LATE BHAUSAHEB HIRAY S.S. TRUST'S INSTITUTE OF COMPUTER APPLICATION, MUMBAI

# Blockchain & Solidity Program Lab Manual

## VIKRAM PATALBANSI, DIVAKAR JHA

Faculty, Master of Computer Application (M.C.A.) Late Bhausaheb Hiray S.S. Trust's Institute of Computer Application



## **BLOCKCHAIN & SOLIDITY PROGRAM LAB MANUAL**

## **BLOCKCHAIN & SOLUDITY PROGRAM LAB MANUAL**

LATE BHAUSAHEB HIRAY S.S. TRUST'S INSTITUTE OF COMPUTER APPLICATION, BANDRA, EAST MUMBAI-51

Author: Vikram Patalbansi Co- Authors: Divakar Jha

Faculty. Master of Computer Application (M.C.A.) Late Bhausaheb Hiray S.S. Trust's Institute of Computer Application



First Edition, 2023

Copyright © Late Bhausaheb Hiray S.S. Trust's Institute Of Computer Application, Bandra (E), Mumbai-51, 2023

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the author, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. For permission requests, write to the publisher at the address below.

This book can be exported from India only by the publishers or by the authorized suppliers. Infringement of this condition of sale will lead to Civil and Criminal prosecution.

Paperback ISBN: 978-81-19221-67-7 eBook ISBN: 978-81-19221-64-6 WebPDF ISBN: 978-81-19221-66-0

Note: Due care and diligence has been taken while editing and printing the book; neither the author nor the publishers of the book hold any responsibility for any mistake that may have inadvertently crept in.

The publishers shall not be liable for any direct, consequential, or incidental damages arising out of the use of the book. In case of binding mistakes, misprints, missing pages, etc., the publishers' entire liability, and your exclusive remedy, is replacement of the book within one month of purchase by similar edition/reprint of the book.

Printed and bound in India by 16Leaves 2/579, Singaravelan Street Chinna Neelankarai Chennai - 600 041, India info@16leaves.com www.16Leaves.com Call: 91-9940638999

### **CONTENTS**

1	Blockchain's Block creation using JavaScript	1
2	Steps for Blockchain program compiling and running using Truffle DApp program using Metamask	5
3	MetaMask Configuration Steps and Transaction	21
4	Blockchain Cryptography Program using Java	33
5	Blockchain Public Key Cryptography	35
6	Blockchain cryptography using Message Digest algorithm in Java	37
7	Program using Solidity to check Balance	39
8	Contract using Structure in Solidity Code	51
9	Ethereum Installation	63
10	Program on Election DApp	75
11	The use of GANACHE Truffle Suite to Deploy a Smart Contract in Solidity (Blockchain)	83
12	How to use MetaMask to Deploy a Smart contract in Solidity (Blockchain)?	91
13	How to Develop Ethereum Smart Contract with Truffle and Ganache	97
14	Blockchain creation program using Java	105
15	Simple Solidity Program in Ethereum	115
16	Ethereum Development program to check balance	125
17	Ethereum program on Solidity to check account details	137
18	Working with Smart Contracts in Ethereum	149
19	Syntaxes in Solidity Programs	171
20	Simple Calculator Solidity Programs	203
21	Creating the Smart Contract	209

22	Smart Contract using Web3.js	223
23	DApp on Election	227
24	Case Study on Blockchain	251
25	j Annexure-I	277

### Prog. 1 Blockchain's Block creation using JavaScript

```
const SHA256 = require("crypto-js/sha256"); class Block
{
      constructor(index,timestamp,data,previoushash=")
      {
        this.index = index;
        this.timestamp = timestamp;
        this.data = data;
        this.previoushash = previoushash;
        this.hash = this.calculateHash();
      }
      calculateHash()
      {
        return SHA256(this.index+this.timestamp+this.previoushash+JSON.stringify(this.data)).toString();
      }
} //close block class class Blockchain
{
      constructor(index,timestamp,data,previoushash=")
     {
        this.index = index;
        this.timestamp = timestamp;
        this.data = data;
        this.previoushash = previoushash;
        this.chain =[this.createGenesisBlock()];
      }
      createGenesisBlock()
      {
        return new Block(0,"23/11/2021","This is First Program of Blockchain creation","0");
      }
      addBlock(newBlock)
      {
        newBlock.previoushash = this.getLatestBlock().hash;
        newBlock.hash = newBlock.calculateHash();
        this.chain.push(newBlock);
      }
      getLatestBlock()
      ł
        return this.chain[this.chain.length-1];
      }
} // close blockchain class
```

let block1 = new Block(1,"22/11/2021","Data1","0"); let block2 = new Block(2,"21/11/2021","Second Block",""); let block3 = new Block(3,"14/05/2021","Third Block",""); let myBlockchain = new Blockchain(); myBlockchain.addBlock(block1); myBlockchain.addBlock(block2); myBlockchain.addBlock(block3); console.log(JSON.stringify(myBlockchain,null,4));

