Q.1 Which of the following is popularly used for storing bitcoins?

Pocket

Wallet

Box

Stack

Q.2 Which site run by Ross Ulbricht was closed by the FBI for letting people buy drugs with Bitcoin?

Silk Road

Lace Place

Silk Street

Dark Alley

Q.3 Which of these US states introduced the BitLicense regulation for cryptocurrency companies?

New York

California

Texas

Washington

Q.4 Cryptographic Hash Function transforms an arbitrary length of a fixed length string that act more or less as a Fingerprint of the document

True

False

Q.5 What is the name of the famous Bitcoin exchange from Japan that collapsed in 2014?

Blockchain.info

Tradehill

Mt. Gox

Bitstamp

Q.6 What does the block in the blockchain consist of?

Transaction data

A Hash point

A Timestamp

All of these

Q.7 After 10 Minutes a new block is formed that contains latest transactions

True

False

Q.8 A bitcoin address collision happens when 2 different payments are made at the same time to the same bitcoin address

True

False

Q.9 What is not a ledger type considered by users in Blockchain?

Distributed Ledger

Decentralized Ledger

Both a and b

None of these

Q.10 What is the impact of information leak for an organization?

Loss in profit

Loss of trust in costumers

Cut down the reputation of the organization

All of these

Q.11 What time did Bitcoin Network Start?

January 2009

September 2001

November 2008

Q.12 How many new Bitcoins are created every day?

2200 Except of leap year

3600

7200

5000

Q.13 What is the initial application for which Blockchain was designed?

Peer-to-peer finance application

Research Project

 Open source finance software to connect Banks

None of these

Q.14 An orphan block is only created when 51% attack is successful

True

False

Q.15 Where is the bitcoin central server located?

Washington DC

Undisclosed Location

London

None of these

Q.16 What does a ledger in blockchain does?

Mapping between owner and object

Identification of objects owned

Identification of owners

Q.17 First step of Blockchain project implementation is?

Requirement identification

Feasible study on the security

Controlling and monitoring the project

Screen idea consideration

Q.18 What is the name of the first academic paper that describes bitcoin commonly referred to as?

The origins of money

The Bitcoin Whitepaper

The great unrevealing

Q.19 Which of the following is important for Blockchain

Database Security

Auditing

Planning

Q.20 How often does Bitcoin ledger reconcile

Every day

Every 3 months

Every 3 Minutes

Every 10 Minutes

General Blockchain Interview Questions

Q 1. What do you know about Blockchain? What is the difference between Bitcoin blockchain and Ethereum blockchain?

The blockchain is a **decentralized distributed database** of immutable records. The technology was discovered with the invention of Bitcoins(the first cryptocurrency). It's a trusted approach and there are a lot of companies in the present scenario which are using it. As everything is secure, and because it's an open source approach, it can easily be trusted in the long run.

Bitcoin Blockchain and Ethereum Blockchain		
Topics	**Bitcoin**	**Ethereum**
Concept	Digital Currency	Smart Contracts
Founder	Satoshi Nakamoto	Vitalik Buterin
Release Method	Genesis Block Mined	Presale
Cryptocurrency Used	Bitcoin(Satoshi)	Ether
Algorithm	SHA-256	Ethash
Blocks Time	10 Minutes	12-14 Seconds
Scalable	Not yet	Yes

Q 2. What is the principle on which blockchain technology is based on?

It enables the information to be distributed among the users without being copied.

Q 3. What are the different types of Blockchains?
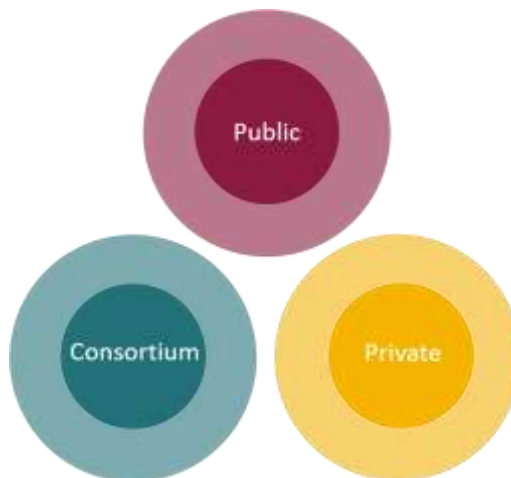
Blockchains are of three types:

Q 4. Why is Blockchain a trusted approach?

