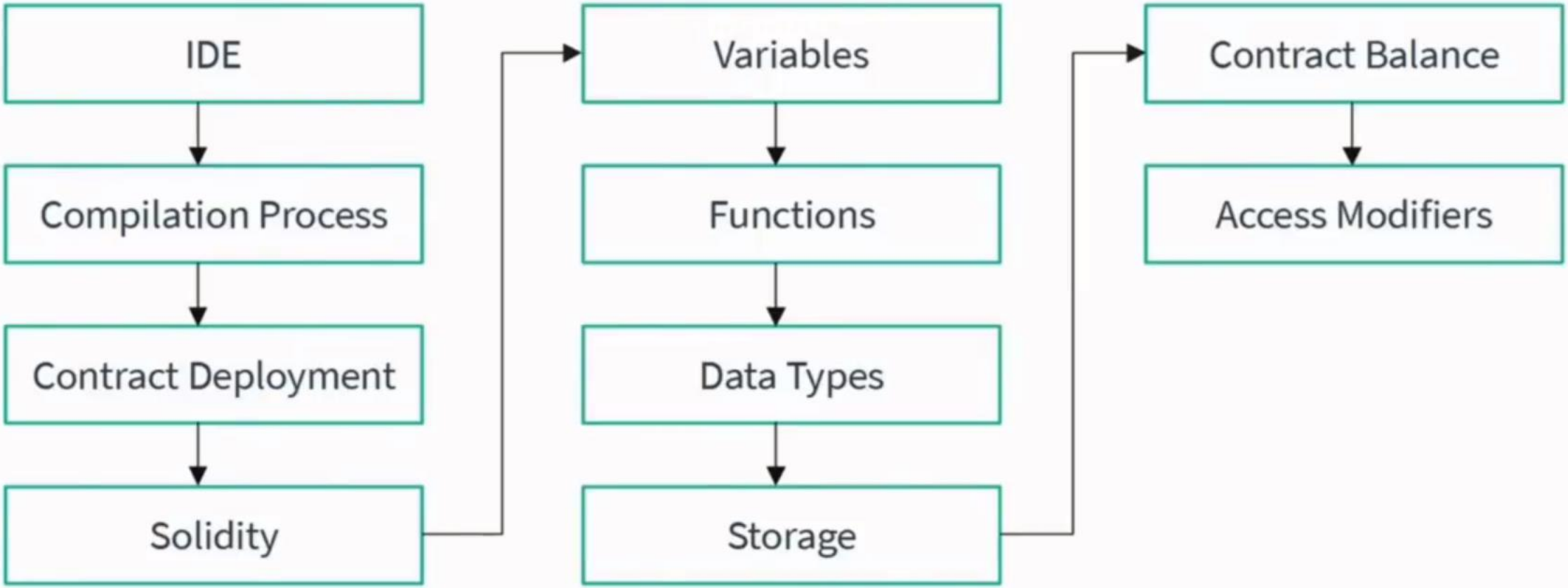
Solidity

Dr. Bahar Ali
Assistant Professor (CS), National University Of Computer and Emerging Sciences, Peshawar.

Solidity Full Course Overview



Prerequisite of Solidity Course

Prerequisite

Blockchain

Ethereum

Know any
Programming Language

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.4+commit.c7e474f2.js

FILE EXPLORERS

Workspaces

default_workspace

- contracts
- scripts
- tests
- README.txt

0 tabs

0 listen on network

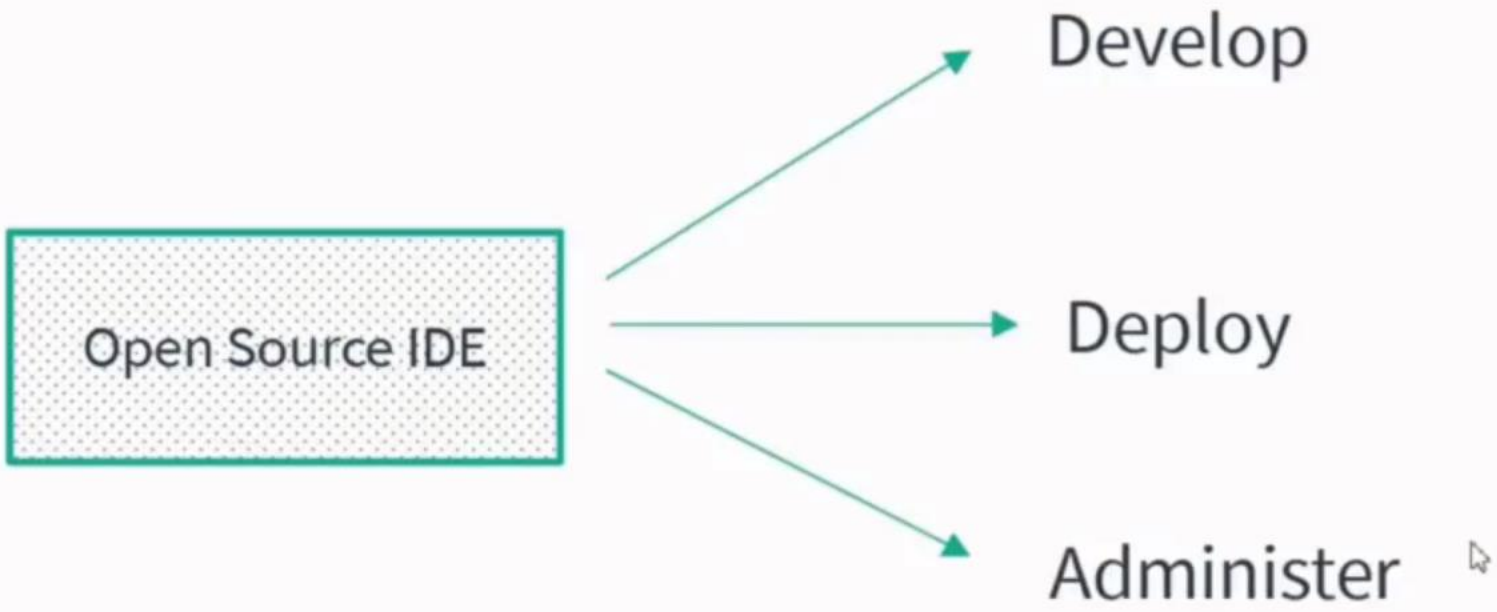
Search with transaction hash or address

```
You can use this terminal to:
 • Check transactions details and start debugging.
 • Execute JavaScript scripts:
     - Input a script directly in the command line interface
     - Select a Javascript file in the file explorer and then run `remix.execute()` or `remix.exeCurrent()` in the command line interface
     - Right click on a JavaScript file in the file explorer and then click `Run`

The following libraries are accessible:
 • web3 version 1.0.0
 • ethers.js
 • swarmgw
 • remix (run remix.help() for more info)
```

>

Remix IDE

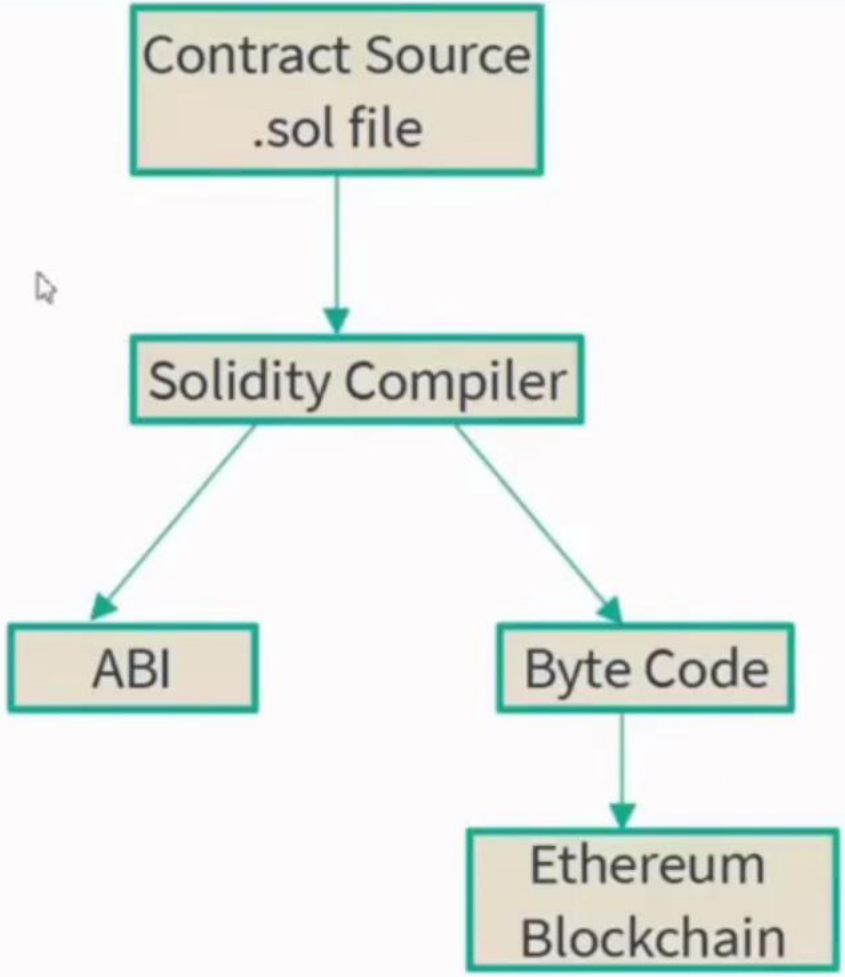


Remix IDE

Some important to know about Remix IDE-

- **Language Support -** Solidity and Vyper
- **Written in -** JavaScript
- **Modules -** Testing , Debugging ,Deploy

Smart Contract Compilation



Remix - Ethereum IDE | Notepad | Online Notes free, no | ethereum opcodes - Google Sea | bytecode to opcode disassembl

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.4+commit.c7e474f2.js

SOLIDITY COMPILER

EVM VERSION

compiler default

COMPILER CONFIGURATION

- Auto compile
- Enable optimization 200
- Hide warnings

Compile 1_Storage.sol

CONTRACT

Storage (1_Storage.sol)

Publish on Swarm

Publish on Ipfs

Compilation Details

ABI Bytecode

Home | 1_Storage.sol | 2 tabs

```
contract Storage {

    uint256 number;

    /**
     * @dev Store value in variable
     * @param num value to store
     */
    function store(uint256 num) public {
        number = num;
    }

    /**
     * @dev Return value
     * @return value of 'number'
     */
    function retrieve() public view returns (uint256){
        return number;
    }
}
```

0 listen on network | Search with transaction hash or address

You can use this terminal to:
- Check transactions details and start debugging.
- Execute JavaScript scripts:
  - Input a script directly in the command line interface
  - Select a Javascript file in the file explorer and then run `remix.execute()` or `remix.exeCurrent()` in the command line interface
  - Right click on a JavaScript file in the file explorer and then click `Run`

The following libraries are accessible:
- web3 version 1.0.0
- ethers.js
- swarmgw
- remix (run remix.help() for more info)

