Task 2

The main risk in not waiting for enough confirmations on the blockchain before the Digital Asset Exchange makes the funds available is a doublespend attack. In this scenario, a malicious user will deposit BTC to the exchange in return for funds, and after the funds are made available, they send falsified transactions that send the BTC back to themselves. This attack only works if a) the attacker's original request to trade BTC for funds is accepted by the network and the victim sends the money and b) the attacker is able to create a branch of blocks that is longer than the branch that contains the first transaction. If the attacker cannot "catch up" to the original transaction in the blockchain and reorganize the blockchain, then the requests to send their BTC back to them is considered invalid (the attack fails).

The first thing to look at would be the size of the transaction (what's the total cost in USD). Most researchers agree that transactions of less than the BTC equivalent of $1000 are not prone to attacks, given the large amount of computational power it takes to steal a relatively small amount of money. In Satoshi Nakamoto's original white paper, he explains that one should wait for 6 confirmations on the blockchain to approve a transaction, such that the risk of reorganization on the blockchain is minimized. Their assumption is that no attacker will have more than 10 percent of the total public hash-rate, and the odds of a doublespend succeeding after 6 confirmation at that hash-rate is 0.1 percent. So considering these factors, for transactions of relative low value, Digital Exchanges can decrease the number of confirmations from 6 because of the low risk of attack and overall loss of funds. In my experience, most people who are actively moving low amounts of bitcoin or exchanging it to USD are using BTC for exchange of goods rather than long-term investing.

For larger transactions, I think it is much more pertinent to consider the mathematical risks involved with a doublespend attack. The first variable that is involved in the success odds of a doublespend attack is the hash-rate of the attacker as a percentage of total public hash-rate. The higher the percentage of total hash-rate, the more likely an attacker can succeed in the attack. In a case where an attacker has more than 50 percent of total hash-rate, they will always succeed in any double-spend attack, simply because they can produce more blocks to add to the blockchain than the entire public. In a paper written by Meni Rosenfeld called "Analysis of hash rate-based double-spending," they derive an equation that explains the mathematical odds of a successful double-spend attack, shown below.

r = probability of successful doublespend
q = probability of new block to be found by attacker
p = probability of new block to be found by honest network
m = confirmations found by attacker
n = confirmations found by honest network

$$
\begin{aligned}
r &= \sum_{m=0}^{\infty} P(m) a_{n-m-1} \\
&= \sum_{m=0}^{n-1} \binom{m+n-1}{m} p^n q^m \left(\min(q/p, 1)\right)^{n-m} + \sum_{m=n}^{\infty} \binom{m+n-1}{m} p^n q^m \\
&= \begin{cases} 1 - \sum_{m=0}^{n} \binom{m+n-1}{m} (p^n q^m - p^m q^n) & \text{if } q < p \\ 1 & \text{if } q \geq p \end{cases}
\end{aligned}
$$

Although unwieldy, it is evident that if the number of confirmations made by the digital exchange (honest network) increase, the odds of doublespend success decrease exponentially. However, it is impossible to know the attacker's total hash-rate, and therefore more considerations must be made.

The most practical next step in thinking is identifying the cost-benefit of the attacker launching an attack. I stated earlier that attacks on a relatively small amount of funds are less likely, and that relates to this very principal. Particularly if one wants to defraud an exchange, with possible legal punishment as a risk, one may assume that they are after a significant sum of money and/or BTC. Increasing the number of confirmations to at least 6 or more is crucial in protecting the exchange from attacks on transactions over $1000USD.

Lastly, Digital Exchanges would be advised to keep an eye on public total hash rate. This is calculated by looking at the total number of blocks mined and the current block difficulty. When there is more hashing power in the network, security is stronger because it'd be harder for a single attacker to own a large percentage of it. Perhaps by keeping time-series data on this, along with any information on previous attacks (total funds lost, time, etc.), one could train a system to identify moments when the exchange is more vulnerable to attack.