madBlocks
Technology:Innovation:Business

Solidity Programming

madBlocks
Technology:Innovation:Business

Session by

Madhu Parvathaneni
Blockchain Developer
mad Blockchain Group
0-7893015625
mad@madblocks.tech

Today’s Agenda

madBlocks
Technology:Innovation:Business

01 What is Solidity?
Quick Tour on Solidity Programming Language

02 Data Types and Operators
Value Types, Units, Operators

03 Functions, Function Calls
Functions, Global Variables, Function Calls

04 Inheritance, Exceptions
Inheritance, Exceptions, Import

madBlocks
Technology:Innovation:Business

Session – 1:
What is Solidity?

What is Blockchain?

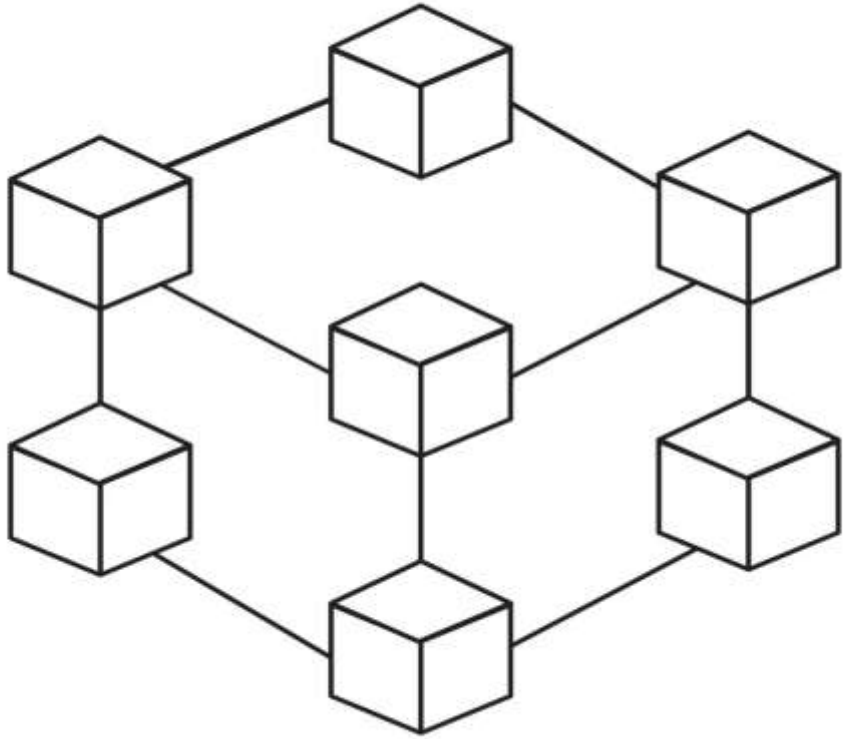
madBlocks
Technology:Innovation:Business

What is Blockchain?

– Blockchain is a distributed peer to peer network which maintains the digital ledger of complete transactions.

– You can’t tamper the data though it is open to everyone as the blocks are completely encrypted and connected.

– Due to its transparency, and immutability the Blockchains are emerging in Industry 4.0



What is Bitcoin?

madBlocks
Technology:Innovation:Business

Bitcoin

– Bitcoin is a digital currency, which is used and distributed electronically.

– It is a decentralized peer-to-peer network. No single bank institution or person controls it.

– Bitcoin is the first cryptocurrency which used Blockchain technology and hence, people started calling it as blockchain, but it is not;

– Bitcoin has the open-source public distributed ledger in p2p network called Blockchain

What is Ethereum?

madBlocks
Technology:Innovation:Business

Ethereum

– Ethereum is the second-largest cryptocurrency platform by market capitalization, behind Bitcoin.

– It is a decentralized open source blockchain featuring smart contract functionality.

