

Experiment: 04

Aim: Hands on Solidity Programming Assignments for creating Smart Contracts

Theory:

1. Primitive Data Types, Variables, Functions – pure, view

In Solidity, primitive data types form the foundation of smart contract development. Commonly used types include:

- **uint / int**: unsigned and signed integers of different sizes (e.g., uint256, int128).
- **bool**: represents logical values (true or false).
- **address**: holds a 20-byte Ethereum account address, often used for storing user accounts or contract addresses.
- **bytes / string**: store binary data or textual data.

Variables in Solidity can be **state variables** (stored on the blockchain permanently), **local variables** (temporary, created during function execution), or **global variables** (special predefined variables such as msg.sender, msg.value, and block.timestamp).

Functions allow execution of contract logic. Special types of functions include:

- **pure**: cannot read or modify blockchain state; they work only with inputs and internal computations.
- **view**: can read state variables but cannot alter them. This classification helps optimize gas usage and enforces function integrity.

2. Inputs and Outputs to Functions

Functions in Solidity can accept input arguments and return one or more output values. Inputs enable users or other contracts to pass data into the contract, while outputs make it possible to return results after computation. For example, a function can accept an amount in Ether and return whether the transfer was successful. Solidity also allows named return variables, which improve readability and debugging.

3. Visibility, Modifiers and Constructors

- **Function Visibility** defines who can access a function:
 - **public**: available both inside and outside the contract.
 - **private**: only accessible within the same contract.
 - **internal**: accessible within the contract and its child contracts.

- **Modifiers** are reusable code blocks that change the behavior of functions. They are often used for access control, such as restricting sensitive functions to the contract owner (onlyOwner).
- **Constructors** are special functions executed only once during contract deployment. They initialize important values, such as setting the deploying account as the owner of the contract.

4. Control Flow: if-else, loops

Control flow in Solidity is similar to traditional programming languages:

- **if-else** allows conditional decision-making in contract logic, e.g., checking if a balance is sufficient before transferring funds.
- **Loops** (for, while, do-while) enable repeated execution of code. For example, iterating through an array of users. However, loops must be used carefully, as excessive iterations increase gas consumption, potentially making the contract expensive to execute.

5. Data Structures: Arrays, Mappings, Structs, Enums

- **Arrays**: Can be fixed or dynamic and are used to store ordered lists of elements. Example: an array of addresses for registered users.
- **Mappings**: Key-value pairs that allow quick lookups. Example: mapping(address => uint) for storing balances. Unlike arrays, mappings do not support iteration.
- **Structs**: Allow grouping of related properties into a single data type, such as creating a struct Player {string name; uint score;}.
- **Enums**: Used to define a set of predefined constants, making code more readable. Example: enum Status { Pending, Active, Closed }.

6. Data Locations

Solidity uses three primary data locations for storing variables:

- **storage**: Data stored permanently on the blockchain. Examples: state variables.
- **memory**: Temporary data storage that exists only while a function is executing. Used for local variables and function inputs.
- **calldata**: A non-modifiable and non-persistent location used for external function parameters. It is gas-efficient compared to memory. Understanding data locations is essential, as they directly impact gas costs and performance.

7. Transactions: Ether and Wei, Gas and Gas Price, Sending Transactions

- **Ether and Wei:** Ether is the main currency in Ethereum. All values are measured in Wei, the smallest unit (1 Ether = 10^{18} Wei). This ensures high precision in financial transactions.
- **Gas and Gas Price:** Every transaction consumes gas, which represents computational effort. The gas price determines how much Ether is paid per unit of gas. A higher gas price incentivizes miners to prioritize the transaction.
- **Sending Transactions:** Transactions are used for transferring Ether or interacting with contracts. Functions like transfer() and send() are commonly used, while call() provides more flexibility. Each transaction requires gas, making efficiency in contract design very important.

