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?
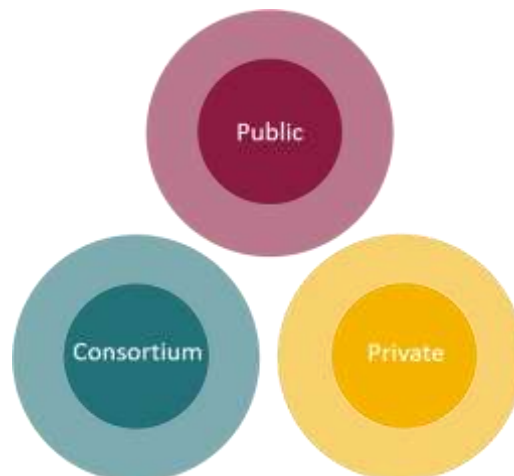
Blockchains are of three types:

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.

First Block
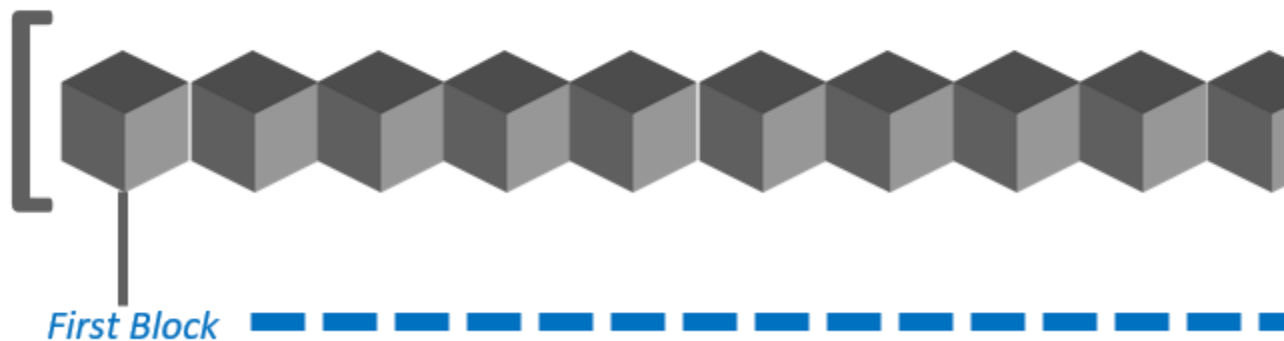
Q 10. How does a block is recognized in the Blockchain approach?

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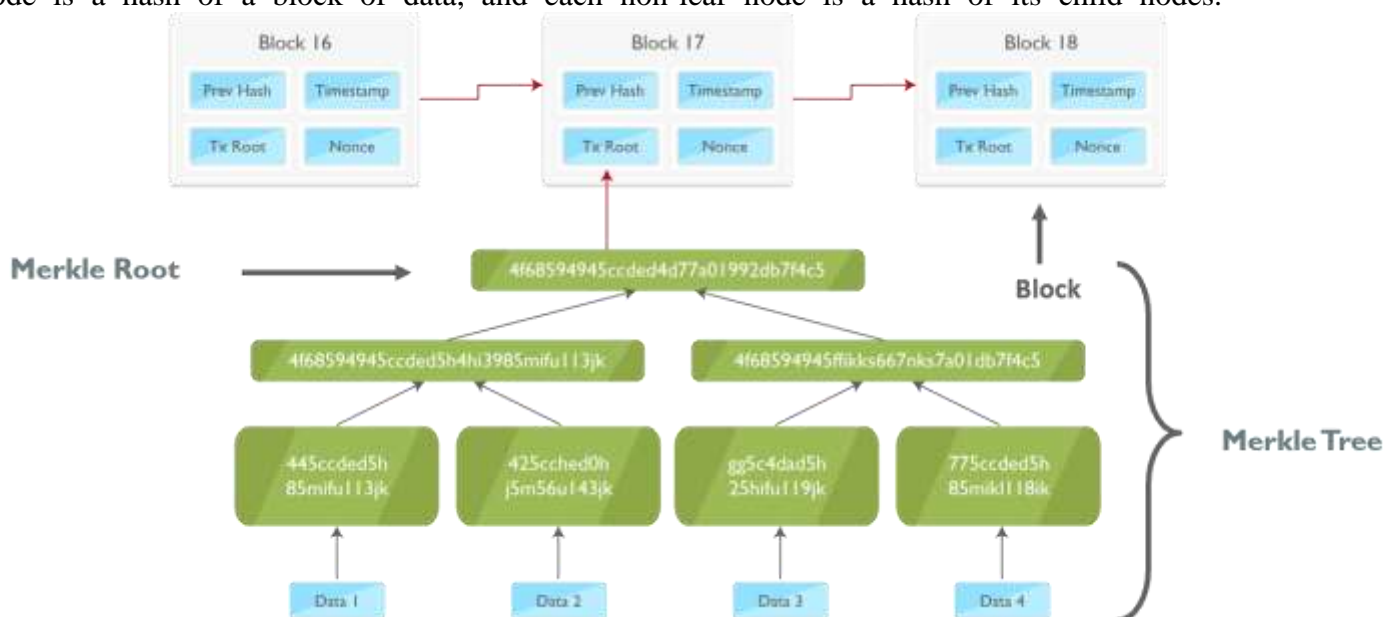
The benefit of using the Merkle Tree in blockchain is that instead of downloading every transaction and every block, a "light client" can only download the chain of block headers.