>

Remix - Ethereum IDE | Notepad | Online Notes free, no | ethereum opcodes - Google Sea | bytecode to opcode disassembl

rapidtables.com/tools/notepad.html

Home › Tools › Notepad

Write With Confidence

File Edit View Help


```
{
    "generatedSources": [],
    "linkReferences": {},
    "object":
"6080604052348015610010576000080fd5b5061012f806100206000396000f3fe6080604052348015600f57600080fd5b506004361060325760003560e01c80632e64cec1146037578063605736 1d146051575b600080fd5b603d6069565b604051
6048919060c2565b604051809103 90f35b606760048036038101906063919060 8f565b6072565b005b60008054905090565b806000819055505056 5b60008135905060898160e5565b92915050565b600060208284031215 60a057600080fd5b600060ac84828501607c565b91505092915050565b60bc8160db565b82525050565b600060208201905060d5600083018460b5565b92915050565b60008190509190505 65b60ec8160db565b811460f657600080fd5b5056fea2646970667358 221220558a01c8b4ee2c526c2ddfcec64def8074ce4d710da74d1e18205ac259207d2564736f6c63430008040033",
    "opcodes": "PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO PUSH2 0x10 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST POP PUSH2 0x12F DUP1 PUSH2 0x20 PUSH1 0x0 CODECOPY PUSH1 0x0 RETURN INVALID PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO PUSH1 0xF JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST POP PUSH1 0x4 CALLDATASIZE LT PUSH1 0x32 JUMPI PUSH1 0x0 CALLDATALOAD PUSH1 0xE0 SHR DUP1 PUSH4 0x2E64CEC1 EQ PUSH1 0x37 JUMPI DUP1 PUSH4 0x6057361D EQ PUSH1 0x51 JUMPI JUMPDEST PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH1 0x3D PUSH1 0x69 JUMP JUMPDEST PUSH1 0x40 MLOAD PUSH1 0x48 SWAP2 SWAP1 PUSH1 0xC2 JUMP JUMPDEST PUSH1 0x40 MLOAD DUP1 SWAP2 SUB SWAP1 RETURN JUMPDEST PUSH1 0x67 PUSH1 0x4 DUP1 CALLDATASIZE SUB DUP2 ADD SWAP1 PUSH1 0x63 SWAP2 SWAP1 PUSH1 0x8F JUMP JUMPDEST PUSH1 0x72 JUMP JUMPDEST STOP JUMPDEST PUSH1 0x0 DUP1 SLOAD SWAP1 POP SWAP1 JUMP JUMPDEST DUP1 PUSH1 0x0 DUP2 SWAP1 SSTORE POP POP JUMP JUMPDEST PUSH1 0x0 DUP2 CALLDATALOAD SWAP1 POP PUSH1 0x89 DUP2 PUSH1 0xE5 JUMP JUMPDEST SWAP3 SWAP2 POP POP JUMP JUMPDEST PUSH1 0x0 PUSH1 0x20 DUP3 DUP5 SUB SLT ISZERO PUSH1 0xA0 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST PUSH1 0x0 PUSH1 0xAC DUP5 DUP3 DUP6 ADD PUSH1 0x7C JUMP JUMPDEST SWAP2 POP POP SWAP3 SWAP2 POP POP JUMP JUMPDEST PUSH1 0xBC DUP2 PUSH1 0xDB JUMP JUMPDEST DUP3 MSTORE POP POP JUMP JUMPDEST PUSH1 0x0 PUSH1 0x20 DUP3 ADD SWAP1 POP PUSH1 0xD5 PUSH1 0x0 DUP4 ADD DUP5 PUSH1 0xB5 JUMP JUMPDEST SWAP3 SWAP2 POP POP JUMP JUMPDEST PUSH1 0x0 DUP2 SWAP1 POP SWAP2 SWAP1 POP JUMP JUMPDEST PUSH1 0xEC DUP2 PUSH1 0xDB JUMP JUMPDEST DUP2 EQ PUSH1 0xF6 JUMPI PUSH1 0x0 DUP1 REVERT JUMPDEST POP JUMP INVALID LOG2 PUSH5 0x6970667358 0x22 SLT KECCAK256 SSTORE DUP11 ADD 0xC8 0xB4 0xEE 0x2C MSTORE PUSH13 0x2DDFCEC64DEF8074CE4D710DA7 0x4D 0x1E XOR KECCAK256 GAS 0xC2 MSIZE KECCAK256 PUSH30 0x2564736F6C6343000804003300000000000000000000000000000000000000 ",
    "sourceMap": "133:356:0:-:0;;;;;;;;;;;;;;;;;;;"
}
```


Line 7, Column 2 Chars 2629, Words 299

Remix - Ethereum IDE | Notepad | Online Notes free, no | ethereum opcodes - Google Se | bytecode to opcode disassembl

google.com/search?q=bytecode+to+opcode+disassembler&oq=bytecode+to+opcode+d&aqs=chrome.1.69i57j0.11435j0j7&sourceid=chrome&ie=UTF-8

Google

bytecode to opcode disassembler

All | Images | Videos | News | Shopping | More | Tools

About 59,700 results (0.49 seconds)

https://etherscan.io › opcode-tool

Bytecode to Opcode Disassembler | Etherscan

Ethercan **ByteCode to Opcodes Disassembler** and Decoder tool enable decoding the low level Contract ByteCodes to Opcodes.

https://hecoinfo.com › opcode-tool

Bytecode to Opcode Disassembler | HecoInfo

Ethercan **ByteCode to Opcodes Disassembler** and Decoder tool enable decoding the low level Contract ByteCodes to Opcodes.

https://docs.python.org › library › dis

dis — Disassembler for Python bytecode — Python 3.9.6 ...

The CPython **bytecode** which this module takes as an input is defined in the file Include/**opcode**.h and used by the compiler and the interpreter. CPython ...

https://github.com › daejunpark › evm-disassembler

EVM ByteCode To Opcode Disassembler - GitHub

EVM **ByteCode To Opcode Disassembler**. Quick Run: $ echo "0x600035601c52" | python3.6 byte2op.py [0] PUSH1 0:0x00 [2] ...

https://ethereum.stackexchange.com › questions › why-...

Why are there missing opcodes when using the disassembler ...

https://etherscan.io/opcode-tool

Remix - Ethereum IDE | Notepad | Online Notes free, no | ethereum opcodes - Google Sea | Bytecode to Opcode Disassembl

etherscan.io/opcode-tool

Etherscan

All Filters | Search by Address / Txn Hash / Block / Token / Ens

Eth: $2,114.75 (-1.04%) | 11 Gwei

Home | Blockchain | Tokens | Resources | More | Sign In

Bytecode to Opcode Disassembler

Attempts to decode the low level Contract ByteCodes to Opcodes

0x

Decode

This website uses cookies to improve your experience and has an updated Privacy Policy. Got it

Etherscan is a Block Explorer and Analytics Platform for

Remix - Ethereum IDE | Notepad | Online Notes free, no | crytic/evm-opcodes: Ethereum o | Bytecode to Opcode Disassembl
github.com/crytic/evm-opcodes

README.md

Table

Opcode	Name	Description	Extra Info	Gas
`0x00`	STOP	Halts execution	-	0
`0x01`	ADD	Addition operation	-	3
`0x02`	MUL	Multiplication operation	-	5
`0x03`	SUB	Subtraction operation	-	3
`0x04`	DIV	Integer division operation	-	5
`0x05`	SDIV	Signed integer division operation (truncated)	-	5
`0x06`	MOD	Modulo remainder operation	-	5
		Signed modulo		

Remix - Ethereum IDE | Notepad | Online Notes free, no | crytic/evm-opcodes: Ethereum o | Bytecode to Opcode Disassembl

rapidtables.com/tools/notepad.html

Home › Tools › Notepad

Write With Confidence

File Edit View Help


```
        "outputs": [
            {
                "internalType": "uint256",
                "name": "",
                "type": "uint256"
            }
        ],
        "stateMutability": "view",
        "type": "function"
    },
    {
        "inputs": [
            {
                "internalType": "uint256",
                "name": "num",
                "type": "uint256"
            }
        ],
        "name": "store",
        "outputs": [],
        "stateMutability": "nonpayable",
        "type": "function"
    }
]
```


Line 28, Column 2 Chars 396, Words 1

Smart Contract Compilation

Some important points to note-:

- Contract bytecode is public in readable form.
- Contract doesn't have to be public.
- Bytecode is immutable.
- ABI act as a bridge between applications and smart contract.
- ABI and Bytecode cannot be generated without source code.

Smart Contract Compilation

- Opcodes

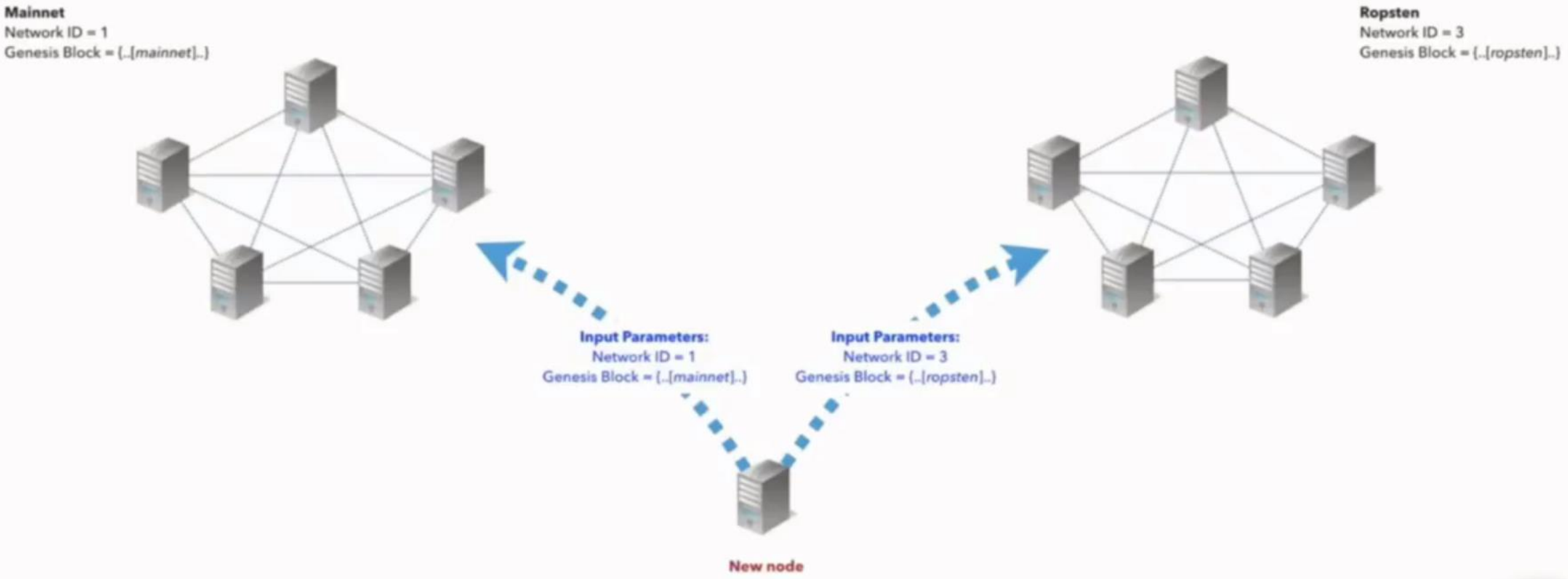
Mainnet vs Testnet

Mainnet	Testnet
Used for actual transactions with value.	Used for testing smart contracts and decentralized applications.
Mainnet's network ID is 1.	Testnets have network IDs of 3, 4, and 42.
Example - Ethereum	Example – Rinkeby Test Network

Crypto Mainnet vs Testnet: Wha | Rinkeby: Network Dashboard | Ethereum Blocks | Etherscan

masterthecrypto... rence/

Rinkeby: Network Dashboard
rinkeby.io



Ropsten is the most popular public testnet for Ethereum and is often used as a testing network for

Crypto Mainnet vs Testnet: Wha | Rinkeby: Network Dashboard | Ethereum Blocks | Etherscan

rinkeby.io/#stats

250% Reset

BEST BLOCK #8,927,765

UNCLES (CURRENT / LAST 50) 0/0

LAST BLOCK 1s ago

AVG BLOCK TIME 15.00s

AVG NE 0.1 H/s

ACTIVE NODES 51/51

GAS PRICE 0 wei

GAS LIMIT 29999943 gas

PAGE LATENCY 119 ms

UPTIME 100%

BLOCK TIME

DIFFICULTY

BLOCK PROPAGATION

LAST BLOCKS MINERS

UNCLE COUNT (28 BLOCKS PER BAR)

TRANSACTIONS

GAS SPENDING

GAS LIMIT

ATTENTION!

This page does not represent the entire state of the ethereum network - listing a node on this page is a voluntary process.