Implementation:

1. Introduction

```
1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.3;
3
4 contract Counter {
5     //Rujuta Medhi
6     uint public count;
7
8     // Function to get the current count
9     function get() public view returns (uint) {    2453 gas
10        return count;
11    }
12
13    // Function to increment count by 1
14    function inc() public {    infinite gas
15        count += 1;
16    }
17
18    // Function to decrement count by 1
19    function dec() public {    infinite gas
20        count -= 1;
21    }
```

2. Basic Syntax

```
pragma solidity ^0.8.3;

contract MyContract{
    string public name = "Rujuta Medhi";
}
```

3. Primitive Data Types

The screenshot shows the Remix Ethereum IDE interface. On the left, there's a sidebar titled "DEPLOY & RUN TRANSACTIONS" with buttons for various operations like "i", "int256", "i8", "neg", "newAddr", "newU", "u", "u256", and "u8". The main area displays a Solidity code editor with the following code:

```

22 // SPDX-License-Identifier: MIT
23 pragma solidity ^0.8.3;
24
25 contract Variables {
26     // State variables are stored on the blockchain.
27     string public text = "Rujuta Medhi";
28     uint public num = 123;
29     uint public blockNumber;
30
31     function doSomething() public {
32         // Local variables are not saved to the blockchain.
33         uint i = 456;
34
35         // Here are some global variables
36         uint timestamp = block.timestamp; // Current block timestamp
37         address sender = msg.sender; // address of the caller
38         blockNumber = block.number;
39     }
40 }

```

The status bar at the bottom shows "Scam Alert" and "Initialize as git repo".

4. Variables

This screenshot shows the same Remix Ethereum IDE interface as the previous one, but with a different Solidity contract named "variables.sol". The code is identical to the one above, demonstrating state variables and their values.

The status bar at the bottom shows "Scam Alert" and "Initialize as git repo".

5. Functions - Reading and Writing to a State Variable

The screenshot shows the Remix Ethereum IDE interface. The left sidebar has sections for 'DEPLOY & RUN TRANSACTIONS' and 'CALLDATA'. The main code editor displays the following Solidity code:

```

1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.3;
3
4 contract SimpleStorage {
5     // State variable to store a number
6     uint public num;
7     bool public b = true;
8     // Rujuta Medhi
9     function get_b() public view returns (bool) {
10         return b;
11     }
12     // You need to send a transaction to write to a state variable.
13     function set(uint _num) public {
14         num = _num;
15     }
16
17     // You can read from a state variable without sending a transaction.
18     function get() public view returns (uint) {
19         return num;
20     }
21 }

```

The 'Explain contract' section at the bottom provides an overview of the contract's functions.

6. Functions - View and Pure

The screenshot shows the Remix Ethereum IDE interface. The left sidebar has sections for 'DEPLOY & RUN TRANSACTIONS' and 'Solidity compiler'. The main code editor displays the following Solidity code:

```

1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.3;
3
4 contract ViewAndPure {
5     uint public x = 1;
6     //Rujuta Medhi
7     // Promise not to modify the state.
8     function addToX(uint y) public view returns (uint) {
9         return x + y;
10    }
11
12    function addToX2(uint y) public {
13        x += y;
14    }
15
16    // Promise not to modify or read from the state.
17    function add(uint i, uint j) public pure returns (uint) {
18        return i + j;
19    }
20 }

```

The 'Explain contract' section at the bottom provides an overview of the contract's functions.

7. Functions - Modifiers and Constructors

```

1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.3;
3
4 contract FunctionModifier {
5     //Rujuta
6     // We will use these variables to demonstrate how to use
7     // modifiers.
8     address public owner;
9     uint public x = 10;
10    bool public locked;
11
12    constructor() {
13        // Set the transaction sender as the owner of the contract.
14        owner = msg.sender;
15    }
16
17    // Modifier to check that the caller is the owner of
18    // the contract.
19    modifier onlyOwner() {
20        require(msg.sender == owner, "Not owner");
21        // Underscore is a special character only used inside

```

Balance: 0 ETH

FUNCTIONMODIFIER AT 0x85

INCREASEX

Y: 33

Calldata Parameters

locked
owner
x

0: uint256: 142

Low level interactions

block hash: 0xf964d9b35ddf79e8ae37f32f89b5a7sc4ed85009776b63658912fe74ee0ce379

block number: 42

from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

to: FunctionModifier.increase_(uint256) @x857ee0797C3fc9205714a577c02F7205b889dF30

transaction cost: 29848 gas

execution cost: 7844 gas

output: 0x

decoded input: { "uint256 y": "33" }

decoded output: ()

logs: []

raw logs: []

call to FunctionModifier.x()