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
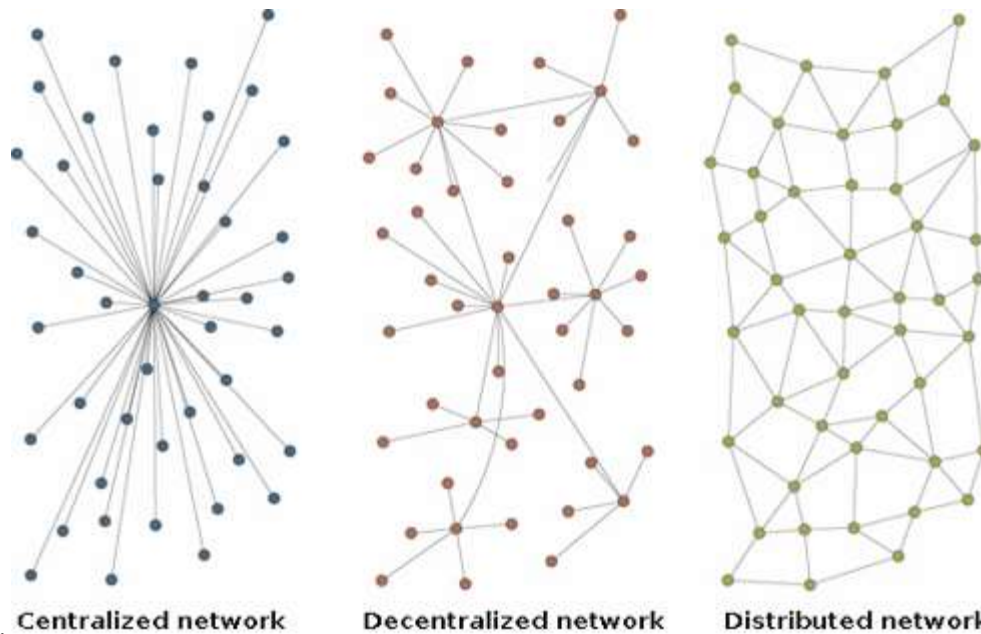
These are:

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:

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

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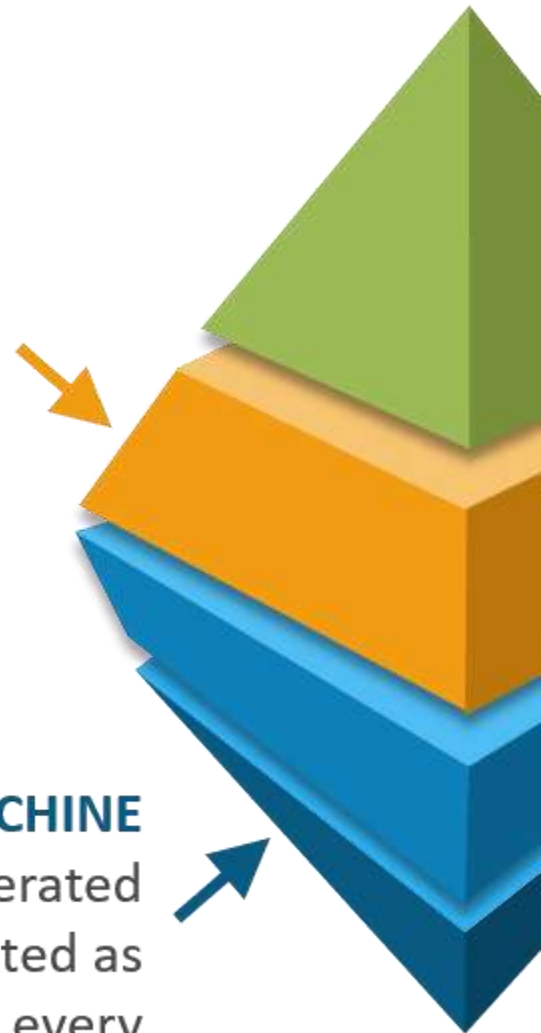
Q 22. State difference between proof-of-work & proof-of-stake?
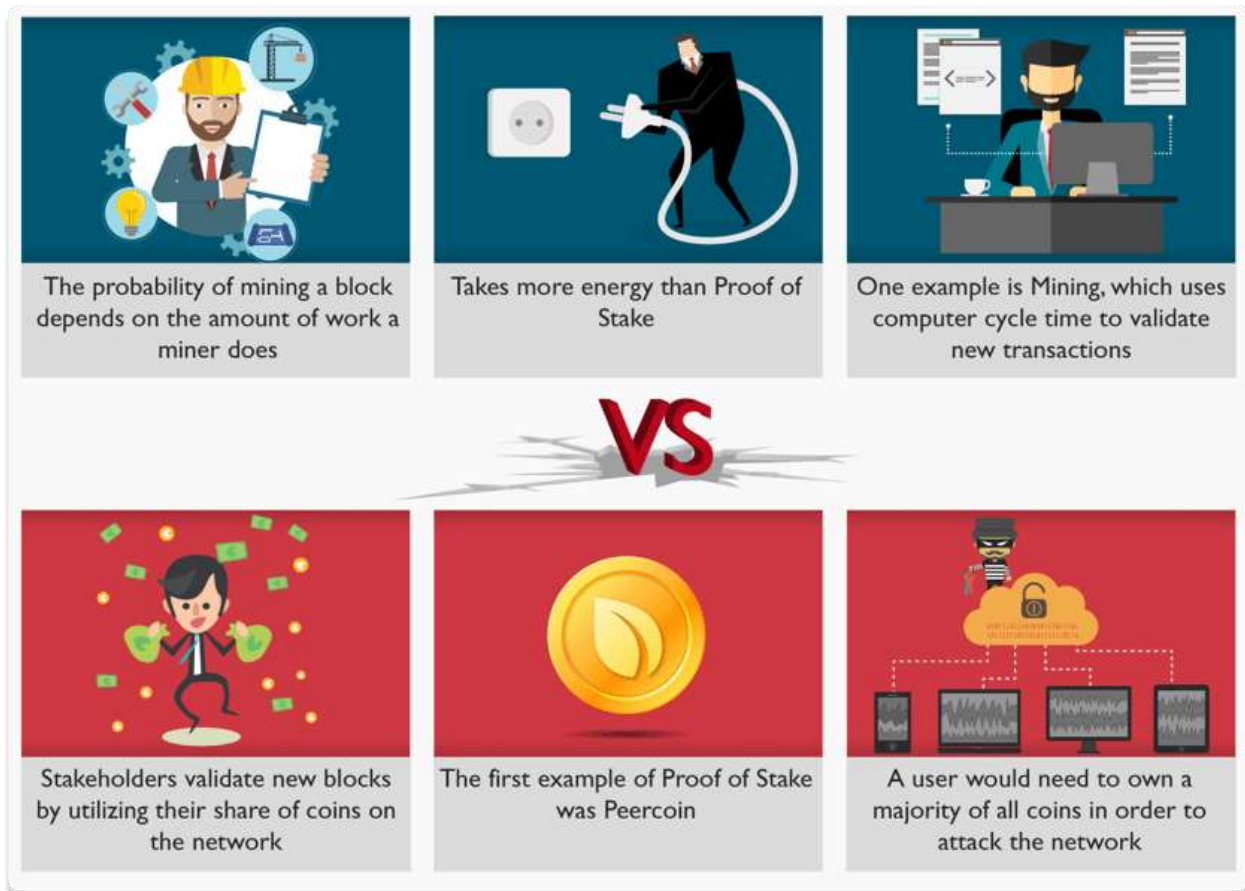
Proof-of-work vs proof-of-stake

