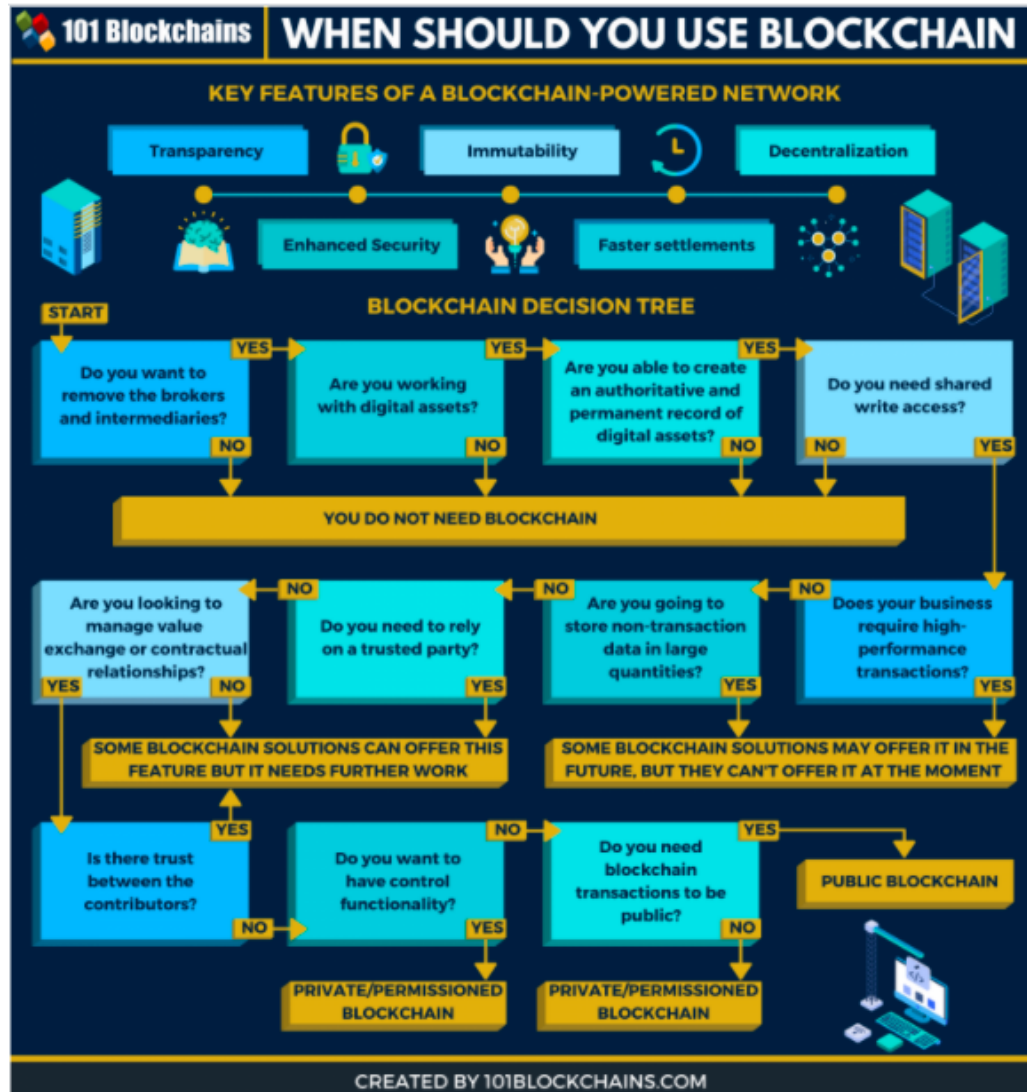


Interview Questions: UPSTAC Covid Application Development

Q1	How to decide on when to use Blockchain for your use case?
Reference	https://101blockchains.com/when-to-use-blockchain/#:~:text=Some%20systems%20do%20need%20Blockchain.any%20other%20technology%20out%20there.
Ans	<p>You need to ask yourself the following few questions before thinking of applying Blockchain to your application:</p> <ul style="list-style-type: none">- Is immutability required in your application?- Is transparency required for your application?- Is it possible that most of your transactions are corrupt?- How will the distributed network fit in your application?- Is there a requirement of certain performance standards and can Blockchain fulfill those requirements? <p>Many more questions may arise. Please refer to the reference link for detailed questions and answers.</p>