#### output:

🖈 File Edit Selectio	n View	50 Run Terminal Help Block.java - Untitled	(Workspace) - Visual Studio Code [Administrat	- 🗆 X
		JS TnxValid.js  Block.java 1 ×		$\triangleright$ ~ $\square$ …
<ul> <li>UNTITLED (WORK</li> <li>blockchainlab</li> <li>node_modu</li> <li>Block.class</li> <li>Block.html</li> <li>Block.java</li> </ul>	es	blockchainlab >  Block.java > 77 78 79 PROBLEMS 8 OUTPUT DEBUG CONSOLE TERM	/INAL	+ v A X
BlockChainD     BlockChainD	emo.class	F:\blockchainlab>npm -v		Di powersnell
BlockChainD BlockChainD BlockChainD BlockChainD BlockChainD BlockChainD	em 4 eem 2 eem 2	F:\blockchainlab>truffle verson Truffle v5.4.22 (core: 5.4.22) Solidity v0.5.16 (solc-js) Node v16.13.0 Web3.js v1.5.3		> powershell
<ul> <li>P nonce</li> <li>Block(int,</li> <li>Calculatel</li> <li>minBlock</li> <li>toString()</li> </ul>	String, S Iash() : (int) : vo : String	F:\blockchainlab>truffle unbox react This directory is non-empty ? Proceed anyway? (Y/n) Starting unbox		
> JAVA PROJECTS	-	Ln 80 Col 1 (6 sele	acted) Spaces 4 LITE-8 CRLF Java 1/2	IavaSE-18 ₽ ∫
■ 2 0 Ħ <b>♥</b>	<b>N N</b>	🖾 📅 📕 Blochain 🕐 🖉 👼 🎯 🙆 🏧	const SHA Blockchain Block.java $\land = 1$	Q (ℓ, Φ)) € ENG 22-12-2021



×	File Edit Selection View	Go Run Terminal Help • jsBlockchainex.js - Untitled (Workspace) - Visual Studio Code [Adminis	×
ſJ1	EXPLORER ····	JS TnxValid.js JS jsBlockchain.js JS jsBlockchainex.js •	□ …
	✓ UNTITLED (WORKSPACE)	blockchainlab > JS isBlockchainex.is >	
Q	DigitalSignatureDe	49	IBEin
	<sup>JS</sup> Hello.js	<pre>50 let myBlockchain = new Blockchain();</pre>	IBS::
90	JS jsBlockchain.js	51 myBlockchain.addBlock(block1);	PLETE STATE
	<sup>JS</sup> jsBlockchainex.js	52 myblockchain.addblock(block2);	NONC
~	MessageDigest2.class	PROBLEMS 8 OUTPUT DEBUG CONSOLE TERMINAL	$+ \cdot \cdot \times$
₫ <sup>&gt;</sup>	MessageDigest 1		> powershell
	MessageDigestEncD	"index": 2,	c node
БЧ	MessageDigestEncD	"timestamp": "21/11/2021",	> powershell
	<pre>{} package-lock.json</pre>	"data": "Second Block",	10
因	{} package.json	previousnasn : bedaca4tbce064t4baddet/9203a740943a7eaeaata4 39c56cdba04a708038aa"	
	PrivateKeyDemo.class	"hash": "b5d6302a69a8fe67bd6d08cd7a86b970c330b10dfb8dd98cc3e9	
		b4faa761a3f2"	
	@] SHA256	},	
	∨ 😫 Block	i "index": 3	
$\bigcirc$	constructor	"timestamp": "14/05/2021",	
8	🛇 calculateHash	"data": "Third Block",	
~h	∨ 🕾 Blockchain	"previoushash": "b5d6302a69a8fe67bd6d08cd7a86b970c330b10dfb8d	
521		d98cc3e9D4taa/6la3t2", "hash": "46f1a9h836af3fc17a4a953dd8ha34a01fe50h90d708261hche8	
⊗ 6.	A 2	Ln 51, Col 31 Spaces: 4 UTF-8 CRLF {} JavaSc	ript 🛆 🗟 🕻
	ନ o 🖽 👯 🦏 🦧	🛛 📅 📕 Blochain 🕐 🔎 👼, 🌀 🙆 🎹 const SHA 🚻 Blockchain 🔊 • jsBlockc 🔨 =d 🖭 C	(//. ↓)) ♥ ENG 09:46 22-12-2021

## Prog. 2 Steps for Blockchain program compiling and running using Truffle DApp program using Metamask

- 1) Open the Ganach
- 2) Open Sublimetext3 editor
- 3) create the folder contest1
- 4) install the truffle in the directory F:/>contest1>npm install truffle -g

#### 5) Make the contract Election.sol using Solidity Program



5

🔰 pragr	ma solidity • (contest1) - Sublime Text (UNREGISTE	RED)			- 8 ×
File Ed	lit Selection Find View Goto Tools Proj	ect Preferences Help			
FOLD	contest1	olidity •	- • • • •		
=	Microsoft Solitaire Collection	ilon		game	
	Microsoft Store		FC Bank	antiny 1	
	Tjji Microsoft Teams	Wednesday Off			
	Microsoft Whiteboard	1			
	💮 Mixed Reality Portal	Ma	il 99+	Xbox Console Photos	
	mysql 🗸		-		
			U	S	
	NetBeans ~	Paint 3D Off	īce	Films & TV Groove Music Skype	
	🛅 Node.js 🛛 🔿	Explore			
	Install Additional Tools for Node.js			1	
	Node.js		e	>	
	Node.js command promot	Microsoft Store	Microsoft Edge		
۲	-⇔ Pin to Start		C. C. M. C. L.		
<b>D</b>	More Node.is website		-⊐⊐ Pin to taskbar		
	Uninstall		🗟 Run as administrator		
			D Open file location		
ሐ	Notepad++				
~					
٢	Office	$\langle \rangle$	* 9		Tab Size: 4 Plain Text
	<u>به</u> 🕸 😫 o	M 🖬 🖿	O 2 (00 Googl	e 🔘 🚺 Meet – 🎹 Docum 🌧 Ganad	he 🍠 pragma 🔨 🖬 🌡 🌈 🕼 🗰 ENG 09:15