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?
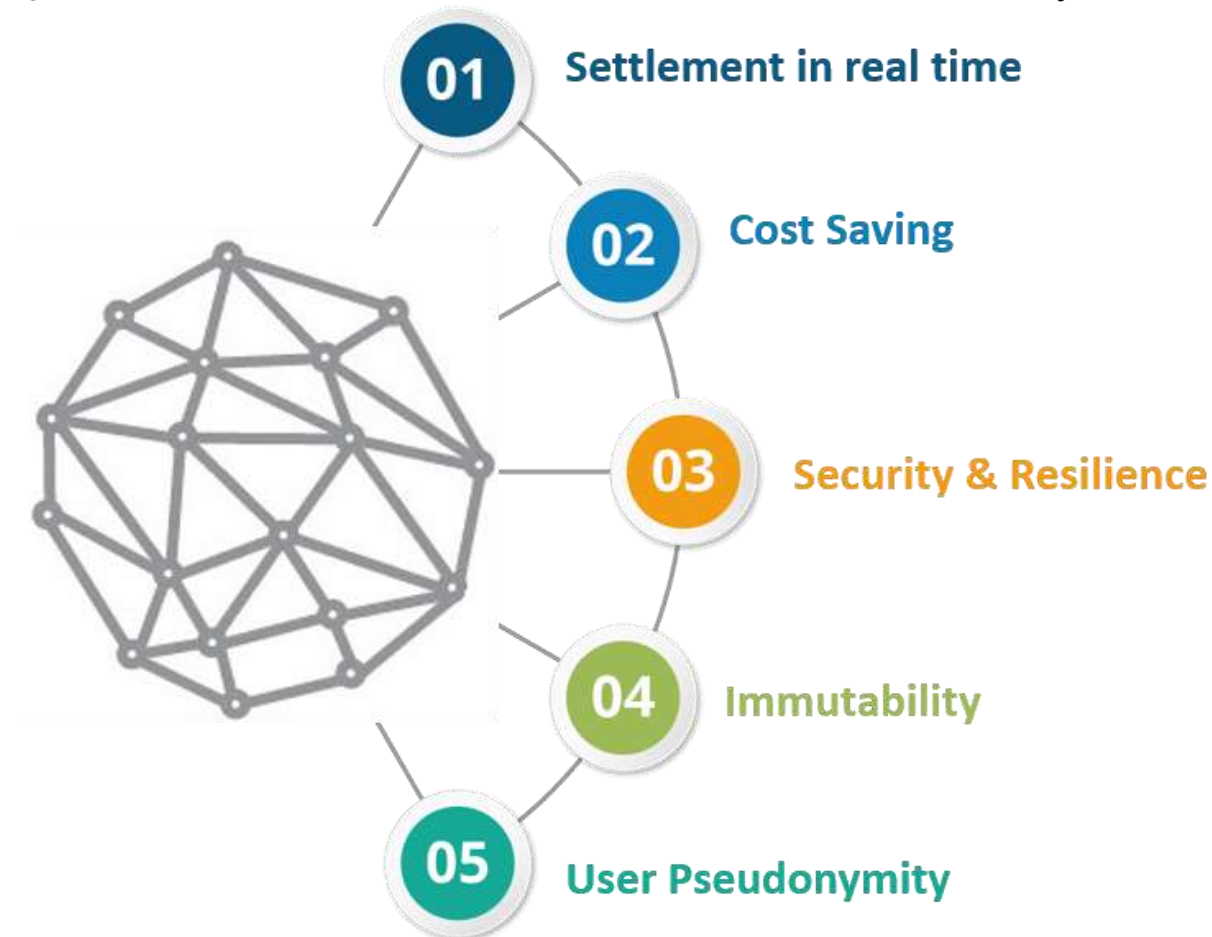
Multiple Choice Blockchain Interview Questions

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

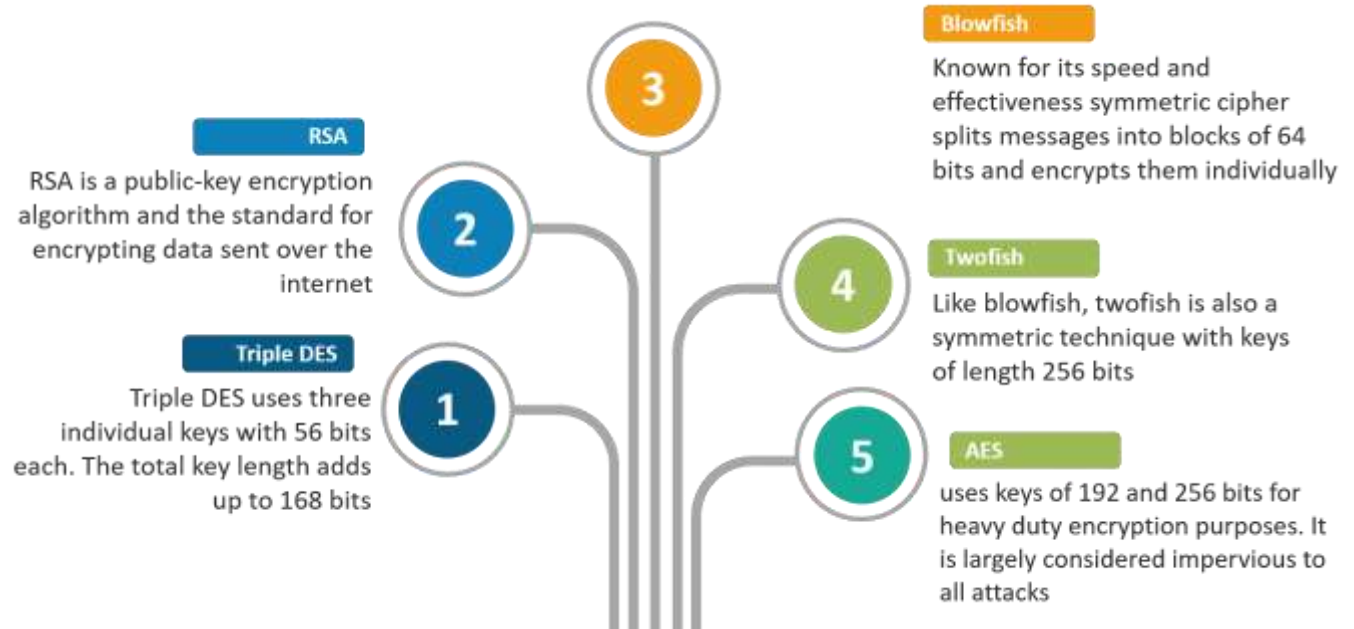## Q 9. Blockchain forks can result in which of the following?