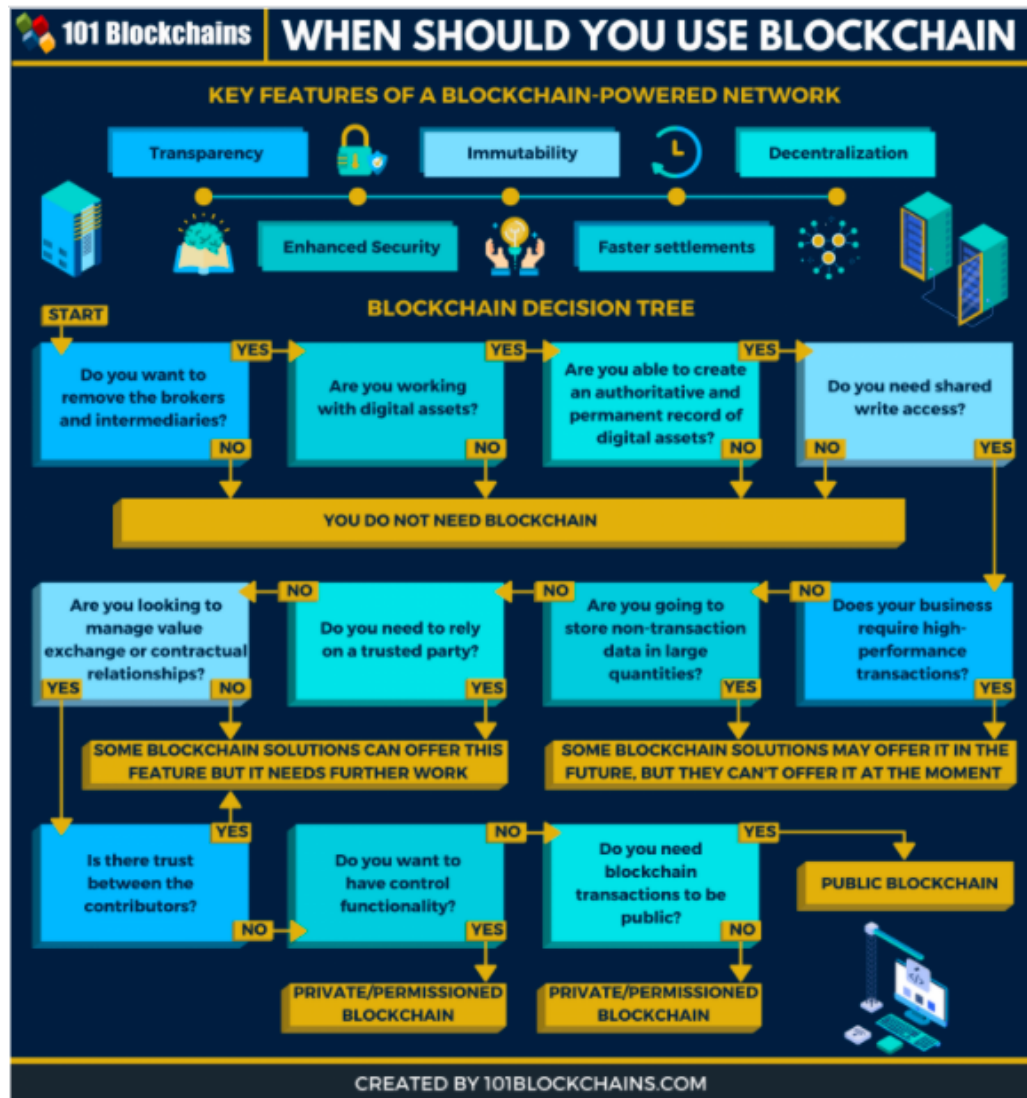


Q2	When is the use of public blockchain advisable? Give some examples.
Reference	https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/#:~:text=If%20one%20desires%20to%20create,go%20for%20a%20public%20blockchain.
Ans	<p>Public blockchains should be used:</p> <ul style="list-style-type: none"> - When a completely open network is required - When complete decentralisation is first priority - When performance is not a priority - When trustlessness is more important