Network Stats

Block Explorer

EF-Rinkeby-Stockholm	Geth/v1.10.5-unstable-2d4eff21-20210625/linux-amd64/go1.16.5	22 ms		102	4	#8,927,765	77bd10df...1d705263	15,238,323	0	0	2 s ago	0 ms		151 ms	100%
Pegasys-HyperledgerBesu	besu/v21.7.0/linux-x86_64/corretto-java-11	100 ms	0 KH/s	17	21	#8,927,765	77bd10df...1d705263	15,238,323	21	0	1 s ago	0 ms		0 ms	100%
Bootnode - AKASHA	Geth/v1.10.5-unstable-10eb654f-20210623/linux-amd64/go1.16.5	15 ms		264	5092	#8,927,765	77bd10df...1d705263	15,238,323	0	0	2 s ago	+61 ms		119 ms	100%
EF-Rinkeby-Paris	Geth/v1.10.5-unstable-2d4eff21-20210625/linux-amd64/go1.16.5	20 ms		97	4	#8,927,765	77bd10df...1d705263	15,238,323	0	0	2 s ago	+65 ms		200 ms	100%
Faucet	Geth/v1.10.5-unstable-00b9226c-20210708/linux-amd64/go1.16.5	12 ms		4	2	#8,927,765	77bd10df...1d705263	15,238,323	0	0	2 s ago	+76 ms		129 ms	100%
Signer - AKASHA	Geth/v1.10.5-unstable-10eb654f-20210623/linux-amd64/go1.16.5	9 ms		116	4	#8,927,765	77bd10df...1d705263	15,238,323	0	0	2 s ago	+85 ms		125 ms	100%
elkoRinkeby	Geth/v1.10.4-stable-aa637fd3/linux-amd64/go1.16.4	16 ms		63	5121	#8,927,765	77bd10df...1d705263	15,238,323	0	0	1 s ago	+95 ms		195 ms	100%
Signer - Infura	Geth/v1.10.5-unstable-9624f92e-20210709/linux-amd64/go1.16.4	53 ms	0 KH/s	317	4	#8,927,765	77bd10df...1d705263	15,238,323	21	0	1 s ago	+114 ms		107 ms	100%
Bootnode - Infura	Geth/v1.10.5-unstable-9624f92e-20210709/linux-amd64/go1.16.4	51 ms		361	8416	#8,927,765	77bd10df...1d705263	15,238,323	21	0	1 s ago	+133 ms		132 ms	100%
Bitski (us-east-1-geth-rinkeby-1)	Geth/v1.10.4-stable-aa637fd3/linux-amd64/go1.16.5	54 ms		84	5098	#8,927,765	77bd10df...1d705263	15,238,323	0	0	1 s ago	+144 ms		166 ms	100%
TechnoTest	Geth/v1.10.4-unstable-7a7abe3d-20210615/linux-amd64/go1.15.8	13 ms		16	5154	#8,927,765	77bd10df...1d705263	15,238,323	0	0	1 s ago	+163 ms		572 ms	100%
Bitski (us-east-1-geth-rinkeby-0)	Geth/v1.10.4-stable-aa637fd3/linux-amd64/go1.16.5	55 ms		60	5099	#8,927,765	77bd10df...1d705263	15,238,323	0	0	1 s ago	+174 ms		320 ms	100%
FunFair Rinkeby 1	Geth/v1.10.4-stable-aa637fd3/linux-amd64/go1.16.5	32 ms		49	5101	#8,927,765	77bd10df...1d705263	15,238,323	0	0	1 s ago	+204 ms		209 ms	100%
FunFair Rinkeby 3	Geth/v1.10.4-stable-aa637fd3/linux-amd64/go1.16.5	15 ms		50	5099	#8,927,765	77bd10df...1d705263	15,238,323	0	0	1 s ago	+232 ms		210 ms	100%
geth-rinkeby-stkhlm	Geth/v1.10.4-stable-aa637fd3/linux-amd64/go1.16.5	19 ms		50	5096	#8,927,765	77bd10df...1d705263	15,238,323	0	0	1 s ago	+243 ms		212 ms	100%
DECoDE	Geth/v1.10.4-stable-aa637fd3/linux-amd64/go1.16.4	15 ms		16	5099	#8,927,765	77bd10df...1d705263	15,238,323	0	0	1 s ago	+262 ms		320 ms	100%
Signer - Cloudflare	Geth/v1.10.4-stable/linux-amd64/go1.16.5	49 ms		16	5	#8,927,765	77bd10df...1d705263	15,238,323	0	0	1 s ago	+283 ms		389 ms	100%
vw-testnet	Geth/v1.10.4-stable-aa637fd3/linux-amd64/go1.16.5	13 ms		32	4836	#8,927,765	77bd10df...1d705263	15,238,323	0	0	1 s ago	+303 ms		2.8 s	100%
FunFair Rinkeby 2	Geth/v1.10.4-stable-aa637fd3/linux-amd64/go1.16.5	16 ms		49	5099	#8,927,765	77bd10df...1d705263	15,238,323	0	0	1 s ago	+323 ms		167 ms	100%
Invictus Capital	Geth/v1.10.4-stable-aa637fd3/linux-amd64/go1.16.5	68 ms		19	8165	#8,927,765	77bd10df...1d705263	15,238,323	0	0	1 s ago	+340 ms		1.8 s	100%

Crypto Mainnet vs Testnet: Wha | Rinkeby: Network Dashboard | Ethereum Blocks | Etherscan

etherscan.io/blocks

Sponsored: Crypto.com - Buy ETH at True Cost - Lowest fees for credit/debit card purchases. Download App.

Block #12816810 to #12816834 (Total of 12,816,835 blocks)

First < Page 1 of 512674 > Last

Block	Age	Txn	Uncles	Miner	Gas Used	Gas Limit	Avg.Gas Price	Reward
12816834	52 secs ago	179	0	xnpool	14,893,716 (99.93%)	14,903,662	71.69 Gwei	3.06779 Ether
12816833	1 min ago	160	0	MiningPoolHub	14,915,859 (99.98%)	14,918,229	29.72 Gwei	2.44337 Ether
12816832	1 min ago	116	0	Spark Pool	14,914,410 (99.88%)	14,932,810	22.46 Gwei	2.335 Ether
12816831	1 min ago	187	0	0x54e23bcc99e5a5818b...	14,910,933 (99.90%)	14,925,542	32.88 Gwei	2.49027 Ether
12816830	1 min ago	191	0	F2Pool Old	14,930,627 (99.94%)	14,940,130	33.31 Gwei	2.4973 Ether
12816829	1 min ago	169	0	2Miners: PPLNS	14,922,755 (99.98%)	14,925,556	25.73 Gwei	2.38403 Ether
12816828	2 mins ago	153	0	Hiveon Pool	14,916,774 (99.84%)	14,940,144	26.27 Gwei	2.3919 Ether
12816827	2 mins ago	196	0	zhizhu.top	14,947,768 (99.95%)	14,954,747	33.79 Gwei	2.50515 Ether
12816826	2 mins ago	157	0	MiningPoolHub	14,933,366 (99.91%)	14,947,468	27.54 Gwei	2.41128 Ether
12816825	2 mins ago	131	0	Spark Pool	14,944,031 (99.88%)	14,962,078	28.57 Gwei	2.42696 Ether

Metamask

- Store Ether
- Send Ether
- Receive Ether
- Run Dapps
- Swap Tokens

MetaMask Download

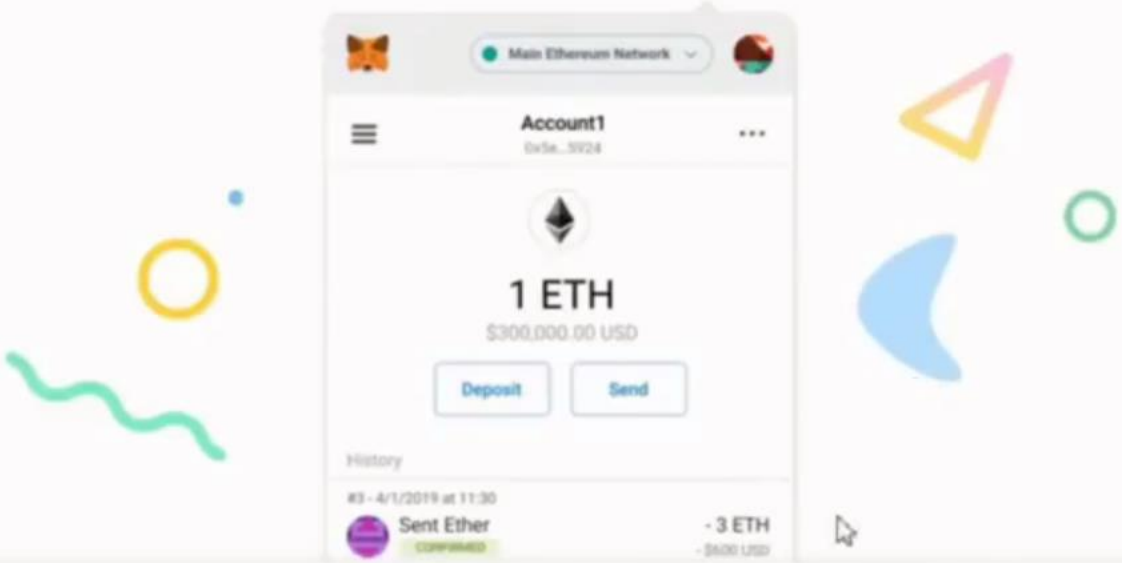
metamask.io/download.html

METAMASK

Features Support About Build Download

Chrome iOS Android

Install MetaMask for your browser



Install MetaMask for Chrome

Rinkeby Faucet

Rinkeby: Authenticated Faucet | (20) Home / Twitter

faucet.rinkeby.io

Rinkeby Authenticated Faucet

Social network URL containing your Ethereum address... | Give me Ether

0xe9ba4684ba8cc615ccdc5fc0193383a50e128c3d | funded

4 peers 8927850 blocks 9.046256971665328e+56 Ethers 577589 funded

How does this work?

This Ether faucet is running on the Rinkeby network. To prevent malicious actors from exhausting all available funds or accumulating enough Ether to mount long running spam attacks, requests are tied to common 3rd party social network accounts. Anyone having a Twitter or Facebook account may request funds within the permitted limits.

To request funds via Twitter, make a tweet with your Ethereum address pasted into the contents (surrounding text doesn't matter).
Copy-paste the tweets URL into the above input box and fire away!

To request funds via Facebook, publish a new **public** post with your Ethereum address embedded into the content (surrounding text doesn't matter).
Copy-paste the posts URL into the above input box and fire away!

You can track the current pending requests below the input field to see how much you have to wait until your turn comes.

The faucet is running invisible reCaptcha protection against bots.

Privacy - Terms

Rinkeby: Authenticated Faucet | (20) kshitij Srivastava on Twitter

twitter.com/kshitij_13hello/status/1414826818868187141

Home
Explore
Notifications
Messages
Bookmarks
Lists
Profile
More
Tweet

kshitij Srivastava
@kshitij_13hello

Tweet

kshitij Srivastava
@kshitij_13hello

0x0C2DE9576F7945cd4B363Bd28b9a47302a211852

Translate Tweet

11:29 AM · Jul 13, 2021 · Twitter Web App

View Tweet activity

Tweet your reply

Reply

Your Tweet was sent. View

Search Twitter

Relevant people

kshitij Srivastava
@kshitij_13hello

What's happening

COVID-19 · LIVE
Here are the latest updates on COVID-19 from news organisations in India

Trending in India
#BoycottPavitraRishta2
12.6K Tweets

Trending in India
#CDSL

POPSUGAR · Last night
Timothée Chalamet's Metallic Cannes Look Stands Out In a Sea Full of Black Suits

World news · Last night
Florida resident detained as key suspect in Haitian president's assassination

Contract Deployment

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.4+commit.c7e474f2.js

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

JavaScript VM (Berlin)

- JavaScript VM (Berlin)
- JavaScript VM (London)
- Injected Web3
- Web3 Provider

Execution environment connects to node at localhost (or via IPC if available), transactions will be sent to the network and can cause loss of money or worse!
If this page is served via https and you access your node via http, it might not work. In this case, try cloning the repository and serving it via http.