- Blockchain can be trusted due to so many reasons.
- Its compatibility with other business applications due to its open-source nature.

- Its security. As it was meant for online transactions, the developers have paid special attention to keeping up the pace when it comes to its security.
- It really doesn't matter what type of business one owns, Blockchain can easily be considered.

Q 5. Name the two types of records that are present in the blockchain database?

These records are block records and transactional records. Both these records can easily be accessed, and the best thing is, it is possible to integrate them with each other without following the complex algorithms.

Q 6. Blockchain is a distributed database. How does it differ from traditional databases?

Properties	Blockchain	Traditional Database
Operations	Only Insert Operations	Can perform C.R.U.D. operations
Replication	Full Replication of block on every peer	Master Slave Multi-Master
Consensus	Majority of peers agree on the outcome of transactions	Distributed Transactions (2 phase commit)
Invariants	Anybody can validate transactions across the network	Integrity Constraints

Q 7. What are the properties of Blockchain?

There are four key features of blockchain:

- Decentralized Systems
- Distributed ledger
- Safer & Secure Ecosystem
- Minting

**Q 8. What is encryption? What is its role in Blockchain?**

Data security always matters. Encryption is basically an approach that helps organizations to keep their data secure.

The encrypted data is encoded or changed up to some extent before it is sent out of a network by the sender and only authorized parties can access that information.In Blockchain, this approach is useful because it simply adds more to the overall security and authenticity of blocks and helps to keep them secure.

Q 9. What do you mean by blocks in the blockchain technology?

Blockchain consists of a list of records. Such records are stored in blocks. These blocks are in turn linked with other blocks and hence constitute a chain called Blockchain.
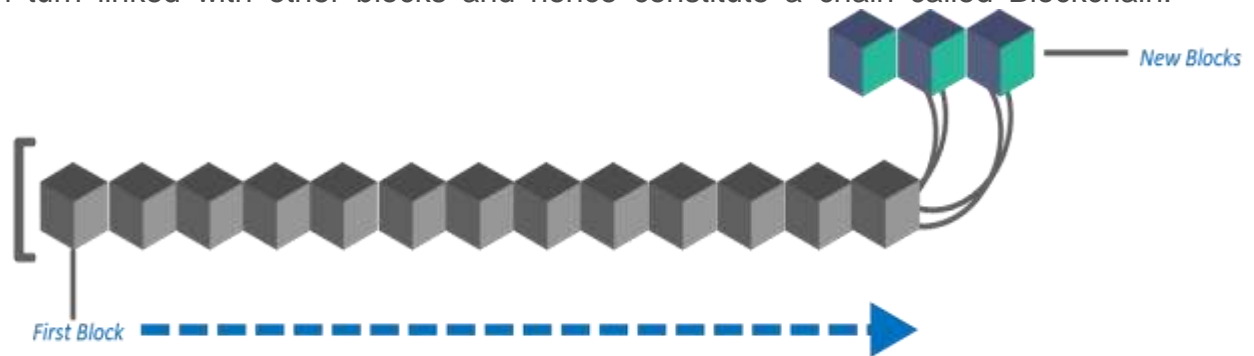
Q 10. How does a block is recognized in the Blockchain approach?

Every block in this online ledger basically consists of a hash pointer which acts as a link to the block which is prior to it, transaction data and in fact a stamp of time.

Q 11. Is it possible to modify the data once it is written in a block?

No, it's not possible to do so. In case any modification is required, the organization simply has to erase the information from all other blocks too. It is because of no other reason than this, data must be given the extreme care of while using this approach.

Q 12. What are Block Identifiers?

In Blockchain, blocks can be identified by the *block header hash* and the *block height*.

Q 13. Is it possible in Blockchain to remove one or more block from the networks?

Yes, it can be done. There are times when only a specific portion of this online ledger is to be considered. With the help of default options and filters, this can easily be done without making a lot of efforts.

Q 14. What exactly do you know about the security of a block?

Well, a block or the entire blockchain is protected by a strong cryptographic hash algorithm. Each block has a unique hash pointer. Any modification in the block constituents will result in the change in the hash identifier of the block. Therefore, it offers an excellent level of security. Thus, one needs not to worry about the safety as well as the security of data that is present in a block.

Q 15. What are Merkle trees? How important are Merkle trees in Blockchains?