Q3	In which scenarios can permissioned or private blockchains be used?
Reference	https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/#:~:text=If%20one%20desires%20to%20create,go%20of%20a%20public%20blockchain.
Ans	<p>Private and permissioned blockchains should be used when:</p> <ul style="list-style-type: none"> - Transactions are not to be shown only to a specific set of users - When performance is a priority and complete decentralisation is not required

- When you can trust a central authority to run the network
- When the network is to be shared only within an enterprise or a set of users



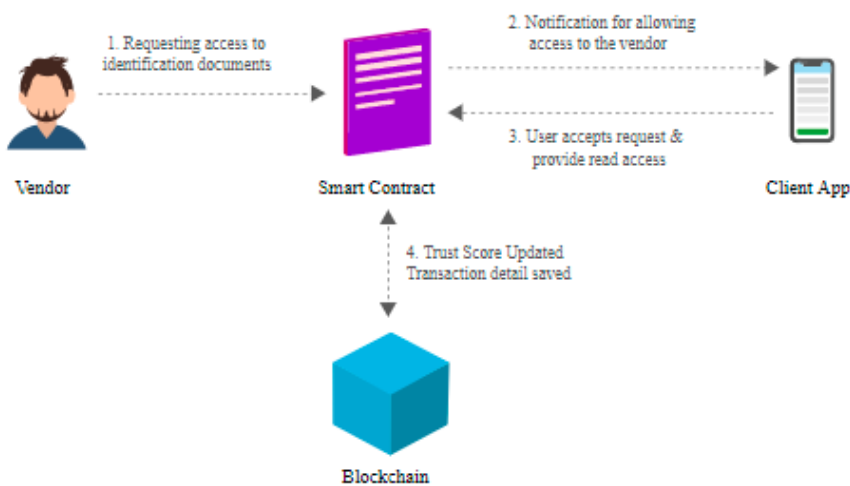
Q4	What are the limitations of Blockchain technology?
Reference	https://101blockchains.com/disadvantages-of-blockchain/
Ans	<p>Some of the disadvantages of the Blockchain technology are:</p> <ul style="list-style-type: none"> - Scalability - Throughput - High transaction cost

	- Non-distributed computing system
--	------------------------------------

Q5	Can we store all the data in a blockchain? Why or why not?
Reference	https://malcoded.com/posts/storing-data-blockchain/
Ans	Storing the entire application data in a blockchain can get costly and will have a lot of overhead. One simple way to reduce the overhead is to store only the hash of the data in a chain and store the actual data off the chain in a database. Usually, storing all the data on a blockchain is not advisable.

Q6	How do we decide which data can be stored in a blockchain?
Reference	https://malcoded.com/posts/storing-data-blockchain/
Ans	<p>Following are some key points to be considered while deciding which data should be stored in a chain and which data should be stored off the chain:</p> <ul style="list-style-type: none"> - Check whether the data is really confidential to store on a public blockchain - Check if the data can be viewed by the entire network or not - Usually, transaction data hashes are stored in the blockchain to get the benefits of the network and also to avoid showing actual data to everyone

Q7	What is an anchor peer in hyperledger fabric? What is its significance?
Reference	https://hyperledger-fabric.readthedocs.io/en/release-1.1/glossary.html#:~:text=it's%20pretty%20enlightening!-,Anchor%20Peer.existing%20peers%20on%20a%20channel.
Ans	An anchor peer is a peer node on a channel that all other peers can discover and communicate with. Each member on a channel has an anchor peer (or multiple anchor peers to prevent single point of failure), allowing for peers belonging to different members to discover all existing peers on a channel.

