In this assignment you will familiarize yourself with the language solidity in the browser - solidity tool.

Q1: Open browser solidity and explore it

https://remix.ethereum.org/

Explore the following sections

- Compile
- Run
- Settings
- Analysis
- Debugger
- Support

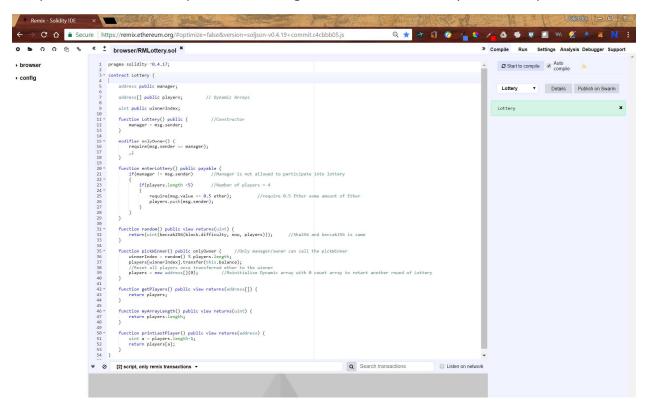
To explore all this, I have one simple lottery system solidity code. I am using to check all above features in Remix online IDE

```
pragma solidity ^0.4.17;
contract Lottery {
   address public manager;
   address[] public players;  // Dynamic Arrays
   uint public winnerIndex;
   function Lottery() public {
                                //Constructor
      manager = msg.sender;
   modifier onlyOwner() {
       require(msg.sender == manager);
   }
   function enterLottery() public payable {
       if(manager != msg.sender) //Manager is not allowed to
participate into lottery
          require (msg.value == 0.5 ether); //require
0.5 Ether some amount of Ether
             players.push (msg.sender);
          }
       }
   }
```

```
function random() public view returns(uint) {
      return(uint(keccak256(block.difficulty, now, players)));
//Sha256 and keccak256 is same
   can call the pickWinner
      winnerIndex = random() % players.length;
      players[winnerIndex].transfer(this.balance);
      //Reset all players once transferred ether to the winner
      array with 0 count array to retart another round of Lottery
   function getPlayers() public view returns(address[]) {
      return players;
   }
   function myArrayLength() public view returns(uint) {
      return players.length;
   function printLastPlayer() public view returns(address) {
      uint a = players.length-1;
      return players[a];
   }
}
```

The code is basically creating a contract for lottery to participate only 4 peoples/accounts. There will be a manager who deploy this contract and pick the winner randomly. There are many public variables to just check the outputs of the different actions. And I have a condition that Manager cannot participate in this lottery system. After picking the winner, the code itself sends the balance to the winner automatically and then lottery balance will be empty.

Compile: Remix browser compiles code as change in the code automatically if Auto Compile Checked.



The Details button give lot of information's about

Contract Name

Metadata

Bytecode

ABI

Web3Deploy

MetaDataHash

SwarmLocation

FunctionHashes

GasEstimates

DEVDOC

UserDoc

RuntimeBytecode

Assembly

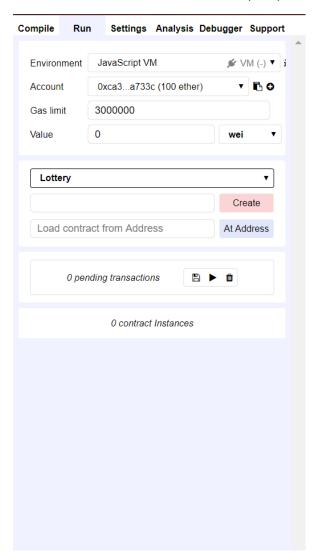


```
SWARMLOCATION 6

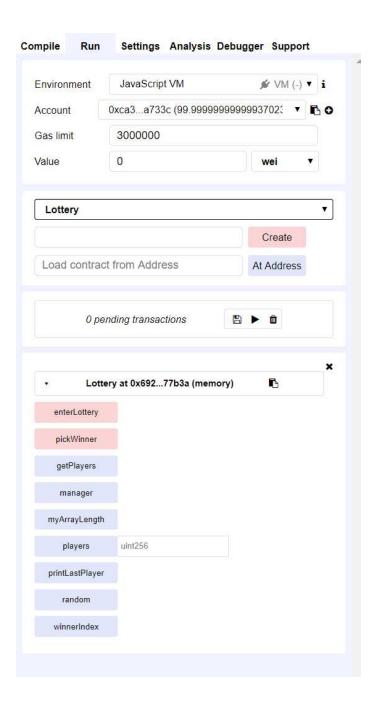
"bzzr://350e1b8b1b57a6808075a36d1df2554d3d627a95b93ec8531d1774c55c6dfe3e"
```

```
GASESTIMATES 🗗 0
{
   "Creation": {
       "codeDepositCost": "415400",
       "executionCost": "20710",
       "totalCost": "436110"
   },
   "External": {
       "enterLottery()": "infinite",
       "getPlayers()": "infinite",
       "manager()": "478",
       "myArrayLength()": "424",
       "pickWinner()": "infinite",
        "players(uint256)": "935",
       "printLastPlayer()": "958",
       "random()": "infinite",
       "winnerIndex()": "518"
}
```

