Q1. What is the difference between hashing and encryption?

Ans. Encryption

a. Encryption is the process of encoding a message or information in such a way that only authorized parties can access it.
b. It uses an algorithm to transform the original message, called plaintext, into an encoded version, called ciphertext, that can be decrypted later with the proper key.
c. Encryption is commonly used to protect data in transit, such as when transmitting data over the internet, as well as to protect data at rest, such as when storing data on a hard drive or in the cloud.

Hashing

a. Hashing, on the other hand, is a process that takes an input (or 'message') and returns a fixed-size string of characters, which represents the original message.
b. This string is known as a 'hash' or 'message digest'.
c. The same input will always produce the same hash, but even a small change to the input will produce a very different hash.
d. Hashing is typically used for data integrity checks, to verify that data has not been tampered with or corrupted.
e. It is also used to create digital signatures and for password storage, among other things.

In summary, the main difference between hashing and encryption is that encryption is reversible (you can go from ciphertext back to plaintext), while hashing is not. Encryption is used to protect the confidentiality of data, while hashing is used to verify the integrity of data.

Q2. Write a short note on distributed consensus.

Ans.

a. Distributed consensus is a process by which a group of distributed nodes (computers) reach agreement on a single value or state of a system.
b. This is typically used in distributed systems where multiple nodes need to agree on a common value in order to maintain consistency and avoid conflicts.
c. There are several algorithms that can be used to achieve distributed consensus, such as the Paxos and Raft algorithms.
d. These algorithms allow nodes to communicate with each other and come to an agreement on the current state of the system, even in the presence of node failures or network partitions.
e. Distributed consensus is an important concept in distributed systems because it allows nodes to reach agreement on a common value despite operating independently and potentially experiencing failures.
f. It is used in various applications, including distributed databases, blockchain technology, and distributed file systems.

Q3. Which are the Properties of Interactive Zero-Knowledge Proofs of Knowledge?

Ans. Interactive zero-knowledge (IZK) proofs of knowledge are a type of protocol that allows one party, known as the prover, to prove to another party, known as the verifier, that

they possess certain knowledge or information without revealing any details about that knowledge. IZK proofs of knowledge have several properties that make them useful in various applications:

1. Completeness: If the prover actually possesses the knowledge being claimed, the verifier will be convinced of this fact.
2. Zero-knowledge: The verifier does not learn any information about the knowledge being claimed other than the fact that the prover possesses it.
3. Soundness: If the prover does not possess the knowledge being claimed, the verifier will not be convinced.
4. Non-interactivity: The proof does not require any interaction between the prover and verifier beyond the initial exchange of information.
5. Perfect zero-knowledge: The proof does not leak any information about the knowledge being claimed, even if the verifier is malicious and tries to extract such information.
6. Succinctness: The proof is relatively short and can be verified quickly.
7. Universality: The proof can be used to prove possession of any knowledge that can be represented in a formal system.

Q4. Explain symmetric and asymmetric algorithm.

Ans. Symmetric algorithms:

1. Symmetric algorithms also known as secret key algorithms, use the same secret key for both encryption and decryption.
2. This means that both the sender and the recipient of an encrypted message must have the same key in order to decrypt the message.
3. Examples of symmetric algorithms include AES, DES, and Blowfish.
4. One advantage of symmetric algorithms is that they are generally faster than asymmetric algorithms, which makes them well-suited for encrypting large amounts of data.
5. However, the key exchange can be a problem with symmetric algorithms because the key must be securely transmitted from the sender to the recipient before the message can be encrypted or decrypted.

Asymmetric algorithms:

1. Asymmetric algorithms, also known as public key algorithms, use a pair of keys: a public key and a private key.
2. The public key is used for encryption and the private key is used for decryption.
3. This means that anyone can use the public key to encrypt a message, but only the owner of the private key can decrypt it.
4. Examples of asymmetric algorithms include RSA, DSA, and Elliptic Curve Cryptography (ECC).
5. One advantage of asymmetric algorithms is that the key exchange problem is solved because the public key can be widely distributed without compromising security.
6. However, asymmetric algorithms are generally slower than symmetric algorithms, which makes them less well-suited for encrypting large amounts of data.
7. They are often used in conjunction with symmetric algorithms to overcome this limitation.

Q5. Explain ECDSA signature generation algorithm.

Ans. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a popular algorithm for generating digital signatures. It is based on the mathematical concept of elliptic curves and is used to generate a pair of keys: a private key and a public key. The private key is used to generate signatures, and the public key is used to verify signatures.

Here is a high-level overview of the ECDSA signature generation algorithm:

1. The sender generates a private key, which is a randomly chosen integer between 1 and a predefined value n.
2. The sender uses the private key to generate a public key, which is a point on an elliptic curve that is calculated using the private key and a predetermined curve equation.
3. The sender hashes the message they want to sign using a cryptographic hash function, such as SHA-256.
4. The sender uses the private key and the hash of the message to generate a digital signature.
5. The sender sends the message, the signature, and the public key to the recipient.
6. The recipient uses the public key and the hash of the message to verify the signature and ensure that it was actually generated by the owner of the private key.
7. ECDSA is widely used in various applications, including securing financial transactions, authenticating users, and establishing trust in online communications.

Q6. What is nothing at the stake problem?

Ans.

a. The nothing at stake problem is a problem that can arise in proof-of-stake (PoS) consensus algorithms, which are used in some cryptocurrencies.
b. In PoS, validators (also known as 'stakers') are chosen to create new blocks and add them to the blockchain based on their stake, or how much of the cryptocurrency they hold.
c. The nothing at stake problem occurs when validators have no "skin in the game" and can validate multiple conflicting blocks without any cost or consequence.
d. This can lead to an attack known as a "bribing attack," where an attacker bribes a validator to validate an illegitimate block, which could allow the attacker to double spend their tokens or perform other malicious actions.
e. One way to solve the nothing at stake problem is to implement a penalty system that punishes validators who try to validate conflicting blocks, thus giving them a stake in the outcome.
f. This can incentivize validators to act in the best interests of the network and discourage them from participating in malicious behavior.
g. Other solutions to the nothing at stake problem include using proof-of-work (PoW) consensus algorithms or hybrid consensus algorithms that combine PoS and PoW.