CALL [call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: FunctionModifier.x() data: 0x0c5...5699c

REMX 1.5.1

DEPLOY & RUN TRANSACTIONS

FUNCTIONMODIFIER AT 0x85

INCREASEX

Y: 33

Calldata Parameters

locked
owner
x

0: uint256: 142

Low level interactions

block hash: 0xf964d9b35ddf79e8ae37f32f89b5a7sc4ed85009776b63658912fe74ee0ce379

block number: 42

from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4

to: FunctionModifier.increase_(uint256) @x857ee0797C3fc9205714a577c02F7205b889dF30

transaction cost: 29848 gas

execution cost: 7844 gas

output: 0x

decoded input: { "uint256 y": "33" }

decoded output: ()

logs: []

raw logs: []

call to FunctionModifier.x()

CALL [call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: FunctionModifier.x() data: 0x0c5...5699c

Did you know? To learn new contract patterns and prototype, you can activate and try the cookbook plugin!

Scan Alert Initialize as git repo

30°C Sunny

Search

ENG US 11:49 03-02-2026

8. Functions - Inputs and Outputs

```

// modifiersAndConstructors.sol
function returnTwo() public pure returns (int i, bool b) {
    i = -2;
    b = true;
}

```

Scam Alert Initialize as git repo Did you know? To learn new contract patterns and prototype, you can activate and try the cookbook plugin! AI copilot (enabled)

30°C Sunny Search ENG US 12:01 03-02-2026

9. Visibility

```

// modifiersAndConstructors_answer.sol
// Inherited contracts do not have access to private functions
// and state variables.
function testPrivateFunc() public pure returns (string memory) {
    return privateFunc();
}

// Internal function call be called inside child contracts.
function testInternalFunc() public pure override returns (string memory) {
    return internalFunc();
}

// Rujuta Medhi
function testInternalVar() public view returns (string memory, string memory) {
    return (internalVar, publicVar);
}

```

Scam Alert Initialize as git repo Did you know? To learn new contract patterns and prototype, you can activate and try the cookbook plugin! AI copilot (enabled)

30°C Sunny Search ENG US 12:06 03-02-2026

10. Control Flow - If/Else

The screenshot shows the REMIX IDE interface. On the left, the sidebar displays "DEPLOY & RUN TRANSACTIONS" with "Transactions recorded 30" and a "Run transactions using the latest compilation result" checkbox. Below it is the "Deployed Contracts" section, which lists "IFELSE AT 0XB9E...C6D72 (MEM)" with a balance of "0 ETH". Under "EVENTCHECK", there's a call to "foo(uint256 x)" with parameters "y: 33" and "ternary: uint256 _x". The main workspace shows the following Solidity code:

```

9   return 1;
10 } else {
11   return 2;
12 }
13
14 function ternary(uint _x) public pure returns (uint) { infinite gas
15   // if (_x < 10) {
16   //   return 1;
17   // }
18   // return 2;
19
20   // shorthand way to write if / else statement
21   return _x < 10 ? 1 : 2;
22 }
23 //Rujuta Medhi
24 function evenCheck(uint y) public pure returns (bool) { infinite gas
25   return y%2 == 0 ? true : false;
26 }
27
28

```

The "Explain contract" panel at the bottom shows a tooltip for "foo" with the value "0". The status bar at the bottom right indicates "RemixAI Copilot (enabled)", the date "03-02-2026", and the time "12:11".

11. Control Flow - Loops

The screenshot shows the REMIX IDE interface. The sidebar is identical to the previous one. The main workspace shows the following Solidity code:

```

4 contract Loop {
5   uint public count;
6   function loop() public{ infinite gas
7     // for loop
8     for (uint i = 0; i < 10; i++) {
9       if (i == 5) {
10         // Skip to next iteration with continue
11         continue;
12       }
13       if (i == 5) {
14         // Exit loop with break
15         break;
16       }
17       count++;
18     }
19 // Rujuta Medhi
20 // while loop
21 uint j;
22 while (j < 10) {
23   j++;
24

```

The "Explain contract" panel at the bottom shows a tooltip for "loop" with the value "0". The status bar at the bottom right indicates "RemixAI Copilot (enabled)", the date "03-02-2026", and the time "12:14".

