PRACTICAL NO. 4

Ethereum

Aim: To develop and deploy Dapp in Ethereum.

Ethereum: [1]

- Ethereum is a decentralized, open-source blockchain with smart contract functionality.
- Ether (ETH or Ξ) is the native cryptocurrency of the platform.
- Amongst cryptocurrencies, Ether is second only to Bitcoin in market capitalization.

Ethereum Virtual Machine (EVM): [1]

- The Ethereum Virtual Machine (EVM) is the runtime environment for transaction execution in Ethereum.

Ether: [1]

- Ether (ETH): Ether (ETH) is the cryptocurrency generated by the Ethereum protocol as a reward to miners in a proof-of-work system for adding blocks to the blockchain.
- It is the only currency accepted in the payment of transaction fees, which also go to miners.

Ether: [1]

- The block reward together with the transaction fees provide the incentive to miners to keep the blockchain growing (i.e. to keep processing new transactions).
- Therefore, ETH is fundamental to the operation of the network. Each Ethereum account has an ETH balance and may send ETH to any other account. The smallest subunit of ETH is known as a Wei and is equal to 10^{-18} ETH.

Accounts: [1]

- There are two types of accounts on Ethereum: user accounts (also known as externally-owned accounts) and contracts.
- Both types have an ETH balance, may send ETH to any account, may call any public function of a contract or create a new contract, and are identified on the blockchain and in the state by their address.

Gas: What is Gas in Ethereum? :

- Gas is a unit of account within the EVM used in the calculation of a transaction fee, which is the amount of ETH a transaction's sender must pay to the miner who includes the transaction in the blockchain. [1]
- The transaction fee is calculated in Gas, and paid for in Ether.
- The gas is the "fuel" of the Ethereum network, which is used to:
    - Conduct transactions
    - Execute smart contracts
    - Launch Dapps.
- Gas indicates the fee for a particular action or transaction.
- **Gas Limit:** is the maximum amount of Gas that a user is willing to pay for performing this action or confirming a transaction.
- **Gas Price:** is the amount that the user is willing to spend on each unit of Gas.

MetaMask: [2] 

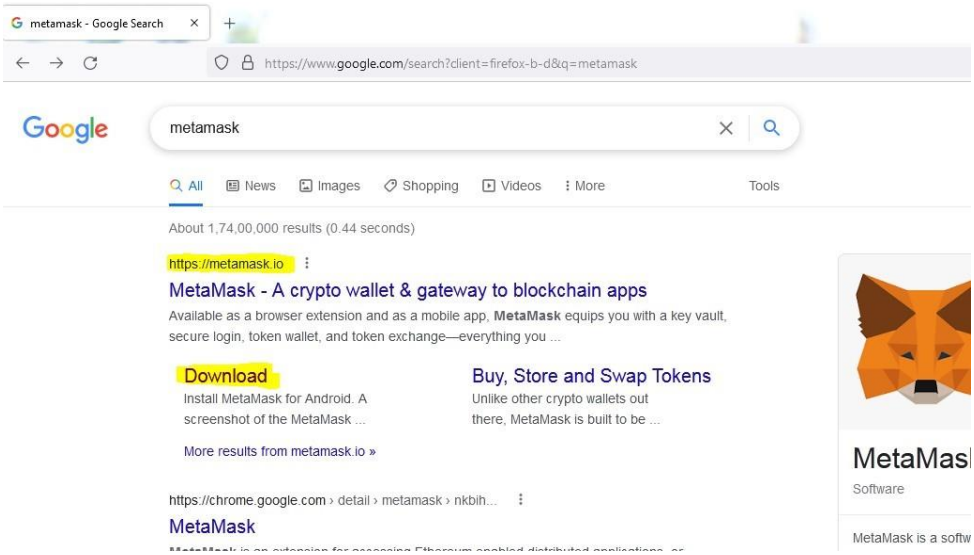
- MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain.
- It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications(Dapps).
- MetaMask is developed by ConsenSys Software Inc., a blockchain software company focusing on Ethereum-based tools and infrastructure.
- MetaMask allows users to store and manage account keys, broadcast transactions, send and receive Ethereum-based cryptocurrencies and tokens, and securely connect to decentralized applications through a compatible web browser or the mobile app's built-in browser.
- The application includes an integrated service for exchanging Ethereum tokens by aggregating several decentralized exchanges (DEXs) to find the best exchange rate. This feature, branded as MetaMask Swaps, charges a service fee of 0.875% of the transaction amount.
- As of April 2021, MetaMask's browser extension had approximately 10 million monthly active users, according to The Financial Times.

Setup a MetaMask Ethereum Wallet:

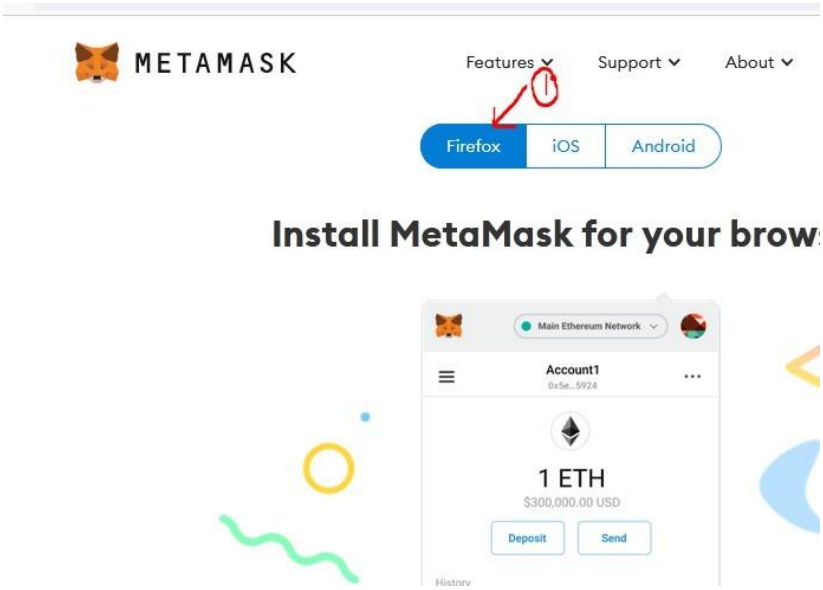
- MetaMask is just an Ethereum Browser and Ether wallet.
- It interacts with Ethereum Dapps and Smart Contracts without running a full Ethereum node.
- MetaMask add-on can be installed on Chrome, Firefox, Opera, and the new Brave browser.
- URL: https://metamask.io/

MetaMask Installation:

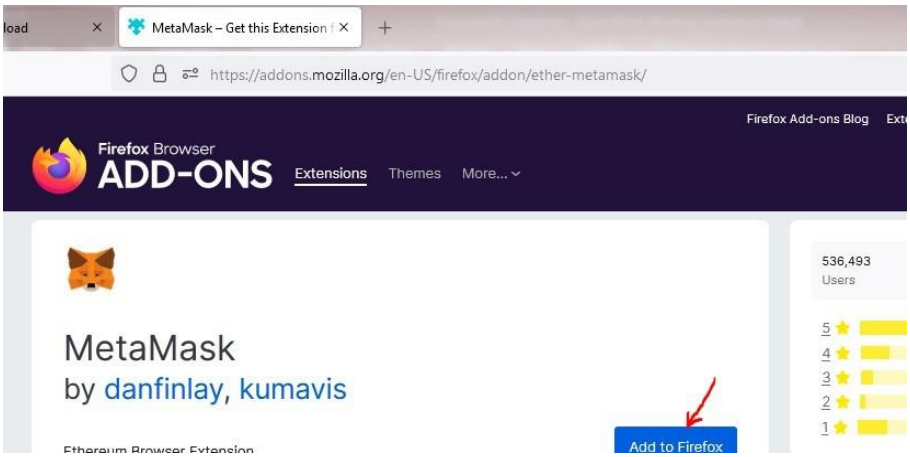
- Install MetaMask
- Add MetaMask extension to the Browser
- MetaMask will show up 12 words recovery key (Seed).
- These 12 words are the only way to restore MetaMask accounts.
- **Use URL: https://metamask.io/ or type metamask in browser. Click on download.**



