Questions and Answers:

Minor 1

Q1: Define the critical characteristics of Blockchain Technology with suitable examples

Q1: Define the critical characteristics of Blockchain Technology with suitable examples

Ans: Characteristics with example

- Blockchain is designed to be **distributed** across networks, which makes it ideal for multi-organizational business networks such as supply chains.
- Before one can execute a transaction, there must be agreement between all relevant parties that the transaction is valid. For example, if you're registering the sale of an assets, that assets must belong to you. This process is known as "**consensus**" and it helps keep inaccurate or potentially fraudulent transactions out of the database.
- The "**increased capacity**" is an important feature of Blockchain. The most remarkable thing about this Blockchain technology is that it increases the capacity of the whole network. Because of the reason that there are a lot of computers working together which in total offers a great power then few of the devices where the things are centralised. For example: mining pool.
- Creating **"immutable ledgers"** is one of also the important parameter of Blockchain. Once the transaction blocks get added on the ledger, no one can just go back and change it. Thus, any user on the network won't be able to edit, delete or update it.
- "**smart contracts**," which helps give confidence that everyone is playing by the rules.

Q2: A user, Alice, wants to send 10 crypto coins to the user Bob. Alice used the blockchain network to send the crypto coin, which works on the Proof-of-Random-Elapsed-Time (PoRET) consensus protocol. The PoRET is the extension of the Proof-of-Work (PoW) consensus algorithm, which identifies who creates the next block for the new set of transactions. In this consensus algorithm, all the nodes do so by waiting for a random amount of time, adding proof of their wait in the block. The created blocks are broadcasted to the network for others' consideration. The winner is the validator which has the least timer value in the proof part. The block from the winning validator node gets appended to the Blockchain. Special hardware is used in the algorithm to stop nodes from always winning the election and stop nodes from generating the lowest timer value. A pseudocode of the PoRET of blockchain implementation is given below. Based on the above consensus algorithm, fill in the blanks and answer the following questions.

1. Start with an initial nonce and Random Number (RN) value.
2. While(RN>----Blank1----)
   {
      Wait()
      RN= -----Blank2-----
   }
3. Compute the hash of the block (Block_Hash, RN).
4. While (Block_Hash< ------Blank3-------)
   {
      a. nonce = nonce + 1
      b. Recompute the hash of block
   }
5. After we've computed the correct hash, we'll send the block to the entire network.

1. Start with an initial nonce and Random Number (RN) value.
2. While(RN>----Blank1----)
   {
      Wait()
      RN= -----Blank2-----
   }
3. Compute the hash of the block (Block_Hash, RN).
4. While (Block_Hash< ------Blank3-------)
   {
      a. nonce = nonce + 1
      b. Recompute the hash of block
   }
5. After we've computed the correct hash, we'll send the block to the entire network.

Ans:

Blank1: zero, 0 (Because, The winner is the validator which has the least timer value in the proof part.)

Blank2: RN-1 (Because, The winner is the validator which has the least timer value in the proof part.So, the RN will decrement by 1 till it reaches to 0.)

Blank3: Difficulty_Level or Target Hash (Because, the line 3 and 4 are for PoW. As it is mentioned that, The PoRET is the extension of the Proof-of-Work (PoW) consensus algorithm, which identifies who creates the next block for the new set of transactions.)

Q2 (A): If the lowest random number of one node is 200, it computes the desired hash in 3 seconds. How much time will it take to confirm the transfer of 10 crypto coins from Alice to Bob? Assume the subtraction operation takes 1 millisecond to compute.

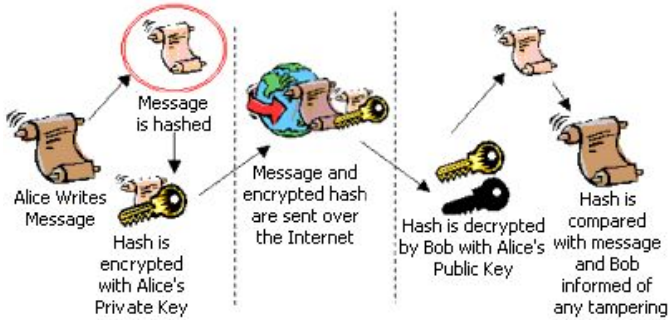
Q2 (A): If the lowest random number of one node is 200, it computes the desired hash in 3 seconds. How much time will it take to confirm the transfer of 10 crypto coins from Alice to Bob? Assume the subtraction operation takes 1 millisecond to compute.

Ans: According to the algorithm, the random number is subtracted by 1 till it reaches to 0, and as mentioned above subtraction operation takes 1 millisecond, hence, it will take 200 millisecond. Next, to compute the desired hash, it takes 3 sec (3000 ms). Let assume the block creation takes x ms. As there is no information about signature verification time,so let assume it's negligible, thus time for transaction confirmation is 3200+x ms.