#### **7)** f:



#### 8) Check the truffle version



#### 9) Write Solidity Program



7

#### 10) Configure the deployment files in migration folder





F:\contest1\migrations\2\_deploy\_election.js (contest1) - Sublime Text (UNREGISTERED)

- 0 ×





13) Deploy the contract on blockchain network i.e. Ganache localhost blockchain







pragma solidity 0.4.24;

```
contract Election
{
      struct Candidate
      {
        uint id;
        string name;
        uint voteCount;
      } // this is store candidate information
        // Fetch candidate information using
        // reference variable
        mapping(uint => Candidate) public candidate;
        //variable for vote counting
        uint public candidateCount;
     //constructor
      function Election() public
      {
        addCandidate("Sourabh");
        addCandidate("Neeta");
      }
```

```
// define addcandidate function
function addCandidate(string memory _name)private
{
    candidateCount++;
    candidate[candidateCount] = Candidate(candidateCount,_name,0);
}
```

14) Recompile the same Election contract





**15)** Deploy the Contract over the Ethereum Ganach





#### 16) Fetching candidate



#### 17) Fetch Individual Ganache node address

📱 🔤 Administrator: C\WINDOWS\system32\cmd.exe - "node" "C:\Users\Vikram\AppData\Roaming\npm\\node_modules\truffle\build\cli.bundled.js" console	2 <u>—</u> 2		×
'0x4ce61e0a1f478234b64f46357424d7b0b6145804',			^
'0x6ad6a00b1c275baec3091ecc0a8bc38a21d75ebe',			
'0x877d120552525ef6835e196183d1e71dc0c27d99',			
'0xc0e570a46cc3555400e96c4727d4b9175e4afccc',			In the second se
'0x99381135f7f11e23132852be8bbbe491e42574dd',			
'0x17921e1c0e6d9e1bea0c4524f36c8f54ba190e2f'			
]			
<pre>truffle(development)&gt; web3.eth.accounts[4]</pre>			
'0x4ce61e0a1f478234b64f46357424d7b0b6145804'			
<pre>truffle(development)&gt;</pre>			
'0x31e489dac46e9f1cb2cf73b2b401cbac2f879b65',			
'0xbac19d44e4659c31f61f4f63699f0e3f28074999',			11
'0x1a9b2628957b15b1a78b3bc50438ba42554100aa',			
'0x4ce61e0a1f478234b64f46357424d7b0b6145804',			
'0x6ad6a00b1c275baec3091ecc0a8bc38a21d75ebe',			
'0x877d120552525ef6835e196183d1e71dc0c27d99',			
'0xc0e570a46cc3555400e96c4727d4b9175e4afccc',			
'0x99381135f7f11e23132852be8bbbe491e42574dd',			
'0x17921e1c0e6d9e1bea0c4524f36c8f54ba190e2f'			~
- 第 - ハ O は ジ 湾 《 🖄 🛱 🖡 migr 🕐 ル 👼 😡 🕼 Mee 💯 Doc 会 Gan ≶ Fitc 🔤 Ad ^ 三q 🗉 🌡 🧟 da	😫 EN	G 09:4	19 2021

18) Open the two library files to deploy contract on Ethereum

#### >> a) https://mochajs.org

#### **b)** www.chaijs.com

Here Mocha is a feature-rich JavaScript test framework running on Node.js and in the browser, making asynchronous testing. Assertion Library: Chai – Chai is a BDD/TDD assertion library for[node](http://nodejs.org) and browser that can be paired with it In the Test folder we have to create election.js file in sublimetext3



const Election = artifacts.require("./Election.sol"); require('chai').use(require('chai-as-promised')).should();

contract("Election",function(accounts){it("initialize with two candidate",function(){return Election.deployed().
then(function(instance){return instance.candidateCount();}).then(function(count){assert.equal(count,2);}));});