12. Data Structures - Arrays

The screenshot shows the REMIX IDE interface with the following details:

- Top Bar:** Shows the REMIX logo, version 1.5.1, a search bar with "learneth tutorials", and buttons for "Login with GitHub", "Theme", and "Settings".
- Left Sidebar:** Titled "DEPLOY & RUN TRANSACTIONS". It includes a "Calldata" section with "push" and "remove" buttons, and a "Parameters" section with "arr", "arr2", "arr3", "get", "getArr", and "myFixedSizeArr" inputs. A "Low level interactions" section shows "0: uint256[3]: 0,1,2" and buttons for "getLength" and "call".
- Middle Panel:** Titled "Compiled". It displays the Solidity code for a contract named "Array".

```
// This will increase the array length by 1.  
arr.push(i);  
  
function pop() public {  
    // Remove last element from array  
    // This will decrease the array length by 1  
    arr.pop();  
}  
  
function getLength() public view returns (uint) {  
    return arr.length;  
}  
  
function remove(uint index) public {  
    // Delete does not change the array length.  
    // It resets the value at index to its default value,  
    // in this case 0  
    delete arr[index];  
}
```
- Bottom Panel:** Includes an "Explain contract" button, a gas usage summary (0 gas), a "Listen on all transactions" checkbox, a search bar, and a "Filter with transaction hash or ad..." input field.

The screenshot shows the REMIX IDE interface with the following details:

- Top Bar:** Shows the REMIX logo, version 1.5.1, a search bar with "learneth tutorials", and buttons for "Login with GitHub", "Theme", and "Settings".
- Left Sidebar:** Titled "DEPLOY & RUN TRANSACTIONS". It includes a "Calldata" section with "call" and "Parameters" section with "arr2", "arr3", "get", "getArr", and "myFixedSizeArr" inputs. A "Low level interactions" section shows "0: uint256[3]: 0,1,2" and buttons for "getLength" and "call".
- Middle Panel:** Titled "Compiled". It displays the Solidity code for a contract named "Array".

```
contract Array {  
    // Several ways to initialize an array  
    uint[] public arr;  
    uint[] public arr2 = [1, 2, 3];  
    // Fixed sized array, all elements initialize to 0  
    uint[10] public myFixedSizeArr;  
    uint[3] public arr3 = [0, 1, 2];  
  
    function get(uint i) public view returns (uint) {  
        return arr[i];  
    }  
  
    // Solidity can return the entire array.  
    // But this function should be avoided for  
    // arrays that can grow indefinitely in length.  
    function getArr() public view returns (uint[3] memory) {  
        return arr3;  
    }  
  
    function push(uint i) public {  
        // Append to array  
    }  
}
```
- Bottom Panel:** Includes an "Explain contract" button, a gas usage summary (0 gas), a "Listen on all transactions" checkbox, a search bar, and a "Filter with transaction hash or ad..." input field.

13. Data Structures - Mappings

```

17     }
18
19     function remove(address _addr) public {
20         // Reset the value to the default value.
21         delete balances[_addr];
22     }
23 }
24
25 contract NestedMapping {
26     //Rujuta Medhi
27     // Nested mapping (mapping from address to another mapping)
28     mapping(address => mapping(uint => bool)) public nested;
29
30     function get(address _addr1, uint _i) public view returns (bool) {
31         // You can get values from a nested mapping
32         // even when it is not initialized
33         return nested[_addr1][_i];
34     }
35
36     function set(uint _gas, address _addr1)
37         address _addr2

```

14. Data Structures - Structs

```

32     Todo storage todo = todos[_index];
33     return (todo.text, todo.completed);
34 }
35
36 // update text
37 function update(uint _index, string memory _text) public {
38     Todo storage todo = todos[_index];
39     todo.text = _text;
40 }
41
42 // update completed
43 function toggleCompleted(uint _index) public {
44     Todo storage todo = todos[_index];
45     todo.completed = !todo.completed;
46 }
47 //Rujuta Medhi -33
48 function remove(uint _index) public {
49     delete todos[_index];
50 }
51