GAS LIMIT

3000000

VALUE

0 wei

CONTRACT

NO COMPILED CONTRACTS

OR

At Address | Load contract from Address

Home | 3_Ballot.sol | 2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.9.0;

/**
 * @title Ballot
 * @dev Implements voting process along with vote delegation
 */
contract Ballot {

    struct Voter {
```

umulated by delegation

0 listen on network

Search with transaction hash or address

You can use this terminal to:
- Check transactions details and start debugging.
- Execute JavaScript scripts:
  - Input a script directly in the command line interface
  - Select a Javascript file in the file explorer and then run `remix.execute()` or `remix.exeCurrent()` in the command line interface
  - Right click on a JavaScript file in the file explorer and then click `Run`

The following libraries are accessible:
- web3 version 1.0.0
- ethers.js
- swarmgw
- remix (run remix.help() for more info)

Contract Deployment

JavaScript Virtual Machine

- Transaction will be executed in a sandbox.
- Own memory blockchain.
- Ideal for testing.

Contract Deployment

Injected Web3

- Deploy a contract or run a transaction on Ethereum main or test net.

Contract Deployment

Web3 Provider-

- Connect to a remote node and Ethereum client.

Studies so far...

Remix IDE

Testnet

Contract Deployment

Compilation Process

Metamask

Mainnet

Rinkeby Faucet

About Solidity

- High-level statically typed programming language.
- With Solidity you can create contracts for uses such as voting, crowdfunding, blind auctions, and multi-signature wallets.
- Case sensitive.
- For latest update- Visit Solidity documentation

Note – You should follow established development best-practices when writing your smart contracts.

The DAO Attack

solidity documentation - Google

google.com/search?q=solidity+documentation&sxsrf=ALeKk02InYjIBjebblCylFDI3Bbx-N-8rw%3A1626159172772&ei=RDjtYJXWLpOR9QOwgoGoCg&oq=solidity+do&gs_lcp=Cgdnd3Mtd2I6EAMYADI...

Google

solidity documentation

All | Videos | News | Images | Shopping | More | Tools

About 74,40,000 results (0.48 seconds)

https://docs.soliditylang.org

Solidity — Solidity 0.8.6 documentation

Solidity is a curly-bracket language. It is influenced by C++, Python and JavaScript, and is designed to target the Ethereum Virtual Machine (EVM). You can find ...

Documentation
1. Understand the Smart Contract Basics · 2. Get to Know Solidity ...

V0.8.0
Solidity is an object-oriented, high-level language for ...

More results from soliditylang.org »

People also ask

- Is solidity easy to learn?
- How do you write solidity code?
- In what language is solidity written?
- What is the latest solidity version?

Feedback

http://solidity.readthedocs.io › ...

Solidity Sample

2.1. Solidity Programming Tutorial Hindi _ Solidity - Ethereum _ Code Eater - Blockchain.mp4 - VLC media player

Media Playback Audio Video Subtitle Tools View Help

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.4+commit.c7e474f2.js

DEPLOY & RUN TRANSACTIONS

Transactions recorded 1

Deployed Contracts

IDENTITY AT 0XD91...39138 (MEMORY)

getAge

0: uint256: 17

getName

0: string: Ravi

Low level interactions

CALLDATA

Transact

Home | identity.sol | Lottery.sol | 1_Storage.sol | 4 tabs

```
pragma solidity >= 0.5.0 < 0.9.0;

contract Identity
{
    string name;
    uint age;

    constructor() public
    {
        name="Ravi";
        age=17;
    }

    function getName() view public returns(string memory)
    {
        return name;
    }

    function getAge() view public returns(uint)
    {
        return  age;
    }
}
```

0 listen on network

Search with transaction hash ...

56:10 3:52:16

100%

Search

4:48 am 14/11/2022

State Variables

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.4+commit.c7e474f2.js

DEPLOY & RUN TRANSACTIONS

CONTRACT

State - state.sol

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 22

Deployed Contracts

STATE AT 0X1C9...2B4BD (MEMORY)

age

0: uint256: 0

Low level interactions

CALLDATA

Transact

Home | state.sol | 2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >= 0.5.0 < 0.9.0;

contract State
{
  uint public age;
  age=20;

  function setAge() public
  {
      age=10;
  }
}
```

FunctionDefinition

0 listen on network

Search with transaction hash or address

State Variable

- To change the default values of the state variable -

Using the contracts constructor.

Initializing the variable at declaration.

Using the setter function.

State Variables

- Permanently stored in contract storage.
- Cost gas(expensive) .
- Storage not dynamically allocated.
- Instance of the contract cannot have other state variables besides those already declared.

Local Variables

Some data types are storage by default i.e String, Struct, Array, etc.

1:06:23 3:52:16
100% 1:06:23/3:52:16

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.4+commit.c7e474f2.js

SOLIDITY COMPILER

EVM VERSION

compiler default

COMPILER CONFIGURATION

Auto compile

Enable optimization 200

Hide warnings

Compile state.sol

CONTRACT

local (state.sol)

Publish on Swarm

Publish on Ipfs

Compilation Details

ABI Bytecode

Home state.sol 2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >= 0.5.0 < 0.9.0;

contract local
{

function store() pure public returns(uint)
{
    string memory name="ravi";
    uint age=11;
    return age;
}
}
```

0 listen on network Search with transaction hash or address

Local Variables

- Declared inside functions and are kept on the stack , not on storage.
- Don’t cost gas.
- There are some types that reference the storage by default.
- Memory keyword can’t be used at contract level.

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.4+commit.c7e474f2.js

SOLIDITY COMPILER

Solidity

EVM VERSION

compiler default

COMPILER CONFIGURATION

Auto compile

Enable optimization 200

Hide warnings

Compile state.sol

CONTRACT

local (state.sol)

Publish on Swarm

Publish on Ipfs

Compilation Details

ABI Bytecode

Home state.sol 2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >= 0.5.0 < 0.9.0;

contract local
{
    string name="ravi"; //state
function store() pure public returns(uint)
{

    uint age=11; //local variable
    return age;
}
}
```

0 listen on network Search with transaction hash or address

Functions-
Setters and Getters

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

getter

0: uint256: 10

Low level interactions

CALLDATA

Transact

LOCAL AT 0XD2A...FD005 (MEMORY)

setter

getter

0: uint256: 12

Low level interactions

CALLDATA

Transact

Home state.sol 2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >= 0.5.0 < 0.9.0;

contract local
{
  uint age=10;

  function getter() public view returns(uint)
  {
      return age;
  }

  function setter(uint newage) public
  {
      age=newage;
  }
}
```

The setter Costs Ethers while the getter not

ContractDefinition local 0 reference(s)

0 listen on network Search with transaction hash or address

Functions

- When you call a setter function it creates a transaction that needs to be mined and costs gas because it changes the blockchain. Vice versa for getter function.
- When you declare a public state variable a getter function is automatically created.
- By default variable visibility is private.

View Vs Pure

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

0: uint256: 10

getter

0: uint256: 10

Low level interactions

CALLDATA

Transact

LOCAL AT 0XD8B...33FA8 (MEMORY)

age

getter

0: uint256: 100

Low level interactions

CALLDATA

Transact

Home state.sol

2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >= 0.5.0 < 0.9.0;

contract local
{
  uint public age=10;

  function getter() public pure returns(uint)
  {
      uint roll=100;
      return roll;

  }

}
```

0 listen on network Search with transaction hash or address

Constructor

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 2

Deployed Contracts

LOCAL AT 0XD91...3913B (MEMORY)

count

0: uint256: 0

Low level interactions

CALLDATA

Transact

LOCAL AT 0XD8B...33FA8 (MEMORY)

Home | state.sol | 2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >= 0.5.0 < 0.9.0;

contract local
{
 uint public count;

 constructor()
 {
     count=8;
 }
}
```

0 listen on network

Search with transaction hash or address

2.1. Solidity Programming Tutorial Hindi _ Solidity - Ethereum _ Code Eater - Blockchain.mp4 - VLC media player

Media Playback Audio Video Subtitle Tools View Help

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

Deployed Contracts

LOCAL AT 0XD91...39138 (MEMORY)

count

0: uint256: 0

Low level interactions

CALLDATA

Transact

LOCAL AT 0XD8B...33FAB (MEMORY)

count

0: uint256: 8

Low level interactions

CALLDATA

Transact

Home state.sol 2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >= 0.5.0 < 0.9.0;

contract local
{
 uint public count;

 constructor(uint new_count)
 {
     count=new_count;
 }
}
```

uint256 count 1 reference(s)

0 listen on network Search with transaction hash or address

1:30:54 3:52:16

100%

Search

12:43 pm
18/11/2022

Constructor

- Executed only once.
- You can create only one constructor and that is optional.
- A default constructor is created by the compiler if there is no explicitly defined constructor.

Integers

int

uint

Signed and unsigned integers can be of various sizes.

int8 to int256

uint8 to uint256

int alias to int256

uint alias to uint256

By default an int is initialized to 0.

Overflow get detected at compile time.

Integers

Range	
int8 : - 128 to +127	**uint8 :** 0 to 255
int16 : - 32768 to +32767	**uint16 :** 0 to 65535
-2^(n-1) to 2^(n-1)-1	0 to 2^(n)-1

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

SOLIDITY COMPILER

EVM VERSION

compiler default

COMPILER CONFIGURATION

Auto compile

Enable optimization 200

Hide warnings

Compile state.sol

No Contract Compiled Yet

```
TypeError: Type int_const 256 is
not implicitly convertible to
expected type uint8. Literal is
too large to fit in uint8. -->
state.sol:7:14: | 7 | uint8
count=256; | ^^^
```

state.sol

1 tabs

```
1 // SPDX-License-Identifier: GPL-3.0
2
3 pragma solidity >= 0.5.0 < 0.9.0;
4
5 contract local
6 {
7  uint8 count=256;
8 }
```

0 listen on network Search with transaction hash or address

Integers

Operators:

- Comparisons: <=, <, ==, !=, >=, > (evaluate to bool)
- Bit operators: &, |, ^ (bitwise exclusive or), ~ (bitwise negation)
- Arithmetic operators: +, -, unary -, unary +, *, /, % (remainder), ** (exponentiation), << (left shift), >> (right shift)

2.1. Solidity Programming Tutorial Hindi _ Solidity - Ethereum _ Code Eater - Blockchain.mp4 - VLC media player
Media Playback Audio Video Subtitle Tools View Help

PeckShield 1.4K Followers About Follow Sign in Get started

New batchOverflow Bug in Multiple ERC20 Smart Contracts (CVE-2018–10299)

PeckShield Apr 23, 2018 · 4 min read

Built on our earlier efforts in analyzing EOS tokens, we have developed an automated system to scan and analyze Ethereum-based (ERC-20) token transfers. Specifically, our system will automatically send out alerts if any suspicious transactions (e.g., involving unreasonably large tokens) occur.

In particular, on 4/22/2018, 03:28:52 a.m. UTC, our system raised an alarm which is related to an unusual **BEC** token transaction (shown in Figure 1). In this particular transaction, someone transferred an extremely large amount of BEC token — *0x8000,0000,0000,0000,0000,0000,0000,0000,0000,0000,0000,0000,00*

1:41:42 3:52:16
75%
Search
1:40 pm 18/11/2022

Remix - Ethereum IDE | New batchOverflow Bug in Mult | Integer Overflow (i.e., proxyOver

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.5.0+commit.1d4f565a.js

DEPLOY & RUN TRANSACTIONS

setter

Low level interactions

CALLDATA

Transact

LOCAL AT 0XD8B...33FAB (MEMORY)

setter

money

0: uint8: 0

Low level interactions

CALLDATA

Transact

state.sol

```solidity
// SPDX-License-Identifier: GPL-3.0

pragma solidity 0.5.0;

contract local
{
 uint8 public money=255;

 function setter() public
 {
     money=money+1;
 }
}
```

Solidity Version in 2018

This problem is resolved in Solidity version 0.8.0, where the transaction will be failed

0 listen on network Search with transaction hash or address

2.1. Solidity Programming Tutorial Hindi _ Solidity - Ethereum _ Code Eater - Blockchain.mp4 - VLC media player

Media Playback Audio Video Subtitle Tools View Help

Remix - Ethereum IDE | New batchOverflow Bug in Multi | Integer Overflow (i.e., proxyOver

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.0+commit.c7dfd78e.js

DEPLOY & RUN TRANSACTIONS

money

0: uint8: 0

Low level interactions

CALLDATA

Transact

LOCAL AT 0XD7A...F771B (MEMORY)

setter

money

0: uint8: 255

Low level interactions

CALLDATA

Transact

state.sol

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity 0.8.0;

contract local
{
 uint8 public money=255;

 function setter() public
 {
      money=money+1;
```

0 listen on network

Search with transaction hash or address

```
transact to local.setter pending ...