### Prog. 3 MetaMask Configuration Steps and Transaction

G Google	K 💓 MetaMask 🗙	+					0	-	٥	×
← → C ① ♠ MetaMas	k   chrome-extension://nkbihfbeogaea	oehlefnkodbefgpgknn/home.html#			7	2 ©	10 D	м	* 0	÷
	🐹 METAMASK			Ropsten Test Network						Î
		Account 1			:					1
		(A)								
		1671								
		Buy Send	Swap							
	Asset	s	A	Activity						
	🔶 1 ЕТН				>					
		Don't see your tok Import tokens	ien?							
		Need help? Contact Meta	Mask Support	Backup your Secret Recove	ry Phrase t	o keep your	wallet an	id funds	secure.	
		II meet.google.com is sharing your screen	. Stop sharing Hid	•			E	Backup	now	
🚛 🔎 O 🖽 😻	考《 🖬 🔒 🛤 (	🕨 🔎 👼 🌀 meet.goo 🧿	MetaMas 🔘 🕻	👔 Meet – xri 🗰 Documen	_ ^ ≣⊲	• <b>\$</b> Į	Q (i.	<b>₫</b> #) EN	NG 12-10	:39 -2021
							-		40	~
G Google :	K MetaMask X	+			,	2 0	<b>०</b> स्टब	-	ہ * Ø	×
G Google ← → C ☆ ♣ MetaMat	MetaMask X     Chrome-extension://nkbihfbeogaea	+ behlefnkodbefgpgknn/home.html#			,	¥ ©	0 2 0	- M	5 * Ø	× :
G Google ← → C 介 ♠ MetaMat	MetaMask x  chrome-extension://nkbihfbeogaea  METAMASK	+ behlefnkodbefgpgknn/home.html#		Ropsten Test Network	,	¥ @	0 5 5	-	5 * 🔇	× :
G Google ← → C 介 ★ MetaMa	MetaMask × chrome-extension://nkbihfbeogaea	+ behlefnkodbefgpgknn/home.html# Account 1 Dxs347003 ©		Ropsten Test Network	, ) ;	¥ ©	0 2 0	- 10	° ★ ♥	×
G Google ← → C û ♠ MetaMar	MetaMask x      chrome-extension://nkbihfbeogaear      METAMASK	+ behlefnkodbefgpgknn/home.html# Account 1 Dx6347e043 T		Ropsten Test Network	7 () i Ac	ک 🕲	o ta ns	-	° ★ ♥	×
G Google : ← → C 介 ★ MetaMa	MetaMask ×     chrome-extension://nkbihfbeogaeau     METAMASK	+ behlefnkodbefgpgknn/home.html# Account 1 Dx6347e063 © () 1 FTH		Ropsten Test Network V	3 ()) : [Ac	2 Sout Optio	o s ns	-	♂ ★ ♥	×
G Google ← → C û ♠ MetaMa	MetaMask x      chrome-extension://nkbihfbeogaear      METAMASK	+ behlefnkodbefgpgknr/home.html# Account 1 Dx6347e039 1 ETH		Ropsten Test Network		ک کی	0 5 10	- 10	5 * 🔇	×
G Google ← → C ☆ ★ MetaMas	MetaMask x      chrome-extension://nkbihfbeogaear      METAMASK	+ behlefnkodbefgpgknr/home.html# Account 1 Dx6347_e069 D E E E H E E H	( Swap	Ropsten Test Network	: Ac	★ ●	ns.	- 10	¤ ★ ♥	×
G Google	MetaMask ×  chrome-extension://nkbihfbeogaeae  METAMASK  Asset	+ behlefnkadbefgpgknr/home.html# Account 1 Dx6347_e063 © IETH We by Sed	( Swap	Ropsten Test Network	3 : Ac	count Optio	o o o	- M	5 * 0	×
G Google	MetaMask x chrome-extension://nkbihfbeogaea METAMASK  METAMASK  Asset	+ behlefnkodbefgpgknn/home.html# DxdS47e0d3	E Swap	Ropsten Test Network	, i Ac	count Optio	ns	- M	°	×
G Google	MetaMask x chrome-extension://nkbihfbeogaeae METAMASK Asset	+ behlefnkadbefgpgknr/home.html# Dx8347_e083	( ) Swop A	Ropsten Test Network	x Acc	Count Optio	<b>○</b>		o * 0	×
G Google ← → C û  MetaMaa	MetaMask x chrome-extension://nkbihfbeogaea METAMASK Asset	+ behlefnkodbefgpgknn/home.html# Account 1 Dx8347e083 © IETH Buy 2 Send s Don't see your tok Import tokens	swap swap	Ropsten Test Network	i Accertain	count Optio	ss.	- Mit (	о * 0	×
G Google	MetaMask x      chrome-extension://nkbihfbeogaeae      METAMASK      Asset	+ behlefnkodbefgpgknr/home.html# Account 1 Dod347e039 IETH W Buy 2 Send s Dorft see your tok Import tokens Need help? Contact Meta	een?	Ropsten Test Network	I Acc	count Optio	vallet an	- M	0 * 0 secure. (	×I
G Google ← → C ♪	MetaMask x      chrome-extension://nkbihfbeogaeau      METAMASK      Asset      IETH	+ behlefnkodbefgpgknn/home.html# Account 1 Dx8347e083 © IETH @ Buy 20 Send s Don't see your tok Import tokens Need help? Contact Meta I meetgoogle.com is sharing your screen	swop A sen? Mask Support Stop sharing Hild	Ropsten Test Network       Activity     Bockup your Secret Recover	i Acception of the second seco	count Optio	wallet an	ad funds	secure.	

