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 order 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.

In Satoshi Nakamoto's paper, *Bitcoin: A Peer-to-Peer Electronic Cash System*, he described the scenario of an attacker's potential progress in trying to generate an alternate chain faster than the true, original chain as a Poisson distribution with the expected value:

$$\lambda = z\frac{q}{p}$$

Where:

z = # of linked blocks after a transaction has been added to a block
q = probability the attacker finds the next block
p = probability that an honest node finds the next block

After a transaction has been added to a block and z blocks have been linked after it (assuming the honest blocks take the average expected time per block, for BTC I believe it is around 10 minutes per block), the probability that the attacker could still catch up is calculated by multiplying the density for each amount of progress he could have made by the probability he could catch up from that specific point:

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right)$$

Satoshi states "Only 6 blocks or 1 hour is enough to make reversal computationally impractical." The keyword here is "impractical". In reality, the number of confirmations required is dependent on your tolerance for risk versus negatively impacting user experience.

Satoshi further outlines the number of confirmations required to be 99.9% sure (or less than 1 in 1,000 chance of attacker succeeding):

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

where P is the chance of the attacker eventually having the longer chain and reversing a transaction (0.1% in this example), q is the percentage of hashing power controlled by the attacker, and z is the number of blocks needed to put the risk of a reversal below P (0.1%).

We can see that 6 blocks is sufficient if the attacker has a small percentage of the hashing power; at the time of writing this was about ~100GH/s for 10% of the network.

However, if the attacker has a greater percentage of hashing power, it takes an increasingly longer amount of time to be sure that a transaction can't be reversed. With q > 50%, the attacker will inevitably end up with the longest chain (although this could take an incredibly long amount of time).

As a reference point, Coinbase uses 3 confirmations for Bitcoin specifically (this specification matters because each coin has a different timeframe for how quickly blocks are mined). This seems to be a good rule of thumb for most exchanges, particularly for sending/receiving amounts between $1,000 - $10,000. The exchange may require more/less confirmations depending upon the user, dollar amount, and frequency.

However, given the reality of Bitcoin mining today and the fact that ErisX has trading products that are significantly more valuable (and requiring significantly more margin), it is reasonable and quite logical to require more than 6 confirmations.

Given that 60 confirmations are needed to have <1% odds of success for an attacker wielding 40% hashing power, ErisX should probably consider requiring a number of confirmations greater than 6 and less than or equal to 60, which again depends on their tolerance for risk versus negative user experiences.

While the wait time is less than ideal for customers, I believe that it is a necessary requirement to ensure the safety of user's funds and for the exchange as a whole. This is particularly true for ErisX because of the larger notional values and associated risks inherent with derivative products.