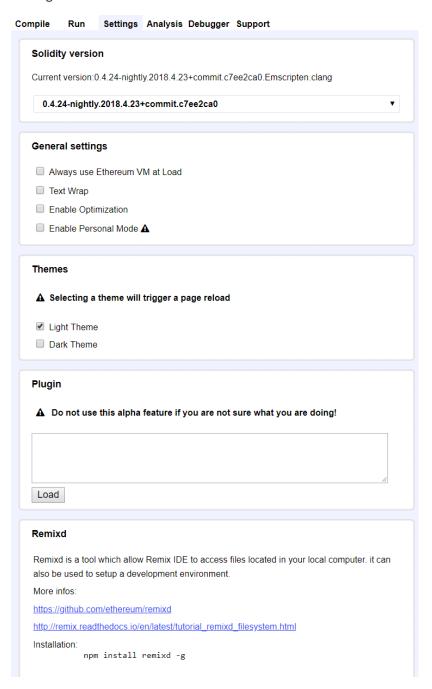
Run Tab: Once there is no error on compile, please click on Run to run and deploy the smart contract.



2nd image is after creating contract.



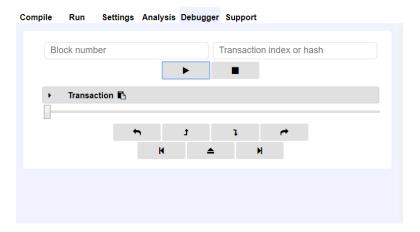
Settings



Analysis

Compile Run Settings Analysis Debugger Support Security Transaction origin: Warn if tx.origin is used Check effects: Avoid potential reentrancy bugs ✓ Inline assembly: Use of Inline Assembly Block timestamp: Semantics maybe unclear Low level calls: Semantics maybe unclear ☑ Block blockhash usage: Semantics maybe unclear Selfdestruct: Be aware of caller contracts. Gas & Economy Gas costs: Warn if the gas requirements of functions are too high. This on local calls: Invocation of local functions via this Miscellaneous Constant functions: Check for potentially constant functions Similar variable names: Check if variable names are too similar no return: Function with return type is not returning Guard Conditions: Use require and appropriately Run Auto run Potential Violation of Checks-Effects-Interaction pattern in <i>Lottery.pickWinner()</i> potentially lead to re-entrancy vulnerability.
 <i>Note:</i> Modifiers are currently not considered by this static analysis more browser/RMLottery.sol:32:49:use of "now": "now" does not mean current time. Now is an alias for block timestamp. Block timestamp can be influenced by miners to a certain degree, be careful. more Gas requirement of function Lottery.getPlayers() high: infinite. If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)

Debugger



Support

Compile Run Settings Analysis Debugger Support

Have a question, found a bug or want to propose a feature? Have a look at the <u>issues</u> or check out the <u>documentation page on Remix</u> or <u>Solidity</u>.

ethereum/remix community chat

like by the time i ask a question, i've spent at least a few hours/days trying to figure it out on my own



hnamzian @hnamzian

Apr 22 05:14

I got it. thank you



imrankhanjoya @imrankhanjoya

Apr 22 11:37

Error:Execution failed for task

':transformClassesWithJarMergingForDebug'.

com.android.build.api.transform.TransformExceptio n: java.util.zip.ZipException: duplicate entry: com/google/android/gms/analytics/internal/Comman d\$1.class

sorry

how to pass values to function Voting(bytes32[] candidateNames) public {

its constructor



CooperLee123 @CooperLee123 Apr 22 22:33



Nina Breznik @ninabreznik

00:39

@inventor-tech Thank you for helping out other members of the community. This is what everyone should try. A little and then we all help each other &



inventor-tech @inventor-tech

00:4

i try when i can. i dont always have time. but yea, people help people.