Merkle Tree also known as 'hash tree' is a data structure in cryptography in which each leaf node is a hash of a block of data, and each non-leaf node is a hash of its child
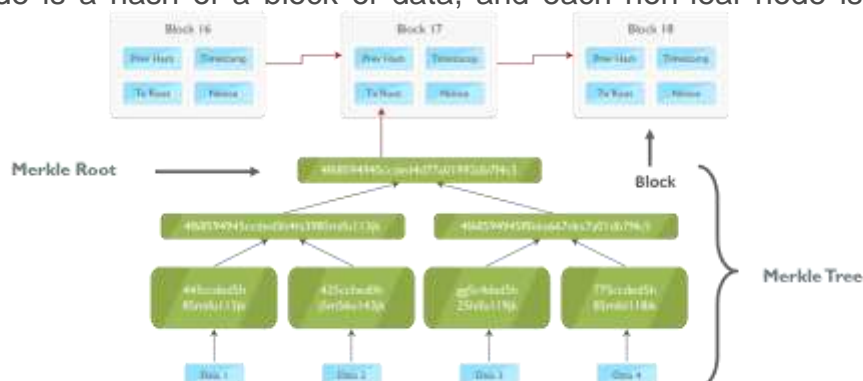

nodes.

The benefit of using the Merkle Tree in blockchain is that instead of downloading every transaction and every block, a "light client" can only download the chain of block headers.

Also, if someone needs to verify the existence of a specific transaction in a block, then he doesn't have to download the entire block. Downloading a set of a branch of this tree which contains this transaction is enough. We check the hashes which are just going up the branch (relevant to my transaction). If these hashes check out good, then we know that this particular transaction exist in this block.

Q 16. What is a ledger? Is Blockchain an incorruptible ledger?

Blockchain is considered incorruptible. Any ill-intentioned individual acting alone is powerless. "To take over the network, an attacker would have to control more than 50 percent of its total computing power," Augier explains. "We hope that's a theoretical scenario, but we can't be sure. Should it happen, the individual would take every precaution to avoid being noticed." Not to mention the energy required to power the computers needed for the blockchain system to work.

Q 17. Name the common type of ledgers that can be considered by users in Blockchain?

Centralized network   Decentralized network   Distributed network
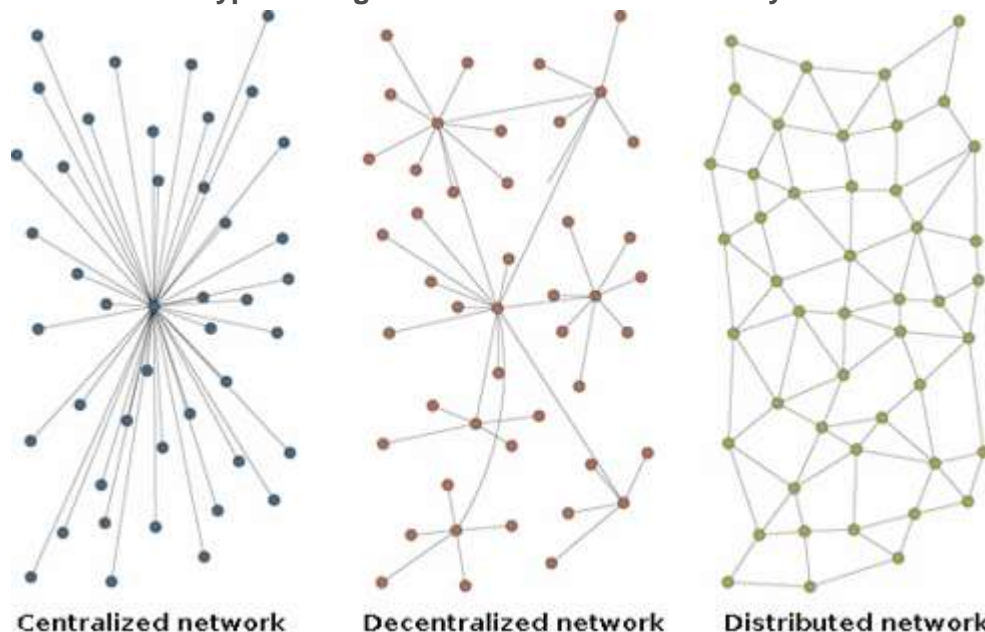
These are:

Q 18. How is a blockchain ledger different from an ordinary one?

