Student: Fengning (Fred) Luo 1004687029 freddy.luo@mail.utoronto.ca

Question 1:

I think this claim is true. For Ethereum, a simple transfer transaction only needs to specify a sender, a recipient, and the amount transferred. This is because the account model in Ethereum maintains a state of balance for each account. On the other hand, for each transaction in UTXO model, the input must be fully spent, and may require inefficient reference of multiple inputs and outputs to ensure the availability of funds. This process can be less space-efficient than the account model in Ethereum.

Question 2:

When a user creates a new address for every transaction, it indeed becomes more challenging to link these addresses to a single identity under the UTXO model, but it is still possible for others to deduces the possibility that these addresses are linked to the same individual through tracking the movement “change” after a transaction and the movement of funds. In contrast, it is generally considered easier to track transaction linkages with the account model with Ethereum.

Question 3:

The main reason for the GAS limit is to prevent malicious or accidental infinite loops or excessive computation. Without such a limit, one contract account could run indefinitely and significantly slow down the network. If we instead use the traditional 1MB block limit, blocks that take up the entire 1MB limit could lead to slower propagation and processing times and can lead to centralization. Blocks that do not take up the entire size limit introduce inefficient use of space.

Question 4:

Different EVM operations can require different computational power. For instance, arithmetic calculations should cost less than modifying storage. Setting up different GAS amounts can reflect this computational difference. This can encourage developers to write more efficient code to minimize gas consumption and lead to more efficient use of resources.