Bitcoin

Need to introduce scarcity of resources - 21 million cap(explain block reward halving and transaction fee as the incentive once the reward becomes miniscule)

A bitcoin user can send a transaction on the network using a digital signature along with the transaction to prove that it is in fact they who sent the transaction. Anyone can use the public key of the sender to decrypt the message sent on the network to ascertain it matches the actual transaction and that the message has not been tampered with.. This prevents fraudulent transaction.

So, bitcoin is now a scarce resource and is protected from fraudulent transaction -i.e. Only owner of a bitcoin can send it to anyone else. But it’s digital, how do we maintain its scarcity? Can’t a malicious actor combined with a malicious node just send the same amount to someone else and cheat the original receiver? Double spend problem? Byzantine fault tolerance which is introduced by proof of work… miners are incentivized to add to the longest chain otherwise other honest nodes would ignore their block and they would lose all the reward transaction fee they had earned and their electricity cost for mining is lost for nothing. Compare how costly a 51% attack would be wrt the reward they would get. Do a cost benefit analysis and discuss how the cost of the attack far outweighs its benefit and therefore the nash equilibrium for all participants is to be honest and add honest transaction blocks to the longest chain.

How is a bitcoin ownership determined? Maintaining a record of accounts in an indelible ledger. How is it implemented? Linked list of blocks containing transactions with each block pointing to the previous block. Miners validate the block by keeping a set of UTXO and validating the signatures on all the unconfirmed transactions they have received, forming a block of valid unconfirmed transactions. What is the criteria for getting to propose a new block? Find a nonce with the required difficulty(difficulty is the inverse of nbits - recomputed after every 2016 blocks)

Blockheader - contains the hash of prev block (actually only the header needs to be hashed) as well as merkle root of the current block and since merkle root is formed by hashing all the transactions in the current block, changing the current block transaction data would also change the merkle root and thus it is a good representative of the block content and therefore it is enough to just hash the merkle root.