Multiple parent blocks
Multiple children blocks *[Ans]*

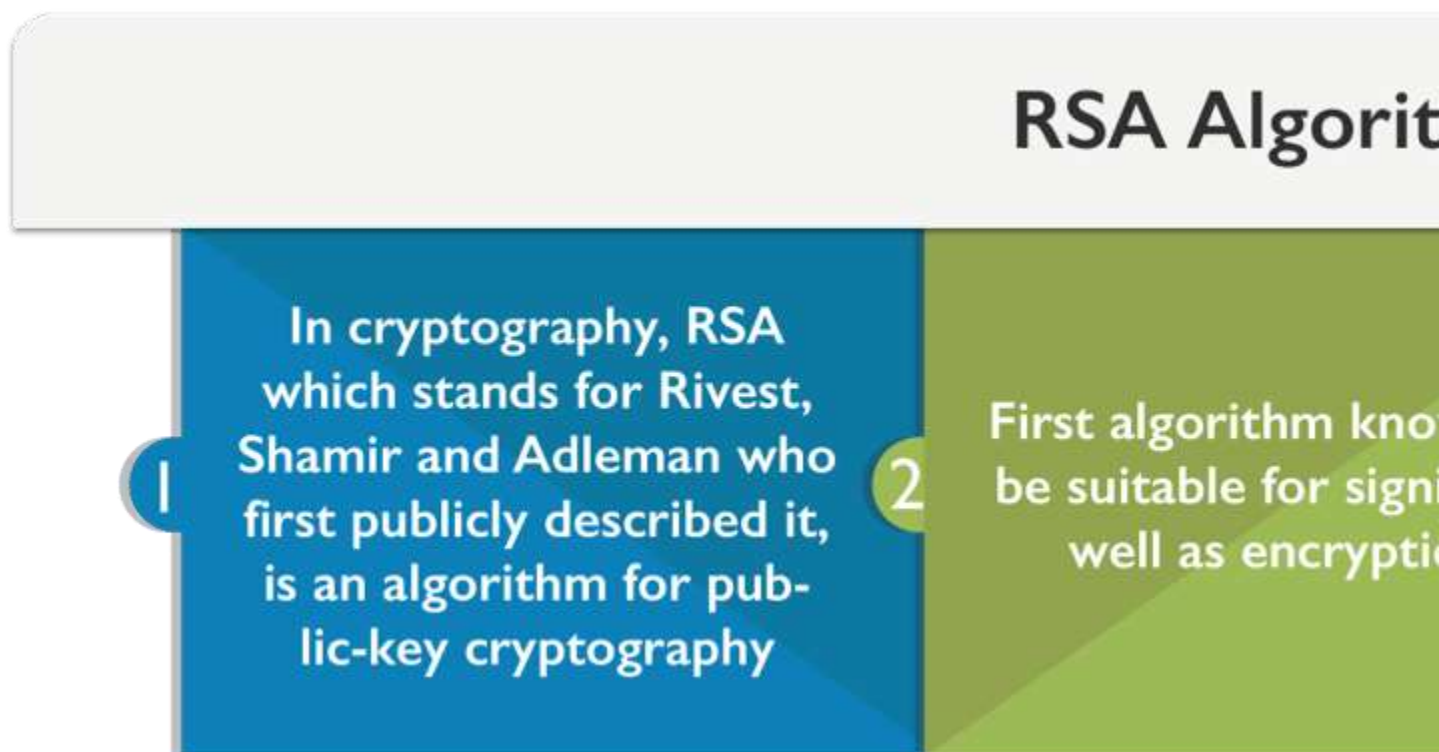## Q 10. Which of the following is asymmetric encryption Algorithm?

Blowfish
Twofish
RSA *[Ans]*
Tripple DEA

Advanced Blockchain Interview Questions

Q 1. Can you tell me some of the widely used cryptographic algorithms?

RSA

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

Triple DES

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

Blowfish

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

Twofish

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

RSA Algorit

In cryptography, RSA which stands for Rivest, Shamir and Adleman who first publicly described it, is an algorithm for pub-lic-key cryptography

First algorithm kno be suitable for signi well as encryptic

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:
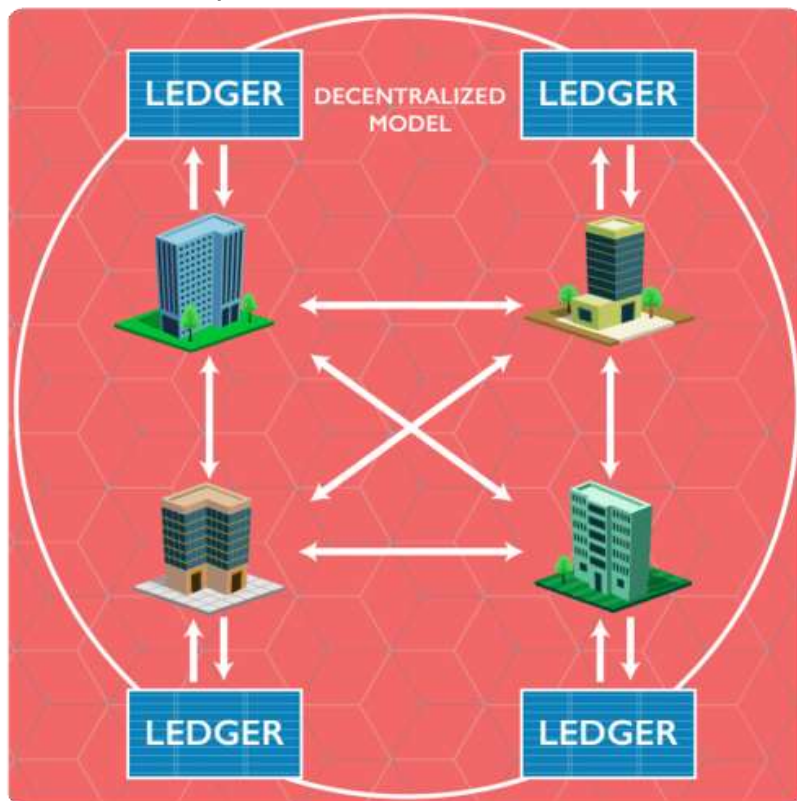
Centralized and expensive

- 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.

