Ethereum Theoretical Exercises

Smart Contract Use Cases

(a) There are many use cases for smart contracts. Write down four of them.

(b) Find a contract for each use case you have listed in the previous subtask.
Hint: `https://etherscan.io/labelcloud` might help.

EVM and Gas

(a) What is gas in the context of Ethereum?

(b) What happens with spare gas if too much gas was provided for a transaction?

(c) Name on relatively expensive and one relatively cheap EVM instruction and briefly explain why. You can use `https://ethereum.org/en/developers/docs/evm/opcodes/`.

(d) Calculate an estimation of how much it approximately costs (in USD) to store 1 KiB of data on the Ethereum blockchain at the moment. For simplicity, consider only the cost of SSTORE operations and disregard everything else. Use current average gas price from Etherscan for your calculation.

(e) Name one instruction that can refund gas.

Storing Data in Smart Contracts

(a) At a very low level, storing data to storage is performed by the EVM instruction SSTORE. According to the yellow paper, the gas cost of an SSTORE operation is 20,000 when storage value is set to non-zero from zero and 5,000 in any other case. Why is it more expensive to set a value from zero to non-zero?

Transactions in Ethereum

(a) In Ethereum there are two types of transactions. Whenever a wallet calls a method on a contract, a transaction is sent. Whenever a contract calls a method on another contract, a virtual message is sent (Sometimes referred as internal transactions). Messages exist "virtually" and are not written to the blockchain. Why are messages not published to blockchain? How could the blockchain be in the same state among all nodes without writing messages to the blockchain?

(b) Name four reasons why a transaction that is sent to the Ethereum network might not get mined.

(c) Name two different ways how a mined transaction can fail.

(d) Why does a mined transaction that fails still cost gas?

True/False

1. Are these statements true or false? Give a short explanation.

   (a) Every pure function is a view function.

   (b) In Ethereum, a smart contract that has no functions that is declared as **payable** cannot receive any Ether.

   (c) If **msg.sender == tx.origin**, then this code was called directly by an externally owned account and not by another smart contract.