Q7. Which of the following does PoW consensus guarantee (or guarantee with all but negligible probability)? a) agreement b) validity c) termination
Ans. a) validity

PoW (Proof-of-Work) consensus algorithms guarantee agreement and validity with all but negligible probability. This means that all nodes in the network will agree on the current state of the blockchain and the blocks in the blockchain will be considered valid, with a very high level of confidence.

b) termination

PoW consensus algorithms do not necessarily guarantee termination, as there may be ongoing work being done to create new blocks and add them to the blockchain. In a PoW system, the creation of new blocks is an ongoing process and there is no predetermined end point.

Q8. Compare PoW and PoS consensus mechanisms.

Ans. Proof-of-Work (PoW) and Proof-of-Stake (PoS) are two different consensus mechanisms that are used in different cryptocurrencies. Here are some key differences between the two:

a. Work required: In a PoW system, validators (also known as 'miners') must perform a certain amount of work (typically, solving a complex computational problem) in order to create a new block and add it to the blockchain. In a PoS system, validators are chosen to create new blocks based on their stake (how much of the cryptocurrency they hold).

b. Energy consumption: PoW systems can be energy-intensive because they require a lot of computational power to solve the cryptographic puzzles. PoS systems are generally less energy-intensive because they do not require as much computational power.

c. Speed: PoW systems can be slower than PoS systems because it takes time to solve the cryptographic puzzles. PoS systems can be faster because validators are chosen based on their stake, rather than on their ability to solve puzzles.

d. Decentralization: PoW systems are generally more decentralized than PoS systems because anyone can participate in the mining process by contributing computational power. In a PoS system, only those with a sufficient stake can participate as validators, which may exclude some individuals or entities.

e. Security: Both PoW and PoS systems can be secure, but they each have their own vulnerabilities. PoW systems are vulnerable to 51% attacks, where a single entity or group of entities controls 51% or more of the network's computational power and can manipulate the blockchain. PoS systems are vulnerable to nothing at stake attacks and long range attacks, where validators can create multiple conflicting blocks without any cost or consequence.

Q9. What are the strength and weaknesses of the PoW.

Ans. Proof-of-Work (PoW) is a consensus mechanism that is used in some cryptocurrencies. It is designed to secure the blockchain and deter malicious behavior, such as double spending and denial of service attacks. Here are some strengths and weaknesses of the PoW consensus mechanism:

Strengths:

a. PoW is a well-established and widely used consensus mechanism that has been used successfully in cryptocurrencies like Bitcoin.
b. PoW is decentralized, meaning that anyone can participate in the mining process by contributing computational power. This makes it resistant to censorship and control by any single entity.
c. PoW provides a strong level of security, as it is very difficult to tamper with the blockchain without controlling a majority of the network's computational power.

Weaknesses:

a. PoW is energy-intensive because it requires a lot of computational power to solve the cryptographic puzzles. This can make it expensive to run a mining operation.
b. PoW can be slower than other consensus mechanisms because it takes time to solve the puzzles. This can limit the speed at which transactions can be processed.
c. PoW is vulnerable to 51% attacks, where a single entity or group of entities controls 51% or more of the network's computational power and can manipulate the blockchain.
d. PoW may not be as decentralized as other consensus mechanisms, as the cost of mining equipment and electricity can be prohibitively high for some individuals or entities. This can lead to a small number of large mining pools that have a significant amount of control over the network.

Q10. Explain steps of the PoB and list advantages and disadvantages of PoB.

Ans. Proof of Burn (PoB) is a consensus mechanism that is used in some cryptocurrencies. It involves "burning" or destroying a certain amount of tokens as a way to demonstrate commitment to the network and to obtain the right to participate in the mining process. Here are the steps of the PoB process:

1. A miner sends a certain amount of tokens to a special "burn address," where they are permanently destroyed and removed from circulation.
2. The miner includes a proof of the burn transaction (a message or data that demonstrates that the burn occurred) in a block that they are trying to mine.
3. Other miners verify the proof of burn and, if it is valid, they add the block to the blockchain.
4. The miner who burned the tokens is now eligible to participate in the mining process and can receive rewards for creating new blocks.

Advantages:

1. PoB can reduce the amount of tokens in circulation, which can potentially increase the value of remaining tokens.
2. PoB can incentivize miners to act in the best interests of the network because they have "skin in the game" in the form of the burned tokens.

3. PoB can be more environmentally friendly than Proof-of-Work (PoW) consensus mechanisms, which can be energy-intensive.

Disadvantages:

1. PoB may not be as decentralized as other consensus mechanisms, as only those who are able to burn a significant amount of tokens will be able to participate in the mining process. This can exclude some individuals or entities.
2. PoB may not provide as strong a level of security as PoW, as it may be easier to manipulate the blockchain by burning tokens than by performing work.
3. PoB may not be as well-suited for large-scale networks, as the cost of burning tokens may become prohibitively high.

Q11. Explain the steps of the PoW and comment on the energy efficiency of the PoW.

Ans. Proof-of-Work (PoW) is a consensus mechanism that is used in some cryptocurrencies, such as Bitcoin. It involves miners performing a certain amount of work (typically, solving a complex computational problem) in order to create a new block and add it to the blockchain. Here are the steps of the PoW process:

1. A miner creates a new block by collecting a group of unprocessed transactions (called a 'candidate block') and adding it to the blockchain.
2. The miner includes a special number (called a 'nonce') in the candidate block and calculates the block's hash (a fixed-size string that represents the block's data).
3. The miner's goal is to find a nonce that produces a hash that is below a certain target value. This is called 'mining' the block.
4. Other miners verify the block and, if the hash is valid, they add the block to the blockchain.
5. The miner who mined the block is rewarded with a certain number of tokens.

The PoW process is designed to be energy-intensive because it requires a lot of computational power to solve the cryptographic puzzles. This can make it expensive to run a mining operation and can also have negative environmental consequences due to the energy consumption. Some alternatives to PoW, such as Proof-of-Stake (PoS) and Delegated Proof-of-Stake (DPoS), are less energy-intensive and may be more energy-efficient than PoW.

Q12. List the advantages of the permissioned blockchain.

Ans.

1. Enhanced Security: Permissioned blockchains are more secure than permissionless ones because they have a pre-defined set of known users and each user can be identified and authenticated.
2. Increased Privacy: Permissioned blockchains allow users to control who has access to the data stored on the blockchain. This makes the data more secure and private.
3. Faster Transaction Times: As permissioned blockchains do not require a consensus mechanism, transaction times are much faster than on permissionless blockchains.
4. Improved Scalability: As permissioned blockchains are more efficient in terms of their use of resources, they are able to scale much better than permissionless blockchains.

5. Streamlined Governance: The permissioned model simplifies governance as there is a defined set of participants who can easily review and approve changes to the blockchain.
6. Reduced Costs: As permissioned blockchains are more efficient, they can reduce the costs associated with running a blockchain.