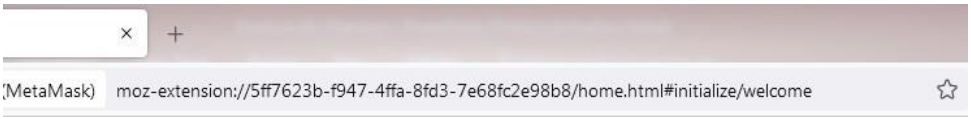
- **Select option firefox (According to browser you have open, it shows you appropriate browser extension) and click on installed metamask for firefox.**



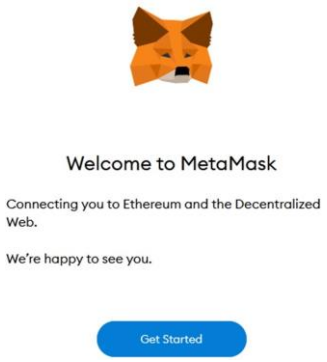
- **Click on add to firefox button.**



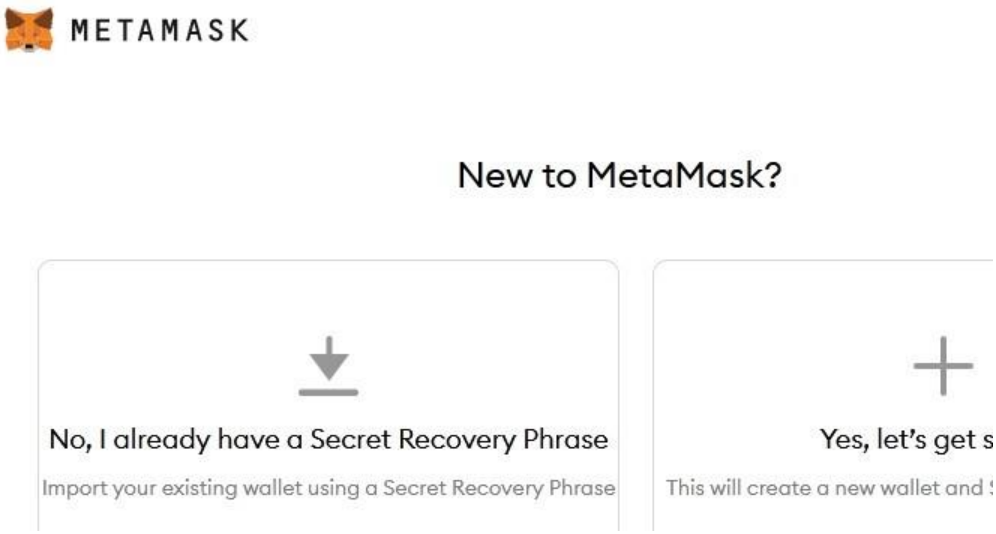
- **Click on logo of metamask.**



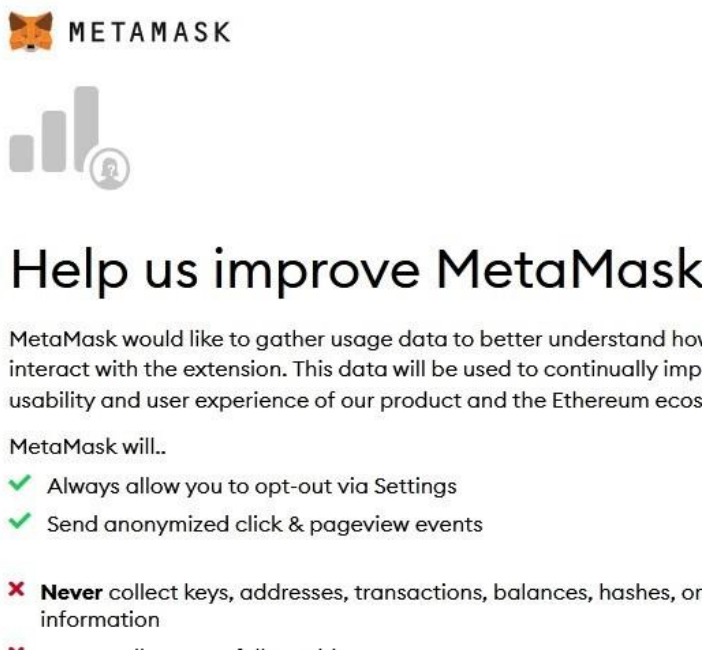
- **Click on Get Started button.**



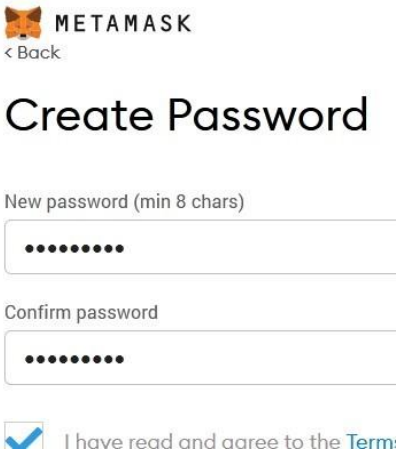
- **Click on Create a Wallet button to create new wallet.**
- **If you have already created wallet we can import here using Import Wallet option. Here you need to pass 12 words recovery key (Seed) which you receive.**



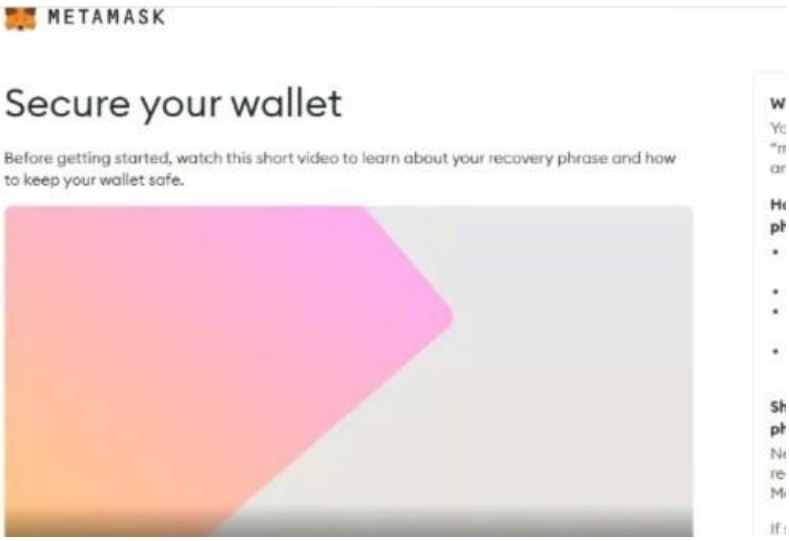
- **Click on I Agree button to accept the terms.**



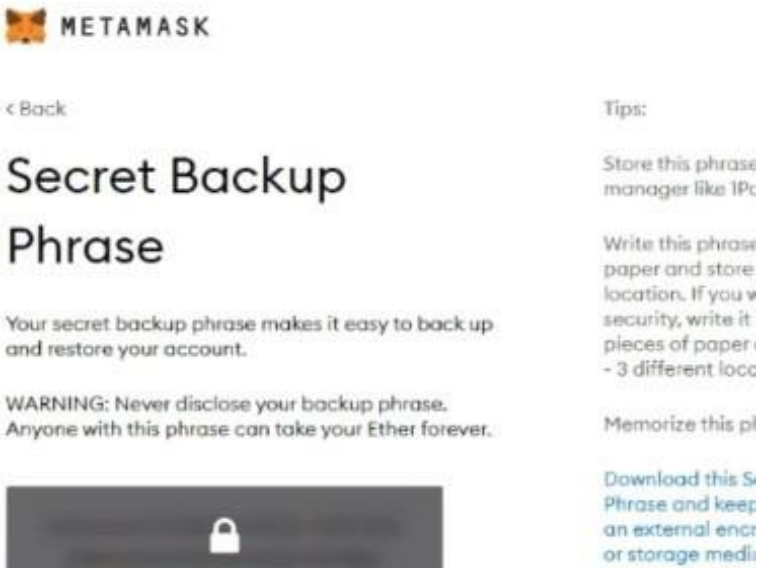
- **Enter new password and confirm password, select check box to accept Terms of Use and then click on create button.**



