UpGrad

Interview Questions: Blockchain Basics

Q1	**How can you create trust in blockchain?**
Reference link	https://medium.com/regen-network/building-a-network-of-trust-using-blockchain-technology-1745b295c6c7
Ans	Blockchain as a technology is a bundle of multiple concepts, including but not limited to Hashing, Distributed Systems and Decentralization. A blockchain-based system has properties such as Immutability and Transparency., These properties of blockchain provide trust between two parties in a trustless environment. For example, in Bitcoin, since all the transactions are stored in a public ledger, anyone across the world can validate these transactions. Hence, all parties involved in a transaction can trust the technology for the validation and consensus process instead of trusting a central authority. Additionally, with the introduction of programmable blockchains such as Ethereum, Cardano, Tron., business logic can be coded in the blockchain; these then also acquire the properties of blockchain, such as security, immutability. This enables the storage of both monetary assets and other digital assets in the blockchain, thereby providing trust between parties. For example, an escrow service provided by banks in the traditional world can be converted to a smart contract, eliminating the need for a central authority and, at the same time, providing the trust required in the ecosystem.

Q2	**What is verifiable proof?**
Reference Link	https://link.springer.com/chapter/10.1007/978-3-030-17253-4_13
Ans	A proof system is publicly verifiable, which means that anyone by looking at the transcript of the proof should be convinced that the corresponding theorem is true. Public verifiability is important in many applications since it allows computing a proof only once while convincing an unlimited number of verifiers. Some examples of verifiable proof are as follows: Digital signature created by using signers' public key and signature hash. Cryptographic hash of a document/file is unique for a file, so if you address the document by a hash, then it will produce the same document every time, such as in the case of IPFS.

Q3	**Why is Bitcoin immutable?**
Reference Link	https://hackernoon.com/why-blockchain-immutability-matters-8ce86603914e
Ans	Bitcoin and other blockchain applications are immutable in nature as these use cryptographic methods that bind the data together in blocks. Even a small change in the data on the blockchain can cause a change in the entire hash of that transaction and the block, thereby invalidating the blockchain itself.

Q4	**List down the trust factors for Bitcoin blockchain.**
Ans	Immutability, transparency and verifiable proof are the major trust factors for Bitcoin blockchain.

Q5	**Shed some light on the history of blockchain or distributed ledger.**
Reference link	https://101blockchains.com/history-of-blockchain-timeline/
Ans	Blockchain as a concept started in 2008 when Bitcoin was introduced to the world by an anonymous entity Satoshi Nakamoto. From then on, blockchain has evolved to become a programmable blockchain in the form of Ethereum and a few others and has permissioned enterprise-level blockchains such as Hyperledger and R3 Corda.

Q6	**Cite some differences between blockchain and 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	A majority of peers agree on the outcome of transactions	Distributed transactions (two-phase commit)
Invariants	Anybody can validate transactions across the network	Integrity constraints

Q7	**Describe the various consensus algorithms and the challenges associated with them.**
Ans	**Proof of Work (PoW):** PoW is one of the most popular and frequently used consensus algorithms in permissionless blockchains such as Bitcoin, Ethereum and Litecoin. PoW involves finding a nonce value for the block that satisfies a specific condition (the number of leading zeroes) set by the algorithm. PoW enables a consensus in the system by eliminating Double Spending attack, Race attack etc. Its disadvantages include very

	high electricity costs, possibility of centralisation of miners due to specialised hardware like ASICs and the requirement of a large capital investment. **Proof of Stake (PoS):** PoS is a common alternative to Proof of Work and this consensus algorithm does not involve the concept of mining. PoS helps overcome a lot of problems faced in Proof of Work, such as electricity usage, large capital investments. In this algorithm, nodes invest in the native cryptocurrency and validators are selected for each block proportionate to their staked investment. Selected nodes validate the validity of the newly submitted transactions and blocks. However, nodes can validate more than one block at a specific time and, hence, might lead to the formation of forks. This phenomenon is usually called the 'Nothing at Stake' problem. **Proof of Elapsed Time (PoET):** PoET uses a Trusted Execution Environment (TEE) which ensures that blocks are validated and generated in a random manner. The time taken for achieving a consensus is based on the time rate provided by the TEE. A major disadvantage of PoET algorithms is the need for a TEE which is a third-party source of truth.

Q8	**Explain nonce and mining.**
Ans	Nonce and mining are concepts related to the Proof-of-Work consensus mechanism used in Bitcoin and Ethereum. To keep all the nodes in consensus of blocks and transactions, there are special nodes called miners that pick the transactions from the transaction pool, form a block and then carry out the mining process. The mining process involves solving a cryptographic puzzle where the miner needs to recursively replace the nonce and find a hash value for the block that satisfies a particular condition. The condition here is to have a minimum number of leading zeros in the block hash. The difficulty in finding the nonce increases with the increase in the number of leading zeros. This is governed by the difficulty target set by the algorithm which changes once every two weeks in the case of Bitcoin.

Q9	**What are the advantages of using blockchains over traditional databases?**
Ans	Blockchains provide various advantages over traditional databases. Most important of them are Decentralisation, Distribution and Trust.

	Traditional databases are managed by a single central party, which acts as the source of truth and trust. Every participant in the network believes and trusts in the central authority, which gives rise to the problem of a single point of authority. On the other hand, blockchain is decentralised in nature; therefore, the source of truth does not lie with one intermediary but is provided by multiple nodes in the network. This removes the authority that the central party has over the network. Blockchains are also distributed in nature, i.e., assume there is a breach in the network and one of the nodes and the data in it is tampered with. Since there are multiple copies of the same data stored in other nodes in the network, these can easily replace the tampered data with the actual data. This provides significant trust in the network. In a traditional database, Create Read Update Delete (CRUD) are the four operations that can be performed. This also enables editing and updating of past data in the traditional database. However, in a blockchain, the updation and deletion of data are not possible due to its decentralized and immutable nature. Hence, it is possible to only create and read data in a blockchain and that provides a lot of trust to the parties involved in a transaction.