[vm] from: 0x5B3...eddC4 to: local.setter() 0xD7A...F771B value: 0 wei data: 0x3f3...108f7 logs: 0
hash: 0x69a...bdfcc

transact to local.setter errored: VM error: revert.

revert
        The transaction has been reverted to the initial state.
Note: The called function should be payable if you send value and the value you send should be less than your current balance.
Debug the transaction to get more information.
```

Debug

1:46:32 3:52:16

75%

Search

1:44 pm
18/11/2022

Remix - Ethereum IDE | New batchOverflow Bug in Mult | Integer Overflow (i.e., proxyOver

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.5.0+commit.1d4f565a.js

DEPLOY & RUN TRANSACTIONS

Transact

LOCAL AT 0XDA0...42B53 (MEMORY)

setter

money

0: uint8: 0

Low level interactions

CALLDATA

Transact

state.sol

1 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity 0.5.0;
```

0 listen on network

Search with transaction hash ...

```
creation of local pending...

[vm] from: 0x5B3...eddC4
to: local.(constructor) value: 0 wei
data: 0x608...90029 logs: 0 hash: 0x22a...68b19

call to local.money

[call]
```

Debug

Arrays

Fixed Size Array

Dynamic Size Array

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.0+commit.c7dfd78e.js

DEPLOY & RUN TRANSACTIONS

Array - state.sol

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 1

Deployed Contracts

ARRAY AT 0XD91...39138 (MEMORY)

arr | 3

0: uint256: 40

Low level interactions

CALLDATA

Transact

Home | state.sol | 2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract Array
{
 uint [4] public arr= [10,20,30,40,50];
}
```

ContractDefinition Array | 0 reference(s)

0 | listen on network | Search with transaction hash or address

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.0+commit.c7dfd78e.js

DEPLOY & RUN TRANSACTIONS

CALLDATA

Transact

ARRAY AT 0xD8B...33FA8 (MEMORY)

setter 3,999

arr 3

0: uint256: 999

Low level interactions

CALLDATA

Transact

ARRAY AT 0x7EF...BCB47 (MEMORY)

setter uint256 index, uint256 value

arr uint256

length

0: uint256: 4

Low level interactions

CALLDATA

Transact

Home state.sol

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract Array
{
 uint [4] public arr= [10,20,30,40];

 function setter(uint index,uint value) public
 {
     arr[index]=value;
 }
 function length() public view returns(uint)
 {
     return arr.length;
 }
}
```

listen on network

Search with transaction hash or address

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

ARRAY AT 0XD7A...F771B (MEMORY)

popElement

pushElement 30

arr 1

0: uint256: 20

len

0: uint256: 2

Low level interactions

CALLDATA

Transact

state.sol

1 tabs

Dynamic Array

```
contract Array
{
uint[] public arr;

function pushElement(uint item) public
{
    arr.push(item);
}
function len() public view returns(uint)
{
    return arr.length;
}
function popElement() public
{
    arr.pop();
}
}
```

FunctionDefinition

0 listen on network

Search with transaction hash or address

Byte Array

- 1 byte = 8 bits
- 1 hexadecimal digit = 4 bits
- Everything that will be stored in the byte array will be in the form of hexadecimal digits.

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.0+commit.c7dfd78e.js

DEPLOY & RUN TRANSACTIONS

At Address | Load contract from Address

Transactions recorded 1

Deployed Contracts

ARRAY AT 0XD91...39138 (MEMORY)

b2

0: bytes2: 0x0000

b3

0: bytes3: 0x000000

Low level interactions

CALLDATA

Transact

state.sol

1 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract Array
{
 bytes3 public b3; //3 bytes array
 bytes2 public b2;  //2 bytes array
}
```

0 listen on network

Search with transaction hash or address

Remix - Ethereum IDE | ASCII Table - ASCII codes,hex,de

rapidtables.com/code/text/ascii-table.html

7	07	BEL	33	21	!	59	3B	;	85	55	U	111	6F	o
8	08	BS	34	22	"	60	3C	<	86	56	V	112	70	p
9	09	HT	35	23	#	61	3D	=	87	57	W	113	71	q
10	0A	LF	36	24	$	62	3E	>	88	58	X	114	72	r
11	0B	VT	37	25	%	63	3F	?	89	59	Y	115	73	s
12	0C	FF	38	26	&	64	40	@	90	5A	Z	116	74	t
13	0D	CR	39	27	'	65	41	A	91	5B	[	117	75	u
14	0E	SO	40	28	(	66	42	B	92	5C	\	118	76	v
15	0F	SI	41	29	)	67	43	C	93	5D	]	119	77	w
16	10	DLE	42	2A	*	68	44	D	94	5E	^	120	78	x
17	11	DC1	43	2B	+	69	45	E	95	5F	_	121	79	y
18	12	DC2	44	2C	,	70	46	F	96	60	`	122	7A	z
19	13	DC3	45	2D	-	71	47	G	97	61	a	123	7B	{
20	14	DC4	46	2E	.	72	48	H	98	62	b	124	7C	|
21	15	NAK	47	2F	/	73	49	I	99	63	c	125	7D	}
22	16	SYN	48	30	0	74	4A	J	100	64	d	126	7E	~
23	17	ETB	49	31	1	75	4B	K	101	65	e	127	7F	DEL
24	18	CAN	50	32	2	76	4C	L	102	66	f			
25	19	EM	51	33	3	77	4D	M	103	67	g			

ASCII,Hex,Dec,Bin,Base64 converter ►

Extended ASCII table

Character encoding

UTF-8 (Unicode)

128	80	□	154	9A	□	180	B4	´	206	CE	Î	232	E8	è

Remix - Ethereum IDE | ASCII Table - ASCII codes,hex,de

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.0+commit.c7dfd78e.js

DEPLOY & RUN TRANSACTIONS

0: bytes3: 0x000000

Low level interactions

CALLDATA

Transact

ARRAY AT 0XD8B...33FA8 (MEMORY)

setter

b2

b3

0: bytes3: 0x616263

Low level interactions

CALLDATA

Transact

state.sol

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract Array
{
 bytes3 public b3; //3 bytes array
 bytes2 public b2;  //2 bytes array

 function setter() public
 {
      b3='abc';
      b2='ab';
 }
}
```

ContractDefinition Array 0 reference(s)

0 listen on network Search with transaction hash or address

Byte Array

bytes3 public b1= ‘abc’

61	62	63
0	1	2

Remix - Ethereum IDE | ASCII Table - ASCII codes,hex,de

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.0+commit.c7dfd78e.js

DEPLOY & RUN TRANSACTIONS

ARRAY AT 0XD8B...33FAB (MEMORY)

setter

b2

0: bytes2: 0x6162

b3

0: bytes3: 0x616263

Low level interactions

CALLDATA

Transact

ARRAY AT 0XD7A...F771B (MEMORY)

setter

b2

0: bytes2: 0x6100

b3

Low level interactions

CALLDATA

Transact

state.sol

```
1  // SPDX-License-Identifier: GPL-3.0
2
3  pragma solidity >=0.5.0 < 0.9.0;
4
5  contract Array
6  {
7   bytes3 public b3; //3 bytes array
8   bytes2 public b2;  //2 bytes array
9
10  function setter() public
11  {
12      b3='abc';
13      b3[0]='d';
14
15
```

```
TypeError: Single bytes in fixed bytes arrays cannot be modified.
  --> state.sol:13:6:
   |
13 |      b3[0]='d';
   |      ^^^^^
```

listen on network

Search with transaction hash or address

Byte Array

- Byte arrays cannot be modified.
- Padding of 0 is added at the end if the value(by which the array is initialized) does not occupy the entire space.

Byte Array

Fixed-Size array

- bytes1,bytes2,bytes3 ..... bytes32.

Dynamic Size array

- bytes which is shorthand for bytes[]

DEPLOY & RUN TRANSACTIONS

getElement 1

0: bytes1: 0x62

Low level interactions

CALLDATA

Transact

ARRAY AT 0X7EF...BCB47 (MEMORY)

pushElement

b1

getElement

getlength

Low level interactions

CALLDATA

Transact

Home state.sol

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract Array
{
 bytes public b1="abc";

function pushElement() public
{
    b1.push('d');
}

function getElement(uint i) public view returns(bytes1)
{
    return b1[i];
}

function getlength() public view returns(uint)
{
    return b1.length;
}
```

ContractDefinition Array 0 reference(s)

listen on network

Search with transaction hash or address

Loops

while

for

do-while

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

At Address | Load contract from Address

Transactions recorded 3

Deployed Contracts

ARRAY AT 0XDA0...42B53 (MEMORY)

arr 1

0: uint256: 0

Low level interactions

CALLDATA

Transact

ARRAY AT 0X358...D5EE3 (MEMORY)

loop

arr 2

0: uint256: 2

count

0: uint256: 0

Low level interactions

CALLDATA

Transact

Home | state.sol

90% Reset

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract Array
{
uint[3] public arr;
uint public count;

function loop() public{
while(count<arr.length)
{
    arr[count]=count;
    count++;
}
}
}
```

ContractDefinition Array 0 reference(s)

0 listen on network Search with transaction hash or address

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

ARRAY AT 0X358...D5EE3 (MEMORY)

loop

arr 2

0 uint256: 2

count

0 uint256: 0

Low level interactions

CALLDATA

Transact

ARRAY AT 0XD2A...FD005 (MEMORY)

loop

arr uint256

count

Low level interactions

CALLDATA

Transact

Home state.sol

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract Array
{
uint[3] public arr;
uint public count;

function loop() public{
for(uint i=count;i<arr.length;i++)
{
    arr[count]=count;
    count++;
}
}
}
```

uint256 count 4 reference(s)

0 listen on network Search with transaction hash or address

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

arr 1

0: uint256: 1

count

0: uint256: 3

Low level interactions

CALLDATA

Transact

ARRAY AT 0X0FC...9A836 (MEMORY)

loop

arr uint256

count

Low level interactions

CALLDATA

Transact

Home state.sol

2 tabs

```
pragma solidity >=0.5.0 < 0.9.0;

contract Array
{
uint[3] public arr;
uint public count;

function loop() public{

do{
    arr[count]=count;
    count++;
}while(count<arr.length);

}
}
```

uint256 count 4 reference(s)

0 listen on network Search with transaction hash or address

If-else

DEPLOY & RUN TRANSACTIONS

GAS LIMIT
3000000

VALUE
0 wei

CONTRACT
Array - state.sol

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 1

Deployed Contracts

ARRAY AT 0X9D8...A5692 (MEMORY)

check -5

0: string: less than zero

Low level interactions

CALLDATA

Transact

Home state.sol

```
function check(int a) public pure returns(string memory)
{
    string memory value;

    if(a>0)
    {
        value="greater than zero";
    }
    else if(a==0)
    {
        value="equal to zero";
    }
    else
    {
        value="less than zero";
    }
    return value;
```

listen on network

Search with transaction hash or address

Booleans

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

VALUE

0 wei

CONTRACT

Array - state.sol

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 1

Deployed Contracts

ARRAY AT 0X5FD...9D88D (MEMORY)

value

0: bool: false

Low level interactions

CALLDATA

Transact

Home | state.sol

2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract Array
{
bool public value=true;

}
```

0 listen on network

Search with transaction hash or address

Booleans

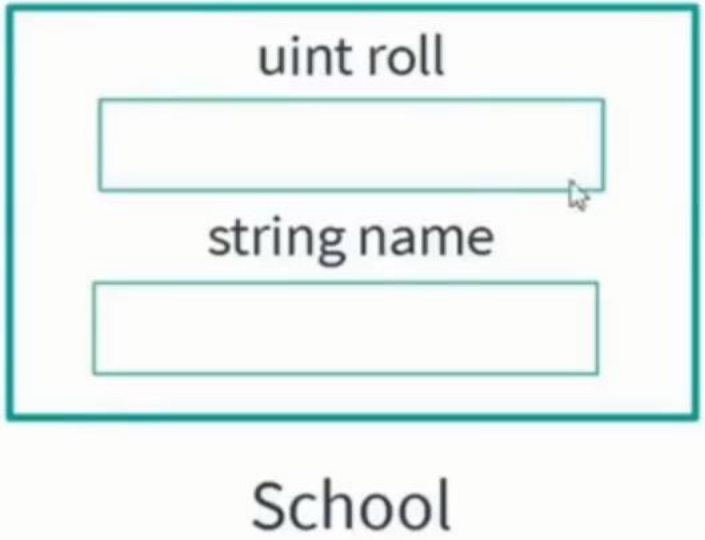
- bool: The possible values are constants true and false.