Q13. List the advantages of the permissionless blockchain.

Ans. Advantages:

1. Increased transparency: All transactions are visible and can be publicly verified on the permissionless blockchain.
2. Decentralized: The network is not controlled by a central authority, allowing for greater autonomy and censorship resistance.
3. Low barriers to entry: No permission is required for users to join the network, allowing anyone to access and become a part of the network.
4. Faster transactions: Because there is no need to wait for approval from a central authority, transactions can be completed much faster.
5. Cost efficiency: As there is no need to pay a third-party to approve the transactions, the cost of operations on the network is greatly reduced.
6. Improved Security: The decentralized nature of the blockchain makes it difficult for attackers to target the network, increasing its security.

Q14. List the disadvantages of the permissioned blockchain.

Ans.

1. Limited Scalability: Permissioned blockchains are limited in terms of scalability due to the limited number of nodes operating on the network.
2. High Setup Costs: The setup costs of permissioned blockchains are high due to the need to register, verify and onboard participants.
3. Centralization: Despite being more secure than public blockchains, permissioned blockchains are more centralized and vulnerable to insider attacks due to the limited number of nodes operating on the network.
4. High Maintenance Costs: Permissioned blockchains require extensive maintenance and resources to ensure the network remains secure and operational.
5. Limited Accessibility: Permissioned blockchains have limited accessibility due to the restricted entry of participants.

Q15. How blockchain is different than the distributed databases.

Ans. Blockchains and distributed databases are both decentralized systems that store and manage data across multiple locations. However, there are some key differences between the two:

1. Structure of data: In a distributed database, the data is structured and organized in a traditional database schema, such as rows and columns in a table. In a blockchain, the

data is organized into blocks that are linked together in a linear fashion, forming a chain.

2. Method of consensus: Distributed databases use a centralized method of achieving consensus, such as a quorum or a voting system. Blockchains use a decentralized method of achieving consensus, such as proof-of-work (PoW) or proof-of-stake (PoS), in which the network reaches consensus through the participation of multiple nodes.
3. Immutability: Distributed databases can be modified by authorized users, whereas data on a blockchain is designed to be immutable and cannot be easily altered once it has been added to the chain.
4. Security: Both distributed databases and blockchains can provide a high level of security, but they do so in different ways. Distributed databases rely on traditional security measures, such as user authentication and access controls. Blockchains use cryptographic techniques and a decentralized consensus mechanism to secure the data.
5. Use cases: Distributed databases are often used for traditional database applications, such as storing and managing data for businesses or organizations. Blockchains are often used for applications that require a high level of security and transparency, such as cryptocurrencies and smart contracts.

Q16. How PoW guarantees ledger consistency?

Ans. In a Proof-of-Work (PoW) consensus algorithm, ledger consistency is achieved through a combination of the decentralized nature of the network and the use of cryptographic techniques to secure the data. Here's how PoW guarantees ledger consistency:

1. Decentralization: PoW networks are decentralized, meaning that they are not controlled by any single entity or organization. This makes it difficult for any single node or group of nodes to manipulate the ledger or tamper with the data.
2. Cryptographic techniques: PoW networks use cryptographic techniques, such as hashing, to secure the data on the ledger. This makes it very difficult for anyone to alter the data without being detected.
3. Consensus mechanism: In a PoW network, new blocks are added to the blockchain through a process called 'mining,' in which miners compete to solve a complex computational problem. This process ensures that the network reaches consensus on the current state of the ledger and ensures that all nodes have a consistent view of the data.
4. Network incentives: In a PoW network, miners are incentivized to act in the best interests of the network and to follow the rules of the consensus algorithm. This helps to ensure that the ledger remains consistent and that miners do not try to tamper with the data.

Q17. How PoW guarantees participant’s privacy?

Ans.

a. Proof-of-Work (PoW) consensus algorithms do not specifically guarantee participant privacy. In fact, the transparency of the blockchain means that transaction data is publicly accessible and can be viewed by anyone.

b. However, it is possible to use techniques such as pseudonymity or zero-knowledge proofs to enhance privacy on a PoW blockchain.
c. Pseudonymity involves using a pseudonym or false name to represent the participant, rather than using their real identity.
d. Zero-knowledge proofs allow a participant to prove that they have certain information without revealing the actual information itself.
e. It is important to note that while these techniques can enhance privacy on a PoW blockchain, they are not foolproof and may not provide the same level of privacy as more privacy-focused blockchain protocols or traditional methods of securing data.
f. If privacy is a major concern, it may be more appropriate to use a different blockchain protocol or technology.

Q18. How PoW guarantees ledger anonymity?

Ans.

a. Proof-of-Work (PoW) is a consensus mechanism used in many blockchain networks.
b. It is designed to be a secure and anonymous way of ensuring that the ledger remains accurate and up to date.
c. In PoW, miners compete to solve a cryptographic puzzle and the first one to solve it is rewarded with a certain amount of cryptocurrency.
d. The miner is then rewarded with the right to add a new block to the blockchain.
e. This new block is verified by other miners on the network, and if all goes well, it is added to the ledger and the miner is rewarded with cryptocurrency.
f. PoW ensures ledger anonymity by making sure that the identity of the miner who adds the block to the ledger is unknown.
g. The miner's identity is protected by the cryptographic puzzle and the fact that the miner's solution to the puzzle is unique.
h. This means that it is impossible to determine the identity of the miner who adds a block to the ledger, thus ensuring anonymity.

Q19. How PoW guarantees ledger transparency?

Ans.

a. Proof-of-Work (PoW) consensus algorithms guarantee ledger transparency because the data on the blockchain is publicly accessible and can be viewed by anyone.
b. This is a key feature of many blockchain networks, as it promotes accountability and trust among the participants.
c. In a PoW network, all transactions are recorded on the blockchain in a transparent manner, meaning that anyone can view the details of the transaction, such as the sender, receiver, and amount transferred.
d. This transparency is achieved through the use of cryptographic techniques, such as hashing, which make it very difficult for anyone to alter the data on the blockchain without being detected.
e. Overall, the combination of decentralization and the use of cryptographic techniques in a PoW network helps to ensure ledger transparency and allows anyone to view and verify the data on the blockchain.

Q20. What are the different types of the blockchains?