1. Differentiate between Blockchain and Hyperledger.

[Blockchain](#) is a decentralized technology of immutable records called blocks, which are secured using cryptography. Hyperledger is a platform or an organization that allows people to build private Blockchain.

Using Blockchain you can build public and private Blockchain whereas with Hyperledger you can only build private Blockchains.

Blockchain is divided into public, private, and consortium Blockchains and Hyperledger is a private Blockchain technology with access to Blockchain data and is limited to predefined users, configurations, and programming.

Blockchain can be used in multiple fields such as business, government, healthcare, etc. while Hyperledger is primarily used for enterprise-based solutions. Wherever we talk about public Blockchain, it refers to the usage of Blockchain on the internet, and Hyperledger-based Blockchain solutions are solutions meant for usage on the intranet, within an organization.

2. How do you explain Blockchain technology to someone who doesn't know it?

Blockchain technology is a distributed ledger, which stores transaction details in the form of immutable records or non-modifiable records (called blocks) which are secured using [cryptography](#).

Let's consider the example of a school where Blockchain is similar to a digital report card of a student. Say, each block contains a student record that has a label (stating the date and time) of when the record was entered. Neither the teacher nor the student will be able to modify the details of that block or the record of report cards. Also, the teacher owns a private key that allows him/her to make new records and the student owns a public key that allows him to view and access the report card at any time. So basically, the teacher owns the right to update the record while the student only has the right to view the record. This method makes the [data secure](#).

3. What is Merkel Tree?

Merkel Tree is a data structure that is used for verifying a block. It is in the form of a binary tree containing cryptographic hashes of each block. A Merkle tree is structured similarly to a binary tree where each leaf node is a hash of a block of transactional data and each non-leaf node is a hash of its leaf node. The Merkel root or hash root is the final hash root of all the transaction hashes. It encompasses all the transactions that are underlying all the non-leaf nodes.

4. What do you mean by blocks in Blockchain technology?

Blockchain is a distributed database of immutable records called blocks, which are secured using cryptography. Refer to the video to see the various attributes of a block.

There are a previous hash, transaction details, nonce, and target hash value. A block is like a record of the transaction. Each time a block is verified, it gets recorded in chronological order in the main Blockchain. Once the data is recorded, it cannot be modified.

5. How is Blockchain distributed ledger different from a traditional ledger?

- A Blockchain distributed ledger is highly transparent as compared to a traditional ledger.

- Blockchain distributed ledgers are irreversible. Information registered on a distributed ledger cannot be modified whereas on a traditional ledger it is reversible.

- A distributed ledger is more secure. It uses cryptography and every transaction is hashed and recorded whereas in traditional ledger security can be compromised.

- In a distributed ledger, there is no central authority. It is a distributed system and the participants hold the authority to maintain the sanity of the network and are

responsible for validating the transactions. Traditional ledgers are based on the concept of centralized control, which controls all transactions.

- In a distributed ledger, identities are unknown and hidden whereas in traditional ledger identities of all participants have to be known before the transactions happen.

- In a distributed ledger, there is no single point of failure as the data is distributed and information is shared across multiple nodes. If one node fails, the other nodes carry the same copy of the information. In comparison, traditional ledgers have a single point of failure. If a single system crashes, the entire network comes to a standstill.

- In a distributed ledger, data modification or change cannot be done but for a traditional ledger, it is possible.

- In a distributed ledger, validation is done by the participants in the network while in a traditional ledger, validation is done by a centralized authority.

- The copy of the ledger is shared amongst participants in a distributed ledger while in a traditional ledger, a single copy is maintained in a centralized location. It is not shared amongst the participants.

6. How can you identify a block?

Every block consists of four fields -

- The hash value of the previous block (thereby getting linked in a blockchain)

- It contains details of several transaction data

- It has a value called the nonce. The nonce is a random value which is used to vary the value of the hash in order to generate hash value less than the target

- Hash of the block itself. It is the digital signature of the block and an alphanumeric value used to identify a block

The hash address is the unique identification of the block. It is a hex value of 64 characters that have both letters and digits. It is obtained by using the SHA - 256 algorithms.

Refer to the video to see how a block is structured. The hash of the previous block, transaction data, and the nonce consolidate the header of the block. They are together passed through a hashing function and then the hash value is generated.

7. What is cryptography? What is its role in Blockchain?

Blockchain uses cryptography to secure users' identities and ensure transactions are done safely with a hash function.

[Cryptography](#) uses public and private keys in order to encrypt and decrypt data. In the Blockchain network, a public key can be shared with all the Bitcoin users but a private key (just like a password) is kept secret with the users.

Blockchain uses SHA - 256 which is secure and provides a unique hash output for every input. The basic feature of this algorithm is whatever input you pass, it will give you a standard alphanumeric output of 64 characters. It is a one-way function from which you can derive an encrypted value from the input, but not vice-versa.

8. What are the different types of Blockchain?

There are three different types of Blockchain - Public, Private, and Consortium Blockchain.

Public Blockchain ledgers are visible to all the users on the internet and any user can verify and add a block of transactions to the Blockchain. Examples, [Bitcoin](#), and [Ethereum](#).

Private Blockchain ledgers are visible to users on the internet but only specific users in the organization can verify and add transactions. It's a permissioned blockchain, although the information is available publicly, the controllers of the information are within the organization and are predetermined. Example, [Blockstack](#).

In Consortium Blockchain, the consensus process is controlled by only specific nodes. However, ledgers are visible to all participants in the consortium Blockchain. Example, [Ripple](#).