– Ether is the cryptocurrency generated by Ethereum miners as a reward for computations performed to secure the blockchain

ethereum

Smart Contract

madBlocks
Technology:Innovation:Business

What is a Smart Contract?

– Smart Contracts are self-executing, business automation applications that run on a decentralized network of a Blockchain.

– Smart Contracts give you:

- Autonomy (Eradicate the third party)
- Trust (No one can stole or tamper)
- Savings (No agents in between parties)
- Safety (Difficulty to hack)
- Efficiency (Saving lot of time)

What is Solidity?

madBlocks
Technology:Innovation:Business

What is Solidity?

– Solidity is an object-oriented programming language used to write smart contracts on Ethereum Blockchain.

– Solidity is influenced by C++, Python and JavaScript to target Ethereum Virtual Machine (EVM).

– Solidity Compiler will convert the program into byte code which can be executed by EVM and then deployed on to a Blockchain network.

What is Remix IDE?

madBlocks
Technology:Innovation:Business

Remix is a powerful, open source tool that helps you write Solidity contracts straight from the browser. Written in JavaScript, Remix supports both usage in the browser and locally.

Remix also supports testing, debugging and deploying of smart contracts and much more.

Yahoo! We are ready to create our first Smart Contract.

Options in Remix IDE

madBlocks
Technology:Innovation:Business

File Explorer – This is an option available on Remix IDE to handle various files associated to a Smart Contract.

Solidity Compiler – This is an option available on Remix IDE to compile the solidity file and push if any errors

Deploy & Run – This is an option available on Remix IDE to deploy and run the smart contract

Let’s walk-through at http://remix.ethereum.org

madBlocks
Technology:Innovation:Business

Session – 2:
Data Types and Operators

pragma

madBlocks
Technology:Innovation:Business

pragma is a keyword in Solidity programming language enables certain compilation features

Syntax:

pragma solidity compiler_version;

For example:

pragma solidity 0.6.6;

Comments

madBlocks
Technology:Innovation:Business

Comments are programmer friendly and Solidity supports comments as C/C++ language

1. Single Line Comment

Syntax:

```
// This line is commented
```

2. Multiple Line Comment

Syntax:

```
/*
 These are the multiple lines
 are commented
*/
```

Data Types

madBlocks
Technology:Innovation:Business

Type of data that involves in Solidity Programming

1. Boolean - bool
2. Unsigned Integer – uint8 to uint256 – uint
3. Signed Integer – int8 to int256 – int
4. Fixed Point Numbers – fixedMxN – M bits, N decimal points
5. Unsigned Fixed Point Numbers – ufixedMxN
6. Address – address - 20 byte value

Fixed Point Numbers / Unsigned Fixed Point Numbers
M should be divisible by 8 (8 to 256)
N should be in range 0 to 80

Variables

madBlocks
Technology:Innovation:Business

Variables are identifiers where you can store a value

1. State Variables
   - whose values are permanently stored in contract storage

1. Local Variables
   - whose values are accessible till function is executing

3. Global Variables
   - whose values are accessible through the Blockchain

1. **Variable Declaration**
2. **Variable Definition**
3. **Variable Initialization**
4. **Variable Assignment**

Scope of Variables

madBlocks
Technology:Innovation:Business

Local Variable scope lies within the function whereas the State Variable scopes are of following:

1. public
   - Both internal and external access through function calls

1. internal
   - only internal access within the contract or derived contracts

3. private
   - only internal access within the contract

Syntax:

dataType scope var_name;

Operators

madBlocks
Technology:Innovation:Business

Operator is used to perform operation. There were different types of operators same as C/C++. Let's see what are they:

1. Arithmetic Operators
   - +, - , *, /, %, ++, --

1. Comparison Operators
   - ==, !=, >, <, >=, <=

3. Logical Operators
   - &&, ||, !

4. Bitwise Operators
   - &, |, ~, ^, <<, >>

5. Assignment Operators
   - =, +=, -=, *=,/=, %=

6. Conditional Operator
   - ?:

Loops

madBlocks
Technology:Innovation:Business

A branch of statements gets executed over and over.
The following were the loops available:

1. while Loop

1. do…while Loop

3. for Loop

4. Loop Control
   - break
   - continue

Decision Making

madBlocks
Technology:Innovation:Business

A branch of statements gets executed on a condition check.
The following were available:

1. if statement

1. if…..else statement

3. if……else if statement

Strings

madBlocks
Technology:Innovation:Business

Solidity supports string literals using either double quote or single quote.