The first and in fact the prime difference is Blockchain is a digital ledger that can be decentralized very easily. The chances of error in this approach are far less than that in an ordinary ledger. An ordinary ledger is what that is prepared by hands or by human efforts while the Blockchain performs all its tasks automatically. You just need to configure it in a proper manner and by following all the guidelines.

Q 19. What type of records can be kept in a Blockchain? Is there any restriction on same?

There is no restriction on keeping records of any type in the Blockchain approach. Industries are using Blockchain for securing all types of records.

The common types of records (to name a few) that can be kept on the Blockchains are:
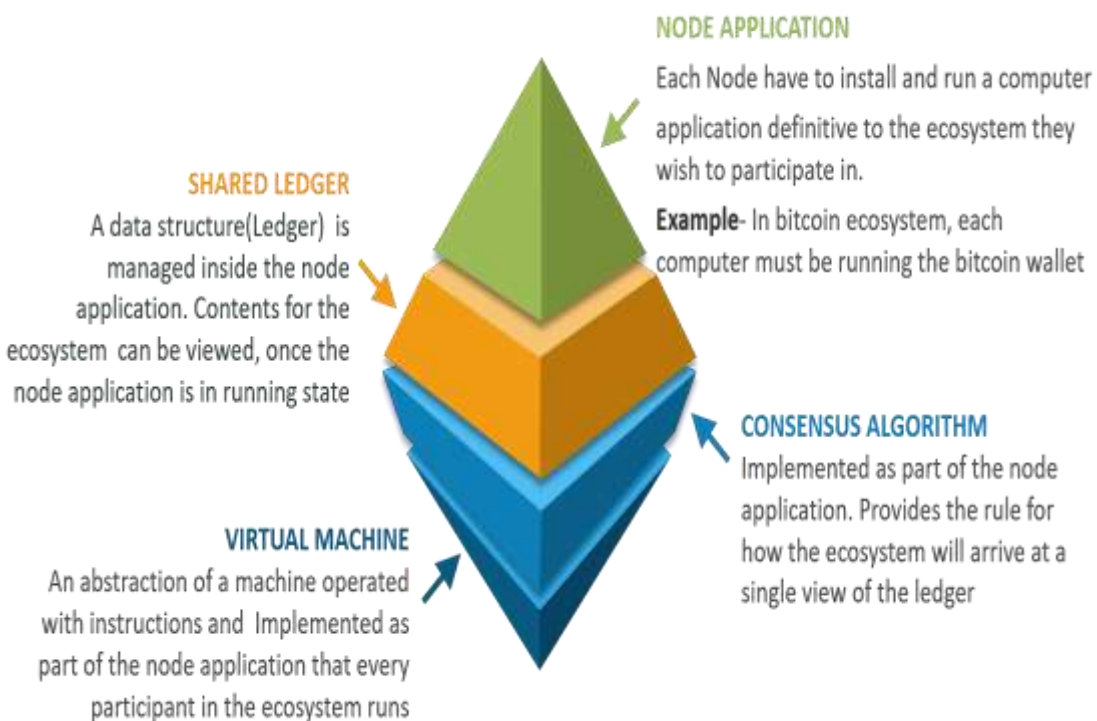
- Records of medical transactions
- Identity management
- Transaction processing
- Business transactions,
- Management activities
- Documentation

Q 20. A distributed digital ledger is used for recording transaction in Blockchain. What does the system rely on?
The system relies on the network servicing protocol and the nodes of the network.

Q 21. Can You explain the components of Blockchain Ecosystem?
Following are the components of blockchain Ecosystem:

NODE APPLICATION

Each Node have to install and run a computer application definitive to the ecosystem they wish to participate in.

Example- In bitcoin ecosystem, each computer must be running the bitcoin wallet

SHARED LEDGER

A data structure(Ledger) is managed inside the node application. Contents for the ecosystem can be viewed, once the node application is in running state

CONSENSUS ALGORITHM

Implemented as part of the node application. Provides the rule for how the ecosystem will arrive at a single view of the ledger

VIRTUAL MACHINE

An abstraction of a machine operated with instructions and Implemented as part of the node application that every participant in the ecosystem runs

Q 22. State difference between proof-of-work & proof-of-stake?

| The probability of mining a block depends on the amount of work a miner does | Takes more energy than Proof of Stake | One example is Mining, which uses computer cycle time to validate new transactions |

VS

| Stakeholders validate new blocks by utilizing their share of coins on the network | The first example of Proof of Stake was Peercoin | A user would need to own a majority of all coins in order to attack the network |