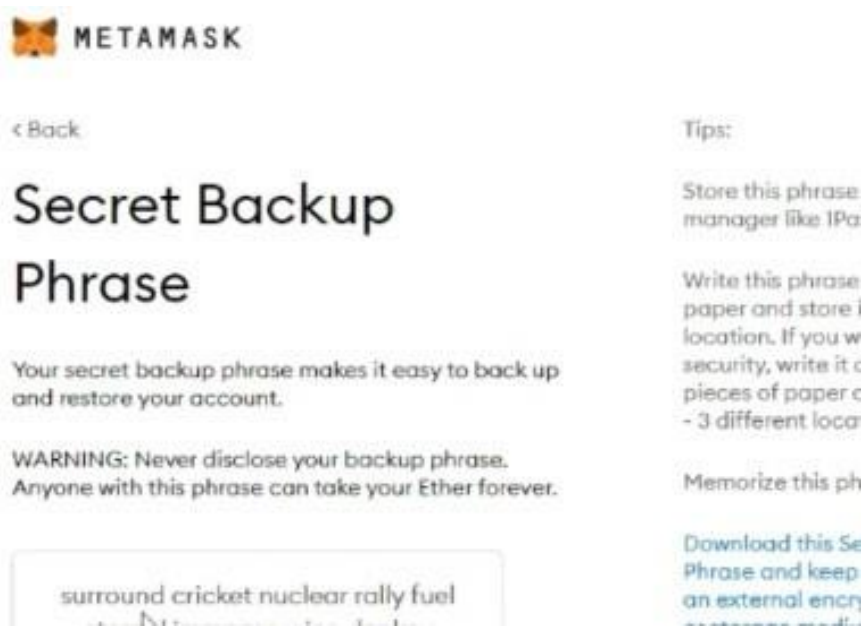
- **Click on next.**



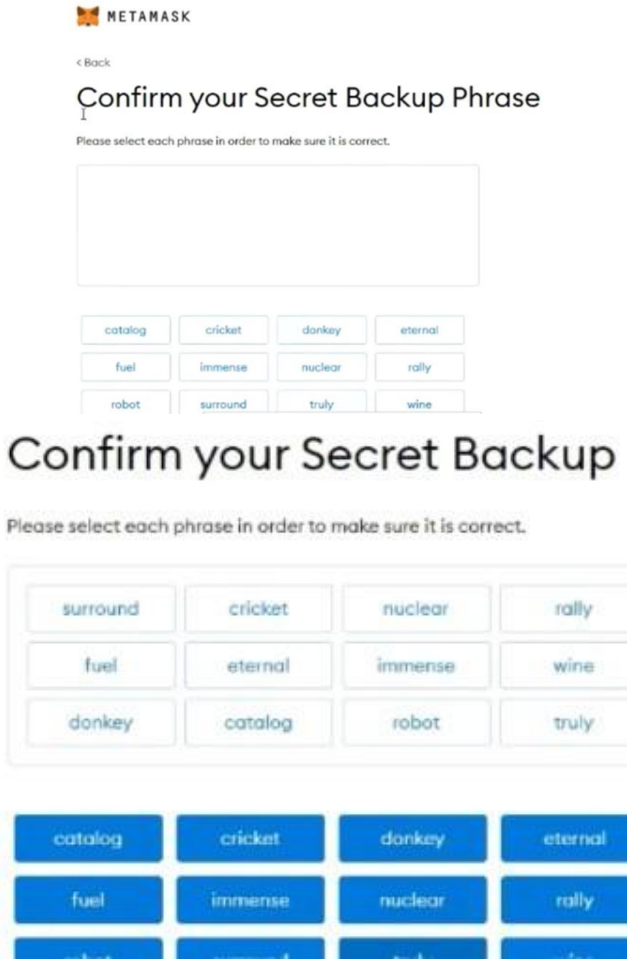
- **Click on Click Here to reveal secret words. This includes 12 secrete words in sequence which can be used to recover the account.**



- **Copy these secrete 12 words in same sequence in other files or take screenshot.**
- **Then click on Next button.**

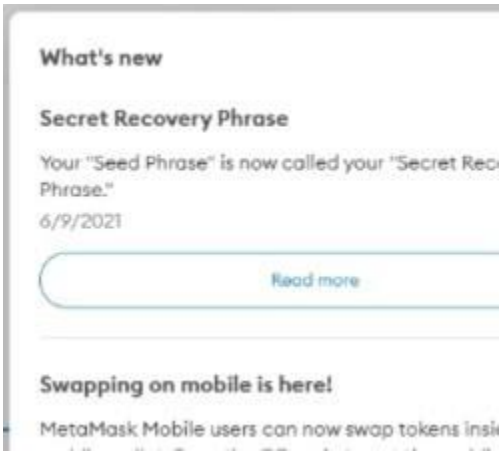


- **Select word of secret phrase in same order which we have seen in earlier step. Then Click on Confirm.**

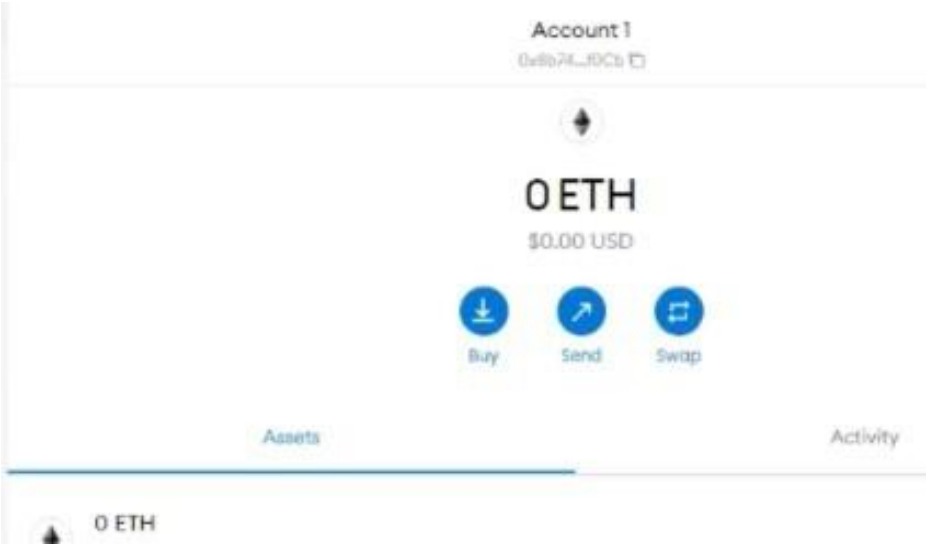


- **After successfully following all steps for new account creation Congratulations message appears. Finally click on All Done.**

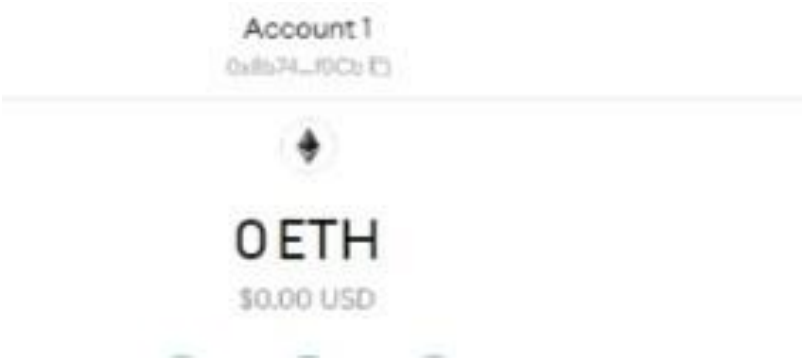
- **A pop up message will appears. Close it.**



