What's happening and you can also wear watchers you know to just that's how people notice that Luna is collapsing because they can see that a lot of the cryptocurrencies are being sold on exchanges and so it's more transparent and how can NFT use beyond artwork so here NFT is was started out as like a tokenized asset to store artwork including paintings you know putting music videos etcetera to show as a proof of ownership but its usage can go beyond that for example identity or say personal records OK OK should that cryptographic techniques what's the difference between symmetric and asymmetric encryption that basically lies in the encryption and decryption process whether they use the same or different keys for encryption and three properties of cryptographic hash functions actually have 4:00 so if you don't remember you can look it up so we can have one to one and one way function and a lack of patience so it's almost and so these are just some of the properties and why it's watching security because those hash are usually used a proof of work right so you don't want people to be able to find a shortcut otherwise Bitcoin will be unable to maintain same minute block interval and it's easy to cheat

how do digital signatures different from option so you can for example this is a clear say question about the differences between subjects and think about this from you know the the purpose for additional signature is not trying to make messages a secret and so it's trying to help you have a way to prove the authenticity whereas encryption is trying to turn the message into something that's hardly readable and interpretable by someone else right so the the major difference is on the purpose but you can also mention that hash is necessary in digital signature right which is not necessarily in question

Bitcoin so the mining difficulty adjustment and 10 minute block time block interval so you can mention concept like target what's the proof of work mining process how do you mine Bitcoin right so that's basically a repetitive process of identifying a nonce which further takes you to a hash value and you need to determine if the hash is slower than the target or not OK so by changing the target you can change the difficulty so when you make the target larger it's going to be easier because the probability is going to go up if we make the target power is going to be more difficult to mine Bitcoin so the difficulty adjustment is based on the overall hash rate of the mining of Bitcoin briefly describe the purpose and approach of Zack with so a sack with it's important to know that sack with is originally was originally proposed to improve the throughput of Bitcoin network it was proposed to solve a very critical bug known as transaction model ability which means that without invalidating A transaction I can tweak the I can tweak the for example the formatting of the digital signature to make it still valid but at the same time the transaction hash will be different such that people cannot find the original transaction so in this case there are they were you know place

The component of digital signature out of this transaction hash computation. Of course, as a side effect, you know they changed the way. And to measure the transaction in terms of this size. So that's why they're actually more room for transactions to be incorporated into the blocks. And then Lightning Network, so there are actually many good things about you know, in addition to the limitations, you might also want to know that Vantage which is definitely make microtransactions more affordable and efficient. So limitations one of them is. To the possibility of making Bitcoin more centralized because. There's usually a few. Feel say notes, which possesses a large amount of bitcoins who can establish connections or say payment channels which are many other small players or say no, it's in the network. So they will be able to control the majority of the flow on the network. So centralization is one problem. Another one is that the entry barrier is pretty high because you need to pay before you actually start the transaction, right? So you need to establish payment channels. There actually are a few more that you can find on the slides with these two will be the more I think major one, then the merge, the merge. Transition Etherium to a new consensus mechanism of POS Proof of Stake.

Name this consensus mechanism and compare it with proof of work, right? So we can include the benefit and drawback. So what's the benefit? The benefit is that you don't need to repeat the payment confirmations of the Hatch. So there's going to be a greener, that's going to be a greener consensus mechanism that saves energy. It could be the bribery and the voting bribery, the you know, the inactivity leagues, you know, the, you know the, the stuff that we have mentioned earlier, the rich gets richer, the Matthew effect, etcetera. And the smart contracts are not, are not immutable to some extent because they can be destroyed because the self destruct. It could also be upgraded through the proxy proxy pattern. Frame the separation into a larger contract or say implementation contract, and a proxy contract then points to the implementation contract.

And then the 34% attack in Etherium. So in Etherium, when a block is to be confirmed, the requirement is to have 60 more than 2/3 of the validators to vote. So if you put 34% of the validators to sleep. Then the network can never reach finality. So you can you sort of stop the blockchain from continuing to confirm transactions. And another one is the double double voting when malicious group of attackers of only 34% dominating, not dominating, controlling the OR selecting the proposed blocks they can. Differently make parallel chains and then through social engineering and lodging they might be able to to to make 2 parallel chains to be both finalized to be confirmed through more than 2/3 of the votes and leading to double finality. The doubts of what are the challenges, One is the inflexibility risk. My contracts may be hardly changeable, but if you use, of course, if you use upgrade, upgrade possible contracts, it would be better. And another one is 51% attack if you have a blockchain network that's very small or if you have a doubt that's really small. Not sufficient users, then one might actually try to dominate the decision making by launching 51%. And also there's a reliance on external Oracle for data accessibility. So when there's something wrong, there's going to be making a negative consequence, for example that. Decentralized exchange that define service we have mentioned earlier and then quadratic voting. Quadratic voting is trying to help the minorities and the example we have is between 4 members and one of them is dominating with the most important credits.

Quadratic what would it helps to mitigate this concern because it downplays single source of voters, but actually emphasize more on the distinct number of voters. But it's not resistant to super attack because if the dominating party splits themselves to. Forged multiple presence in the network, they will be able to exploit the characteristics of super tech to be able to. OK. Decision making process in Windows and then 2016 down hack with the reentrance attack, right. So we're because of the characteristics of the callback function. Such that because the balance update was not timely, it was going to happen after the transaction of the transfer of the token to the hacker. However, because of the callback function, the callback function will immediately activate another round of withdrawal that leads to the draining of the target.

Contract So a simple medication is to say that we should update the balance before we give them the money, and in this case, even if they reenter, this will not influence. This would not be able to take the frontage of the. Of the of the callback function OK and finally Hyperledger Fabric, they have a channel and then the channel fish that the channels can be created within the Fabric network. So it's more like a network of network so organizations can have private channels within them which can otherwise. Which cannot be otherwise accessed by. Other parties within the network, including the network administrators and in terms of the raft. In the rough consensus mechanism, the maximum. The notes that it can tolerate is 50%, so because they have an election process, right, So you have to go above 50% in order to be able to elect a leader, so. The maximum number of no failure is 2, right? You can if you you have 3 nodes failed, then you can never reach majority in the voting process. And finally ask the difficult authorities is important to help the. Members to identify, to, to, to say verify actually to verify the authenticity of the identities of the peer members of the network because you know you can use the public key issue by the certificate authority to to compare the identity with the digital signature. Make sure that if the person that you're talking to you're communicating with is actually the person that you think they should be alright so this is a simple of