Proof-of-work vs proof-of-stake

Q 23. Name some popular platforms for developing blockchain applications

After the development of bitcoin, various blockchain platforms started coming up. Ethereum came right after the evolution of Bitcoins, and is one of the popular public platforms for building Blockchain based applications.
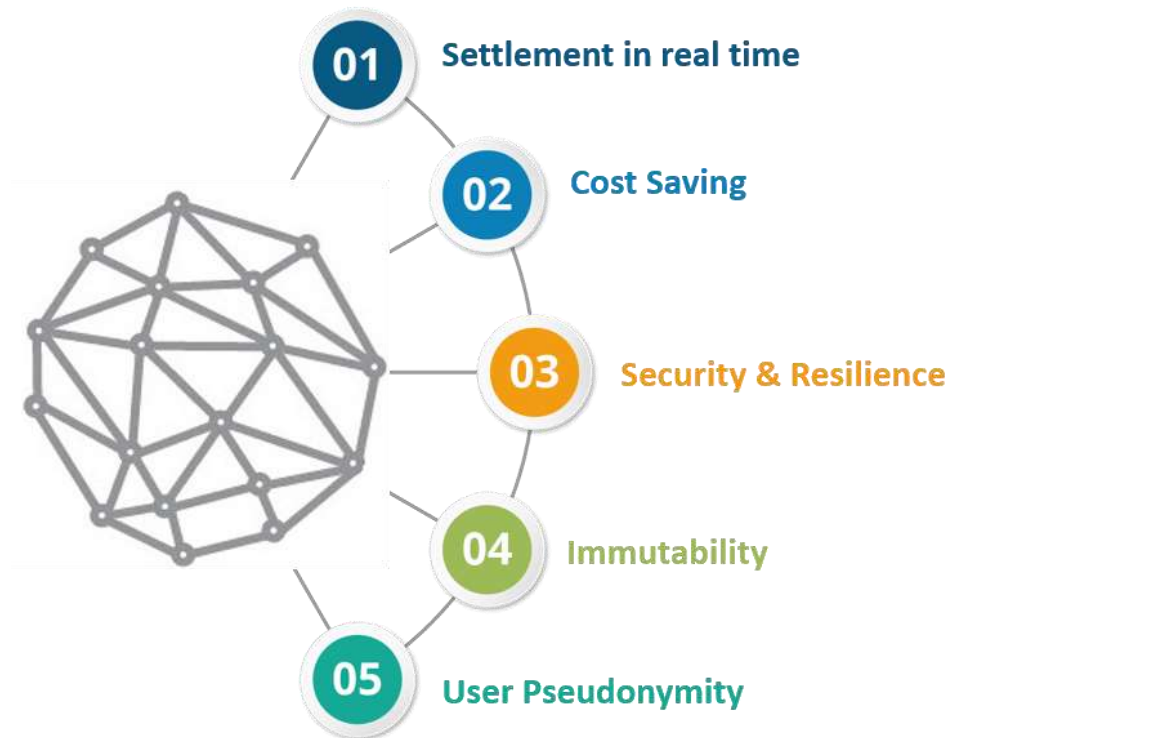
Then there is a Hyperledger community for building enterprise-based solutions. Also, Qtum, IOTA, EOS are some of the widely used platforms for building Blockchain.

Q 24. What is Double Spending? Is it possible to double spend in a Blockchain system?

It's a condition when one digital token is spent multiple times because the token generally consists of a digital file that can easily be cloned. It simply leads to inflation and organizations must bear a huge loss. One of the primary aims of Blockchain technology is to eliminate this approach up to the possible extent.

Blockchain prevents double spending by confirming a transaction by multiple parties before the actual transaction is written to the ledger. It's no exaggeration to say that the entirety of bitcoin's system of Blockchain, mining, proof of work, difficulty etc, exist to produce this history of transactions that is computationally impractical to modify.

Q 25. What are the benefits of Blockchain that you know?

