UpGrad

Interview Questions: Blockchain Features

Q1	**What is asset digitisation?**
Ans	Securitization in the financial world is a process through which illiquid assets (both digital and physical) are converted into smaller chunks. This enables the sales of that asset to multiple parties and increases liquidity and diversification possibilities. In a blockchain, these assets can be converted into tokens and sold to multiple parties. This process of converting an asset into multiple smaller units is called tokenization or digitization. Tokens can be converted into other cryptocurrencies or exchanged with other tokens and, hence, provide the required liquidity. Tokens are of two types: fungible and non-fungible. Fungible tokens can be exchanged with other tokens of the same type without any issues. For instance, a company's shares can be exchanged as they are all the same. Non-fungible tokens are unique to each asset and cannot be interchanged with similar types of tokens. For example, graduation certificates and land records.

Q2	**How can one tokenize a property?**
Reference Link	https://hackernoon.com/how-to-represent-physical-assets-on-a-blockchain-with-erc20-fu1yo3vkz
Ans	Any physical asset or digital asset in the world can be tokenized using a smart contract in a programmable blockchain. The tokenization of an asset into smaller units allows for better efficiency in managing the asset and increases the liquidity of the asset. For example, if a real estate property is tokenized using ERC-20 standards in Ethereum, every user who wants to invest in the property can buy some tokens of the property and share the ownership with other owners. Therefore, one person need not invest in the property completely, which reduces the total amount of investment required for the purchase. Also, if an individual wants to selll 20% of their property to meet some financial need, they can just sell those many units of tokens in the secondary market

	and need not wait for the entire property to be sold.

Q3	**How can you create immutable assets over blockchain/distributed ledger?**
Ans	One can use tools such as smart contracts, cryptographic hashes, digital signatures to create immutable assets on blockchain.

Q4	**What are coloured coins?**
Reference Link	https://unblock.net/what-are-colored-coins/
Ans	The **coloured coins** are tokens that represent real-world assets on the blockchain. You can use **coloured coins** to prove ownership of any physical asset, from precious metals to vehicles to real estate, or equities and bonds.

Q5	**What is immutability? What are the challenges associated with it?**
Reference Link	https://www.coindesk.com/blockchain-immutability-myth
Ans	Immutability of records (transactions) is one of the most important features achieved by blockchain technology. Immutability means that once a transaction enters a block and becomes a part of the blockchain, this transaction cannot be tampered with or hacked by anyone. This property is achieved by the use of cryptographic methods, especially hashing.

	Immutability is a good feature provided by blockchains, but it involves several challenges. First, when a user performs a transaction incorrectly, the transaction cannot be reverted to its original state. This can be achieved in the traditional systems as there will be a dedicated team which can alter or update the existing data in a database. Such a feature is not available in blockchains. Second, during an ICO, if a user sends cryptocurrencies directly to a smart contract address instead of using a function to invest money in the ICO, the cryptos are lost in the blockchain and cannot be recovered. These lost cryptos cannot be used again by anyone else in the network. Millions of dollars have been lost in the blockchains due to the loss of private keys and the errors mentioned above. Third, once a smart contract code is deployed in the blockchain, there is no control over the code for the developer or anyone else in the network. If there is an error in the smart contract code, it is not possible to reverse the code and re-deploy the code so easily. Smart contracts work with the logic of 'Code is Law', for example, the DAO attack.

Q6	**Compare private, public and consortium blockchains.**
Reference Link	https://dragonchain.com/blog/differences-between-public-private-blockchains/
Ans	Public blockchains (Permissionless) are open-source and anyone in the world can be nodes, miners or developers in such networks. All the transactions in the blockchain are completely transparent, and this makes validation by the peer nodes very easy in a public blockchain. Game theory, which talks about rewards and recognition, is regarded highly in a public blockchain. Some examples of public blockchains include Bitcoin, Ethereum, Litecoin, etc. Private blockchains (Permissioned), on the other hand, require the nodes to be identified and authenticated before they join the blockchain. Transactions in a private blockchain are not public and can only be viewed by a specific set of nodes which are authorised by the network. Hence, private blockchains lack the decentralization feature of blockchains. However, this increases the transaction throughput due to the lack of mining. Some examples of private blockchains include Hyperledger, R3 Corda, Quorum, etc.

	Consortium blockchains can be considered as a subset of private blockchains where the blockchain is governed by multiple central parties instead of one. Multiple companies competing in a particular industry can come together to form a consortium blockchain so that the regulatory authorities within that industry can achieve real-time tracking of the transactions happening within that industry. TradeLens, which is jointly developed by IBM and Maersk, is a good example of consortium blockchains.

Q7	**What are smart contracts?**
Ans	Smart contracts in a blockchain are self-executing contracts written on top of programmable blockchains like Ethereum. Smart contracts hold the business logic and the terms of the agreement between the parties as lines of code. These lines of code are enforced when they meet a particular condition. Since the contracts are stored in a blockchain, they are completely transparent and immutable. Hence, a smart contract cannot be manipulated by central authorities. The use of smart contracts can help eliminate the interference by many central authorities and intermediaries. For example, escrow services and banks can be eliminated in the financial system as smart contracts can hold monetary assets and data within them.

Q8	**What is litecoin? Why is it faster than Bitcoin?**
Reference Link	https://www.thestreet.com/markets/currencies/litecoin-vs-Bitcoin-14757788
Ans	Litecoin is an altcoin that was introduced in 2011. This blockchain differs from Bitcoin in a few key factors, but the most important of them is that Litecoin block time is just 2.5 minutes as opposed to Bitcoin's 10 minutes. This makes litecoin faster than Bitcoin.

Q9	**Differentiate between Symmetric and Asymmetric Encryption.**
Reference Link	https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences
Ans	Symmetric encryption used the same key for both encryption and decryption of the message. Asymmetric encryption used a pair of keys for this purpose. The public and private keys, which are mathematically related to each other, are used to encrypt/decrypt the message.