- **Finally, it shows you the MetaMask wallet interface.**

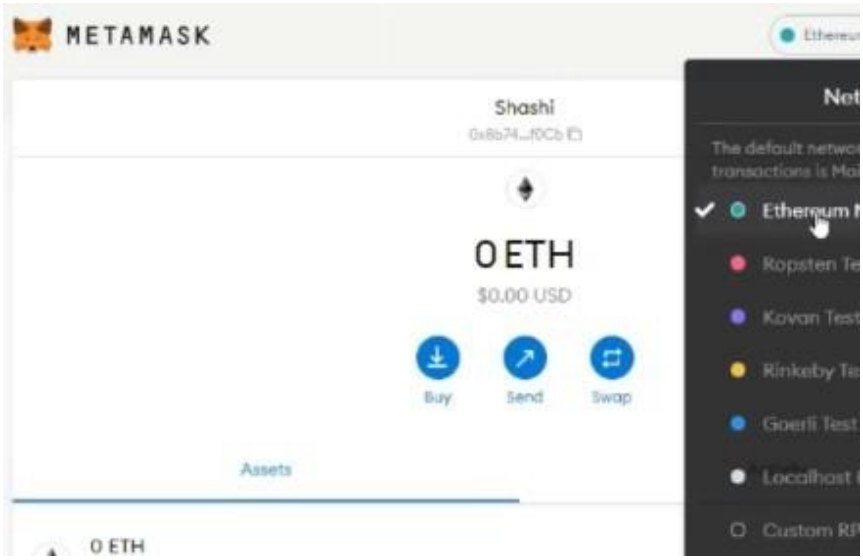


- **Click on three vertical dot i.e. Account option. Then select Account Details.**



- Here you can get option to change account name to any name. And also shows:
  - QR code of account
  - Wallet address i.e. public key
- You can also get private key
- For that click on Export Private Key
- Here it asks to enter password.

- **You can select any networks from the listed networks.**



Perform the following task:

- Connect to any test networks and request for ether using buy option.
- Create another account for e.g. Account 2
- Transfer some ether to another account i.e. Account 2. Here gas fee will be applicable which is transaction fee of transaction.
- Check the transaction details.

What are Smart Contracts?

- Smart contracts are lines of code that are stored on blockchain and automatically execute when predetermined terms and conditions are met.
- It's a computer protocol. It is called smart because of its ability to verify and execute a contract without any help from third parties. The contract exists in the decentralized Blockchain network and contains all the terms of a particular agreement.
- The blockchain is then updated when the smart contract is completed.

Benefits of Smart Contracts:

- Security: Blockchain transactions records are encrypted, and that makes them very hard to hack. Because each individual record is connected to previous and subsequent records on a distributed ledger.
- Savings: Smart contracts remove the need for intermediaries because participants can trust the visible data and the technology to properly execute the transaction.
- Trust: Smart contracts automatically execute transactions following predetermined rules, and the encrypted records of those transactions are shared across participants.
- Speed and accuracy: Smart contracts are digital and automated, so you won't have to spend time processing paperwork and correcting the errors.

How smart contracts works?

1. Two users create smart contract.
2. All contract terms are written as a code.
3. Smart contract is stored in blockchain.
4. Smart contract executes itself when events are triggered.

Task to be performed:

1. Develop the smart contract.
2. Compiling the smart contract.
3. Deploying the smart contract.
4. Interacting with smart contract.
5. Adding more functions to our code to make it more practical.

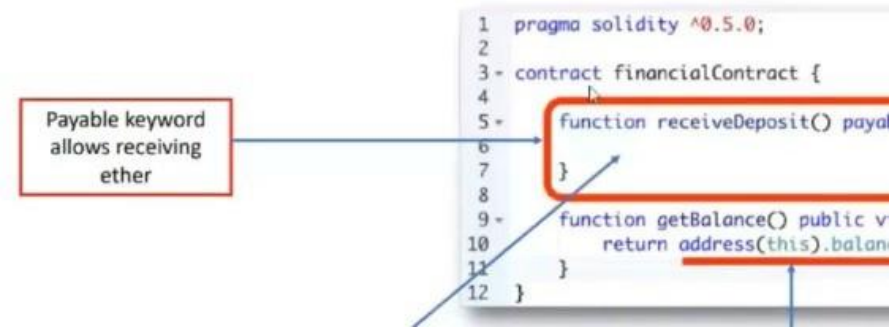
Remix IDE: Deployment Parameters:

1. **JavaScriptVM:** All the transactions will be executed in a sandbox blockchain the browser.
2. **Injected Provider:** Remix will connect to an injectedweb3 provider. Mist and Metamask are example of providers that inject web3, thus they can be used with this option.
3. **Web3Provider:** Remix will connect to a remote node. You will need to provide the URL address to the selected provider: geth, parity or any Ethereum client.

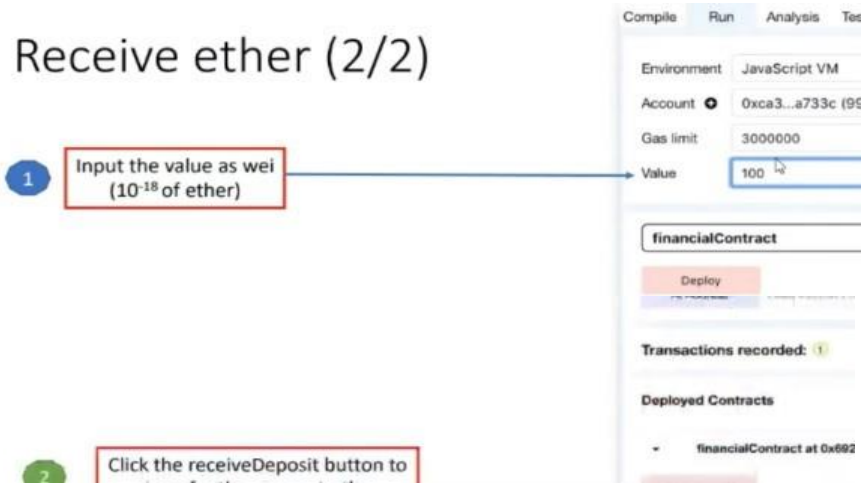
Example of Contract - Financial Contract in JavaScriptVM environment:

```
pragma solidity ^0.5.0;
contract FC
{
        uint balance=10500;
        function getBalance() public view returns (uint)
        {
                return balance;
        }
        function  deposit(uint  newDeposit)  public
        {
                balance = balance + newDeposit;
        }
}
```

Transfer Funds (money) from account to the Contract:



Transfer Funds (money) from account to the Contract:



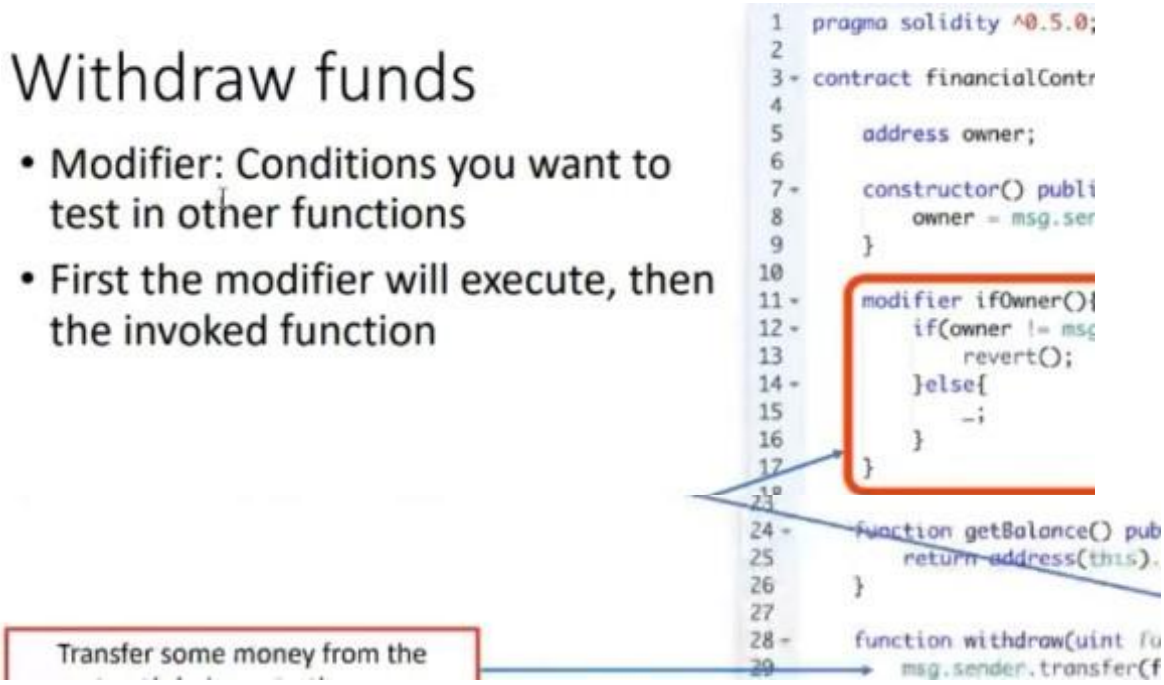
Save the address of the Contract Creator:

Here we can write constructor which will be called at the creation of the instance of the contract.

```
1  pragma solidity ^0.5.0;
2
3  contract financialContract {
4
5      address owner;
6
7      constructor() public{
8          owner = msg.sender;
9      }
10
11     function receiveDeposit() payable public{
12
13     }
```

Withdraw the funds (transferring fund from contract to account back):

Here we use modifier to apply and check condition before executing function.

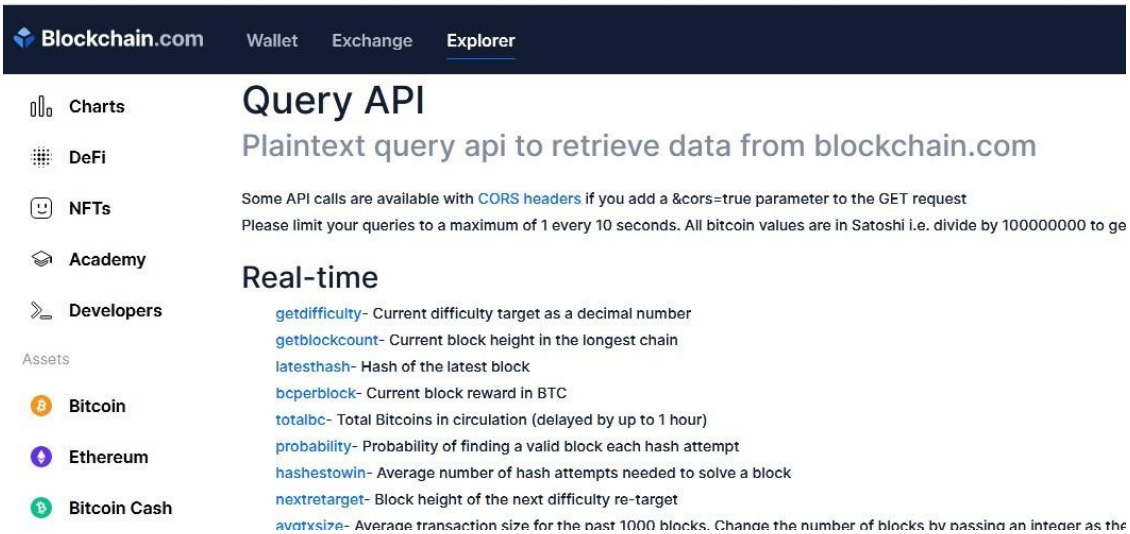


Use of special variables:

Use special variables in solidity contract to get information about blockchain and transaction details.

Name	Returns
blockhash(uint blockNumber) returns (bytes32)	Hash of the given block - or most recent, excluding c
block.coinbase (address payable)	Current block miner's
block.difficulty (uint)	Current block dif
block.gaslimit (uint)	Current block ga
block.number (uint)	Current block nu
block.timestamp (uint)	Current block timestamp a: unix epoch
gasleft() returns (uint256)	Remaining g
msg.data (bytes calldata)	Complete call
msg.value (uint)	Number of wei sent with
now (uint)	Current block time
tx.gasprice (uint)	Gas price of the tra

Use of Query API: Use Query API to get information about blockchain and transaction details. Use following URL https://www.blockchain.com/api/q



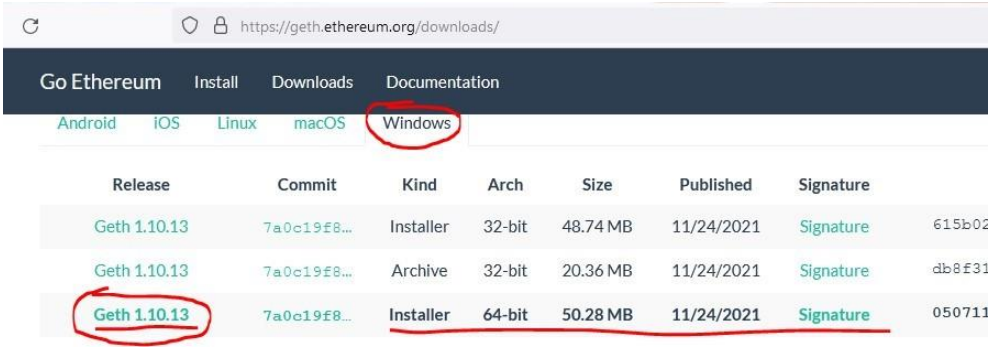
Setting up an Ethereum Node:[3]

- Ethereum node is any device that is running the Ethereum protocol (blockchain).
- When we connect to the Ethereum protocol we are on the Ethereum blockchain network.
- By running an Ethereum node we can connect to other nodes in the network, have direct access to the blockchain, and even do things like mine blocks, send transactions, and deploy smart contracts.

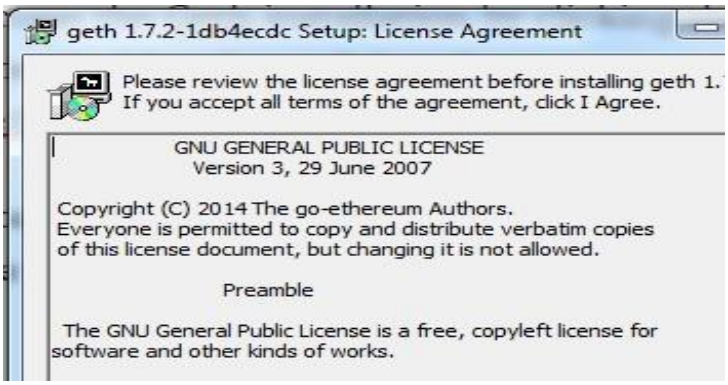
Creating private Ethereum blockchain using Geth (Go-Ethereum):[3]

Steps to install Geth:

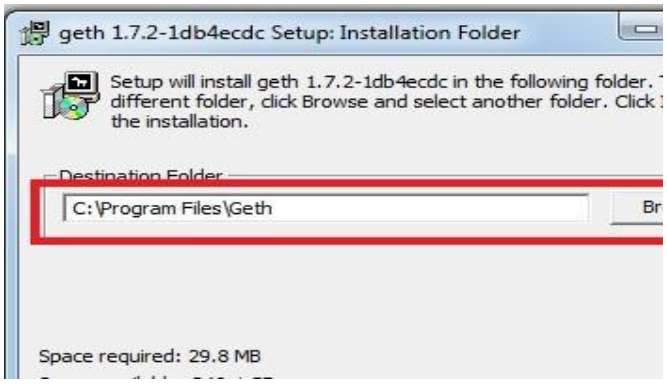
- Visit the Go Ethereum website and install Geth
- Visit here http://geth.Ethereum.org/downloads/
- Download the latest release of Geth for Windows, make sure you download the 64-bit version.