Ans. Different types of blockchains are:

1. Public blockchains: Public blockchains, also known as permissionless blockchains, are decentralized networks that are open to anyone. They are often used for cryptocurrencies and other applications that require a high level of transparency and accessibility. Examples of public blockchains include Bitcoin and Ethereum.
2. Private blockchains: Private blockchains, also known as permissioned blockchains, are restricted to certain users or entities. They are often used in enterprise settings where there is a need for control over who can participate in the network and access the data. Private blockchains may be more scalable and efficient than public blockchains, but they may be less decentralized and may not provide the same level of transparency.
3. Consortium blockchains: Consortium blockchains are a type of private blockchain that is governed by a consortium, or group, of organizations. They are often used in industries where multiple parties need to collaborate and share data, such as in supply chain management or financial services. Consortium blockchains may be more decentralized than private blockchains, but they may still be less decentralized than public blockchains.
4. Hybrid blockchains: Hybrid blockchains are a combination of public and private blockchains, and they allow for a certain degree of customization and flexibility. They may be used in cases where there is a need to balance the benefits of both public and private blockchains.
5. Sidechains: Sidechains are separate blockchain networks that are connected to a main blockchain through a two-way peg, which allows assets to be transferred between the two chains. Sidechains can be used to test new features or technologies without affecting the main chain, or to enable the use of different consensus mechanisms or smart contract platforms.

Q21. What is Hash function? Write down the properties of good hash functions.

Ans. A hash function is a mathematical function that takes an input (or 'message') and returns a fixed-size string of characters, which is called the 'hash value' or 'digest.' The input can be of any size, but the output is always of a fixed size. Hash functions are used in many different applications, such as data integrity checks, password storage, and blockchain systems.

Here are some properties of good hash functions:

1. Deterministic: A good hash function should always produce the same output for a given input. This means that if the input message is hashed multiple times, the output should be the same each time.
2. Unique: A good hash function should produce a unique output for each unique input. This means that it is very unlikely that two different input messages will produce the same hash.
3. Efficient: A good hash function should be efficient, meaning that it should be able to process large amounts of data quickly.
4. Secure: A good hash function should be resistant to attack, meaning that it should be difficult for an attacker to reverse engineer the input message from the hash or to find two different input messages that produce the same hash.

5. Collision-resistant: A good hash function should be collision-resistant, meaning that it should be difficult to find two different input messages that produce the same hash.
6. Non-invertible: A good hash function should be non-invertible, meaning that it should be difficult to recreate the input message from the hash. This helps to protect the privacy and security of the input message.

Q22. Write short note on Cybil attack.

Ans.

1. A cybil attack is a type of cyber-attack in which an attacker creates multiple fake identities or online profiles in order to manipulate or deceive others.
2. This can be done for a variety of purposes, such as to spread misinformation, influence public opinion, or gain access to sensitive information.
3. Cybil attacks can be difficult to detect and prevent because the attackers often take great care to create realistic and believable profiles.
4. They may use stolen or fake photos, forge documents, or use other tactics to create a convincing identity.
5. To protect against cybil attacks, it is important to be cautious when interacting with people online and to verify the authenticity of their identities.
6. It is also a good idea to use strong passwords and to enable two-factor authentication whenever possible.

Q23. Write short note on eclipse attack.

Ans.

1. An eclipse attack is a type of cyber-attack that targets a decentralized network, such as a blockchain or peer-to-peer network.
2. It involves an attacker isolating a specific node or group of nodes from the rest of the network and manipulating their communication with the other nodes.
3. In a blockchain, an eclipse attack can be used to disrupt the consensus process and prevent the network from reaching agreement on the state of the ledger.
4. This can allow the attacker to manipulate the blockchain and potentially double spend tokens or perform other malicious actions.
5. To protect against eclipse attacks, it is important for decentralized networks to have a diverse and decentralized set of nodes and to use robust communication protocols that are resistant to interference.
6. It is also important for network participants to be vigilant and to report any suspicious activity.

Q24. Write short note on majority attack.

Ans.

1. A majority attack, also known as a '51% attack', is a type of cyber-attack that targets a decentralized network, such as a blockchain or cryptocurrency network.

2. In a majority attack, the attacker is able to gain control of a majority of the nodes on the network, giving them the ability to manipulate the network in a number of ways.
3. For example, an attacker with a majority of the nodes on a blockchain network could double-spend their own coins, block transactions from being processed, or reverse previous transactions.
4. Majority attacks can be difficult to prevent because they rely on the attacker gaining control of a large number of nodes on the network.
5. To protect against majority attacks, it is important to implement security measures such as secure communication protocols and network monitoring tools.
6. It is also a good idea to regularly update and patch network software to help prevent vulnerabilities that could be exploited by attackers.
7. Additionally, decentralized networks may use consensus algorithms that are designed to make it difficult for a single entity to gain control of a majority of the nodes on the network.

Q25. Write short note on blockchain difficulty.
Ans.

1. In a blockchain network, the 'difficulty' refers to the level of computational power or effort required to solve a mathematical problem that is used to create new blocks or to validate transactions.
2. This process, known as mining, is a key part of the consensus mechanism in many blockchain networks.
3. The difficulty of the mathematical problem is typically adjusted over time to ensure that the rate at which new blocks are added to the blockchain is consistent.
4. If the difficulty is too low, new blocks will be added to the blockchain too quickly, leading to an increase in the size of the blockchain and potentially making it more vulnerable to attacks.
5. If the difficulty is too high, new blocks will be added too slowly, which can slow down the overall performance of the network.
6. The difficulty of the mathematical problem is typically measured in terms of the number of leading zeros that must be present in the solution.
7. The higher the difficulty, the more leading zeros are required, which means that it will take more computational power to find a solution.

Q26. Write short note on PoW energy utilization.
Ans.

1. Proof-of-Work (PoW) is a consensus mechanism that is used by some blockchain networks to validate transactions and create new blocks.
2. In a PoW system, miners compete to solve a complex mathematical problem in order to create a new block and earn a reward.
3. The process of solving this problem requires a significant amount of computational power, which consumes a large amount of energy.
4. The energy utilization of PoW systems has been a subject of controversy and concern because of the high levels of energy consumption required to maintain the network.

5. According to some estimates, the energy consumption of the Bitcoin network, which uses a PoW consensus mechanism, is equivalent to the energy consumption of entire countries.
6. Critics argue that the high energy consumption of PoW systems is not sustainable and may have negative environmental impacts.
7. Some alternative consensus mechanisms, such as Proof-of-Stake (PoS), have been proposed as more energy-efficient alternatives to PoW. However, PoW systems have also been praised for their security and decentralization, and many continue to use them for these reasons.