G Google X	🗱 MetaMask	× +		• - • ×
← → C ☆ 🏞 MetaMask	chrome-extension://nkbihfbeog	gaeaoehlefnkodbefgpgknn/home.html#	\$	
	METAMASK		Ropsten Test Network	Î
		Account 1	1	
		0xe34/e0a31	## Account details	
		٠	🖉 View on Etherscan	
		1ETH	Ocnnected sites	
				_
		Buy Send Swap		
			Antility	
			Activity	
	• 1 ETH		>	
		Don't see your token?		
		Import tokens	Backup your Secret Recovery Phrase to keep	o your wallet and funds secure. 🕕
		Need help? Contact MetaMask Support		Backup now
		meet.google.com is sharing your screen. Stop sharing	Hide	
📰 🔎 O 🗄 🗱	🧠 🔍 🖬 🖬	🗖 😕 🚌 🖓 meet.goo 🖓 MetaMas 🔇		🔁 📕 🔯 🌈 🕼 ENG 🕺 12:40
	_	337	Meet - xri W Documen A = 🕁 📼 🕏	12-10-2021
G Google X	📷 MetaMask	x +	🔤 🛄 Meet-xri — 🚻 Documen 🧄 🧃 🖬 🤅	• - • ×
G Google x ← → C ☆ MetaMask	WetaMask	x + gaeaoehlefnkodbefgpgknn/home.html#	© Meet-xri W Documen ∧ =q HD t	• - ○ × • ± • ₩ ★ ♥ :
G Google x ← → C ♪ MetaMask	MetaMask	X +	Meet-xri W Document A = ( B) (	⊙ - ○ × ⊙ ≝ ∅ ₩ ♣ ♥ :
G Google x ← → C û ♠ MetaMask	MetaMask chrome-extension://nkbihfbeog METAMASK	x + gaeaoehlefnkodbefgpgknn/home.html#	Meet-xri Wig Document ∧ =i( IB) t ☆	0 - 5 × ⊙ 5 € 6 M ★ 0 :
G Google X ← → C û ♠ MetaMask	MetaMask chrome-extension://nkbihfbeog	x + gaeaoehlefnkodbefgpgknn/home.html#	Met-xti  Met-x	(2-10-24) ⊙ - 0 × ⊙ ± 0 M ★ () :
G Google x ← → C û ♠ MetaMask	MetaMask   chrome-extension://nkbihfbeog	x + gaesoehlefnkodbefgpgknn/home.html# Sweetu	Meet-xri W Document ∧ = ( ■) (	● 1
G Google x ← → C ☆ ★ MetaMask	MetaMask chrome-extension://nkbihfbeoc	x + gaeaoehlefnkodbefgpgknn/home.html# Sweetu	Met-xri W Documen ∧ = ( ■) ( ☆ ) • Ropsten Test Network ∨ )	o - o × ⊙ ± ø m * 0 :
G Google X ← → C ♪ MetaMask	MetaMask chrome-extension://nkbihfbeog	x + yaeaoehlefnkodbefgpgknn/home.html# Sweetu	Met-xri. W Document. A = 1 ID t	© - 0 × © ⊈ 0 M ★ ♥ :
G Google X ← → C ♪ MetaMask	MetaMask   chrome-extension://nkbihfbeog	x + yaeaoehiefnkodbefgpgknr/home.html#	Met-xti  Met	© - 0 × © ⊈ 6 M ≉ ♥ :
G Google X ← → C ☆ ★ MetaMask	MetaMask chrome-extension://nkbihfbeog	x + yaeaoehlefnkodbefgpgknr/home.html# Sweetu	Met-xri. W Documen. ∧ = i ■ t ★ Ropsten Test Network → :	● - ♂ × ● I
G Google X ← → C A ★ MetaMask	MetaMask chrome-extension://nkbihfbeog	x + paeaoehlefnkodbefgpgknr/home.html#  Sweetu  Cx63472B55544115F624234cA94c6EDE2	Met-xri. W Document. A T III III	© - 0 × ⊙ - 0 ×
G Google X ← → C ♪ MetaMask	MetaMask chrome-extension://nkbihfbeog	x + yaesoehiefnkodbefgpgknr/home.html# Swestu Swestu Ox6947285554415F624234cA94c6EDE2 ssets View on Etherson	Met-xri. W Document. A R I I I I I I I I I I I I I I I I I I	© - 0 × © ⊈ 6 M ≉ ♥ :
G Google X ← → C û ★ MetaMask	MetaMask chrome-extension://nkbihfbeog	x + yaeaoehlefnkodbefgpgknr/home.html# Sweetu Sweetu Dx6947285564415F624234cA94c6EDE2 Sesets View on Etherscon	Met-xiii W Document A = 1 = 1	
G Google X	MetaMask chrome-extension://nkbihfbeog	x + yaeaoehlefnkodbefgpgknr/home.html#  Sweetu  Sweetu  Cx63472B5564415F624234cA94c6EDE2_  Sasets  View on Etherscon  Export Private Key	Met-xii. W Document. A R R R R R R R R R R R R R R R R R R	
G Google × ← → C ♪ MetaMask	MetaMask chrome-extension://nkbihfbeog METAMASK A A 1ETH	x + paesoehlefnkodbefgpgknr/home.html#  Swestu  Swestu  Swestu  Dx6347285564415F624234cA94c6E0E2  Ssets  View on Etherscon  Export Private Key  Import tokens	Met-xiii W Documenti A I I I I I I I I I I I I I I I I I I	
G Google x	MetaMask chrome-extension://nkbihfbeog	x + paeaoehlefnkodbefgpgknr/home.html#  Sweetu  Sweetu  Sweetu  Sweetu  View on Etherscon  Export Private Key  Import tokens  Need help? Contact MetaMask Support	Meet-xri. W Document. A T I I I I I I I I I I I I I I I I I I	C C C C C C C C C C C C C C C C C C C
G Google × ← → C ♪ MetaMask	MetaMask chrome-extension://nkbihfbeog METAMASK A A 1ETH	x +  paesoehiefnkodbefgpgknr/home.html#  Sweetu  Sweetu  Sweetu  View on Etherscon Export Private Key  Import tokens  Neeed help? Contact MetaMask Support  I metgoogle.com is sharing your screen. Stop during	Met-xiii W Documenti A T(10)	> your wallet and funds secure.

G Google X	💓 MetaMask 🛛 🗙	+			0	-	Ø	×
← → C ① 🏞 MetaMask	chrome-extension://nkbihfbeogaeao	ehlefnkodbefgpgknn/home.html#	\$	0	题 (	6 M	* 0	
	METAMASK	Ropsten Test Network						
		K Back X Account 1	i					
		0x83472B5564415F624234cA94c6E0E2						
		Show Private Keys Type your MetaMask password						
	Assets	Warning: Never disclose this key. Anyone with Activity your private keys can steal any assets held in your account.						
	🔶 1етн	Cancel	>					
		Import tokens Backup your Secret Recove	ery Phrase to	keep you	r wallet	and fund	s secure.	0
		Need help? Contact MetaMask Support II meetgoogle.com is sharing your screen. Stop sharing Hide			C	Backu	p now	
# P O # <b>\$</b>	🦔 🚳 🖬 💼 🕅	🕨 🔎 👩 meet.goo 🌀 MetaMas 🚫 🖪 Meet - xri 🎹 Documen	. ∧ ≣d (	• • •	Q	<i>低</i> (1)) 1	NG 12-	12:40