01 Settlement in real time

02 Cost Saving

03 Security & Resilience

04 Immutability

05 User Pseudonymity

Multiple Choice Blockchain Interview Questions

Q 1. Each block of a Blockchain consists of which of the following?
A hash pointer to the previous block
Timestamp
List of transactions
All of the above *[Ans]*

Q 2. Which of the following is first distributed blockchain implementation?
Bitcoin *[Ans]*

Ethereum

Q 3. Bitcoin is based on _____ blockchain?
Private

Public *[Ans]*

Public Permissioned

Permissioned

Q 4. Blockchain can be stored as which of the following?
A flat file
A Database
Both of the above *[Ans]*
None of the above

Q 5. In blockchain, blocks are linked _____?
Backward to the previous block *[Ans]*
Forward to next block
Not linked with each other

Q 6. The primary benefit of immutability is…
Scalability

Improved Security

Tamper Proof

Increased Efficiency *[Ans]*

Q 7. Hash identifying each block in the Blockchain is generated using which of the following cryptographic algorithm?
SHA128
SHA256 *[Ans]*

Q 8. A block in the blockchain can never have more than one parent block?
True *[Ans]*

False

Q 9. Blockchain forks can result in which of the following?
Multiple parent blocks
Multiple children blocks *[Ans]*

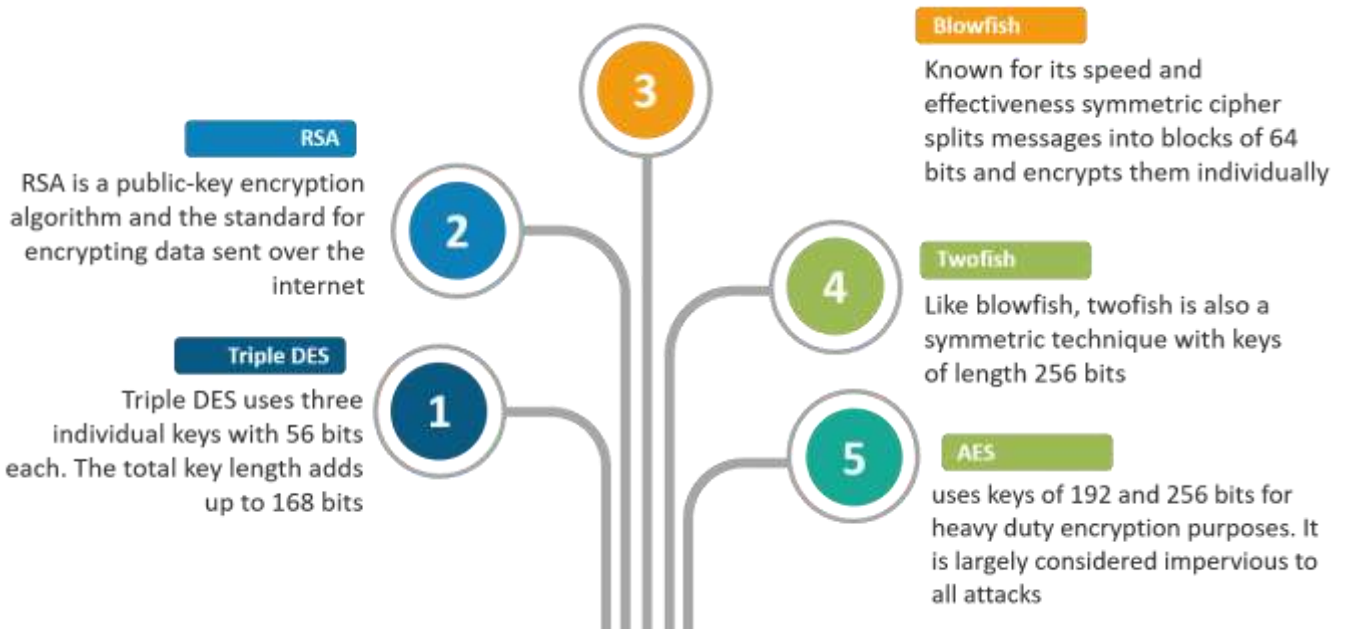**Q 10. Which of the following is asymmetric encryption Algorithm?**
Blowfish

Twofish
RSA *[Ans]*
Tripple DEA

Advanced Blockchain Interview Questions
Q 1. Can you tell me some of the widely used cryptographic algorithms?

Blowfish
Known for its speed and effectiveness symmetric cipher splits messages into blocks of 64 bits and encrypts them individually

RSA
RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet

Twofish
Like blowfish, twofish is also a symmetric technique with keys of length 256 bits

Triple DES
Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits

AES
uses keys of 192 and 256 bits for heavy duty encryption purposes. It is largely considered impervious to all attacks

Q 2. Tell me more about RSA algorithm? How secure is this algorithm?

Security of R.S.A.