9. What happens when you try to deploy a file with multiple contracts?

In Blockchain, deploying a file with multiple contracts is not possible. The compiler only deploys the last contract from the uploaded file and the remaining contracts are neglected.

10. What is a Genesis Block?

- The genesis block is the first block in the Blockchain which is also known as block 0

- In Blockchain, it is the only block that doesn't refer to its previous block.

- It defines the parameters of the Blockchain such as,

  - level of difficulty,

  - consensus mechanism etc. to mine blocks

> Interested to learn about Blockchain, Bitcoin, and cryptocurrencies? Check out the [Blockchain Certification Training](#) and learn them today.

Blockchain Interview Questions - Intermediate Level

11. How is the hash (Block signature) generated?

The process of generating a block signature involves:

- Passing transaction details through a one-way hash function i.e., SHA-256.

- Running the output value through a signature algorithm (like ECDSA) with the user's private key.

- Following these steps, the encrypted hash, along with other information (such as the hashing algorithm), is called the digital signature.

12. List down some of the extensively used cryptographic algorithms.

Here are a few popular algorithms:

- SHA - 256

- RSA (Rivest-Shamir-Adleman)

- Triple DES

- Ethash

- Blowfish

13. What is a smart contract and list some of its applications?

[Smart contracts](#) are self-executing contracts which contain the terms and conditions of an agreement between the peers

Some of the applications are:

Transportations: Shipment of goods can be easily tracked using smart contracts

Protecting copyrighted content: Smart contracts can protect ownership rights such as music or books

Insurance: Smart contracts can identify false claims and prevent forgeries

Employment contract: Smart contracts can be helpful to facilitate wage payments

14. What is the Ethereum network and how many Ethereum networks are you familiar with?

Ethereum is a blockchain-based distributed computing platform featuring smart contract functionality that enables users to create and deploy their decentralized applications

There are three types of networks in Ethereum:

- Live network (main network) - Smart contracts are deployed on the main network

- Test network (like Ropsten, Kovan, Rinkeby) - Allow users to run their smart contracts with no fees before deploying it on the main network

- Private network - Are those which are not connected to the main network. They run within the premises of the organization but carry the features of an Ethereum network.

15. Where do nodes run a smart contract code?

Nodes run smart contracts code on Ethereum Virtual Machine (EVM). It is a virtual machine designed to operate as a runtime environment for Ethereum-based smart contracts.

EVM is operated in a sandboxed environment (isolated from the main network). This is a perfect testing environment.

You can download the EVM, run your smart contract locally in an isolated manner and once you have tested and verified it, you can deploy it on the main network.

16. What is a Dapp and how is it different from a normal application?

Dapp:

- A Dapp is a decentralized application which is deployed using smart contract
- A Dapp has its back-end code (smart contract) which runs on a decentralized peer-to-peer network
- Process:
    - Front-end
    - Smart contract (backend code)
    - Blockchain (P2P contract)

Normal application:

- Normal application has a back-end code which runs on a centralized server
- It's a computer software application that is hosted on a central server
- Process:
    - Front-end
    - API
    - Database (runs on the server)

17. Name some leading open source platforms for developing Blockchain applications.

- Ethereum is one of the popular platforms for building Blockchain-based applications

- Eris is used for building enterprise-based solutions

Some of the other widely used platforms for building Blockchain include Hyperledger, Multichain, Open chain.

18. What is the very first thing you must specify in a Solidity file?

It is necessary to specify the version number of Solidity at the beginning of code as it eliminates incompatibility errors that can arise while compiling with another version. This is a mandatory clause that has to be there at the top of any Solidity code you write. You also need to mention the correct version number for the code.

19. What is the difference between Bitcoin and Ethereum?

Criteria	Bitcoin	Ethereum
Concept	P2P currency	P2P currency and smart contract
Consensus mechanism	Proof of work	Proof of work/ Proof of stake
Hashing Algorithm	SHA-256	Ethash

Time is taken to mine a block	10 Minutes (approx.)	12-15 seconds
Reward	12.5 BTC	3 ETH
Transaction fee	Optional	A fee is calculated in gas
Value (8/21/18)	1 BTC = 6934.34 USD	1 ETH = 278.98 USD

20. What is the nonce and how is it used in mining?

In Blockchain, mining is a process to validate transactions by solving a difficult mathematical puzzle called proof of work. Now, proof of work is the process to determine a number (nonce) along with a cryptographic hash algorithm to produce a hash value lower than a predefined target. The nonce is a random value that is used to vary the value of hash so that the final hash value meets the hash conditions.

Blockchain Interview Questions - Expert Level

21. Name the steps that are involved in the Blockchain project implementation.

Requirement identification:

- Identify the problem and goal

- Identify the most suitable consensus mechanism

- Identify the most suitable platform

- Account for implementation and deployment costs

Planning stage

- In this stage and individual evaluates all requirements and decides a suitable blockchain platform to be implemented.

Development and implementation of a project

- Designing the architecture

- Designing the user interface

- Building the APIs

Controlling and monitoring the project

- Applying Proof of Concept (POC)

- Identifying and fixing issues

22. Explain a real-life use-case where Blockchain is being used.

In supply chain management, smart contracts provide permanent transparency and validation of transactions shared by multiple supply chain partners. Check out our diagrammatic display of supply chain management using Blockchain in our video.

23. List and explain the parts of EVM memory.

The memory of an EVM is divided into three types:

Storage:

- Storage values are stored permanently on the Blockchain network

- It is extremely expensive

Memory:

- Memory is a temporary modifiable storage

- It can be accessed only during contract execution. Once the execution is finished, its data is lost

Stack:

- A stack is temporary and non-modifiable storage.

- Here, when the execution completes, the content is lost.

24. What happens if the execution of a smart contract costs more than the specified gas?

Initially, your transaction will be executed, but if the execution of a smart contract costs more than the specified gas, then the miners will stop validating your contract. The Blockchain will record the transaction as failed, also the user doesn't get a refund.

25. What does the gas usage in a transaction depend on and how is the transaction fee calculated?

Gas usage depends upon the amount of storage and set of instructions (codes) used in a smart contract. The transaction fee is calculated in Ether, which is given as:

Ether = Tx Fees = Gas Limit * Gas Price

26. What is the fork? What are some of the types of forking?

In simple terms, updating a [cryptocurrency](#) protocol or code is called forking. Fork implies that a Blockchain splits into two branches. It can happen when the participants of the network cannot come to an agreement with regards to the consensus algorithm and new rules to validate transactions.