Q27. Write short note on bitcoin incentive mechanism.

Ans.

1. The bitcoin incentive mechanism is a set of rules that incentivize participants in the bitcoin network, known as miners, to validate transactions and create new blocks.
2. Miners earn a reward for their efforts in the form of newly-minted bitcoins, as well as transaction fees from the transactions that they include in the block.
3. The bitcoin incentive mechanism is an important part of the bitcoin network because it helps to ensure that the network remains secure and decentralized.
4. By providing miners with a financial incentive to participate in the network and follow the rules of the consensus algorithm, the incentive mechanism helps to ensure that there is a sufficient number of miners working to validate transactions and create new blocks.
5. The bitcoin incentive mechanism has also been praised for its ability to align the interests of miners with the overall health and security of the network.
6. Because miners are rewarded for their efforts, they have an incentive to act in the best interests of the network and to follow the rules of the consensus algorithm.
7. This helps to ensure that the bitcoin network remains decentralized and secure.

Q28. PoS is more energy efficient than PoW, Justify.

Ans.

1. Proof-of-Work (PoW) and Proof-of-Stake (PoS) are two different consensus mechanisms that are used by some blockchain networks to validate transactions and create new blocks.
2. PoW systems require miners to solve a complex mathematical problem in order to create a new block, while PoS systems require participants to 'stake' their tokens in order to validate transactions and create new blocks.
3. PoS systems are generally considered to be more energy-efficient than PoW systems because they do not require miners to perform energy-intensive computations in order to create new blocks.
4. In a PoS system, the level of computational power required to create a new block is much lower than in a PoW system, which means that less energy is needed to maintain the network.

5. Additionally, because PoS systems do not rely on miners to create new blocks, there is less competition for rewards, which means that the overall energy consumption of the network may be lower.
6. This makes PoS systems a potentially more sustainable alternative to PoW systems for some applications.
7. It is important to note, however, that PoS systems may have other drawbacks, such as reduced security or decentralization, depending on the specific design of the system.

Q29. What are the limitations of the blockchain?

Ans.

1. Scalability: One of the main limitations of many blockchain networks is scalability, meaning that they may struggle to handle large numbers of transactions or users. This can lead to slow transaction speeds and high fees.
2. Lack of regulation: Blockchain technology is still relatively new and is not yet fully regulated, which can create uncertainty and make it difficult for businesses to use it.
3. Limited privacy: While some blockchain networks offer privacy-enhancing features, many do not provide the same level of privacy as traditional systems. This can be a concern for some users or applications.
4. Complexity: Blockchain technology can be complex and may require a certain level of technical knowledge to use and understand. This can be a barrier to adoption for some users.
5. Lack of standardization: There are many different blockchain platforms and technologies, and there is currently no industry-wide standard. This can make it difficult for different systems to interoperate and may create confusion for users.
6. Vulnerability to attack: Like any computer system, blockchain networks are vulnerable to cyber-attacks and other security threats. This can be a concern for users who rely on the security of the network.

Q30. Explain the working of the GHOST mechanism.

Ans.

1. GHOST (short for 'Greedy Heaviest Observed Subtree') is a mechanism that is used to improve the efficiency of Proof-of-Work (PoW) consensus algorithms, which are used by some blockchain networks to validate transactions and create new blocks.
2. In a PoW system, miners compete to solve a complex mathematical problem in order to create a new block and earn a reward.
3. The first miner to solve the problem and create a valid block is rewarded and the block is added to the blockchain.
4. The GHOST mechanism works by allowing miners to include the 'uncles' (or stale blocks) of other miners in the block that they create.
5. Uncles are blocks that were created by other miners but were not included in the main blockchain because they were not the first to solve the mathematical problem.
6. By including uncles in the block, the GHOST mechanism allows miners to build upon the work of other miners and reduces the overall amount of wasted computational power.

7. The GHOST mechanism is used in the Ethereum blockchain, and it has been credited with improving the efficiency and security of the network.
8. It has also been adopted by other blockchain networks that use PoW consensus algorithms.

Q31. Explain hard forking and soft forking in terms of bitcoin blockchain.

Ans.

1. A hard fork is a significant change to the protocol of a blockchain network that is not backward-compatible with the previous version of the protocol.
2. This means that in order to continue participating in the network, all users and nodes must upgrade to the new version of the protocol.
3. If some users do not upgrade, they will be unable to validate transactions or create new blocks, and they may be separated from the main blockchain.
4. A soft fork, on the other hand, is a change to the protocol that is backward-compatible with the previous version.
5. This means that users and nodes do not need to upgrade in order to continue participating in the network.
6. However, they may choose to upgrade in order to take advantage of the new features or improvements introduced by the soft fork.
7. In the context of the bitcoin blockchain, hard forks and soft forks have been used to introduce new features or to address security vulnerabilities.
8. For example, the SegWit (Segregated Witness) soft fork, which was implemented in 2017, introduced a number of improvements to the bitcoin network, including increased capacity and improved security.
9. It is important to note that hard forks and soft forks can be controversial and may lead to disagreement within the community of users and developers.
10. In some cases, hard forks can result in the creation of two separate blockchain networks, each with its own set of users and miners.
11. This can be a concern for users and investors who hold tokens on the blockchain, as the value of their tokens may be affected by the fork.

Q32. How bitcoin blockchain handles temporary forking?

Ans.

1. In a blockchain network, a temporary fork, also known as a 'chain split', occurs when two miners create a new block at the same time and the network is unable to determine which block should be added to the main chain.
2. This can happen when two miners solve the mathematical problem that is used to create new blocks at the same time, or when two miners independently create a new block based on a block that has been orphaned (or rejected) by the network.
3. When a temporary fork occurs, the network will typically choose the block with the most proof-of-work (PoW) as the valid block and add it to the main chain.
4. The other block and any transactions it contains will be rejected and will not be added to the main chain.

5. In the bitcoin blockchain, temporary forks are relatively rare because the probability of two miners solving the mathematical problem at the same time is low.
6. However, they can still occur, and the network is designed to handle them by choosing the block with the most PoW as the valid block.
7. It is important to note that temporary forks do not create a permanent split in the blockchain, and they do not result in the creation of two separate blockchain networks.
8. They are simply a temporary disruption that is resolved when the network chooses the valid block.

Q33. How blockchain provides immutability, transparency, and privacy?