<u>Operators:</u>

- ! (logical negation)
- && (logical conjunction, “and”)
- || (logical disjunction, “or”)
- == (equality)
- != (inequality)

Struct

```
struct school
{
 uint roll;
string name;
}
```



Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

0 wei

CONTRACT

Demo - state.sol

Deploy 1, Ravi

Publish to IPFS

OR

At Address Load contract from Address

Transactions recorded 2

Deployed Contracts

DEMO AT 0XD91...39138 (MEMORY)

s1

0: uint256: roll 1

1: string: name Ravi

Low level interactions

CALLDATA

Transact

DEMO AT 0XDBB...33FAB (MEMORY)

Home state.sol Lottery.sol

```
pragma solidity >=0.5.0 < 0.9.0;


 struct Student{
     uint roll;
     string name;
 }

contract Demo
{
    Student public s1;

    constructor(uint _roll,string memory _name)
    {
        s1.roll =_roll;
        s1.name=_name;
    }

    function change(uint _roll, string memory _name) public
    {
        Student memory new_student=Student({

        roll:_roll,
        name:_name
        });

        s1=new_student;
    }
}
```

ContractDefinition Academy 0 reference(s)

0 listen on network Search with transaction hash or address

Type here to search

ENG 21:26 26-07-2021

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

Transactions recorded 5

Deployed Contracts

STATE AT 0XB27...07C2C (MEMORY)

u1

0: uint8: 0

Low level interactions

CALLDATA

Transact

STATE AT 0XCD6...99DF9 (MEMORY)

STATE AT 0XAE0...96B8B (MEMORY)

u1

0: uint8: 2

Low level interactions

CALLDATA

Transact

state.sol

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract State
{
 enum user{allowed,not_allowed,wait}

 user public u1= user.allowed;
 uint public lottery=1000;
 function owner() public {
     if(u1==user.allowed)
     {
         lottery=0;
     }
 }

 function changeOwner() public{
     u1=user.not_allowed;
 }
}
```

ContractDefinition State 0 reference(s)

0 listen on network

Search with transaction hash or address

Mapping

- Concept of keys and values.
- mapping(key=>value)

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 4

Deployed Contracts

DEMO AT 0XD91...39138 (MEMORY)

setter | 2,"reena"

roll_no | 2

0: string: reena

Low level interactions

CALLDATA

Transact

Home | state.sol

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;
contract demo
{
  mapping(uint=>string) public roll_no;

  function setter(uint keys,string memory value) public
  {
      roll_no[keys]=value;
  }
}
```

0 listen on network

Search with transaction hash or address

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

FILE EXPLORERS

Workspaces

default_workspace

- contracts
- scripts
- tests
- College
- artifacts
- README.txt
- Lottery.sol
- state.sol

Home | state.sol | 2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;
contract demo
{
  struct Student{
      string name;
      uint class;
  }
  mapping(uint=>Student) public data;

  function setter(uint _roll,string memory _name ,uint _class) public
  {
      data[_roll]= Student(_name,_class);
  }
}
```

0 listen on network Search with transaction hash or address

Mapping

- The key cannot be types mapping ,dynamic array ,enum and struct.
- The values can be of any type.
- Mappings are always stored in storage irrespective of whether they are declared in contract storage or not.

Storage Vs Memory

Storage	Memory
Holds state variables.	Holds local variables defined inside functions if they are reference types.
Persistent	Not persistent
Cost gas	No gas
Like a computer HDD	Like a computer RAM

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

Transactions recorded 2

Deployed Contracts

DEMO AT 0XDDA...5482D (MEMORY)

sto

mem

student 0

0: string: Akash

Low level interactions

CALLDATA

Transact

Home state.sol 2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract demo
{
 string[] public student=['Ravi','Rita','Aman'];

 function mem() public view
 {
     string[] memory s1=student;
     s1[0]='Akash';
 }
  function sto() public
 {
     string[] storage s1=student;
     s1[0]='Akash';
 }

}
```

0 listen on network Search with transaction hash or address

Storage Vs Memory

```
string[] public student =['Ravi', 'Rita', 'Aman'];
```

Ravi	Rita	Aman
0	1	2

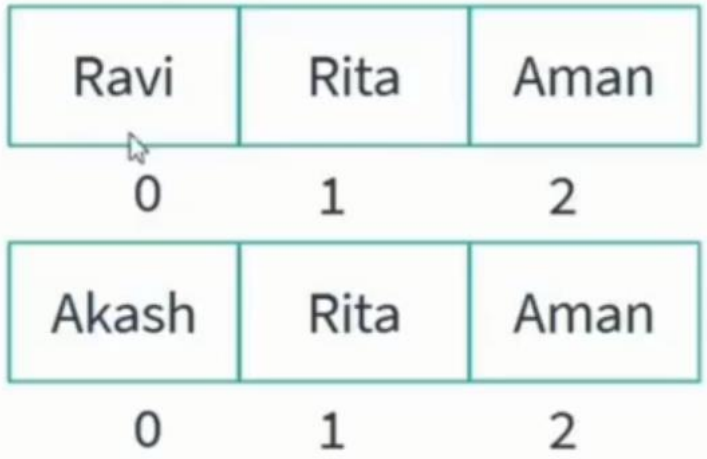
```
string[] memory s1=student;
```

Akash	Rita	Aman
0	1	2

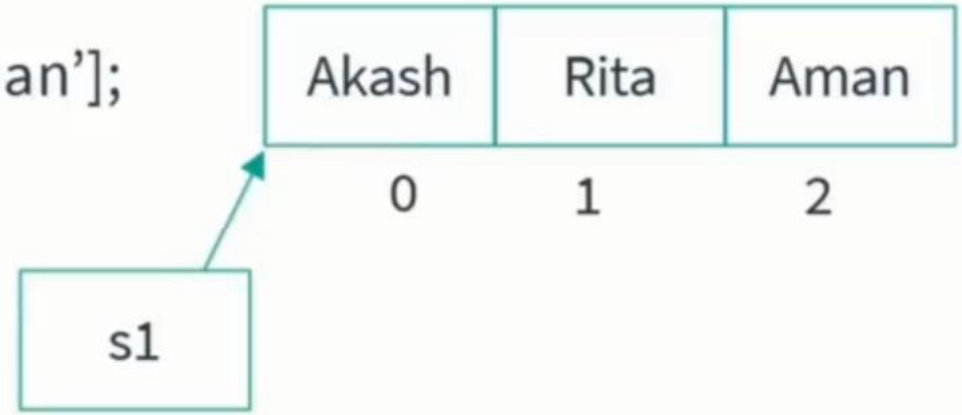
```
s1[0]='Akash';
```

Storage Vs Memory

```
string[] public student =['Ravi', 'Rita', 'Aman'];
string[] memory s1=student;
s1[0]='Akash';
```




```
string[] public student =['Ravi', 'Rita', 'Aman'];
string[] storage s1=student;
s1[0]='Akash';
```



Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

VALUE

0 wei

CONTRACT

demo - state.sol

Deploy

Publish to IPFS

OR

At Address Load contract from Address

Transactions recorded 1

Deployed Contracts

DEMO AT 0XD91...39138 (MEMORY)

getter

0: uint256: block_no 1

1: uint256: timestamp 1627580751

2: address: msgSender 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

Low level interactions

CALLDATA

Transact

Home state.sol

2 tabs

Global Variables in Solidity

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract demo
{
    function getter() public view returns(uint block_no,uint timestamp,address msgSender)
    {
        return(block.number,block.timestamp,msg.sender);
    }
}
```

0 listen on network

Search with transaction hash or address

Contract Balance

Transfer and get Ethers

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

JavaScript VM (Berlin)

ACCOUNT

0xAb8...35cb2 (100 ether)

GAS LIMIT

3000000

VALUE

0 ether

CONTRACT

pay - state.sol

Deploy

Publish to IPFS

OR

At Address Load contract from Address

Transactions recorded 0

Deployed Contracts

Home state.sol 2 tabs

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract pay
{
 function payEther() public payable
 {
 }
}
```

Simply this method is enough for transferring ethers

Execution cost: 120 gas *FunctionDefinition* payEther 0 reference(s)

0 listen on network Search with transaction hash or address

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

JavaScript VM (Berlin)

ACCOUNT

0xCA3...a733c (101 ether)

- 0x5B3...eddC4 (88.999999999998818717 ether)
- 0xAb8...35cb2 (97.999999999999860843 ether)
- 0xCA3...a733c (101 ether)
- 0x4B2...C02db (96.999999999999791227 ether)
- 0x787...cabaB (100 ether)
- 0x617...5E7f2 (100 ether)
- 0x17F...8c372 (100 ether)
- 0x147...C160C (100 ether)
- 0x5c6...21678 (100 ether)
- 0x03C...D1Ff7 (100 ether)
- 0x1aE...E454C (100 ether)
- 0x0A0...C70DC (100 ether)
- 0x4B0...4D2dB (100 ether)
- 0x583...40225 (100 ether)
- 0xdD8...92148 (100 ether)

At Address | Load contract from Address

Transactions recorded 3

Deployed Contracts

PAY AT 0X9EC...DDEB4 (MEMORY)

payEther

sendEtherAcc...

Home | state.sol

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 < 0.9.0;

contract pay
{
 address payable user=payable(0xCA35b7d915458EF540aDe6068dFe2F44E8fa733c);
 function payEther() public payable
 {

 }
 function getBalance() public view returns(uint)
 {
     return address(this).balance;
 }
 function sendEtherAccount() public
 {
     user.transfer(1 ether);
 }
}
```

FunctionDefinition

0 listen on network

Search with transaction hash or address

Visibility

Public	Private	Internal	External
Outside	x	x	Outside
Within	Within	Within	x
Derived	x	Derived	x
Other	x	x	Other

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

FILE EXPLORERS

Workspaces

default_workspace

- contracts
- scripts
- tests
- College
- artifacts
- README.txt
- Lottery.sol
- state.sol

Home | state.sol

```
pragma solidity >=0.5.0 < 0.9.0;

contract A {

function f1() public pure returns(uint)
{
    return 1;
}
function f2() private pure returns(uint)
{
    return 2;
}

function f3() internal pure returns(uint)
{
    return 3;
}
function f4() external pure returns(uint)
{
    return 4;
}

}
```

ContractDefinition B | 0 reference(s)

0 | listen on network | Search with transaction hash or address

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 1

Deployed Contracts

A AT 0XD91...39138 (MEMORY)

f1

f4

Low level interactions

CALLDATA

Transact

Home | state.sol | 2 tabs

```
5  contract A {
6
7  function f1() public pure returns(uint)
8  {
9      return 1;
10 }
11 function f2() private pure returns(uint)
12 {
13     return 2;
14 }
15
16 function f3() internal pure returns(uint)
17 {
18     uint x=f4();
19     return 3;
20 }
21 function f4() external pure returns(uint)
22 {
23     return 4;
```

0 listen on network

Search with transaction hash or address

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT: JavaScript VM (Berlin)

ACCOUNT: 0x5B3...eddC4 (99.999999

GAS LIMIT: 3000000

VALUE: 0 wei

CONTRACT: A - state.sol

Deploy

Publish to IPFS

OR

At Address

Transactions recorded

Deployed Contracts

A AT 0xD91...39138 (MEMORY)

f1

f4

Low level interactions

CALLDATA

Transact

Home | state.sol

```
contract A {

function f1() public pure returns(uint)
{
    return 1;
}
function f2() private pure returns(uint)
{
    return 2;
}

function f3() internal pure returns(uint)
{

    return 3;
}
function f4() external pure returns(uint)
{
    return 4;
}

}
contract B is A
{
    uint public bx=f3();
}
```

compilerMetadata is modifying artifacts/B.json

Execution cost: 315 gas | FunctionDefinition f1 | 1 reference(s)

listen on network

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

f1

f4

Low level interactions

CALLDATA

Transact

B AT 0XD8B...33FA8 (MEMORY)

bx

0: uint256: 3

f1

f4

Low level interactions

CALLDATA

Transact

Home state.sol

