Homework2

Junhong Chen

Ethereum uses account model to store the blockchain state. One claims that the account model can reduce the average size of simple transfer transactions comparing to the UTXO model. Do you think this is true or not? Explain why.

More UTXOs the transaction refers, more data the transaction needs to include. In the UTXO model, when a user initializes a transaction, the user may include multiple UTXOs as the inputs and create multiple UTXOs as the outputs of the transaction, which can result in a large transaction size. In the account model, a transaction only specifies a signature, the receiver, the amount, an optional data field, and STARTGAS and GASPRICE values, which are smaller in size, compared with the UTXO model.

One claims that compared to the account model in Ethereum, the UTXO model can provide anonymous transactions if the user creates a new address for every transaction. Do you think this is true or not? Explain why.

True. In the UTXO model, the user can consume the previous UTXOs and create a new UTXO with the new address as one of the outputs of a transaction. If the user has several addresses, that user can also include the UTXOs associated with those addresses as the inputs of a transaction. Therefore, it’s hard to track the flow of funds and link multiple transactions with a specific user. In the account model, the user can also change the address for every transaction, but as a transaction only contains only one digital signature and one recipient address, the UTXO model can provide more anonymous transactions than the account model.

Why Ethereum introduces a GAS limit for the block? What if we remove the GAS limit and put back the traditional block limit of 1MB like Bitcoin?

The GAS limit specifies the maximum amount of computational power that can be consumed within a block. This prevents malicious entities from using harmful start contracts containing infinite loops to consume massive amounts of resources of miners to shut them down. The GAS limit will also help miners know ahead of time how many steps the computation needs to take and help miners control the growth of a block. If we remove the GAS limit and put back the traditional block limit of 1MB like Bitcoin, the network might become vulnerable to DOS attack because malicious entities can use expensive operations or infinite loops to significantly consume excessive resources. Blocks would also lose control of the growth of a block.

Ethereum sets up a different GAS amount for different EVM operations. Why?

Different EVM operations can consume different amounts of resources and computation costs, so they are set up a different GAS amount. For example, the ADD operation computes the addition of two values, reducing 3 gas, but the ADDMOD operation takes 8 gas because it not only adds two numbers together but also performs a modulo operation.