Ans. Blockchain technology has several characteristics that make it unique and powerful. Here is how it provides immutability, transparency, and privacy:

1. Immutability:
    a. Blockchain technology is designed to be resistant to tampering and revision. Once a block of data has been added to the blockchain, it is extremely difficult to change or delete it.
    b. This is because each block is secured using cryptographic techniques, and the data in each block is linked to the data in the previous block.
    c. This means that any attempt to change the data in a block would require the attacker to also change all of the subsequent blocks, which is practically infeasible.
2. Transparency:
    a. While blockchain technology can provide privacy for users, it is also designed to be transparent.
    b. This means that the transactions and data recorded on the blockchain are visible to all users of the network.
    c. This can be useful for a variety of applications, such as supply chain management or financial reporting, where transparency is important.
3. Privacy:
    a. While the transparency of the blockchain can be a useful feature, it can also be a concern for users who want to protect their privacy.
    b. Many blockchain networks, such as those that use the Zero-Knowledge Proof (ZKP) protocol, have built-in privacy features that allow users to keep their data private while still using the blockchain.
    c. For example, ZKP allows users to prove that they have certain information without actually revealing the information itself.
    d. This can be used to provide privacy in a variety of applications, such as voting or medical records.

Q34. Explain practical byzantine fault tolerance mechanism.

Ans.

1. Practical Byzantine Fault Tolerance (PBFT) is a consensus mechanism that is used to ensure that a distributed system, such as a blockchain network, can continue to function even if some of its nodes are behaving incorrectly or maliciously.
2. In a PBFT system, each node communicates with the other nodes in the network and reaches a consensus about the current state of the system.
3. If a node behaves incorrectly, it may be excluded from the consensus process.
4. This helps to ensure that the network can continue to function even if some of its nodes are behaving maliciously or are experiencing technical issues.
5. PBFT is designed to be efficient and scalable, making it well-suited for use in large, distributed systems.
6. It is also resistant to the 'Byzantine Generals' problem, which refers to the challenge of achieving consensus in a distributed system when some of the nodes may be behaving dishonestly or have conflicting information.
7. PBFT has been used in a number of blockchain and distributed systems, including the Hyperledger Fabric blockchain platform and the Google Cloud Spanner database system.
8. It is often praised for its security and efficiency, although it may be less decentralized than some other consensus mechanisms.

Q35. Write short note on double spending in bitcoin.

Ans.

1. Double spending is a potential issue in a digital currency system, such as bitcoin, where it is possible to spend the same digital token multiple times.
2. This can occur when a user is able to create multiple copies of a digital token and use each copy to make a separate transaction.
3. To prevent double spending, the bitcoin network uses a distributed ledger, known as the blockchain, to keep track of all transactions.
4. Each transaction is validated by multiple nodes on the network, and once a transaction is added to the blockchain, it is extremely difficult to change or reverse.
5. This helps to ensure that a digital token can only be spent once.
6. Despite the safeguards in place to prevent double spending, it is still theoretically possible for an attacker to attempt a double-spend attack.
7. However, such attacks are rare and are generally not successful because they require a significant amount of computational power and would be easily detected by the network.
8. Overall, the use of a decentralized, distributed ledger helps to ensure that the bitcoin network is resistant to double spending and other types of fraud.

Q36. How to decide that 1KKhtG8XygZM7ioyWFWUzSwGZTjFcs8nR4 bitcoin address has suspicious activities.

Ans.

1. First visit to bitcoinabuse portal to verify that address belongs to bitcoin blockchain.
2. Verify that the address is reported by someone as a malicious or not if yes then the address is malicious otherwise we need to check financial transactions of that account.

3. Visit bitref and insert suspected bitcoin address in the search box and hit enter. This will give us details about list of transactions are done by that address.
4. Search number of transactions and intended source and recipient for those transaction on blockchain.com
5. If after six or more hopes bitcoin is again resend to this address it indicates that address is suspicious.
6. Search current address and all other suspicious address on bitcoinwhoswho portal to get its IP.
7. Search that IP on the passivedns to get URL for that IP address.
8. After getting URL finally search who owns that URL on the whois.domaintolls.com

Q37. Explain bitcoin transaction flow. How miner solves bitcoin block cryptopuzzle.

Ans. The process of a bitcoin transaction can be broken down into the following steps:

1. A user initiates a transaction by sending a message to the bitcoin network, indicating the amount of bitcoin they want to send and the address of the recipient.
2. The transaction is broadcast to the network and is picked up by miners, who are responsible for validating transactions and creating new blocks.
3. Miners verify the transaction to ensure that the sender has sufficient funds and that the transaction follows the rules of the bitcoin network.
4. Once the transaction has been verified, it is added to a pool of unconfirmed transactions, known as the mempool.
5. Miners compete to solve a complex mathematical problem, known as the 'block cryptopuzzle', in order to create a new block. The block cryptopuzzle is designed to be difficult to solve, but easy to verify once a solution has been found.
6. The first miner to solve the block cryptopuzzle creates a new block, which includes the verified transactions from the mempool. The miner is rewarded with newly-minted bitcoins for their efforts.
7. The new block is broadcast to the network and is added to the blockchain, a decentralized, distributed ledger that records all bitcoin transactions.
8. Once the transaction has been added to the blockchain, it is considered to be complete and cannot be reversed.

Overall, the process of a bitcoin transaction involves multiple parties, including the sender, the recipient, and the miners who validate and record the transaction. The use of the block cryptopuzzle helps to ensure the security of the network by making it difficult for attackers to manipulate transactions.

Q38. Differentiate between permissioned and permissionless blockchain?

Ans. Permissioned blockchain:

1. Also known as 'private' or 'consortium' blockchain.
2. Requires users to have permission to join the network and participate in the consensus process.
3. Usually has a restricted set of nodes or users who are allowed to validate transactions and create new blocks.

4. May have a centralized authority that controls access to the network and makes decisions about changes to the network.
5. Examples include Corda, Hyperledger Fabric, and Ripple.

Permissionless blockchain:

1. Also known as 'public' blockchain.
2. Allows anyone to join the network and participate in the consensus process.
3. Has a decentralized network of nodes that validate transactions and create new blocks.
4. Does not have a centralized authority that controls access to the network.
5. Examples include Bitcoin and Ethereum.

Overall, permissioned blockchain is often used for applications that require a higher level of control or privacy, such as financial systems or supply chain management. Permissionless blockchain, on the other hand, is often used for applications that require a higher level of decentralization or transparency, such as public record-keeping or cryptocurrency.

Q39. Write short note on the forking and its variations in the bitcoin blockchain.

Ans.

