Question 1

a).

There are several drawbacks for reducing the time between two blocks in bitcoin.

1. As a block takes time to be broadcasted throughout the entire network, with shorter amount of time between two blocks we will see a lot of forks within the network and consensus will be harder to reach in this case.
2. More wastage of hash power. Consider the case where nodes are generated in 5 min, in this case every node that does not know about the new block will be mining on the last block in the blockchain and will discard all the computation once the new block comes. The shorter the time, the more wastage of hash power on calculating the next block.

b).

Ethereum uses a novel protocol called GHOST(Greedy Heaviest Observed Subtree) for mining and this ensure new blocks every 12~15 seconds whereas making sure that the hash power is not getting wasted. In the protocol, every miner that was mining on top of the chain does not discard the block he was mining when a new block comes in. Instead, he completes his block which gets later added as an uncle block while the one that came in goes to the block chain. The uncle block is not the part of the main block chain.

Miners who mine the uncle blocks are also rewarded which makes sure that the user who is proposing such blocks also gets incentivized.

The time cannot be reduced to say 1 second because of the time taken for propagation of the blocks. According to a 2013 paper from Decker and Wattenhofer, it takes about 12 seconds for a block to reach 95% of the nodes. If we reduce the time between two block to be less than 12 seconds, then there is a possibility that the miner will be mining over the stale block which will result in a wastage of hash power.

Reference: https://medium.facilelogin.com/the-mystery-behind-block-time-63351e35603a

c).

The main drawback of bitcoin's POW algorithm is the problem of mining centralization, where a group of companies get considerably high hash power using ASIC(Application specific integrated circuit) chips. Ethereum uses Ethash algorithm as POW, which is ASIC resistant. They achieved this by making sure that their algorithm consumes the entire available memory access bandwidth. Memory cards compete very strongly to achieve this, which means that it is difficult for a ASIC designer to make such a chip.

Reference: https://github.com/ethereum/wiki/wiki/Ethash-Design-Rationale,
https://ethereum.stackexchange.com/questions/14/what-proof-of-work-function-does-ethereum-use

Question 2

a).

The protocol protects the players by ensuring a deposit money d = B(N-1), where N is the number of players and B is the bid amount. If the player is cheating, he does not get his deposit back and the amount is distributed amongst the other players. The protocol relies on timed-commitments to ensure that the no user can cheat.

b). The code is attached in the zip as lottery.sol file. We need to pass in the hash in the bytes_32 field with a 0x appended to it. So if the hash is "e89e12d0c8e31221fb55552a4757122d687b10d320ee6f52836f7d095e94d68f" then we need to pass "0xe89e12d0c8e31221fb55552a4757122d687b10d320ee6f52836f7d095e94d68f" in the bytes32 value.

c).

Protocol

1. The lottery is started by the contractor owner who cannot participate in the lottery and is a honest user.
2. All three users who want to participate in the lottery must register first. The user needs to deposit 30 ether to participate in the lottery where he will receive 20 ether if he is the winner and loses 10 ether otherwise. If the user is not following the protocol or tries to cheat, he loses 20 ether.
3. After registering the user is supposed to bid on a value from 0, 1 or 2 and send a hash(keccak256) of a string x, where x = [0,1,2][random 10 digit number]. The length of string x is 11 and the first character of the string should be a value in 0,1 or 2. This is done to ensure that the other players do not learn of the value that is proposed by the user.
4. After all three players place a bid, the owner will start opening bids, which means he will give all participants 5 minutes to reveal the value and the random 10 digit number. If a players fails to deliver this in 5 minutes, he is found violating the protocol and 20 ether from his wallet are distributed to other participants and the lottery is closed after returning all the amount that the contract holds to valid users.
5. If a user tries to cheat and sends in a wrong {value,10 digit number pair}, then the user is penalized and 20 ether from his balance are distributed to other participants.
6. If all the users have provided their input value within the time limit, then the protocol find the winner by (i1 + i2 + i3)%3 = [0,1,2], where i is the input provided by each participant. The winner is the user who registered on that index.
7. Once the winner is declared, he gets rewarded by 20 ether and the balances of the rest of the participants is updated accordingly.

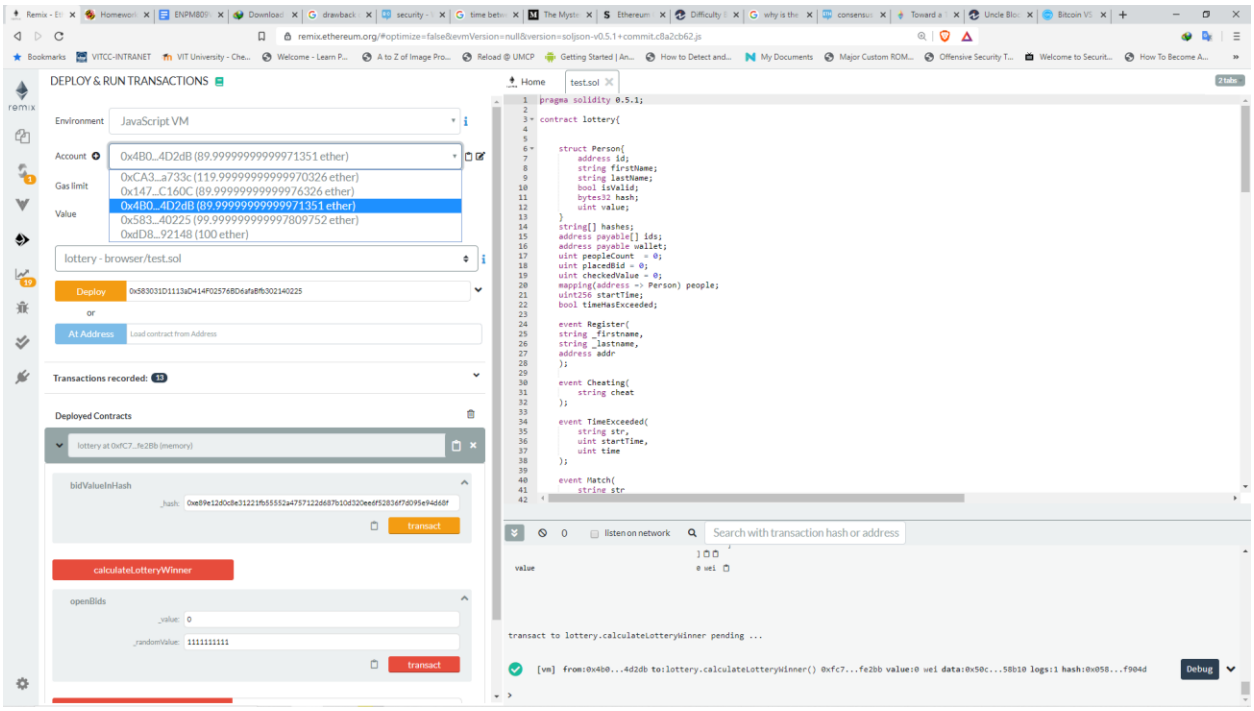

Figure 1:Showing updated wallet value when a user is the winner.(All wallet started from 100 ether)