There are different approaches used in attacking the RSA algorithm:

- **Brute force:** It involves all possible secret keys
- **Mathematical attacks:** In mathematical attack, we are using different techniques, which is similar in effort to factor the product of two primes

Q 3. Explain the significance of blind signature and how it is useful?

It is a form of digital signature in which the content of a message is disguised (blinded) before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message in the manner of a regular digital signature.

Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes.

Q 4. What is Secret Sharing? Does it have any benefit in Blockchain technology?

It is a well-known fact that security matters a lot in digital transactions. Secret sharing is an approach meant for same. In Blockchain technology it is an approach that divides secret or personal information into different units and sent them to the users on the network.

The original information can only be combined when a participant to whom a share of the secret is allocated agree to combine them together with others. There are several security-related benefits it can offer in Blockchain technology.

Q 5. Can you explain what are off-chain transactions?

An off-chain transaction is the movement of value outside of the blockchain. While an on-chain transaction – usually referred to as simply 'a transaction' – modifies the blockchain and depends on the blockchain to determine its validity an off-chain transaction relies on other methods to record and validate the transaction.

Q 6. What exactly do you know about executive accounting? Does Blockchain support the same?

Executive accounting is nothing but a special type of accounting which is designed exclusively for a business that offers services to the people. There is no strict upper limit on services and a business can manage any through the executive accounting. Blockchain has algorithms that are specially meant to handle executive accounting. In fact, it cut down many problems that are associated with the same.

Q 7. What are the threats to the information you are familiar with?

There are lots of threats to information in the present scenario. Due to increase in online transactions over the internet, many hackers have become active and are adopting new approaches to hack information and servers that contain financial information.

The major threat is software attack, identity theft, information extortion, as well as sabotage. In addition to this, Trojan horses, worms, and viruses are other trouble creators.

Q 8. How will you handle the risk management when it comes to securing the transactions records?

It is basically a process of finding the threats and all the vulnerabilities to the financial records of an organization. The best thing that can be done with this approach is to take the right countermeasures against them immediately.

Another approach is to pay attention to a backup plan. Based on the value of information, more approaches such as buying new risk management software can simply be considered. The prime risk to information is from black-hat hackers.

Q 9. What is 51% attack?

51% Attack refers to a situation where a group of miners who hold more than 50% of the Network Hash Rate could manipulate with the New transactions (Stopping the transactions to proceed or gaining conformations) or able to reverse the transactions that were recently confirmed and kind of doing Double spend. It is Highly unlikely to be able to do that today but it is possible.

Q 10. What challenges information leak can impose on an organization?

An information leak can cut down the reputation of an organization up to an excellent extent. In addition to this, it can be the reason for organization bearing huge losses. Many organizations who fail to implement security protocols to keep their data secure have already lost the trust of their customers and are struggling very hard to get the same reputation again. The overall profits of any organization can reduce up to 80% if no attention is paid to the online transaction security.

Q 11. What is information processing according to you? What are the key challenges that are associated with it?

The information is often shared on a network. Before actually transmitting it over a network, it needs to be changed into formats that can fit the standards of the channels (the channel is a link between the sender and a receiver).

The work done to convert the information at both sender and receiver end is generally regarded as information processing. The biggest challenge to information processing is securing it during that time. Another challenge is processing bulk information can impose a limit on performance.

Q 12. Name organizations that can use Blockchain technology?

There is no strict upper limit on the category of business who can consider this approach. The fact is almost all the businesses are engaged in online or financial transactions that they need to make to run the processes smoothly. Large-scale corporations, financial institutions, private businesses, government departments and even defense organizations can trust this technology very easily.

Q 13. What are the core requirements for a Business Blockchain?
A business blockchain requires a shared ledger, smart contract functionality, privacy and trust.

Q 14. What are the key principles in Blockchain that are helpful in eliminating the security threats that needs to be followed?

Yes, there are a few principles that need to be followed with respect to time. They are:
1.Auditing
2.Securing applications
3. Securing testing and similar approaches
4. Database security
5. Continuity planning
6. Digital workforce training

All these principles are basic and are easy to implement. They are helpful in making the transactions records useful.

Q 15. What is a security policy?
A security policy defines what exactly needs to be secured on a system. It bounds a network user under some core protocols that they all must agree and follow to enhance the overall security. When it comes to information or financial records of an organization, multiple security policies are implemented than just one.