There are three types of forking:

- Hard forks
- Soft forks
- Accidental forks

27. Differentiate between Proof of Work vs Proof of Stake.

Proof of Work (PoW):

In Blockchain, PoW is the process of solving a complex mathematical puzzle called mining. Here, the probability of mining a block is based upon the amount of computational work done by a miner. Miners spend a lot of computing power (with hardware) for solving the cryptographic puzzle.

Proof of Stake (PoS):

PoS is an alternative to PoW in which the Blockchain aims to achieve distributed consensus. The probability of validating a block relies upon the number of tokens you own. The more tokens you have, the more chances you get to validate a block. It was created as a solution to minimize the use of expensive resources spent in mining.

28. What is a 51% attack?

In Blockchain, a 51% attack refers to a vulnerability where an individual or group of people controls the majority of the mining power (hash rate). This allows attackers to prevent new transactions from being confirmed. Further, they can double-spend the coins. In a 51% attack, smaller cryptocurrencies are being attacked.

29. What are function modifiers in Solidity? Mention the most widely used modifiers.

In Solidity, function modifiers are used to easily modify the behavior of your smart contract functions. In simple terms, it can build additional features or apply restrictions on the function of smart contracts. The most extensively used function modifiers in solidity are:

- View, which are functions that cannot modify the state of a smart contract. They are read-only functions. Refer to our video to see an example of a View function

- Pure, which are functions that neither read nor write the state of a smart contract. They return the same result determined by its input values. Refer to our video to see an example of a Pure function

30. Write a crowd-sale smart contract code in Solidity programming language.

Refer to our video to know how to write a Crowd function.

Enroll in our Blockchain Developer Certification course and learn to work with Ethereum deployment tools and bitcoin transaction process.

What is blockchain, where is it used, and will it become mainstream?

These are just some of the questions on the lips of the public as the word—and cryptocurrency in general—are becoming more widely used.

But if you're new to the idea of blockchain, it can seem a tricky concept to get your head around. With this in mind, we recently sat down with Dr. Ying-Ying Hsieh, Assistant Professor of Innovation and Entrepreneurship at Imperial College Business School, to talk about blockchain and its applications in cryptocurrency and beyond.

Here are her confusion-busting answers to some of the public's most common questions.

1. What is blockchain?

Blockchain is simply a piece of software that enables the sharing of value, such as payments, between peers online. Importantly, blockchain allows the information to be shared without the need to go through any third-party intermediaries such as banks or payment companies. As its name suggests, it is made of blocks that are connected in chains and each block stores a small part of the history of the transactions that have taken places on the blockchain.

2. When was blockchain first created?

Blockchain is not so much an original idea as it is a combination of a number of pre-existing technologies such as cryptography, peer-to-peer computing and others. The successful first digital implementation of blockchain was in 2008, with the publication of a whitepaper by an anonymous developer, nicknamed Satoshi Nakamoto, in which the idea of blockchain-mediated cryptocurrency, known as bitcoin, was first proposed.
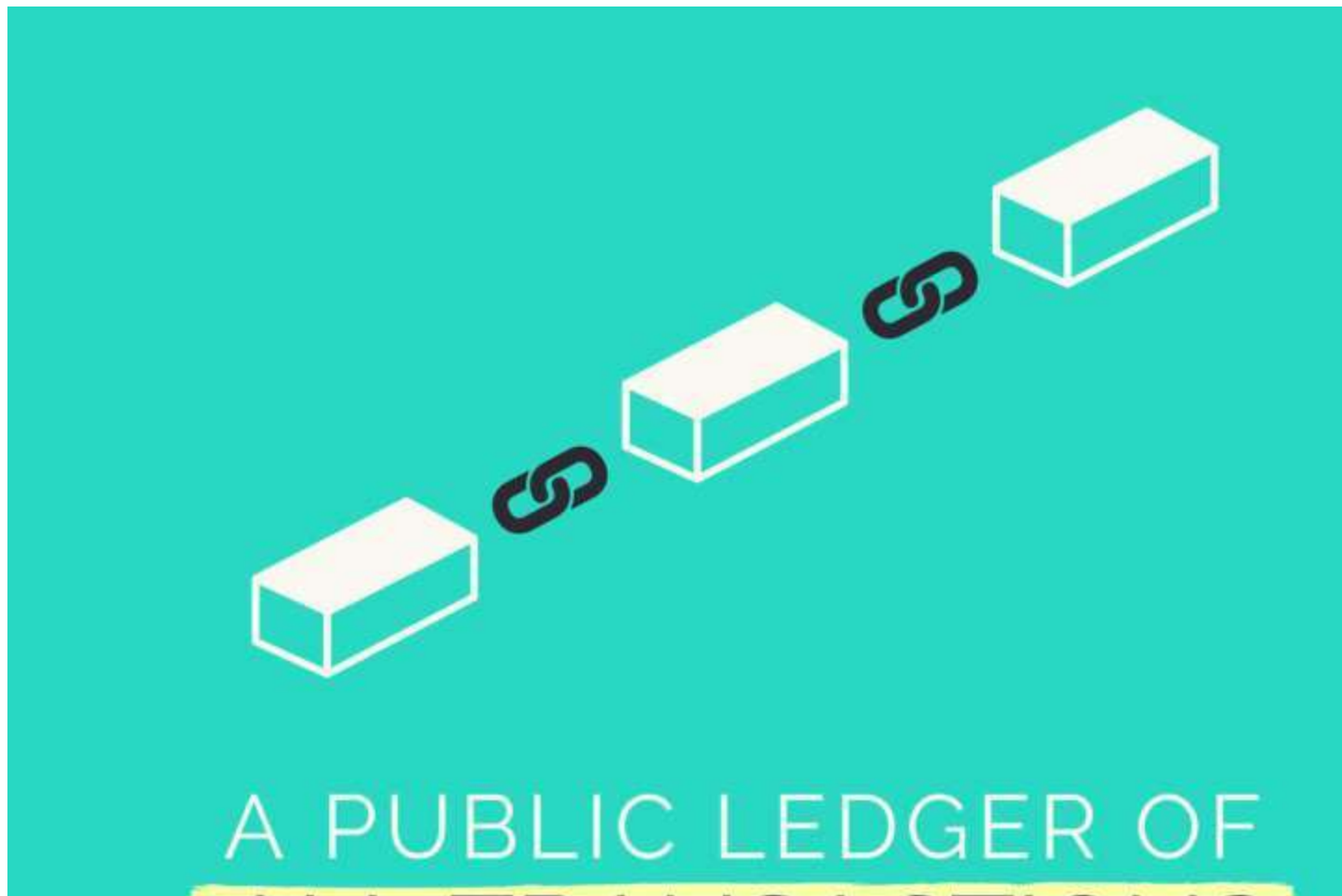
Credit: Imperial College London