1. In the context of the bitcoin blockchain, a fork refers to a change to the rules of the network that is not backward-compatible with the previous version of the software.
2. This can occur when the developers of the bitcoin software introduce a change to the protocol that is not supported by all users of the network.
3. There are two main types of forks in the bitcoin blockchain: hard forks and soft forks.
    a. A hard fork is a significant change to the protocol that is not backward-compatible and requires all users to upgrade to the new version of the software. This can result in the creation of two separate blockchain networks, each with its own set of users and miners. Hard forks are often used to introduce new features or address security vulnerabilities.
    b. A soft fork, on the other hand, is a change to the protocol that is backward-compatible and does not require all users to upgrade. Soft forks are usually less disruptive than hard forks, as they do not result in the creation of two separate blockchain networks.
4. There are also several variations of forks, including accidental forks, intentional forks, and contentious forks.
5. An accidental fork occurs when two miners create a new block at the same time, resulting in a temporary split in the blockchain.
6. An intentional fork is a planned change to the protocol that is carried out by the developers of the bitcoin software.
7. A contentious fork is a fork that is opposed by a significant portion of the community and may result in the creation of two separate blockchain networks.
8. Overall, forks can be a complex and controversial topic in the bitcoin community, and they can have significant implications for users and investors.
9. It is important to carefully consider the potential consequences of a fork before deciding whether to support it.

Q40. Write short note on blockchain identity management?

Ans.

1. Blockchain identity management is the use of blockchain technology to create, store, and manage digital identities.
2. A digital identity is a representation of an individual or entity on the internet, and it can be used for a variety of purposes, such as verifying the identity of a user or granting access to a particular service.
3. There are several benefits to using blockchain for identity management.
    a. Blockchain technology is secure and resistant to tampering, which makes it well-suited for storing sensitive personal information.
    b. Blockchain can provide a decentralized and transparent way to manage identities, which can help to reduce the risk of fraud or identity theft.
    c. Blockchain can enable users to have more control over their own identity and personal data, as they can store and manage it on the blockchain rather than relying on a centralized authority.
4. There are a number of different approaches to using blockchain for identity management, including the use of self-sovereign identity systems and decentralized identity systems.
5. Self-sovereign identity systems allow users to create and manage their own digital identities, while decentralized identity systems use blockchain technology to create a decentralized network of identity providers.
6. Overall, blockchain identity management has the potential to revolutionize the way that we think about and manage digital identities, and it has applications in a wide range of industries, including finance, healthcare, and government.

Q41. Explain overall working of the bitcoin blockchain.

Ans.

1. The bitcoin blockchain is a decentralized, distributed ledger that records all bitcoin transactions.
2. It is a key component of the bitcoin network and is responsible for ensuring the integrity and security of the network.
3. The bitcoin blockchain works by using a network of nodes, or computers, that communicate with each other to validate and record transactions.
4. When a user wants to send bitcoin to another user, they create a transaction message and broadcast it to the network.
5. Miners, who are special nodes on the network, are responsible for verifying the transaction and adding it to the blockchain.
6. They do this by solving a complex mathematical problem, known as the 'block cryptopuzzle', in order to create a new block.
7. The block cryptopuzzle is designed to be difficult to solve, but easy to verify once a solution has been found.
8. Once a miner has solved the block cryptopuzzle, they create a new block that includes the verified transaction and broadcast it to the network.
9. Other miners on the network verify the block and, if it is valid, add it to the blockchain.
10. In this way, the bitcoin blockchain is able to securely and transparently record all bitcoin transactions, ensuring the integrity of the network.

11. The decentralized and distributed nature of the blockchain means that it is resistant to tampering and censorship, and it enables users to securely transfer value without the need for a central authority.

Q42. How blockchain can handle real time day to day challenges?

Ans. Blockchain technology has the potential to address a wide range of real-time challenges in various industries, including finance, supply chain management, and healthcare. Here are a few examples of how blockchain can handle real-time challenges:

1. Financial transactions: Blockchain can be used to facilitate real-time financial transactions, such as cross-border payments or stock trades. By using blockchain, these transactions can be completed more quickly and securely, as they do not need to go through a central authority or clearinghouse.
2. Supply chain management: Blockchain can be used to create a transparent and immutable record of the movement of goods through the supply chain. This can help to reduce the risk of fraud or counterfeiting, as well as improve efficiency by providing real-time visibility into the status of shipments.
3. Healthcare: Blockchain can be used to create a secure and decentralized record of patient medical records, allowing healthcare providers to access and share important information in real-time. This can improve patient care and reduce the risk of errors.

Overall, the use of blockchain technology can help to improve efficiency, security, and transparency in a wide range of real-time challenges across various industries.

Q43. What are the challenges in the blockchain regulation in the India?

Ans. There are several challenges that have been identified in relation to the regulation of blockchain technology in India. Some of these challenges include:

1. Lack of clear guidelines: There are currently no comprehensive guidelines or regulations in place in India that specifically address blockchain technology. This lack of clarity can make it difficult for businesses and individuals to understand how to comply with the law when using blockchain.
2. Lack of understanding: Many regulators and policy-makers in India may not have a thorough understanding of blockchain technology and its potential applications, which can make it difficult to craft effective regulations.
3. Complex legal issues: Blockchain technology raises a number of complex legal issues, such as how to handle disputes or fraud, that will need to be addressed in order to effectively regulate the technology.
4. Balance between innovation and regulation: There is a tension between the need to encourage innovation and the need to protect consumers and the financial system. Striking the right balance between these competing priorities will be a challenge for regulators in India.

Q44. Define blockchain.

Ans.

1. A blockchain is a decentralized, distributed ledger that is used to record transactions across a network of computers.
2. It consists of a series of blocks, each of which contains a record of multiple transactions.
3. The blocks are connected in a chronological chain, with each block containing a reference to the previous block.
4. The decentralized nature of the blockchain means that it is not controlled by any single entity, such as a government or financial institution.
5. Instead, the network is maintained by a decentralized network of computers, known as nodes, that work together to validate and record transactions.
6. The use of a blockchain allows for secure, transparent, and immutable record-keeping, as it is extremely difficult to alter the information stored on the blockchain once it has been added.
7. This makes it well-suited for a variety of applications, including financial transactions, supply chain management, and record-keeping.

Q45. Explain DAO and DAO attack.

Ans.

