1. What is the maximum number of Bitcoins? How to calculate it?

There will be a maximum of 21 million Bitcoins.

A block is mined every 10 minutes. The initial reward for a mined coin is 50 Bitcoins. The reward is halved every four years.

6 blocks/ hr \* 24 hrs/day \* 365 days/year \* 4 years per cycle = 210,240 (approx. 210,000)

So reward is halved every 210,000 blocks until the rewards will be less than the lowest unit value of a Bitcoin (Satoshi).

The rate will continue halving, to 25, 12.5, 6.25, and so on. the smallest fraction is 0.00000001  
  
Sum of all the block rewards:  
50 BTC + 25 BTC + 12.5BTC... + 0.00000001 = 100 BTC

therefore, 210,000 \* 100 = 21 million total Bitcoins possible

e. What is double-spending? How does the Bitcoin network achieve consensus?

Paying more people with the exact same digital currency on more than one transactions is called double spending.

Every transaction goes into transactions pool. For example, If a user with one bitcoin, makes two transactions of 1 Bitcoin, each transaction is taken from the pool and checked for validity before being added to block. The first transaction is valid since user had one bitcoin. The second transaction is invalid since he has no bitcoins left.

Each transaction usually waits for 6 confirmations before it is considered to be complete.

Therefore, If both transactions are processed by two different branches at the same time, the transaction that gets the first confirmation will be considered as valid transaction.

Bitcoin achieves consensus through Proof of work. The miner should solve a computationally intensive mathematical puzzle to add a block in the network. Then he broadcasts the block to the network. More than 50% of the nodes in the network should validate the block and then the block will be added to the blockchain.

What are the routine tasks of a Bitcoin miner? What strategic considerations would a miner have? What is a 51% attack?

1. Collect transactions in memory pool.
2. Select transactions from memory pool and mine block.
3. Listen for new transactions and for new blocks mined by other nodes.
4. When a new block is received, it is validated. The miner also removes the transactions which were included in the newly created block, from the memory pool. Only unconfirmed transactions are available in the memory pool.
5. The miner constructs a candidate block with unconfirmed transactions.
6. If miner finds the value for the nonce , solution to Proof of work algorithm, his block becomes valid.

Strategic considerations

Block withholding

When a miner finds a block, he does not broadcast it to the network. He withholds the block and tries to find another block. If he is successful, when a new block is added, the miner broadcasts his two blocks, thus making his chain longest.

Join mining pools

To improve chances of mining , miners join their collective computational power and form pools. On winning the profit is shared with all miners. The share is proportional to computational power contributed to mining.

Blocks are created through consensus of nodes in the network. If a participant has resources to control 51% of the nodes to reach consensus or enough hash power to take over longest chain , the block creation can be manipulated.

It can lead to

selfish mining - they have computational advantage. They can keep mining on top of their blocks without letting the network know and collect all rewards.

blockchain becomes too big - they can add more blocks to their chain thus always having the longest chain

cancelling mining -  they can chose not to add other's transactions to their block.

double spending

spam transactions

random forks

What are the bottlenecks of the Bitcoin system?

What are the bottlenecks of the Bitcoin system?

**Average Block Creation Time and Block Size Limits**

Every block has a limit of 1MB

It takes 10 minutes to mine a block. So there is a limit to the amount of transactions that can be added into the block.Though several thousand transactions can be made in 10 minutes, only 2000 to 3000 transactions can be added in a block. So remaining transactions can be confirmed only in the next block or will have to wait for blocks that come later.

**Storage**

The size of the blockchain continually grows over time; every block added to the blockchain increases the time required for a full-node to join the network

Fixes or changes to some of these problems can only happen when everyone agrees.

Explain the interconnection between block size, block generation interval, number of stale blocks, number of forks, length of forks, and block propagation time. [12 marks]

**Increase in block size** will enable more transactions to be added in the block. It leads to increase in **block propagation time** since it takes more time for the block to be broadcasted across the network. Hence the nodes near the center of the newly created block starts mining well before the nodes in the edge of the network. New blocks might be created by edge nodes before they learn about the latest block added to blockchain. This leads to increase in the **number of forks**. Blockchain takes time to converge into one main chain because it depends on the computational power. In the mean time, the **length of the forks** increase. When one fork is merged into the blockchain, the blocks in other forks becomes orphan blocks or stale blocks. The increase in stale rate leads to double spending thereby weakening the security of the chain.

Decrease in network difficulty decreases **block generation interval**. This increases the size of the blockchain. Thus, increase in block generation rate leads to the same problem.