3. How does blockchain support bitcoin?

Bitcoin is a cryptocurrency that one can think of as digital cash. Bitcoin only exists online and therefore, its exchange needs to be recorded digitally. Blockchain essentially acts as a digital ledger to record all transactions happening between the peers online and provides a secure and decentralised record for all of the exchanges.

4. What does a decentralised blockchain mean?

It means that the information in the blockchain is not stored in a single place but it is distributed across the network of people who are using it. For example, standard cash, such as pounds or dollars, are issued by the central banks that keep the records of where the money is going. However, with bitcoin, there is no single entity that is responsible for issuing bitcoins and keeping the records. Bitcoin works through an anonymous network of people who provide nodes to the blockchain. Anyone can join or exit the

blockchain at any time and the cross-validation between the nodes is required to record anything on the ledger.

5. Does the decentralised nature of the blockchain make it more secure?

Yes, here is an example: if you have a pot of gold you can store it in the vault and trust the people who own the vault, i.e. banks and their personnel, to keep it safe for you. But if your gold is analogous to bitcoin, then, rather than putting your pot of gold into a bank vault, you actually put it in someone's house in some imaginary village and it gets moved to a new house every 10 minutes or so. No one knows where your gold will be moved, which makes it very difficult for any burglar to know where it will be at any given time. Moreover, to enter the houses in which your gold is stored, the burglar would need to solve complicated equations, which are both time consuming and extremely energy expensive.

6. But there have been many reports of bitcoins being stolen, so it is possible to hack the blockchain, right?
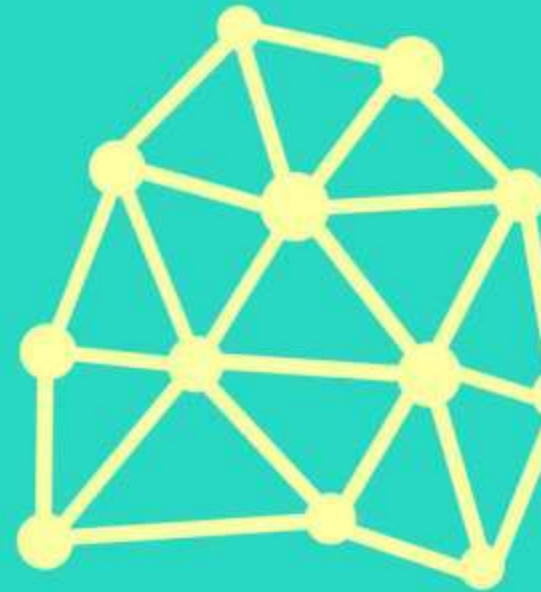
Well, most of those reports actually refer to the hacking of exchanges in which the cryptocurrencies are being traded and not the blockchain itself. In fact, we can still find the stolen currency on the blockchain we just do not have the access to it or know who has stolen it.
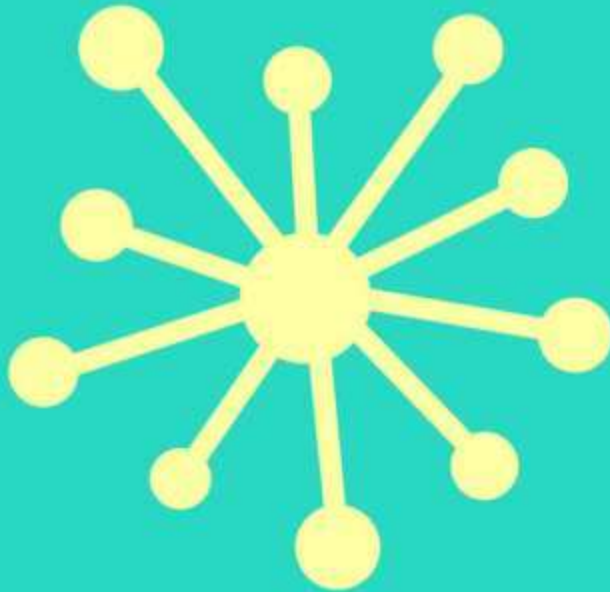
Credit: Imperial College London

7. Can anyone start a blockchain?

Yes, in principle anyone with some computing knowledge can do it, but the start is the easy part. The success and value of the blockchain comes from its size and to make it attractive to the users the creator of the new blockchain needs to be able to grow it fast by adding as many blocks as possible to the chain. The scaling of the blockchain is referred to as bootstrapping and it is often done through the so-called initial coin offerings at the early stages of a cryptocurrency creation.

8. Are there different types of blockchains?

Currently there are several different types of blockchains, which were mostly developed to improve the original bitcoin blockchain. Another very popular blockchain is the Ethereum blockchain developed to exchange ether tokens online. Ethereum blockchain is more energy efficient, allows smart contracts (transfer of currency only under certain conditions) and

also uses proof-of-stake rather than proof-of-work protocols to validate transactions.

9. Is there any disadvantage to using a blockchain?

Perhaps the biggest disadvantage from the government's perspective is that blockchain-based technologies are very difficult to track. The decentralised nature of the blockchain makes it difficult to regulate transactions happening online and therefore, it is very attractive for criminals to use it for illegal trade and money laundering purposes. In fact, we often see bitcoins being the preferred payment method during the ransomware attacks and in online black market for weapons and drugs.

10. Can blockchain be used outside the cryptocurrency field?

There are many potential avenues for the use of blockchain, though, so far, it has been used more as a proof-of-concept and not yet fully implemented. Essentially, any situation where trust is of key importance could make use of blockchain, whether that is the financial industry or electronic voting systems. In the shipping industry the blockchain could be used to track where the goods versus the money is, and in the healthcare system it could be used for the secure storage of patient data.