Homework4

When Bitcoin determines the Proof of Work problem for a new block, it considers all information in the block including:

1. The hash of the previous block
2. The other block header information such as timestamp
3. The transactions in the block

Specifically, the miner needs to find a nonce such that the one-way hash result of the concatenation of the nonce and **all** of the above information has enough leading zeros (determined by current difficulty).

Why the PoW problem has to consider the hash of previous block? What would happen if the miner only needs to find a nonce such that the one-way hash result of the concatenation of the nonce, the other block header information, and the transactions has enough leading zeros? Any security problem?

What would happen if the PoW problem does not consider the timestamp? (Consider the case a malicious miner solves PoW once and put multiple different timestamp)

What would happen if the PoW problem does not consider the transactions?