```
12 {
13     return 2;
14 }
15
16 function f3() internal pure returns(uint)
17 {
18
19     return 3;
20 }
21 function f4() external pure returns(uint)
22 {
23     return 4;
24 }
25
26 }
27 contract B is A
28 {
29     uint public bx=f4();
30 }
31
```

Execution cost: infinite gas FunctionDefinition f3 1 reference(s)

0 listen on network Search with transaction hash or address

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

CONTRACT

A - state.sol

Deploy

Publish to IPFS

OR

At Address

Transactions recorded 4

Deployed Contracts

A AT 0XD91...39138 (MEMORY)

f1

f4

Low level interactions

CALLDATA

Transact

B AT 0XD9B...E3FA8 (MEMORY)

bx

0: uint256: 3

f1

f4

Low level interactions

CALLDATA

Transact

Home state.sol

```
6
7  function f1() public pure returns(uint)
8  {
9      return 1;
10 }
11 function f2() private pure returns(uint)
12 {
13     return 2;
14 }
15
16 function f3() internal pure returns(uint)
17 {
18
19     return 3;
20 }
21 function f4() external pure returns(uint)
22 {
23     return 4;
24 }
25
26 }
27 contract C
28 {
29     A obj= new A();
30     uint public cx=obj.f4();
31 }
```

compilerMetadata is modifying/artifacts/C.json

ContractDefinition B

0 reference(s)

Algorithm

Participants >=3

2 ether

Contract Balance

Contract Address

Points to note

- Participant must have a wallet.
- A participant can transfer ether more than one time but the transferred ether must be 2 ether.
- As the participant will transfer ether its address will be registered.
- Manager will have full control over the lottery.
- The contract will be reset once a round is completed.

The receive() function does not take parameters, has no return value, and must be external . This function will be called every time we send ethers to the contract. If no receive function is provided, a fallback function should be defined to handle everything.

1. A Receive method can be used once in a contract
2. This method should be external
3. This method will be payable

Remix - Ethereum IDE | Ethereum Unit Converter | Ether

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

OR

At Address | Load contract from Address

Transactions recorded 3

Deployed Contracts

LOTTERY AT 0XD91...39138 (MEMORY)

getBalance

manager

0: address: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

participants 0

0: address: 0xAb8483F64d9C6d1EcF9b849Ae677dD315835cb2

Low level interactions

CALLDATA

Transact

Lottery.sol

1 tabs

```
1  //SPDX-License-Identifier: GPL-3.0
2
3  pragma solidity >=0.5.0 <0.9.0;
4
5  contract Lottery{
6      address public manager;
7      address payable[] public participants;
8
9      constructor()
10     {
11         manager=msg.sender; //gloabal variable
12     }
13
14     receive() external payable
15     {   require(msg.value==1 ether);
16         participants.push(payable(msg.sender));
17     }
18
19     function getBalance() public view returns(uint)
20     {   require(msg.sender== manager);
21         return address(this).balance;
22     }
23 }
```

0 listen on network

Search with transaction hash or address

Remix - Ethereum IDE | Ethereum Unit Converter | Ether | New Tab

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

Transactions recorded 4

Deployed Contracts

LOTTERY AT 0XD91...39138 (MEMORY)

getBalance

0: uint256: 3000000000000000000

manager

participants uint256

random

0: uint256: 77792950366883996884816755811925646291823423472385471780240928595334746043637

Low level interactions

CALLDATA

Transact

Lottery.sol

```
    {   require(msg.value==1 ether);
        participants.push(payable(msg.sender));
    }

    function getBalance() public view returns(uint)
    {   require(msg.sender== manager);
        return address(this).balance;
    }

    function random() public view returns(uint){
        return uint(keccak256(abi.encodePacked(block.difficulty,block.timestamp,part
    }

    function selectWinner() public view returns(address)
    {
        require(msg.sender==manager);
        require(participants.length>=3);
        uint r=random();
        address payable winner;
        uint index = r % participants.length;
        winner=participants[index];
        return winner;
    }
}
```

compilerMetadata is modifying/artifacts/Lottery.json .json

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

Injected Web3

Rinkeby (4) network

ACCOUNT

0x0C2...11852 (4.7484984

GAS LIMIT

3000000

VALUE

0 wei

CONTRACT

Lottery - Lottery.sol

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 0

Lottery.sol

```
//SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 <0.9.0;

contract Lottery{
    address public manager;
    address payable[] public participants;

    constructor()
    {
        manager=msg.sender; //gloabal variable
    }

    receive() external payable
    {   require(msg.value==1 ether);
        participants.push(payable(msg.sender));
    }

    function getBalance() public view returns(uint)
    {   require(msg.sender== manager);
        return address(this).balance;
    }

    function random() public view returns(uint){
        return uint(keccak256(abi.encodePacked(block.difficult
    }

    function selectWinner() public {
        require(msg.sender==manager);
        require(participants.length>=3);
        uint r=random();
        address payable winner;
        uint index = r % participants.length;
        winner=participants[index];
        winner.transfer(getBalance());
        participants=new address payable[](0);
```

Execution cost: undefined gas FunctionDefinition 0 reference(s)

0 listen on network Search with transaction hash or address

1 tabs

Rinkeby Test Network

Connected

Account 1

0x0C2D...1852

4.7485 ETH

Buy Send Swap

Assets Activity

4.7485 ETH

Add Token

Need help? Contact MetaMask Support

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

Injected Web3

Rinkeby (4) network

ACCOUNT

0x0C2...11852 (4.7484984

GAS LIMIT

3000000

VALUE

0 wei

CONTRACT

Lottery - Lottery.sol

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 0

Lottery.sol

```
//SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 <0.9.0;

contract Lottery{
    address public manager;
    address payable[] public participants;

    constructor()
    {
        manager=msg.sender; //gloabal variable
    }

    receive() external payable
    {   require(msg.value==1 ether);
        participants.push(payable(msg.sender));
    }

    function getBalance() public view returns(uint)
    {   require(msg.sender== manager);
        return address(this).balance;
    }

    function random() public view returns(uint){
        return uint(keccak256(abi.encodePacked(block.difficult
    }

    function selectWinner() public {
        require(msg.sender==manager);
        require(participants.length>=3);
        uint r=random();
        address payable winner;
        uint index = r % participants.length;
        winner=participants[index];
        winner.transfer(getBalance());
        participants=new address payable[](0);
```

0 listen on network

Search with transaction hash or address

1 tabs

Rinkeby Test Network

Connected

Account 1

0x0C2D...1852

4.7485 ETH

Buy Sell Swap

Assets Activity

4.7485 ETH

Add Token

Need help? Contact MetaMask Support

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

Injected Web3

Rinkeby (4) network

ACCOUNT

0x0C2...11852 (4.7484984

GAS LIMIT

3000000

VALUE

0 wei

CONTRACT

Lottery - Lottery.sol

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 0

Lottery.sol

```
//SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 <0.9.0;

contract Lottery{
    address public manager;
    address payable[] public participants;

    constructor()
    {
        manager=msg.sender; //gloabal variable
    }

    receive() external payable
    {   require(msg.value==1 ether);
        participants.push(payable(msg.sender));
    }

    function getBalance() public view returns(uint)
    {   require(msg.sender== manager);
        return address(this).balance;
    }

    function random() public view returns(uint){
        return uint(keccak256(abi.encodePacked(block.difficult
    }

    function selectWinner() public {
        require(msg.sender==manager);
        require(participants.length>=3);
        uint r=random();
        address payable winner;
        uint index = r % participants.length;
        winner=participants[index];
        winner.transfer(getBalance());
        participants=new address payable[](0);
```

0 listen on network

Search with transaction hash or address

1 tabs

Rinkeby Test Network

Send Cancel

0xAbaC...b9Cb

Asset: ETH
Balance: 4.748498 ETH

Amount: 1 ETH
Max
No Conversion Rate Available

Transaction Fee: Gas Price (GWEI) 1.000000008 Gas Limit 21000

Cancel Next

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT

Injected Web3

Rinkeby (4) network

ACCOUNT

0x0C2...11852 (4.7484984!

GAS LIMIT

3000000

VALUE

0 wei

CONTRACT

Lottery - Lottery.sol

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 0

Lottery.sol

```
//SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 <0.9.0;

contract Lottery{
    address public manager;
    address payable[] public participants;

    constructor()
    {
        manager=msg.sender; //gloabal variable
    }

    receive() external payable
    {   require(msg.value==1 ether);
        participants.push(payable(msg.sender));
    }

    function getBalance() public view returns(uint)
    {   require(msg.sender== manager);
        return address(this).balance;
    }

    function random() public view returns(uint){
        return uint(keccak256(abi.encodePacked(block.difficult
    }

    function selectWinner() public {
        require(msg.sender==manager);
        require(participants.length>=3);
        uint r=random();
        address payable winner;
        uint index = r % participants.length;
        winner=participants[index];
        winner.transfer(getBalance());
        participants=new address payable[](0);
```

0 listen on network

Search with transaction hash or address

1 tabs

Edit

Rinkeby Test Network

Account 1 → Dummy

SENT ETHER

1

GAS FEE 0.000021

No Conversion Rate Available

Gas Price (GWEI) 1.000000008

Gas Limit 21000

AMOUNT + GAS FEE

TOTAL 1.000021

No Conversion Rate Available

Reject

Confirm

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

GAS LIMIT

3000000

VALUE

0 wei

CONTRACT

Lottery - Lottery.sol

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 1

Deployed Contracts

Currently you have no contract instances to interact with.

Lottery.sol

```
//SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 <0.9.0;

contract Lottery{
    address public manager;
    address payable[] public participants;

    constructor()
    {
        manager=msg.sender; //gloabal variable
    }

    receive() external payable
    {   require(msg.value==1 ether);
        participants.push(payable(msg.sender));
    }

    function getBalance() public view returns(uint)
    {   require(msg.sender== manager);
        return address(this).balance;
    }

    function random() public view returns(uint){
        return uint(keccak256(abi.encodePacked(block.difficulty,block.timestamp,
    }

    function selectWinner() public {
        require(msg.sender==manager);
        require(participants.length>=3);
        uint r=random();
        address payable winner;
        uint index = r % participants.length;
        winner=participants[index];
        winner.transfer(getBalance());
        participants=new address payable[](0);
```

1 listen on network

Search with transaction hash or address

MetaMask Notification

Rinkeby Test Network

Account 1 → New Contract

https://remix.ethereum.org

CONTRACT DEPLOYMENT

0

DETAILS DATA

GAS FEE 0.000478

No Conversion Rate Available

Gas Price (GWEI) 1.000000008

Gas Limit 477637

AMOUNT + GAS FEE

TOTAL 0.000478

No Conversion Rate Available

Reject Confirm

Remix - Ethereum IDE

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

ACCOUNT

0x0C2...11852 (3.7479998

GAS LIMIT

3000000

VALUE

0 wei

CONTRACT

Lottery - Lottery.sol

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 1

Deployed Contracts

LOTTERY AT 0X36C...4CBA2 (BLOCKCH

Lottery.sol

1 tabs