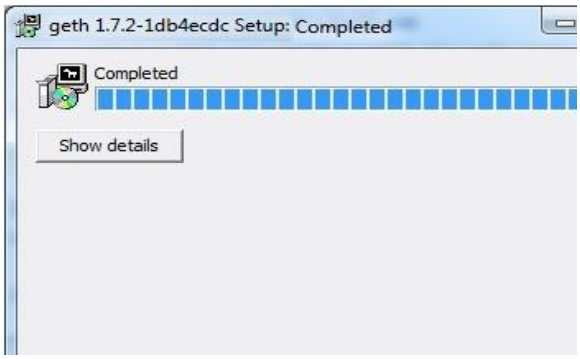
- Once your download is complete, open the installer and click "I Agree"



- You'll be prompted to select a destination folder for your download. By default, Geth will install under C:\Program Files\Geth



- **Close installation once complete**



Creating private Ethereum blockchain using Geth (Go-Ethereum):[3]

Establishing Our Own Private Ethereum Network:

- Create a new folder on your desktop called “private-chain”.
- Open command prompt in this folder and create a data directory folder for our chaindata by typing “mkdir chaindata”.
- Next, we need to create and save our genesis.json block in our Private Chain folder, as the genesis block will be used to initialize our private network and store data in the data directory folder “chaindata”.

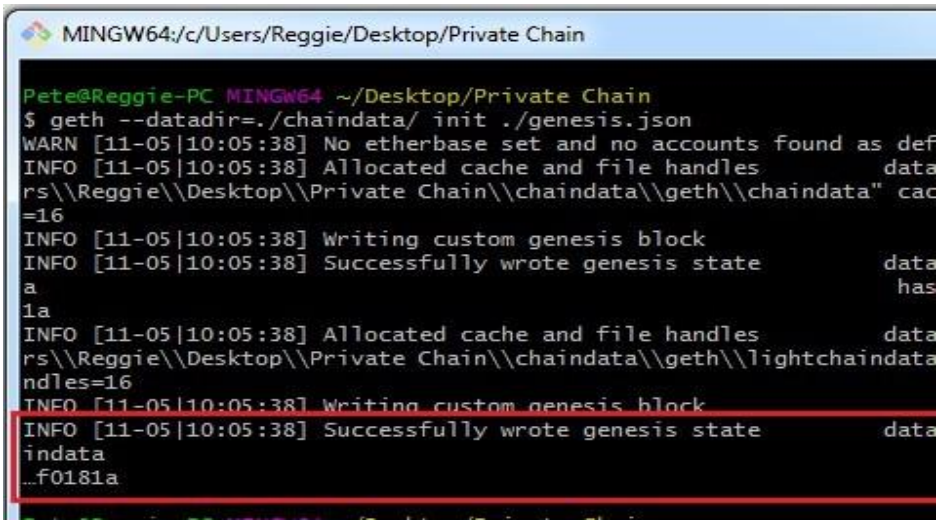
Open up notepad, copy & paste the code below into a new file called “genesis.json” and save this file in our Private-Chain folder.

```
{ "coinbase" : "0x0000000000000000000000000000000000000001",
  "difficulty" : "0x20000",
  "extraData" : "",
  "gasLimit" : "0x2fefd8",
  "nonce"    : "0x0000000000000042",
  "mixhash" : "0x0000000000000000000000000000000000000000000000000000000000000000",
  "parentHash" : "0x0000000000000000000000000000000000000000000000000000000000000000",
  "timestamp" : "0x00",
  "alloc": {},
  "config": {
      "chainId": 15,
      "homesteadBlock": 0,
      "eip155Block": 0,
      "eip158Block": 0,
      "eip150Block": 0 }}
```

Start the Ethereum peer node (Start the Blockchain)

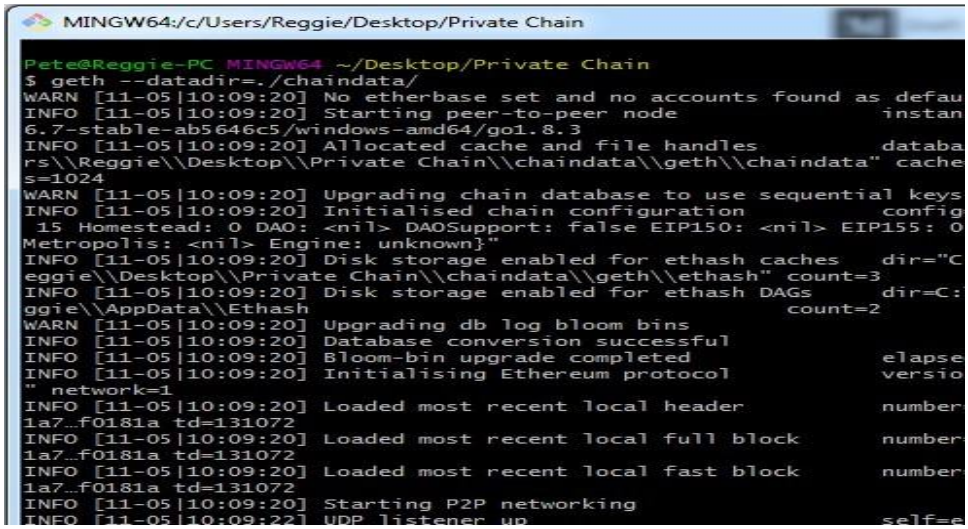
Run the following command:

geth --datadir chaindata init genesis.json



Now we can start Geth and connect to our own private chain.

geth --datadir=./chaindata/



- Minimize the terminal and Open new terminal.
- Type the command: Here is IPC is used to interact with Geth
  geth attach ipc:\\.\pipe\geth.ipc
- Command to create new account (here you need to account password) personal.newAccount()
- To know the all accounts eth.accounts
- To know the main account eth.coinbase
- To get balance of account eth.getBalance(eth.accounts[0])
- Start mining miner.start()
- Stop mining miner.stop()
- Again check the balance of same account eth.getBalance(eth.accounts[0])
- Create another account personal.newAccount()

Transaction:

- Unlock the account 0 to send transaction - personal.unlockAccount(eth.accounts[0])
- Command to send transaction – eth.sendTransaction({from: eth.coinbase, to: eth.accounts[1], value: web3.toWei(10, "ether")})

start mining and stop mining:

- Start mining miner.start() Stop mining miner.stop()
- Check the account balance after successfully mining the block, some ethers will be added to accounts 0 in Wei unit eth.getBalance(eth.accounts[0])
- Also check the balance of account 1 in Wei unit eth.getBalance(eth.accounts[1])
- Balance of second account in ether web3.fromWei(eth.getBalance(eth.accounts[1]), "ether")
- To get details of latest block eth.getBlock("latest")
- To get details of specific block eth.getBlock(35)

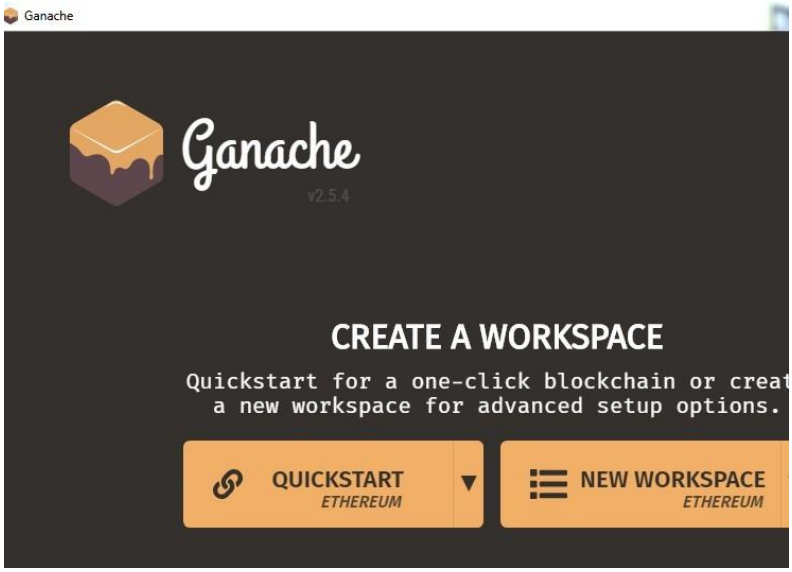
The Complete Blockchain Developer Toolkit :[3]

