Exercise 1

1. Look at the steps in InputOutputCoin to verify that a transaction is valid. What is the computationally most expensive step?

   > Checking that a referenced output is not already spent is the most computationally expensive step: it requires checking that no transaction in the blockchain references that output. In other words, all transactions in the blockchain after that output have to be checked to not reference that output.

2. What do you propose to make this step less computationally expensive?

   > Instead of just storing the blockchain, we also store the set of unspent transaction outputs, the *utxo set*, and we update it with every new block we receive. See here for some utxo set data.