b84ced9f4968a896a38de6828be39f2811b9ce6109253b8509d17ee33fa4ff44

G Google X	MetaMask × +	0	-	o ×
← → C ① 🏞 MetaMask	chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#	050	10 24	<b>V</b> :
	METAMASK RinkebyTest Network V			Í
	Account 1			
	۲			
	OETH			
	Buy Send Swap			
	Assets Activity			
	• 0 ETH >			
	Don't see your token? Import tokens			
	Need help? Contact MetaMask Support			
	II meet.google.com is sharing your screen. Stop sharing Hide			
🖬 🔎 O 🛱 👯	🦔 🦚 🖻 🖶 💽 🔎 🖟 🧓 🞯 meet.goo 🞯 MetaMas 🕲 🗋 Meet - xri 🚻 Documen 🔿 🕫	• <b>\$ \$ Q</b> #	dが) ENG	12:42 12-10-2021



0x63472B5564415F624234cA94c6E0E24786bce063

0x63472B5564415F624234cA94c6E0E24786bce063

0x63472b5564415f624234ca94c6e0e24786bce063

b84 ced 9f 4968 a 896 a 38 de 6828 be 39f 2811 b 9 ce 6109253 b 8509 d 17 ee 33 fa 4ff 44 be a 1000 be a 10000 be a 1000 be a 10000 be a 1000 be a 1000 be



G Google X	WetaMask x +			¢	) –	٥	×
← → C ☆ MetaMask	chrome-extension://nkbihfbeogaeaoehlefnkodbefgpgknn/home.html#		☆ ©	1	6 M	* 🛛	) :
	METAMASK   Ropsten Test Network		)				Î
	Account 1 0x6347e043 🗅	i					1
	۲						
	2.4998 ETH						
	Buy Send Swap						
	Assets Activity						
	Send Oct 12 - Tot 0xee3b99fl	3 ETH -3 ETH					
	Cet 12 - From: 0x3a6002b5     Bookup your Secret Record	very Phras	e to keep y	our wallet	and fund	s secure.	0
	Send     Oct 12 - To: Dxee/d00d9     II meetgoogle.com is sharing your screen. Stop sharing Hide	BETH			Backu	p now	
🚛 🔎 O 🖽 😻	🧠 🦚 🔛 💼 🗟 🖉 🔎 🖉 🧓 🎯 meet.goo 🎯 MetaMas 🙆 💽 Meet - xri 🎹 Documer	n ∧ ≡	4 o 4	I Q	<i>侃</i> (小)) E	ING 12-1	3:34 0-2021
G Google X	₩ MetaMask x S Test Ether Faucet x +			G		٥	×
← → ♂ ☆ ⓐ faucet.meta	imaskio		☆ ©	) (S	6 M	* 0	) :
MetaMask Eth	er Faucet						Â
faucet							
address: 0x81b7e08 balance: request 1 ether fr	3165bdf5648606c89998a9cc8164397647 om faucet						
user							
address: 0x63472b6 balance: donate to faucet: 1 ether 10 et	5564415f624234ca94c6e0e24786bce063						
transactions	3						
	II meet.google.com is sharing your screen. Stop sharing Hide					4	* 335
🖬 🔎 🔿 🖽 🐯	🧠 📽 🔛 🧰 🖪 🕐 🖉 1999, 🞯 meet.goo 🕥 Test Ether 🕥 🗂 Meet - xri 🎹 Documer	···· ^ =	a 🖸 🏶	Ų Q	<i>備</i> (4)) E	NG 12-1	0-2021

G Google X	🗱 MetaMask	K 🔇 Test Ether Faucet	× +			0	-	٥	×
← → C △ ■ faucet.metal	masklio				☆ ©	10 e	м	* 0	
MetaMask Eth	er Faucet								
faucet									
address: 0x81b7e08	f65bdf5648606c89998a9cc8164397	647							
balance: 83417675.6	2 ether								
request 1 ether fro	om faucet								
user									
address: 0x63472b5 balance: 2.50 ether	564415f624234ca94c6e0e24786bc	2063							
donate to faucet:	tos 100 albos								
1 einer 10 ein	ner 100 etner								
transactions									
		II meet.google.com is sharing your sc	reen. Stop sharing	Hide					
🖬 🔎 O 🖽 🐯	🧟 🥰 🖬 🛗 🛤	💽 🏓 🛐 🖓 meet.goo	🌀 Test Ether 🔘	C Meet - xri W Documen 🔨	t 🖸 🗘 🕯	<b>Q</b> (i.	(\$1) E	NG 12-1	13:35 10-2021
G Google X	MetaMask	K 🙆 Test Ether Faucet	× MetaMask	x   +		0	_	Ø	×
← → C ☆ MetaMask	chrome-extension://nkbihfbeogae	aoehlefnkodbefgpgknn/home.html#	1		\$ ©	5 6	м	* 0	
		0x6347e06	30	1					^
		۲							1
		4.8998	ETH						. 1
									. 1
		Buy Send	Swap						. 1
		**		A set inter					. 1
	Asse			Activity	-				. 1
	Receive     Oct 12 - From: 0x3a6002b6			1 ETH					
	Receive     Oct 12 - From: 0xee7d00ds			0.4 ETH					
	Receive     Oct 12 - From: 0x81b77647			1 ETH				_	_
				Backup your Secret Recovery Phra	se to keep you	ır wallet ar	nd fund:	s secure.	0
	Send Oct 12 - To: Oxee3b998	II meet.google.com is sharing your sc	reen. Stop sharing	Hide		I	Backup	o now	
🖬 🔎 O 🖽 😻	<b>4</b> 4 1 <b>1 1</b>	2 5 199+ 0 meet.goo	MetaMas	🔲 Meet – xri 🗰 Documen 🔿	4 io 🕄 i	. Q <i>(i</i> .	(⊈#) E	NG 12-1	13:39

