Assignment 08

1) **Read Blockchain Basics from Solidity Read The Docs PDF and create notes on each topic**

Ans: Blockchain Basics:

Transactions: A blockchain is a globally shared, transactional database. This means that everyone can read entries in the database just by participating in the network. If you want to change something in the database, you have to create a so-called transaction which has to be accepted by all others.

Blocks: The transactions will be bundled into what is called a "block" and then they will be executed and distributed among all participating nodes. If two transactions contradict each other, the one that ends up being second will be rejected and not become part of the block.

These blocks form a linear sequence in time and that is where the word "blockchain" derives from. Blocks are added to the chain in rather regular intervals - for Ethereum this is roughly every 17 seconds.

2) **Read The EVM from Solidity Read The Docs PDF and create notes on each topic.**

Ans: Ethereum Virtual Machine: Ethereum Virtual Machine or EVM is the runtime environment for smart contracts in Ethereum. It is not only sandboxed but actually completely isolated, which means that code running inside the EVM has no access to network, filesystem or other processes.

Accounts: There are two kinds of accounts in Ethereum which share the same address space: **External accounts** that are controlled by public-private key pairs and **contract accounts** which are controlled by the code stored together with the account.

Gas: each transaction is charged with a certain amount of gas that has to be paid for by the originator of the transaction (tx.origin).

Storage, Memory and the Stack:

Each account has a data area called storage, which is persistent between function calls and transactions. Storage is a key-value store that maps 256-bit words to 256-bit words.

memory, of which a contract obtains a freshly cleared instance for each message call. Memory is linear and can be addressed at byte level, but reads are limited to a width of 256 bits, while writes can be either 8 bits or 256 bits wide.

The EVM is not a register machine but a stack machine, so all computations are performed on a data area called the stack. It has a maximum size of 1024 elements and contains words of 256 bits.

Instruction Set:

The instruction set of the EVM is kept minimal in order to avoid incorrect or inconsistent implementations which could cause consensus problems. All instructions operate on the basic data type, 256-bit words or on slices of memory.

Message Calls:

Contracts can call other contracts or send Ether to non-contract accounts by the means of message calls. Message calls are similar to transactions, in that they have a source, a target, data payload, Ether, gas and return data. I

Logs: It is possible to store data in a specially indexed data structure that maps all the way up to the block level. This feature called **logs** is used by Solidity in order to implement events.

3) What is the gas usage of SLOAD, SSTORE, MLOAD, MSTORE?

Ans: MLOAD means load word from memory.

It uses 3 gwei gas.

MSTORE means save word to memory. It also uses 3 gwei gas. It uses 200 gwei gas for storage operation. SSTORE means save word to storage.

SLOAD means load word from stoage.

4 If you add non-zero value it will take 20000 gas, if you will set this value to 0 it will cost 5000 gas.

4) selfdestruct in Solidity?

Ans: Destroy the current contract, sending its funds to the given Address and end execution. Note that selfdestruct

has some peculiarities inherited from the EVM:

the receiving contract's receive function is not executed.

the contract is only really destroyed at the end of the transaction and revert s might "undo" the destruction.

Furthermore, all functions of the current contract are callable directly including the current function.

5) The contracts that we will cover from read the docs must be Verified and Published on the Goerli Testnet. - You have to add the contract URL of Etherscan.

Ans: 0xf3d14a568ffbb1fa993f645d91621f294f7b5893163aa999424297cf430d1ed1

https://goerli.etherscan.io/tx/0xf3d14a568ffbb1fa993f645d91621f294f7b5893163aa999424297cf430d1ed1