Introduction to Ganache:

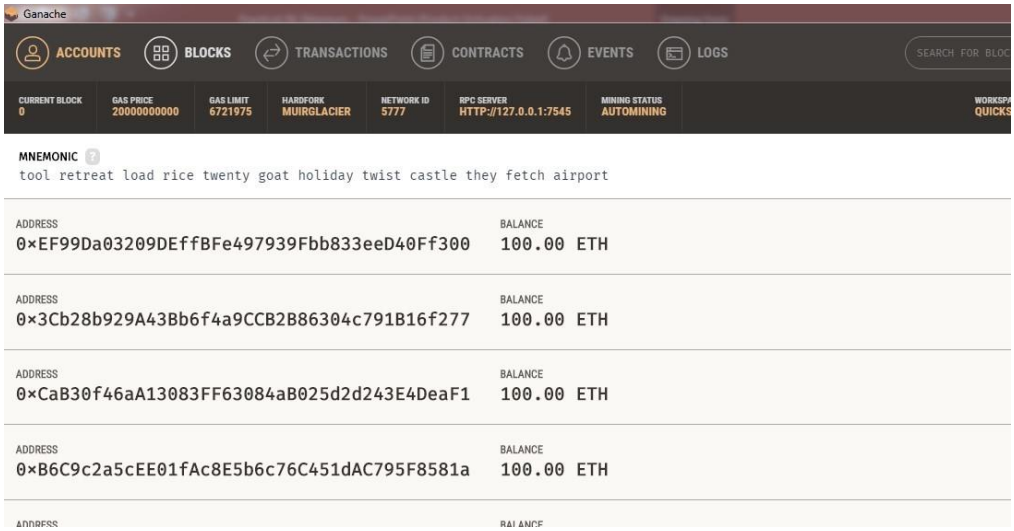
- Ganache as your personal blockchain for Ethereum development.
- It will allow you to deploy smart contracts, develop applications, and run tests.
- From the above URL link downloaded the archived package, extract the installer and run through the setup steps.

Ganache Personal Blockchain Interface consist of:

- Accounts Page - this shows you all of the accounts that are automatically generated, along with their balances.
- Blocks Page - this shows you each block that has been mined on the personal blockchain network, along with the gas cost and transactions.
- Transactions Page - this list all the transactions that have taken place on the personal blockchain.
- Logs Page - this shows you all the server logs that you might need when debugging your application.
- Link to download Ganache https://www.trufflesuite.com/ganache
- Open the Ganache and then select the workspace QUICKSTART.



Ganache Personal Blockchain Interface :



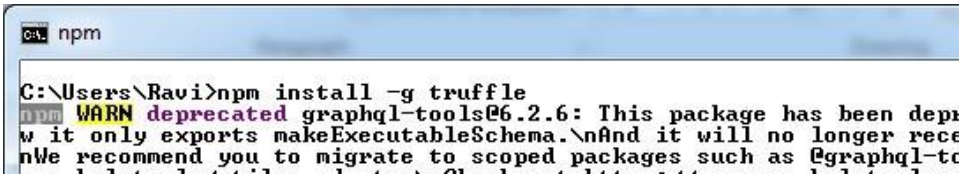
Developing smart contracts using Truffle:[4]

- Install **Node JS** and **Truffle Suite** to develop and migrate the smart contracts into the Private Blockchain network.
- Make use of Truffle tools like compile, migrate and test for compilation, migration and testing the smart contracts through Blockchain.
- Note that you have a private blockchain running, you need to configure your environment for developing smart contracts.
- The first dependency you'll need is Node Package Manager, or NPM, which comes with Node.js.
- You can see if you have node already installed by going to your terminal and typing: **node –v**
- Otherwise, Download from: URL: https://nodejs.org/en/

Truffle Framework:[4]

- Truffle Framework provides a suite of tools for developing Ethereum smart contacts with the Solidity programming language.
    - Smart Contract Management
    - Automated Testing
    - Deployment of smart contract
    - Migration of smart contract onto private blockchain network
    - Network Management
    - Script Runner
    - Client Side Development
- You can install Truffle with NPM in your command line like this:

    npm install -g truffle



Create a new truffle project:[4]

- Go to cmd prompt :

    mkdir blockchain-toolkit

cd blockchain-toolkit

truffle init

- Command to install touch for windows: **npm install -g touch-for-windows**
- Command to create file: **touch package.json**
- copy-and-pasting the below code into **package.json** file (It's configuration file required to run truffle project):

```
{
"name": "blockchain-toolkit",
"version": "1.0.0",
"description": "The Complete Blockchain Developer Toolkit for 2019 & Beyond",
"main": "truffle-config.js",
"directories": {
"test": "test"
},
"scripts": {
"dev": "lite-server",
"test": "echo \"Error: no test specified\" && sexit 1"
},
"author": "gregory@dappuniversity.com",
"license": "ISC",
"devDependencies": {
```

- copy-and-pasting the below code into **package.json** file

```
"bootstrap": "4.1.3",
"chai": "^4.1.2",
"chai-as-promised": "^7.1.1",
"chai-bignumber": "^2.0.2",
"dotenv": "^4.0.0",
"ganache-cli": "^6.1.8",
"lite-server": "^2.3.0",
"nodemon": "^1.17.3",
"solidity-coverage": "^0.4.15",
"truffle": "5.0.0-beta.0",
"truffle-contract": "3.0.6",
"truffle-hdwallet-provider": "^1.0.0-web3one.0"
}
}
```

- Save **package.json** file
- Run the following commad:

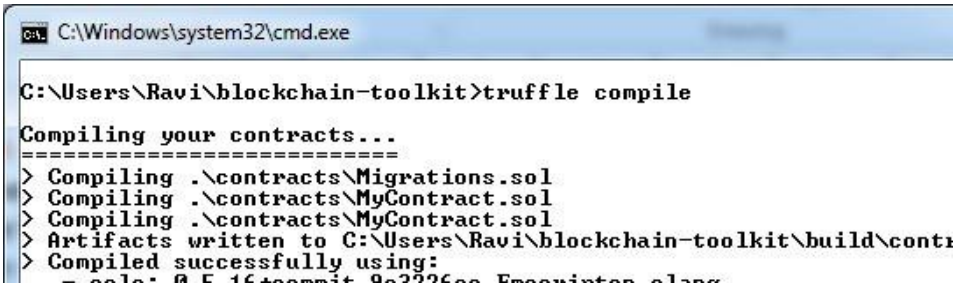
  npm install
- **Start developing a smart contract using solidity:**
- Run the touch command to create new contract:

  touch ./contracts/MyContract.sol
- Copy the below contract code and save in MyContract.sol

```
pragma solidity ^0.5.0;
contract MyContract {
string value;
constructor() public {
value = "myValue"; }
function get() public view returns(string memory) {
return value; }
function set(string memory _value) public {
value = _value; }
}
```

- Run the following command:

  truffle compile



- **Update the project configuration file to specify the personal blockchain network we want to connect to (Ganache):**
- Find the file **truffle-config.js** and paste the following code:

```
module.exports = {
networks: {
development: {
host: "127.0.0.1",
port: 7545,
network_id: "*" // Match any network id
}
},
solc: {
optimizer: {
enabled: true,
runs: 200
        }
  }
}
```