G Google X	MetaMask X	Test Ether F	aucet ×	🐹 MetaMask		×   +			0	-	٥	×
← → C ⚠ ♠ MetaMask	chrome-extension://nkbihfbeogaeao	ehlefnkodbefgp	gknn/home.html#send				☆	0 :	5 6	ы	* 0	
	💓 METAMASK				(	Ropsten Test Network 🗸						
		Send Cancel			ncel							
		Oxee3b99FI X			×							
		New address book.	a detected! Click here to a	add to your address								
		New address detected! Click here to add to your address   book.     Asset:    ETH    Balance: 4.89982! ETH     Amount:   0   ETH   Max   No Conversion Rate Available     Max     Not     Max     Not     Max     O ETH   No Conversion Rate Available     Max     Not     Metal Max     Not										
		Amount: Max	0 ETH No Conversion Rate A	Available	†,							
		Il meet.google.	com is sharing your screen.	Stop sharing	Hide							
	<b></b>	. 11 📾	meet.goo	MetaMas		Meet-xri M Documen	~ R 🗉		0 6	da) E	NG <sup>1</sup>	13:39
		99-				_					12-	10-2021
G Google X	MetaMask X	Test Ether F	aucet ×	1 MetaMask		×   +			0	-	٥	×
← → C ☆ 🏞 MetaMask	chrome-extension://nkbihfbeogaeao	ehlefnkodbefgp	gknn/home.html#send				☆	•	5 6	ы	* 0	) :
	💓 METAMASK				(	Ropsten Test Network 🗸						
			Send	Ca	ncel							
		Amount: No Conversion Rate Available Text there faced: X Text the										
		New address book.	a detected! Click here to a	add to your address								
		Asset:	ETH Balance: 6.7991	1821 ETH								
		Amount:	1.5 ETH No Conversion Rate A	Available	†,							
meet.google.com is sharing your screen.	Stop sharing Hide											
		Ca	ncel	Next								
🖬 🔎 O 🖽 😻	49 49 🖬 🖻 🖄 🕅	وم ۲	g meet.goo 9	) MetaMas		Meet – xri 🚻 Documen	^ ⁼⊲ ⊑	t (	Q (1.	<b>₫</b> )) E	NG 12-	13:40 10-2021

G Google X	💓 MetaMask 🛛 🗙	Test Ether Faucet	🗙   🗱 MetaMask	×   +			0	-	٥	×
← → C ☆ 🏞 MetaMask	chrome-extension://nkbihfbeogaeao	ehlefnkodbefgpgknn/home.htm	l#confirm-transaction/8983695	232839229/send-ether	☆	•	6	16 s	• •	÷
	📰 METAMASK			Ropsten Test Network						
		K Edit								
		Account 1	→ ● 0xee3b99F1							
		New address detected! Click book.	here to add to your address							
		SENDING ETH								
		<b>♦</b> 1.5								
		Estimated gas fee Likely in < 30 seconds	EDIT 0.000032 0.000032 ETH Max fee: 0.000032 ETH							
meet.google.com is sharing your screen.	Stop sharing Hide	<b>Total</b> Amount + gas fee	1.500032 <b>1.500032 ETH</b> Max amount: 1.500032 ETH							
		Reject	Confirm							
🔳 🔎 O 🖽 😻	4 4 N A R C	D D meet.goo	🕥 MetaMas 🔘 🖸	Meet – xri 🗰 Documen	^ ⁼⊲ ⊡		a la	(↓)) EN(	3 13	:40
									12-10	LOLI
G Google X	💓 MetaMask 🗙 🗙	Test Ether Faucet	🗙   🐹 MetaMask	×   +			0	-	٥	×
← → C ① ♠ MetaMask	chrome-extension://nkbihfbeogaeao	ehlefnkodbefgpgknn/home.htm	l#confirm-transaction/8983695	232839229/send-ether	☆	0 5	ø	M 1	• •	:
	💓 METAMASK			Ropsten Test Network						
		K Edit								
		Account1	→ Oxee3b99F1							
		New address detected! Click book.	here to add to your address							
		SENDING ETH								
		<b>♦</b> 1.5								
		Estimated gas fee (6) Very likely in < 15 seconds	EDIT 0.000042 0.000042 ETH Max fee: 0.000042 ETH							
meet.google.com is sharing your screen.	Stop sharing Hide	Total	1.500042 1.500042 ETH							
		Amount + gas fee	Max amount: 1,500042 ETH							
		Reject								
🖷 🔎 O 🖽 👯	🤻 < 🖬 🖻 🗖	🕨 🔏 🤴 Meet.goo	🕥 MetaMas 🕥 🖸	Meet – xri 🚻 Documen	^ ⁼⊲ ⊡ (		ı <i>li</i> .	¢0) EN(	3 13 12-10	:40 1-2021