Q8	How can identity management be used in blockchain?
Reference	<p>https://tykn.tech/identity-management-blockchain/</p> <p>https://www.leewayhertz.com/blockchain-identity-management/#:~:text=Once%20the%20profile%20is%20created,access%20the%20user's%20identification%20documents.&text=After%20the%20user%20gets%20ID,addresses%20stored%20in%20the%20blockchain.</p>
Ans	<p>In identity management, a distributed ledger (a 'blockchain') enables everyone in the network to have the same source of truth about which credentials are valid and who attested to the validity of the data inside the credential without revealing the actual data.</p> <p>Through the infrastructure of a blockchain, the verifying parties do not need to check the validity of the actual data in the provided proof but can rather use the blockchain to check the validity of the attestation and attesting party (such as the government) from which they can determine whether to validate the proof.</p> <p>For example, when an identity owner presents a proof of their date of birth, rather than actually checking the truth of the date of birth itself, the verifying party will validate the government authority's signature that issued and attested this credential to then decide whether they trust the government's assessment about the accuracy of the data or not.</p>  <pre> graph LR Vendor[Vendor] -- "1. Requesting access to identification documents" --> SC[Smart Contract] SC -- "2. Notification for allowing access to the vendor" --> CA[Client App] CA -- "3. User accepts request & provide read access" --> SC SC <--> "4. Trust Score Updated Transaction detail saved" BC[Blockchain] </pre>

Q9	What is IPFS and how can it be used in an application?
Reference	https://medium.com/wolverineblockchain/what-is-ipfs-b83277597da5
Ans	<p>IPFS stands for interplanetary file system. It is a distributed file system used to store data in a decentralised manner. Because of the similarity in their structure, IPFS and blockchains can work well together. In fact, Juan Benet, the inventor of IPFS calls this a “great marriage”. IPFS is one of the few projects that are part of a group called Protocol Labs, which was also founded by Benet. Some projects from Protocol Labs closely related to IPFS are inter-planetary linked data (IPLD) and Filecoin. IPLD is a data model for distributed data structures like blockchains. This model allows for easy storage and access of blockchain data through IPFS. Users willing to store IPFS data are rewarded with Filecoin. IPLD allows users to seamlessly interact with multiple blockchains and has been integrated with Ethereum and Bitcoin.</p> <p>The diagram illustrates the IPFS data storage process. It shows three data entries in blue boxes: 'Fox', 'The red fox runs across the ice', and 'The red fox walks across the ice'. Each entry is processed by a 'Hash function' (yellow box) to generate a unique 'Key' (pink box): 'DFCD3454', '52ED879E', and '46042841' respectively. These keys are then mapped to a 'Distributed Network' (orange cloud) which contains 'Peers' (blue dots). The entire structure is labeled 'Distributed Hash Table'.</p>

Q10	What are the privacy considerations for any blockchain application?
Reference	https://developer.ibm.com/technologies/blockchain/articles/how-to-secure-blockchain-solutions/
Ans	<p>A blockchain network is very susceptible to attacks and there are concerns in terms of how much privacy can the blockchain network provide. Some of the privacy and other risks involve the following:</p> <ul style="list-style-type: none"> - Public blockchains are public in nature and anyone can join them and validate transactions. They are generally more risky (for example, cryptocurrencies). This includes risks where anyone can be part of the blockchain without any level of control or restrictions. - A blockchain solution has a decentralised governance process that creates risks around lack of control over policy compliance and decision-making. Lack of centralised governance can also cause reduced control over who can access the platform and the level of access provided to every user. This can be a larger issue if members have different ways of categorising users in their respective organisations. - Blockchain identity keys and transaction tokens are an important component of the solution. Challenges with certificate and key expiration, renewal, archive and revocation can bring huge risks to the functioning of the platform. - Smart contracts are an important component of a blockchain solution, and any logical flaws in the implementation of these contracts or their transactions can result in validation of incorrect contracts or transactions.

Q11	How can privacy concerns be addressed?
Reference	https://developer.ibm.com/technologies/blockchain/articles/how-to-secure-blockchain-solutions/
Ans	<p>Following ways can be used to mitigate these risks:</p> <ul style="list-style-type: none"> - Define and enforce the appropriate endorsement policies based on business contracts.

	<ul style="list-style-type: none">- Partition and adopt best practices for namespaces to regulate access.- Enforce identity and access controls to access the blockchain solution and data.- Use API security best practices to safeguard API-based transactions.- Use data structure and design techniques to limit the personal data they actually store on blockchains (see avoid or limit personal data stored on blockchains).- Adopt alternative data encryption and destruction techniques to protect personal data.
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------