Solidity

Cheatsheet

By Param_eth

Function Visibility

public - accessible to all

private - accessible only to contract

internal - accessible to contract and subcontracts

external - accessible only outside contract

Function Types

pure - does not access the blockchain

view - does not modify the blockchain

payable - can receive Ether

*pure and view functions do not cost any gas.

Data Location

storage - stored on the blockchain
memory - stored in memory

Parameter Types

- int / uint {8/256}
- string
- bool
- address / address payable

Structures

struct StructureName {
<parameter type> var1;
<parameter type> var2;
… }

Array and Mappings

<parameter type>[] arrayName;
mapping (<parameter type> => <parameter type>)
mappingName;

Contract

contract contractName {...

....}

Constructor

constructor(<parameter types>)

{public|private|internal|external}

{...}

Functions

function functionName(<parameter types>) {public|private|internal|external} [pure|view|payable] [modifiers] [returns (<return types>)] {...}

Interface

function functionName(<parameter types>) {public|private|internal|external} [pure|view|payable] [modifiers] [returns (<return types>)];

Modifiers

modifier modifierName(<parameter types>) {...
...}

- Use _; to continue with the function after running modifier code

Events

event eventName(<parameter types>);
emit eventName(<parameters>);

- Events are defined at contract root and emitted inside functions.

Useful links

Remix ide - https://remix.ethereum.org/

Solidity Documentation - https://docs.soliditylang.org/en/latest/index.html

Security

Use Ownable contract to define owner of a contract and restrict usage of some functions using onlyOwner modifier.

Mind Overflow/Underflow when using integers. Use OpenZeppelin SafeMath library to prevent problems