1. A Decentralized Autonomous Organization (DAO) is a type of organization that is run using smart contracts on a blockchain platform.
2. A DAO is decentralized in the sense that it is not controlled by any single individual or entity, but rather operates according to rules and protocols that are encoded into its smart contracts.
3. DAOs are often used to facilitate decentralized decision-making and funding, as they allow stakeholders to vote on proposals and allocate funds in a transparent and secure manner.
4. A DAO attack refers to an attempt to exploit vulnerabilities in a DAO's smart contracts or to manipulate the decision-making process of the DAO in some other way.
5. For example, an attacker may try to gain control of a significant portion of the voting power in a DAO in order to influence the outcome of votes.
6. One of the most well-known DAO attacks occurred in 2016, when an attacker exploited a vulnerability in the smart contract of the Ethereum-based DAO and was able to drain approximately $50 million worth of ether from the organization.
7. The attack led to a hard fork in the Ethereum blockchain and had significant implications for the Ethereum community.
8. Overall, DAO attacks highlight the need for careful design and testing of smart contracts in order to ensure the security and integrity of DAOs and other decentralized organizations.

Q46. What is Smart Contract? Explain it with example.

Ans.

1. A smart contract is a type of computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract.

2. Smart contracts allow the performance of credible transactions without third parties.
3. These transactions are trackable and irreversible.
4. For example, a smart contract could be used to facilitate the exchange of money, property, shares, or anything of value in a transparent, conflict-free way while avoiding the services of a middleman.
5. In this example, the smart contract would be programmed to automatically transfer the asset to the buyer once the agreed-upon conditions are met, such as the receipt of payment.

Q47. Explain the concept of digital signature in Blockchain in detail.

Ans.

1. A digital signature is a cryptographic technique used to authenticate the identity of the individual or entity that created or signed a document or transaction.
2. Digital signatures use public key cryptography to provide a secure and tamper-proof way of verifying the authenticity of digital documents and transactions.
3. In blockchain, digital signatures are used to verify the validity of transactions and confirm the identity of the sender.
4. Each transaction is digitally signed with the sender's public key and the receiver's public key.
5. This ensures that only the sender can sign the transaction and only the receiver can validate it.
6. Digital signatures are an important component of blockchain technology as they help to ensure that the data stored in the blockchain is authentic and has not been tampered with.
7. They also provide an additional layer of security by preventing malicious actors from making unauthorized changes to the blockchain.
8. As such, digital signatures are an essential part of any blockchain-based system.

Q48. What is Gas and Gas limit? Explain all the cases.

Ans.

1. In the context of the Ethereum blockchain, gas refers to the unit of measurement for the amount of computational work required to execute a transaction or smart contract.
2. Every action on the Ethereum network, such as executing a smart contract or sending a transaction, requires a certain amount of gas.
3. The gas limit is a parameter that sets the maximum amount of gas that can be used in a particular block.
4. The gas limit is set by the miner who creates the block, and it is included in the block header.
5. There are several factors that can affect the amount of gas required to execute a transaction or smart contract, including the complexity of the code, the number of operations being performed, and the current state of the network.
6. If a transaction or smart contract requires more gas than is available in the gas limit, it will fail and the associated fees will not be refunded.

7. On the other hand, if a transaction or smart contract uses less gas than the gas limit allows, the excess gas will be refunded to the sender.
8. Overall, gas and the gas limit are important considerations for users of the Ethereum network, as they can affect the cost and success of transactions and smart contracts.

Q49. Explain the role of Merkle tree in Blockchain.

Ans.

1. A Merkle tree, also known as a hash tree, is a data structure that is used to efficiently summarize and verify the integrity of large sets of data.
2. In the context of blockchain, a Merkle tree is used to create a digital fingerprint, or hash, of a set of transactions, and to verify the integrity of the transactions with a high level of efficiency.
3. Each leaf node in a Merkle tree represents a transaction, and each non-leaf node represents the hash of its child nodes.
4. The root node of the tree is a single hash that summarizes the entire set of transactions.
5. The use of a Merkle tree in blockchain allows for efficient and secure verification of the transactions in a block.
6. When a new block is added to the chain, the miner includes the root hash of the block's Merkle tree in the block header.
7. This allows any node in the network to verify the integrity of the transactions in the block by recalculating the root hash and comparing it to the one provided in the block header.
8. Overall, the use of a Merkle tree is an important part of the security and efficiency of many blockchain systems, as it allows for fast and secure verification of large sets of transactions.

Q50. Explain role of Blockchain in Medical Record Management System.

Ans.

1. We face a lot of issues, such as doctor’s appointments, report organization in one spot, and report follow-ups. People now bring a large number of papers to the doctor’s chamber.
2. They carry prescriptions, reports, and X-ray files, among other things. It complicates everyone’s life as a result.
3. All of the reports must be reviewed by doctors on a regular basis. It is difficult to read old reports on a regular basis, and patients do not receive the correct medications or treatment.
4. Doctors also find it extremely difficult to comprehend handwritten prescriptions. Data security, authenticity, time management, and other areas of data administration are dramatically improved when blockchain (smart contract) technology is linked with standard database management solutions.
5. Blockchain is a groundbreaking, decentralized technology that protects data from unauthorized access.

6. After smart contracts are implemented, the management will be satisfied with the patients.
7. As a result, maintaining data privacy and accountability in the system is tough.
8. It signifies that the information is only accessible to those who have been authenticated.
9. Blockchain focuses on limiting third-party engagement in medical health data and improving data security.
10. Throughout the process, this will improve accessibility and time efficiency.
11. People will feel safer during the payment procedure, which is the most significant benefit.
12. A smart contract and a peer-to-peer encrypted technology were used.
13. The hacker will not be able to gain access to this system since this document uses an immutable ledger.
14. They will not be able to change any of the data if they gain access to the system. If the items are found to be defective, the transaction will be halted.
15. Transaction security will be a viable option for recasting these problems using cryptographic methodologies.

Q51. What is Quantum Computing? Explain its need in Blockchain.

Ans.

1. Quantum computing is a method of solving problems that are too large or complex for traditional computers by employing the laws of quantum mechanics.
2. This branch of computer science employs quantum theory principles. Quantum theory explains how energy and matter behave at the atomic and subatomic levels.
3. Qubits, or quantum bits, are the fundamental unit of information in quantum computing. In traditional computing, this is analogous to a binary bit.
4. Whereas traditional computers use bits with either 0s or 1s to store information, quantum computers use qubits.
5. Qubits carry information in a multidimensional quantum state.
6. Quantum Key Distribution (QKD) uses quantum mechanics laws to allow two parties to exchange secure data for detecting whether a third party is attempting to eavesdrop on their exchange.
7. Using quantum keys in conjunction with a blockchain network could help protect against attacks from both classical and quantum computers.