**-------------Task 2-----------------**

**Please describe how you would approach assessing the number of confirmations that a Digital Asset exchange like ErisX should wait before it considers a transaction (deposit to the exchange) in the BTC blockchain as valid in order to minimize the risk of being affected by a potential reorganization in the blockchain but also not having a negative impact on the user experience making the user wait for too long.**

**In other words, what measures, data and calculations would you look at to**

**determine how many blockchain confirmations should an exchange wait when a client makes a BTC deposit before making the funds available for a client**

**to trade with.**

*The way transactions are processed on the Bitcoin Blockchain is through Mining. Once the client sends a transaction out, it enters into the Mempool, where it awaits to be picked up by a Miner. Miners pick the transactions with the highest fee and smallest size first. Because they have a block size limit of 1MB and want to earn the highest reward for that block by filling it with as many high-fee transactions as possible. The higher the transaction fee the client appoints, the quicker the processing time will be.*

*However for reasons of security, the Bitcoin blockchain has a mechanism called proof-of-work in place, which makes miners solve a cryptographic challenge in order to get their block approved. This serves the purpose of keeping the network safe of attackers who try to alter the blockchains history by intentionally rises the processing time of 1 block to 10 minutes.*

*While other blockchains have different consensus mechanisms that allow for faster block processing (and can require up to 20 block confirmations to consider a transaction safe), the Bitcoin blockchain is still amongst the slowest. In the Bitcoin blockchain the generally agreed-upon number of blocks that it takes to consider a transaction immutable is only 6 blocks (or 60min). Having 6 confirmed blocks after the client‘s block makes sure that the client‘s block won‘t be a stale block and technically makes it very difficult for any malevolent group to outspeed the honest miners and create a longer ‚fake‘ chain.*

*Technically, as soon as the transaction lands in the Mempool , the tokens are gone from the sender‘s account. However it is still possible that the transaction ends up in a stale block (or with lesser chance, that a hacker sabotages the chain)- which would mean that depositing the money into the receivers account before a safe amount of block confirmations is received, could result in the sender getting his money back, while the receiver has already been credited the money. The exchange would carry the responsibility for that double spend.*

*Various exchanges adopt different policies with varying degrees of risk when it comes to block confirmation requirements.*

*The measures I would look at to determine how many blockchain confirmations an exchange should wait with the Bitcoin Blockchain are:*

*- Average confirmation requirements of other exchanges (Coinbase:3, Kraken:4, Binance:1): Most big exchanges seem to require less block confirmations than the Bitcoin blockchain itsself. They take the risk in order to give their customers the convenience of shorter waiting times for deposits.*

*- Dangers the exchange faces for not getting enough block confirmations:*

*The receiver could spend money that isn‘t his and the exchange would have to carry the costs of this as transactions on the blockchain are irreversible.*

*Because the exchange technically has not received the Bitcoin before 6 block transactions have passed, and if they allow deposit and spending before that, they are basically lending the receiver a Bitcoin to bridge the time gap between sending and receiving. So the exchange would need a marginal reserve of liquidity to enable this.*

*Another consideration is that in this gap time the price of Bitcoin could considerably drop, so the exchange would lose money.*

*- Which reversal mechanisms does the exchange have in place in the case of doublespend: In case that ErisX would consider to require less than 6 block confirmations, it should calculate the possible losses of doublespends into their risk assessment and/or have worked out reversal solutions for doublespend scenarios.*

*- Confirmation requirements of the blockchain itsself: The block confirmations suggestion from the blockchain itself are a good guidance to what is safe and should be kept if one wants to go 100% safe.*

*- Average transaction time of other asset classes than crypto: In the usual banking industry, transactions clear in seconds, but take days to be deposited. So one could say the general public is used to waiting multiple days for money transfers, and compared to that, one hour is not a high waiting time.*

*- Security of the blockchain: The whole technology/congruity of the code of the blockchain, it‘s consensus mechanism and history of hacks is also an important consideration when deciding if one can lower the number of block confirmations.*