Q2 (B): Explain the digital signature mechanism used to verify the transaction (10 crypto coins)

Q2 (B): Explain the digital signature mechanism used to verify the transaction (10 crypto coins)

Ans: Digital Signature is a process that guarantees that the contents of a message have not been altered in transit. When you, the server, digitally sign a document, you add a one-way hash (encryption) of the message content using your public and private key pair. Your client can still read it, but the process creates a "signature" that only the server's public key can decrypt. The client, using the server's public key, can then validate the sender as well as the integrity of message contents. Whether it's an email, an online order or a watermarked photograph on eBay, if the transmission arrives but the digital signature does not match the public key in the digital certificate, then the client knows that the message has been altered.



Q3: what would happen if consensus failed and there were in fact, a 51% attacker, somehow, who controls 51% or more of the mining power in the Bitcoin network.

A. Can this attacker steal coins from an existing address?

Q3: what would happen if consensus failed and there were in fact, a 51% attacker, somehow, who controls 51% or more of the mining power in the Bitcoin network.

A. Can this attacker steal coins from an existing address?

Ans: A 51% attack is an attack on a blockchain by a group of miners who control more than 50% of the network's mining hash rate (the number of hash operations done in a given amount of time). Attackers with majority network control can interrupt the recording of new blocks by preventing other miners from completing blocks. The 51% attacker creates an invalid block that contains an invalid transaction. That represents stealing Bitcoins from an existing address that the attacker doesn't control and transferring them to his own address. Now, this attacker can pretend that that's a valid transaction, and pretend that that's a valid block. He keeps building upon this block and even succeeds in making that the longest branch. But the other honest nodes are simply not going to accept this invalid block, and are going to keep mining based on the last valid block that they found at the network. From the point of view of the attacker trying to spend these invalid coins and send them to some merchant, Bob, and buy something in exchange. Now, Bob will presumably be running a Bitcoin node himself, and that will be an honest node. And that node is going to say, this might be the longest branch, but it's not a valid branch because it contains an invalid transaction because the crypto, the signatures, didn't check out. So it's going to simply ignore this longest branch because it's an invalid branch. Because of that, the subverting consensus is not enough, we have to subvert cryptography to steal coins from an existing address. So we conclude that this attack is not possible for a 51% attacker.

Q3: what would happen if consensus failed and there were in fact, a 51% attacker, somehow, who controls 51% or more of the mining power in the Bitcoin network.

B. Can the attacker suppress some transactions? Let's say there are some users, say, Alice, whom the attacker really doesn't like. And the attacker knows some of Alice's addresses and wants to make sure that no coins belonging to any of those addresses can possibly be spent. Is that possible?

Q3: what would happen if consensus failed and there were in fact, a 51% attacker, somehow, who controls 51% or more of the mining power in the Bitcoin network.
B. Can the attacker suppress some transactions? Let's say there are some users, say, Alice, whom the attacker really doesn't like. And the attacker knows some of Alice's addresses and wants to make sure that no coins belonging to any of those addresses can possibly be spent. Is that possible?

Ans: The attacker, since he controls the consensus process of the blockchain. Can simply refuse to create any new blocks that contain transactions from one of Alice's addresses, and can, in fact, also refuse to build upon blocks that contain such transactions, and the attacker will be successful at that. However, the attacker can not prevent these transactions from even being broadcast to the peer-to-peer network. Because the peer-to-peer network doesn't depend on the block chain, doesn't depend on consensus, and we're assuming that the attacker doesn't fully control the network, so the transactions are still going to find a way to reach the majority of nodes. So even if the attacker tries this attack, it will be very clear that the attack is not happening because the peer-to-peer network will still receive these transactions.

Q3: what would happen if consensus failed and there were in fact, a 51% attacker, somehow, who controls 51% or more of the mining power in the Bitcoin network.

C. Can the attacker change the block reward? Can the attacker start pretending that the block reward is instead of 25 Bitcoins, 100 Bitcoins or something like that?

Q3: what would happen if consensus failed and there were in fact, a 51% attacker, somehow, who controls 51% or more of the mining power in the Bitcoin network.
C. Can the attacker change the block reward? Can the attacker start pretending that the block reward is instead of 25 Bitcoins, 100 Bitcoins or something like that?

Ans: This sort of corresponds to changing the rules of the system and because of a reasoning similar to what we applied for stealing Bitcoins from an existing address. This is also not possible because the attacker doesn't control the copies of the Bitcoin software that all of the honest nodes are running. So that's also not possible.

Q3: what would happen if consensus failed and there were in fact, a 51% attacker, somehow, who controls 51% or more of the mining power in the Bitcoin network.
D. Can the attacker destroy confidence in Bitcoin?

Q3: what would happen if consensus failed and there were in fact, a 51% attacker, somehow, who controls 51% or more of the mining power in the Bitcoin network.
D. Can the attacker destroy confidence in Bitcoin?

Ans: If there were a variety of double spending attack attempts, and behavior of not extending the longest valid branch and other such attempted attacks, then people are going to look at this and decide that Bitcoin is no longer acting as a decentralized ledger that they can trust. And so, people will simply lose confidence in the currency, and we might expect that the exchange rate of Bitcoin is going to plummet. In fact, if there is a 51% attacker, and this is known, even if the attacker is not necessarily trying to launch any attacks, it's possible that this might happen. So this we can classify as not only possible but, in fact, likely that a 51% attacker of any sort will simply destroy confidence in the currency.