Syntax:

string data='text';

1. \r – Carriage Return
1. \n – new line
3. \\ - Backslash
4. \t – tab space
5. \x – Hexadecimal Value

Arrays

madBlocks
Technology:Innovation:Business

Collection of values of similar dataType same as arrays in C programming language

Syntax:

```
uint[3] a = [1,2,3];
```

You can access the members of the array through index.
Index value starts with 0
You can also create both static and dynamic arrays

enums

madBlocks
Technology:Innovation:Business

The values in the enumerated list are called enums

Syntax:

enum madhu {ORANGE, MANGO, APPLE}

madhu ms;
ms=madhu.ORANGE // 0
ms=madhu.MANGO // 1
ms=madhu.APPLE // 2

structures

madBlocks
Technology:Innovation:Business

Collection of values of different dataType same as structures in C programming language

Syntax:

```
struct abc
{
        string a;
        uint b;
}
```

You can access the members of the structure through structure variable.
You can use dot operator to access its members

ethers

madBlocks
Technology:Innovation:Business

Lets look at the denomination of ethers

1. 1 wei = 1
1. 1 sazboo = 1e12
3. 1 finney = 1e15
4. 1 ether = 1e18

madBlocks
Technology:Innovation:Business

Questions??

Every engineer has a tendency to tinker on a problem, lets answer few of them.

madBlocks
Technology:Innovation:Business

Session – 3: Functions, Function Calls, Modifiers

Functions

madBlocks
Technology:Innovation:Business

Group of reusable code which can be called anywhere throughout the program which is same as functions in C/C++

Syntax:

```
function function_name (parameters) scope returns () {
        _____
        _____
        _____
}
```

function definition has to be created before you make a function call
scope – public/private/view/pure

Function Calls

madBlocks
Technology:Innovation:Business

If you want to execute a branch of reusable code, then you have to make a function call so that the branch will gets executed.

Syntax:

```
function function_name (parameters) scope returns () {
        _____
        _____
        _____
}

function_name(parameters);
```

Function Modifier

madBlocks
Technology:Innovation:Business

Function Modifiers are the modifiers which modifies the function behaviour and they were widely used in Smart Contracts.

Syntax:

```
modifier modifierName {
        require (parameters);
        _;
}
```

madBlocks
Technology:Innovation:Business

Questions??

Every engineer has a tendency to tinker on a problem, lets answer few of them.

madBlocks
Technology:Innovation:Business

Session – 4: Inheritance, Exceptions

Inheritance

madBlocks
Technology:Innovation:Business

Inheritance is a way to extend functionality of a contract. Solidity supports both single as well as multiple inheritance.

Syntax:

```
contract A
{
}

contract B is A
{
}
```

Error Handling

madBlocks
Technology:Innovation:Business

Solidity provides various functions for error handling.
Generally when an error occurs, the state is reverted back to its original state.

Following are some of the important methods used in error handling −

assert(bool condition)
− In case condition is not met, this method call causes an invalid opcode and any changes done to state got reverted. This method is to be used for internal errors.

require(bool condition, string memory message)
− In case condition is not met, this method call reverts to original state. - This method is to be used for errors in inputs or external components. It provides an option to provide a custom message.

revert(string memory reason)
− This method aborts the execution and revert any changes done to the state. It provides an option to provide a custom message.

Thank You

Happy to host you today.