```
//SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 <0.9.0;

contract Lottery{
    address public manager;
    address payable[] public participants;

    constructor()
    {
        manager=msg.sender; //gloabal variable
    }

    receive() external payable
    {   require(msg.value==1 ether);
        participants.push(payable(msg.sender));
    }

    function getBalance() public view returns(uint)
    {   require(msg.sender== manager);
        return address(this).balance;
    }

    function random() public view returns(uint){
        return uint(keccak256(abi.encodePacked(block.difficulty,block.timestamp,participants.length)));
    }

    function selectWinner() public {
        require(msg.sender==manager);
        require(participants.length>=3);
        uint r=random();
        address payable winner;
        uint index = r % participants.length;
        winner=participants[index];
        winner.transfer(getBalance());
        participants=new address payable[](0);
```

0 listen on network Search with transaction hash or address

Google Chrome

Confirmed transaction

Transaction 9 confirmed! View on Etherscan

Remix - Ethereum IDE | Rinkeby Transaction Hash (Txhas

rinkeby.etherscan.io/tx/0x6ac25e9f2813e74b45aa0aec714aa14495ddd126d4d24bfd7080f68bbb101f1f

Etherscan

Rinkeby Testnet Network

All Filters | Search by Address / Txn Hash / Block / Token / Ens

Home | Blockchain | Tokens | Misc | Rinkeby

Transaction Details

Overview | State

[This is a Rinkeby **Testnet** transaction only]

Transaction Hash:	0x6ac25e9f2813e74b45aa0aec714aa14495ddd126d4d24bfd7080f68bbb101f1f
Status:	Success
Block:	9045355 1 Block Confirmation
Timestamp:	10 secs ago (Aug-02-2021 03:56:03 PM +UTC)
From:	0x0c2de9576f7945cd4b363bd28b9a47302a211852
To:	[Contract 0x36c44a0115a61a1341f5cb36f60003664324cba2 Created]
Value:	0 Ether ($0.00)
Transaction Fee:	0.00047763700382 Ether ($0.00)
Gas Price:	0.000000001000000008 Ether (1.000000008 Gwei)
Txn Type:	0 (Legacy)

This website uses cookies to improve your experience and has an updated Privacy Policy. Got It

Remix - Ethereum IDE | Rinkeby Transaction Hash (Txhas

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

Lottery - Lottery.sol

Deploy

Publish to IPFS

OR

At Address | Load contract from Address

Transactions recorded 1

Deployed Contracts

LOTTERY AT 0X36C...4CBA2 (BLOCKCH

selectWinner

getBalance

manager

participants uint256

random

Lottery.sol

```
//SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 <0.9.0;

contract Lottery{
    address public manager;
    address payable[] public participants;

    constructor()
    {
        manager=msg.sender; //gloabal variable
    }

    receive() external payable
    {   require(msg.value==1 ether);
        participants.push(payable(msg.sender));
    }

    function getBalance() public view returns(uint)
    {   require(msg.sender== manager);
        return address(this).balance;
    }

    function random() public view returns(uint){
        return uint(keccak256(abi.encodePacked(block.difficult
    }

    function selectWinner() public {
        require(msg.sender==manager);
        require(participants.length>=3);
        uint r=random();
        address payable winner;
        uint index = r % participants.length;
        winner=participants[index];
        winner.transfer(getBalance());
        participants=new address payable[](0);
```

Now sending ethers on Contract Account

Rinkeby Test Network

Send | Cancel

0x36c4...cba2

New address detected! Click here to add to your address book.

Asset: ETH
Balance: 3.899869 ETH

Amount: 0 ETH
No Conversion Rate Available
Max

Transaction Fee: Gas Price (GWEI) 1.000000008 | Gas Limit 21000

Cancel | Next

0 listen on network

Search with transaction hash or address

Remix - Ethereum IDE | Rinkeby Transaction Hash (Txhas | Rinkeby Transaction Hash (Txhas

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

Transactions recorded 1

Deployed Contracts

LOTTERY AT 0X36C...4CBA2 (BLOCKCH

selectWinner

getBalance

0: uint256: 3000000000000000000

manager

participants uint256

random

Low level interactions

CALLDATA

Transact

Lottery.sol

1 tabs

```
//SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 <0.9.0;

contract Lottery{
    address public manager;
    address payable[] public participants;

    constructor()
    {
        manager=msg.sender; //gloabal variable
    }

    receive() external payable
    {   require(msg.value==1 ether);
        participants.push(payable(msg.sender));
    }

    function getBalance() public view returns(uint)
    {   require(msg.sender== manager);
        return address(this).balance;
    }

    function random() public view returns(uint){
        return uint(keccak256(abi.encodePacked(block.difficulty,block.timestamp,participants.length)));
    }

    function selectWinner() public {
        require(msg.sender==manager);
        require(participants.length>=3);
        uint r=random();
        address payable winner;
        uint index = r % participants.length;
        winner=participants[index];
        winner.transfer(getBalance());
        participants=new address payable[](0);
```

0 listen on network Search with transaction hash or address

Remix - Ethereum IDE | Rinkeby Transaction Hash (Txhas | Rinkeby Transaction Hash (Txhas

remix.ethereum.org/#optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.6+commit.11564f7e.js

DEPLOY & RUN TRANSACTIONS

Transactions recorded 1

Deployed Contracts

LOTTERY AT 0X36C...4CBA2 (BLOCKCH

selectWinner

getBalance

0: uint256: 3000000000000000000

manager

participants uint256

random

Low level interactions

CALLDATA

Transact

Lottery.sol

1 tabs

```
//SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 <0.9.0;

contract Lottery{
    address public manager;
    address payable[] public participants;

    constructor()
    {
        manager=msg.sender; //gloabal variable
    }

    receive() external payable
    {   require(msg.value==1 ether);
        participants.push(payable(msg.sender));
    }

    function getBalance() public view returns(uint)
    {   require(msg.sender== manager);
        return address(this).balance;
    }

    function random() public view returns(uint){
        return uint(keccak256(abi.encodePacked(block.difficulty,block.timestamp,participants.length)));
    }

    function selectWinner() public {
        require(msg.sender==manager);
        require(participants.length>=3);
        uint r=random();
        address payable winner;
        uint index = r % participants.length;
        winner=participants[index];
        winner.transfer(getBalance());
        participants=new address payable[](0);
```

0 listen on network Search with transaction hash or address

Remix - Ethereum IDE | Rinkeby Transaction Hash (Txhas | Rinkeby Transaction Hash (Txhas | Rinkeby Transaction Hash (Txhas

rinkeby.etherscan.io/tx/0x98e17c6d56caa9856e811854ecbaca3d31a68d0971187f7c91bd16c2a3ffaff6

Overview | Internal Txns | State

Transaction Hash:	0x98e17c6d56caa9856e811854ecbaca3d31a68d0971187f7c91bd16c2a3ffaff6
Status:	Success
Block:	9045370 1 Block Confirmation
Timestamp:	26 secs ago (Aug-02-2021 03:59:49 PM +UTC)
From:	0x0c2de9576f7945cd4b363bd28b9a47302a211852
To:	Contract 0x36c44a0115a61a1341f5cb36f6000 0x10c1b2c1d3c74761eef468ea9309198b849827af TRANSFER 3 Ether From 0x36c44a0115a61a1341f5cb36f... To → 0x10c1b2c1d3c74761eef468ea...
Value:	0 Ether ($0.00)
Transaction Fee:	0.00004394700035 Ether ($0.00)
Gas Price:	0.000000001000000008 Ether (1.000000008 Gwei)
Txn Type:	0 (Legacy)

Click to see More

Powered by Ethereum

Preferences

This website uses cookies to improve your experience and has an updated Privacy Policy. Got It

https://rinkeby.etherscan.io/address/0x10c1b2c1d3c74761eef468ea9309198b849827af

Remix - Ethereum IDE | Rinkeby Transaction Hash (Txhas | Rinkeby Transaction Hash (Txhas | Address 0x10c1b2c1d3c74761ee

rinkeby.etherscan.io/address/0x10c1b2c1d3c74761eef468ea9309198b849827af

Etherscan

Rinkeby Testnet Network

All Filters | Search by Address / Txn Hash / Block / Token / Ens

Home | Blockchain | Tokens | Misc | Rinkeby

Address 0x10C1b2C1d3C74761eef468ea9309198b849827aF

Overview

Balance: 4.19985493499883948 Ether

More Info

More

My Name Tag: Not Available

Transactions | Internal Txns

Latest 4 from a total of 4 transactions

Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
0x8845ab8f39f1d185132...	Transfer	9045363	2 mins ago	0x10c1b2c1d3c74761eef...	OUT	0x36c44a0115a61a1341...	1 Ether	0.000048355
0xfe38bf4d720ace6a70b...	Transfer	9045245	32 mins ago	0x10c1b2c1d3c74761eef...	OUT	0x2c319d474f5d10f038a...	1 Ether	0.000048355
0xf2d95931ccaf048f449...	Transfer	9042819	10 hrs 40 mins ago	0x10c1b2c1d3c74761eef...	OUT	0x8179fa524442004696...	0.1 Ether	0.000048355
0x012664336bf5a9fe924...	Transfer	9042791	10 hrs 47 mins ago	0x0c2de9576f7945cd4b...	IN	0x10c1b2c1d3c74761eef...	3 Ether	0.000021

[Download CSV Export]

This website uses cookies to improve your experience and has an updated Privacy Policy. Got It

Remix - Ethereum IDE | Rinkeby Transaction Hash (Txhas | Rinkeby Transaction Hash (Txhas | Address 0x10c1b2c1d3c74761ee

rinkeby.etherscan.io/address/0x10c1b2c1d3c74761eef468ea9309198b849827af

Etherscan

Rinkeby Testnet Network

All Filters | Search by Address / Txn Hash / Block / Token / Ens

Home | Blockchain | Tokens | Misc | Rinkeby

Address 0x10C1b2C1d3C74761eef468ea9309198b849827aF

Overview

Balance: 4.19985493499883948 Ether

More Info

More

My Name Tag: Not Available

Transactions | Internal Txns

Latest 4 from a total of 4 transactions

Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
0x8845ab8f39f1d185132...	Transfer	9045363	2 mins ago	0x10c1b2c1d3c74761eef...	OUT	0x36c44a0115a61a1341...	1 Ether	0.000048355
0xfe38bf4d720ace6a70b...	Transfer	9045245	32 mins ago	0x10c1b2c1d3c74761eef...	OUT	0x2c319d474f5d10f038a...	1 Ether	0.000048355
0xf2d95931ccaf048f449...	Transfer	9042819	10 hrs 40 mins ago	0x10c1b2c1d3c74761eef...	OUT	0x8179fa524442004696...	0.1 Ether	0.000048355
0x012664336bf5a9fe924...	Transfer	9042791	10 hrs 47 mins ago	0x0c2de9576f7945cd4b...	IN	0x10c1b2c1d3c74761eef...	3 Ether	0.000021

[Download CSV Export]

This website uses cookies to improve your experience and has an updated Privacy Policy. Got It

Remix - Ethereum IDE | Rinkeby Transaction Hash (Txhas | Rinkeby Transaction Hash (Txhas | Address 0x10c1b2c1d3c74761ee

rinkeby.etherscan.io/address/0x10c1b2c1d3c74761eef468ea9309198b849827af#internaltx

Etherscan

Rinkeby Testnet Network

All Filters | Search by Address / Txn Hash

Address 0x10C1b2C1d3C74761eef468ea9309198b849827aF

Overview

Balance: 4.19985493499883948 Ether

More Info

My Name Tag: Not Av

Transactions | Internal Txns

Latest 2 internal transactions

Parent Txn Hash	Block	Age	From	To
0x98e17c6d56caa9856e...	9045370	1 min ago	0x36c44a0115a61a1341...	0x10c1b2c
0xf3f3dbcd760f7a9750a...	9042833	10 hrs 36 mins ago	0x8179fa524442004696...	0x10c1b2c

Rinkeby Test Network

Not connected

Participant 2

0x10C1...27aF

4.1999 ETH

Buy | Send | Swap

Assets | Activity

Contract Interaction -1 ETH
Aug 2 · metamask -1 ETH

Contract Interaction -1 ETH
Aug 2 · metamask -1 ETH

This website uses cookies to improve your experience and has an updated Privacy Policy. Got It

Remix - Ethereum IDE | Rinkeby Transaction Hash (Txhas | Rinkeby Transaction Hash (Txhas | Rinkeby Transaction Hash (Txhas

rinkeby.etherscan.io/tx/0x98e17c6d56caa9856e811854ecbaca3d31a68d0971187f7c91bd16c2a3ffaff6

Overview | Internal Txns | State

From:	0x0c2de9576f7945cd4b363bd28b9a47302a211852
To:	Contract 0x36c44a0115a61a1341f5cb36f60003664324cba2 TRANSFER 3 Ether From 0x36c44a0115a61a1341f5cb36f... To → 0x10c1b2c1d3c74761eef468ea...
Value:	0 Ether ($0.00)
Transaction Fee:	0.00004394700035 Ether ($0.00)
Gas Price:	0.000000001000000008 Ether (1.000000008 Gwei)
Txn Type:	0 (Legacy)
Gas Limit:	54,933
Gas Used by Transaction:	43,947 (80%)
Nonce Position	10 13
Input Data:	Function: selectWinner() *** MethodID: 0x33a99e04

View Input As

Click to see Less

This website uses cookies to improve your experience and has an updated Privacy Policy. Got It