```

15. Data Structures - Enums

```

function getSize() public view returns (Size) {
    return sizes;
}

// Update status by passing uint into input
function set(Status _status) public {
    status = _status;
}

// You can update to a specific enum like this
function cancel() public {
    status = Status.Canceled;
}

// Rujuta Medhi]
// delete resets the enum to its first value, 0
function reset() public {
    delete status;
}

```

16. Data Locations

```

function _f(
    uint[] storage _arr,
    mapping(uint => address) storage _map,
    MyStruct storage _myStruct
) internal {
    // do something with storage variables
}

// You can return memory variables
function _g(uint[] memory _arr) public returns (uint[] memory) {
    // do something with memory array
    arr[0] = 1;
}

function _h(uint[] calldata _arr) external {
    // do something with calldata array
    _arr[0] = 1;
}

```

17. Transactions - Ether and Wei

```

1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.3;
3
4 contract EtherUnits {
5     uint public oneWei = 1 wei;
6     // 1 wei is equal to 1,000,000,000 (10^9) wei.
7     bool public isOneWei = 1 wei == 1;
8
9     uint public oneEther = 1 ether;
10    // 1 ether is equal to 10^18 wei
11    bool public isOneEther = 1 ether == 1e18;
12
13    uint public oneGwei = 1 gwei;
14    // 1 ether is equal to 10^9 wei
15    bool public isOneGwei = 1 gwei == 1e9;
16 }

```

Assignment

- Create a `public uint` called `oneGwei` and set it to 1 `gwei`.
- Create a `public bool` called `isOneGwei` and set it to the result of a comparison operation between 1 `gwei` and 10^9 .

Tip: Look at how this is written for `gwei` and `ether` in the contract.

Check Answer **Show answer**

Well done! No errors.

18. Transactions - Gas and Gas Price

```

1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.3;
3
4 contract Gas {
5     //Rujuta
6     uint public i = 0;
7     uint public cost = 170367;
8
9     // Using up all of the gas that you send causes your transaction to fail.
10    // State changes are undone.
11    // Gas spent
12    function() payable {
13        // H
14        // a
15        while (i < cost) {
16            i += 1;
17        }
18    }
19 }

```

Assignment

Create a new `public` state variable in the `Gas` contract called `cost` of the type `uint`. Store the value of the gas cost for deploying the contract in the new variable, including the cost for the value you are storing.

Tip: You can check in the Remix terminal the details of a transaction, including the gas cost. You can also use the Remix plugin `Gas Profiler` to check for the gas cost of transactions.

Check Answer **Show answer**

Well done! No errors.

19. Transactions - Sending Ether

The screenshot shows the REMIX IDE interface. On the left, there's a sidebar with various icons and a 'LEARNETH' section. The main area displays a Solidity code editor with a 'Charity' contract. The code includes a constructor, a 'donate' function (payable), and a 'withdraw' function. A tip at the bottom suggests testing the contract by deploying it and sending Ether. Below the code editor are buttons for 'Check Answer', 'Show answer', and 'Next'. At the bottom, a message says 'Well done! No errors.' On the right side of the interface, there are tabs for other files like 'gasAndGasPrice_answer.sol', 'sendingEther.sol', and 'sendingEther_answer.sol'. The bottom right corner shows the 'Welcome to Remix 1.5.1' message.

```
49     }
50   }
51 }
52
53 contract Charity {
54   address public owner;
55
56   constructor() {
57     owner = msg.sender;
58   }
59
60   function donate() public payable {
61     require(gasleft() >= 165452 gas 141000 gas);
62   }
63
64   function withdraw() public {
65     uint amount = address(this).balance;
66
67     (bool sent, bytes memory data) = owner.call{value: amount}("");
68     require(sent, "Failed to send Ether");
}
```

Conclusion: This experiment provided practical exposure to Solidity programming and the process of creating smart contracts on a blockchain platform. Through hands-on implementation, the fundamental concepts of blockchain such as decentralization, immutability, and trustless execution were clearly understood. Designing and deploying smart contracts helped in learning Solidity syntax, data types, functions, modifiers, and transaction handling.