Q 16. Is the Blockchain Different from Banking Ledgers?
Banks and accounting systems use ledgers to track and timestamp transactions. The difference is that the blockchain is completely decentralized and an open source. This means that people do not have to rely on or trust the central bank to keep track of the transactions. The peer-to-peer blockchain technology can keep track of all the transactions without the fear of having them erased or lost.

Furthermore, the blockchain, because of its open-source nature, is more versatile and programmable than central banking ledgers. If programmers need new functionality on the blockchain, they can simply innovate on top of already existing software through consensus. This is difficult for central banks because of all of their regulations and central points of failure.

Q 17. Can you list some of the popular consensus algorithms? Why we need different consensus mechanisms?

Some of the popular consensus algorithms are:

- PBFT (Practical Byzantine Fault Tolerance)
- Proof-of-work
- Proof-of-stake
- Delegated proof-of-stake
- Proof-of-elapsed time

Now, the possible reasons why we need consensus mechanism more than "proof-of-work" are"

- Different business needs
- Different use cases
- Also:

- Cryptography/Strength of Algorithm
- Regulation requirements
- Implementation
- Performance
- Tokenization
- Security
- Privacy

Q 18. Is there any network specific conditions for using Blockchain technology in an organization?

There is no specific condition of using it. However, the network must be a peer-to-peer network under the concerned protocols. It validates the new block simply and helps organizations to keep up the pace in this matter without investing in third-party applications.

Q 19. Name the steps that are involved in the Blockchain project implementation?

Well, there are total six steps involved in this process and they are:

1. Requirement identification
2. Screen ideas consideration
3. Project development for Blockchain
4. Feasible study on the security
5. Implementation
6. Controlling and monitoring the project

Q 20. Explain a real-life use-case where Blockchain is being used?

Blockchain in Stock Market

Problems in Present Stock Market:

Centralized and expensive

- Depositories and transfer agents are a single point of failure
- Registration, transfer, distribution, scrutineering, courier fees

- The more widely held, the higher the administration costs

Limited Transparency

- Information asymmetry leads to market advantages
- Forged securities still a concern
- Counterparty risk is systemic

How Blockchain solves the problem

The centralized hub can be removed and the blockchain can be used to directly transfer share ownership between investors.
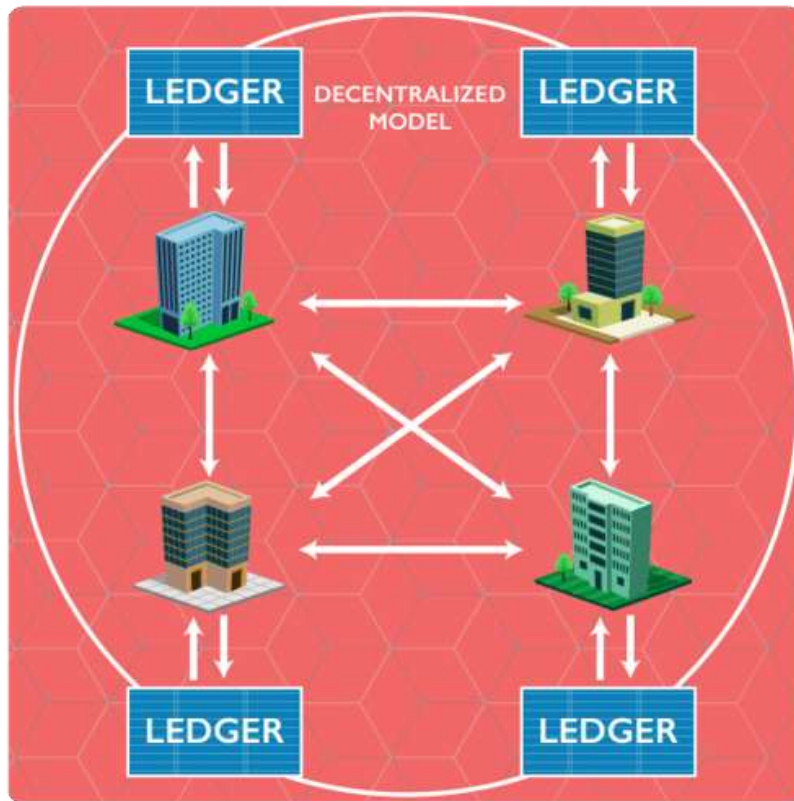
A ledger updated in minutes could save millions in collateral and settlement costs, while also automating banks' creaky and expensive back office systems.