START CHATTING

Sign in to start chatting.

Q2: Install Solc Compiler in Ubuntu Machine.

First, download Nodejs and install npm from the bin folder of extracted nodejs folder.

```
🥦 🗐 📵 rajendra@rajendra-VirtualBox: ~
  Command 'din' from package 'din' (universe)
bin: command not found
rajendra@rajendra-VirtualBox:~/nodejs/node-v10.0.0-linux-x64$ cd bin
rajendra@rajendra-VirtualBox:~/nodejs/node-v10.0.0-linux-x64/bin$ ls
node npm npx
rajendra@rajendra-VirtualBox:~/nodejs/node-v10.0.0-linux-x64/bin$ npm install
The program 'npm' is currently not installed. You can install it by typing:
sudo apt install npm
 rajendra@rajendra-VirtualBox:~/nodejs/node-v10.0.0-linux-x64/bin$ npm version
The program 'npm' is currently not installed. You can install it by typing:
sudo apt install npm
rajendra@rajendra-VirtualBox:~/nodejs/node-v10.0.0-linux-x64/bin$ sudo apt install npm
[sudo] password for rajendra:
Reading package lists... Done
Building dependency tree
Reading state information... Done

The following additional packages will be installed:

gyp javascript-common libjs-inherits libjs-jquery libjs-node-uuid libjs-underscore libssl-dev libssl-doc

node-ansi node-ansi-color-table node-archy node-async node-block-stream node-combined-stream node-cookie
    node-forever-agent node-form-data node-fstream node-fstream-ignore node-github-url-from-git node-glob no
    node-ini node-json-stringify-safe node-lockfile node-lru-cache node-mime node-minimatch node-mkdirp node
   node-normalize-package-data node-npmlog node-once node-osenv node-qs node-read node-read-package-json no node-semver node-sha node-sigmund node-slide node-tar node-tunnel-agent node-underscore node-which nodej
   zlib1g-dev
 Suggested packages:
apache2 | lighttpd | httpd node-hawk node-aws-sign node-oauth-sign node-http-signature debhelper python-
The following NEW packages will be installed:
gyp javascript-common libjs-inherits libjs-jquery libjs-node-uuid libjs-underscore libssl-dev libssl-doc
node-ansi node-ansi-color-table node-archy node-async node-block-stream node-combined-stream node-cookie
node-forever-agent node-form-data node-fstream node-fstream-ignore node-github-url-from-git node-glob no
   node-ini node-json-stringify-safe node-lockfile node-lru-cache node-mime node-minimatch node-mkdirp node node-normalize-package-data node-npmlog node-once node-osenv node-qs node-read node-read-package-json no node-semver node-sha node-sigmund node-slide node-tar node-tunnel-agent node-underscore node-which nodej
   zlib1g-dev
0 upgraded, 61 newly installed, 0 to remove and 90 not upgraded.
Need to get 8,673 kB of archives.
```

Now, install solidity compiler using command sudo npm install -g solc

```
© □ rajendra@rajendra-VirtualBox:~
rajendra@rajendra-VirtualBox:~S sudo npm install -g solc
/usr/local/bin/solcjs -> /usr/local/lib/node_modules/solc/solcjs
/usr/local/lib
solc@0.4.23

fs.extr.@0.30.6

graceful-fs@4.1.11

Jsonfile@2.4.9

klaw@1.3.1

path-is-absolute@1.0.0

infilight@1.0.6

wrappy@1.0.2

inherits@2.0.3

minimatch@3.0.4

brace-expansion@1.1.11

balanced-match@1.0.0

concet1.4.0

nemorystream@0.3.1

require-from-string@1.2.1

senver@5.5.0

yars@4.8.1

cliu@3.2.0

strtp-ansi@3.0.1

ansi-regex@2.1.1

wrap-ansi@2.1.0

decamelize@1.2.0

get_caller_file@1.0.2

lodssh.assign@4.2.0

bs-locale@1.4.0

led@1.0.0

red@4.by.0.0

red@4.by.0.0

rede_decay.0.0

livert-kv@1.0.0

rede_decay.0.1.1

find-up@1.1.2
```

Q3: Deploy a Smart contract using Remix Browser IDE in Local Block chain environment

Note: Here are the Minimum Requirements

- Understanding of Remix Browser
- Usage of Ganache / Test RPC
- Understanding of Basic Solidity functions.