Q10	**What are the types of records that can be kept in the blockchain?**
Ans	Blockchain, at the core of it, is a transaction-based ledger. It is also a distributed ledger where all the nodes involved in a network store copies of the same data. Hence, blockchains are not very useful to store large sets of data such as heavy documents or movies. If such data are stored in a blockchain, the data will be replicated in 10,000 to 20,000 nodes, making it very inefficient in terms of storage. Hence, the only type of data that should be stored in a blockchain are small amounts of very important data that require a high level of security, such as financial information, transactions and other similar data.

Q11	**What are hashing and hashing algorithms?**

Ans	Hashing is the concept of creating a digital fingerprint of digital data. Any digital data can be encrypted into a fixed-length unique hash consisting of hexadecimal numbers. Hashing has the following properties: ● Fixed length ● One-way ● Deterministic ● Collision resistant ● Avalanche effect By creating a hash for digital data, one can verify the integrity of data while transferring it from one location to another. If the data is tampered with during the transfer process, the hash changes; hence, it is very easy to find out whether the data has been tampered with. The various types of hashing algorithms include **SHA256, SHA512, MD150, MD5** and **Keccak256** among others**.**

Q12	**What is a 51% attack?**
Reference Link	https://www.youtube.com/watch?v=UxyGt58EPa4
Ans	A 51% attack can happen when one entity owns more than 50% of the computing power in a network. This attack is possible in the Proof-of-Work consensus algorithm-based blockchains such as Bitcoin, Ethereum and Bitcoin Gold. When one entity owns more than half of the computing power in the network, it can generate blocks faster than the rest of the network. In this case, double-spending can take place by isolating from the network for a while, creating more number of blocks than that in the network and suddenly coming online to the network. When the nodes try to sync across, the smaller chain is discarded and all the transactions in the chain get invalidated. Thus, double-spending becomes possible by the 51% attack. For example, Bitcoin Gold underwent a 51% attack in January 2020 and $70,000 worth BTG were double spent.

Q13	**What is double-spending? Why is it a problem when it comes to digital money? Can double-spending occur with fiat currencies?**
Reference Link	https://medium.com/innerquest-online/how-does-a-blockchain-prevent-double-spending-of-Bitcoins-fa0ecf9849f7

Ans	Double-spending means spending the same digital coin twice on two different entities. This is a problem in the digital currency world as digital data can be copied multiple times without any quality loss. Since fiat currencies have a physical form and physical data loses quality when copied, double-spending does not create a big problem in fiat currencies.

Q14	**How can double-spending be prevented in the bitcoin network?**
Reference Link	https://medium.com/innerquest-online/how-does-a-blockchain-prevent-double-spending-of-Bitcoins-fa0ecf9849f7
Ans	Double-spending is prevented in Bitcoin by maintaining a trail of all Bitcoins in a universal ledger. It follows the UTXO model of transactions, so one cannot spend the same coin again. Also, timestamping helps in the prevention of double-spending in the Bitcoin network.

Q15	**How can double-spending be prevented in the Ethereum network?**
Reference Link	https://Ethereum.stackexchange.com/questions/27432/what-is-nonce-in-Ethereum-how-does-it-prevent-double-spending
Ans	Ethereum, unlike Bitcoin, does not use the UTXO concept of transactions and, hence, follows a different methodology to prevent double-spending of Ether. In an Ethereum transaction, there is something called nonce for each account. This number tracks the number of transactions done. So, if the same amount is spent twice, the nonce of the latter transaction will be higher than the previous one and, hence, the network will not accept this transaction as valid.

Q16	**It is generally advised to wait for a few more blocks to get added to the blockchain to ensure that the transaction is confirmed. Explain the reason for this.**
Reference Link	https://Bitcoin.stackexchange.com/questions/8172/what-happens-if-two-miners-mine-the-next-block-at-the-same-time
Ans	In a PoW-based blockchain, there is a possibility of the 51% attack in the network. However, the more the number of blocks, the lesser the probability for that block to be attacked by the 51% attack, since it is more difficult to hack so many blocks. Thus, it is

	recommended to wait for the confirmation of some more blocks after a transaction to ensure the transaction is valid and tamper-proof.

Q17	What is a consensus algorithm? What is the difference between validation and consensus?
Reference Link	https://businessandleaders.it/2019/02/27/blockchain-validation-vs-consensus/
Ans	Consensus means that all the nodes in the network maintain the same ledger at any point in time. The nodes should be in the same state and the consensus mechanism takes care of the same. However, validation helps to ensure the transaction or the block is not tampered with or double spent, etc.

Q18	What is ECDSA and ECC?
Reference Link	https://en.Bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm
Ans	ECDSA or Elliptic Curve Digital Signature Algorithm is used in Bitcoin and other major blockchains to derive the public and private keys for accounts. ECC or Elliptic Curve Cryptography is the method with which public keys are arrived at from private keys. The reverse is not possible using ECC.

Q19	What is a side chain?
Reference Link	https://hackernoon.com/what-are-sidechains-1c45ea2daf3
Ans	A sidechain is a seperate blockchain running parallel to the parent blockchain and is connected to each other using a two-way peg. This two-way interface allows the transfer of assets and information between the two blockchains when required.