster. Settlement is made easier and smooth.** 9. **Cost Reduction: As blockchain needs no third man it reduces the cost for the businesses and gives trust to the other partner.**   **Disadvantages of Blockchain Technology:**  **1. Scalability: It is one of the biggest drawbacks of blockchain technology as it cannot be scaled due to the fixed size of the block for storing information. The block size is 1 MB due to which it can hold only a couple of transactions on a single block.**  **2. Immaturity: Blockchain is only a couple-year-old technology so people do not have much confidence in it, they are not ready to invest in it yet several applications of blockchain are doing great in different industries but still it needs to win the confidence of even more people to be recognized for its complete utilization.**  **3. Energy Consuming: For verifying any transaction a lot of energy is used so it becomes a problem according to the survey it is considered that 0.3 percent of the world’s electricity had been used by 2018 in the verification of transactions done using blockchain technology.**  **4. Time-Consuming: To add the next block in the chain miners need to compute nonce values many times so this is a time-consuming process and needs to be speed up to be used for industrial purposes.**  **5. Legal Formalities: In some countries, the use of blockchain technology applications is banned like cryptocurrency due to some environmental issues they are not promoting to use blockchain technology in the commercial sector.**  **6. Storage: Blockchain databases are stored on all the nodes of the network creates an issue with the storage, increasing number of transactions will require more storage.**  **7. Regulations: Blockchain faces challenges with some financial institution. Other aspects of technology will be required in order to adopt blockchain in wider aspect.** |
| **2. b) Enlist and explain the applications of blockchain in detail.** |
| **Ans 2. b)** |
| **3. a) Differentiate between Public and Private Ledgers.** |
| **Ans 3. a)** |
| **3. b) What do you understand by the term Hyperledger? Draw and explain its framework.** |
| **Ans 3. b)** |
| **4. a) Explain the use of Cryptography in Cryptocurrencies.** |
| **Ans 4. a)** |
| **4. b) Describe cryptographic algorithm - SHA 256.** |
| **Ans 4. b)** |
| **5. a) Discuss in brief about Hardness of Bitcoin Mining.** |
| **Ans 5. a)** |
| **5. b) How does Double Spending Happen? What are its type?** |
| **Ans 5. b)** |
| **6. a) What do you understand by Bitcoin Wallet? Discuss different types.** |
| **Ans 6. a)** |
| **6. b) Write short notes on POW and POS.** |
| **Ans 6. b)** |
| **7. a) What do you understand by Ethereum Virtual Machine (EVM)? How Does EVM Works?** |
| **Ans 7. a)** |
| **7. b) Discuss about pros and cons in case of EVM.** |
| **Ans 7. b)** |
| **8. a) Write short notes on Ethereum Solidity.** |
| **Ans 8. a)** |
| **8. b) What are smart contracts on blockchain?** |
| **Ans 8. b)** |
| **9. a) Discuss about different Blockchain Implementation Challenges.** |
| **Ans 9. a)** |
| **9. b) Explain about Zero Knowledge proofs and protocols in Blockchain.** |
| **Ans 9. b)** |
| **10. ) Write notes on:**  **i) Succinct non interactive argument for Knowledge (SNARK)**  **ii) Pairing on Elliptic curves**  **iii) Zcash - attacks on Blockchains** |
| **Ans 10. )**  **i) Succinct non interactive argument for Knowledge (SNARK)** |
| **ii) Pairing on Elliptic curves** |
| **iii) Zcash - attacks on Blockchains** |