G Google X	🗱 MetaMask 🛛 🗙	Test Ether Faucet	×	MetaMask		×   +			0	-	٥	×
← → C ☆ 🏞 MetaMask	chrome-extension://nkbihfbeogaeaoe	hlefnkodbefgpgknn/hom	e.html#				\$ 0	) C	6	10 1	• •	:
		Oxe	6347e063 [	i i		1						^
			۲									
		5.29	998 E	ТН								1
		Buy	Send	CD Swap								
	Assets				Activity							
	Send Oct 12 - To: 0xee3b99fl					-1.5 ETH -1.5 ETH						1
	(1) Receive Oct 12 · From: 0x3a6002b5					<b>1.9 ETH</b> 1.9 ETH						
meet.google.com is sharing your screen.	Stop sharing Hide Oct 12 - From: 0x3a6002b5				Backu	1 ETH p your Secret Recovery Phras	e to keep y	your wal	let and	l funds s	ecure.	0
	(±) Receive Oct 12 - From: 0xee7d00d9					0.4 ETH 0.4 ETH			Вс	ackup r	now	D
🔳 २ ० 🖽 😻	🧟 🧠 🖬 🖻 🛤 🖸	🕨 🔎 📷 😡 me	et.goo	🕽 MetaMas 🔘	Meet - xri	i 🎹 Documen 🤿 🗉	4 🗆 📢		1	\$1) EN(	3 12-10	40 -2021

## Prog. 4 Blockchain Cryptography Program using Java

```
import java.security.*; import javax.crypto.*;
/* Use of Private Key in Encryption*/
public class PrivateKeyDemo
{
      static Key key;
      static Cipher cipher;
      static String algorithm = "AES";
      public static void main(String args[]) throws Exception
{
      key = KeyGenerator.getInstance(algorithm).generateKey();
      cipher = Cipher.getInstance(algorithm);
      String text = "FYMCA 2020 Batch Hiray College";
      byte[] encryptionBytes = encrypt(text);
      System.out.println("Original Text: "+text);
      System.out.println("Key: "+key.toString());
      System.out.println("Encrypted Text: "+encrypt(text));
      System.out.println("Decrypted Text: "+decrypt(encryptionBytes));
} // End of Main Method
public static byte[] encrypt(String input) throws Exception
{
      cipher.init(Cipher.ENCRYPT_MODE, key);
      byte [] inputBytes = input.getBytes();
      return cipher.doFinal(inputBytes);
} // close of encrypt method
public static String decrypt(byte[] encryptionBytes) throws Exception
{
      cipher.init(Cipher.DECRYPT MODE, key);
      byte[] convertDecrypt = cipher.doFinal(encryptionBytes);
      String convertString = new String(convertDecrypt);
      return convertString;
} // close decrypt method
```

```
}
```

#### Output:



## Prog. 5 Blockchain Public Key Cryptography

```
import java.security.*;
import javax.crypto.*;
import java.util.*;
// Public Key Example
public class PublicKeyDemo
{
      static KeyPair keyPair;
      static String algorithm = "RSA";
      public static void main(String args[]) throws Exception
{
      KeyPairGenerator keyPairGenerator = KeyPairGenerator.getInstance(algorithm);
      keyPairGenerator.initialize(512);
      keyPair = keyPairGenerator.generateKeyPair();
      Cipher cipher = Cipher.getInstance(algorithm);
      String text = " University of Mumbai";
      System.out.println("Public Keys is: "+keyPair.getPublic().toString());
      System.out.println("Private Key is: "+keyPair.getPrivate().toString());
      System.out.println(" "+text);
      // Encrypt the text
      cipher.init(Cipher.ENCRYPT MODE, keyPair.getPublic());
      byte[] encryptedText = cipher.doFinal(text.getBytes());
      String ciphertext = new String(Base64.getEncoder().encode(encryptedText));
      System.out.println("Encrypted Text is: "+ciphertext);
      // Decryption using Private key
      cipher.init(Cipher.DECRYPT_MODE, keyPair.getPrivate());
      byte[] ciphertextByte = Base64.getDecoder().decode(ciphertext.getBytes()); byte[] decryptedByte = cipher.
      doFinal(ciphertextByte);
      String decryptedString = new String(decryptedByte);
      System.out.println("After decryption text is:"+decryptedString);
}
}
```

Output:

W	Blockchain_Lab_Journal - Microsoft Word (Product Activation Failed)	7 <u>-</u> 3		×
File Home Insert Page Layout References Mailings Review	View Developer		1000	0
Administrator: C:\Windows\System32\cmd.exe		-		×
F:\blockchainlab>javac Public	KeyDemo.java			
F:\blockchainlab≻java PublicK	CeyDemo			
Public Kevs is: Sun RSA publ	ic kev. 512 bits			
modulus: 881763915439200829	3467420091018195379192334493030777367663572	102	921	5
20126261724220214765220200407	20072115551010101010101010101010101000000000	125	:10	
36220301724223314703333330437	00/544555/10222500152501525/1051/0255554/70	тэ-	40	
031153831				
public exponent: 65537				
Private Key is: sun.security.	rsa.RSAPrivateCrtKeyImpl@c1a			
University of Mumbai				
Encrypted Text is: XGU4YEZCpT	3U+C2Jy1u8TfIeWhEx2HaTHeoCiBBLNGNVwQtsGoj6t	lfr	·kS'	Т
0U0fXkZEuIBaeVh/NRtRtvYNPPw==				
After decryption text is Uni	versity of Mumbai			
Arter deeryption text ist oni	versity of Humber			
C.\				
F:\DIOCKCNalnlad>				Į.
📹 🔎 O 🖽 😻 🧠 🚳 💼 File Exp	🕐 🗵 🚋 😡 🕵 🎹 Micros 刘 • Block 🔤 Admini 🥒 Private 🔨 🖬 Q 🌾 40)	🔹 EN	G 10 22-1	):54 2-2021