- **Create a migration script inside the migrations directory to deploy the smart contract to the personal blockchain network.**
- Run the following command:

  touch migrations/2_deploy_contracts.js
- Copy the below script into **2_depoy_contracts.js**

```
var MyContract = artifacts.require("./MyContract.sol");
```

```
module.exports = function(deployer)
{
deployer.deploy(MyContract);
};
```

- **Run the newly created migration script to deploy the smart contract to the personal blockchain network:**

  truffle migrate

- **Run the following commands:** truffle console

  MyContract.deployed().then((instance) => { app = instance })

- **Now we can read the storage value**

  app.get()

  Output as 'myValue'

- **Now we can set a new value like this:**

  app.set('New Value')

- **We can read that the value was updated like this:**

app.get()

Output as 'New Value'

- **You can exit the Truffle console by typing this command:**

  .exit

References:

1. https://en.wikipedia.org/wiki/Ethereum
2. https://en.wikipedia.org/wiki/MetaMask
3. https://codeburst.io/build-your-first-ethereum-smart-contract-with-solidity-tutorial-94171d6b1c4b
4. https://www.dappuniversity.com/articles/blockchain-developer-toolkit
5. https://www.tutorialspoint.com/solidity/solidity_quick_guide.htm

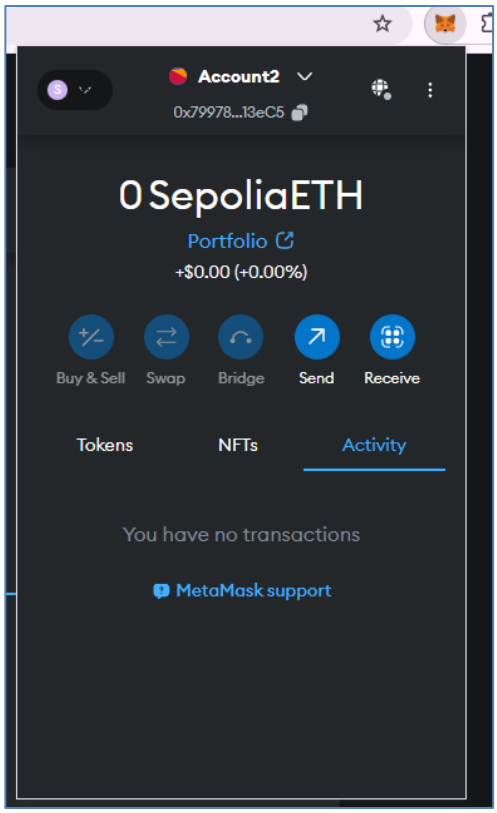
Exercise:

1. Install the metamask in browser. Setup the metamask digital cryptocurrency wallet. Create multiple accounts in metamask and connect with one of the etherum blockchain test network. Perform the taskbuy ethers and send ethers from one account to another. Take the screenshots of created accounts, account assets and account transactions which showing the details of transaction.

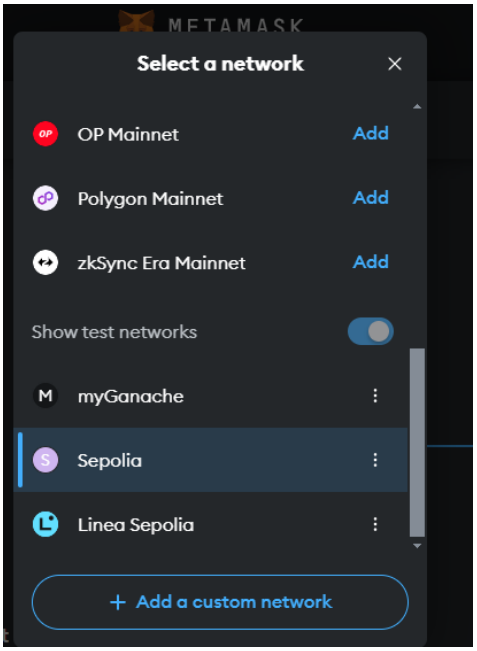
   (Use following url to get free ether for Sepolia Test Network: https://faucets.chain.link/sepolia)

   Output :

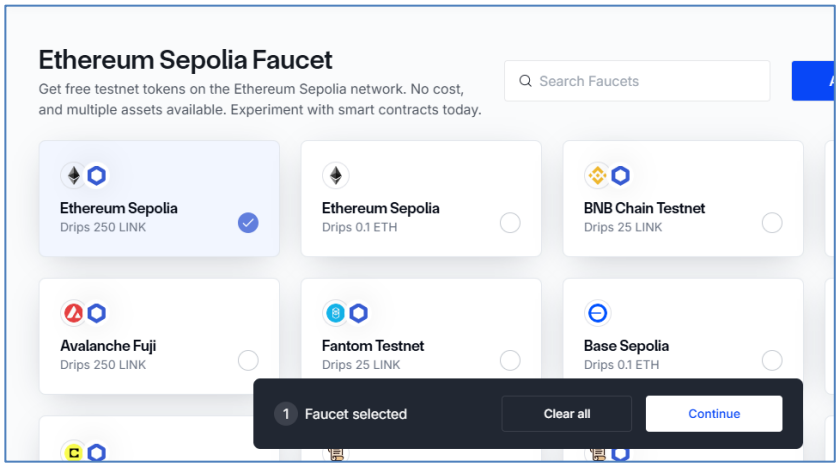
   1. Installed metamask and metamask Account

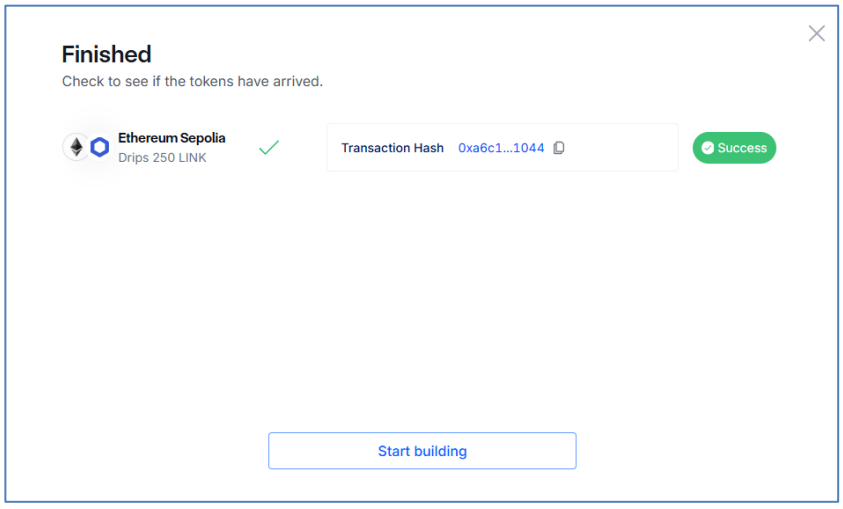


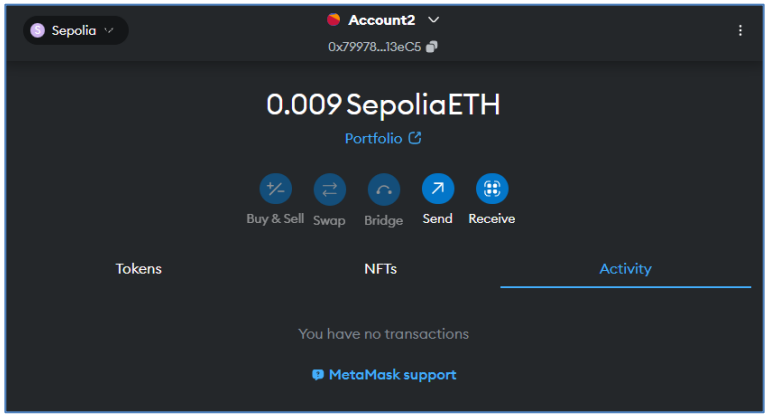
2. **Connection with one of the etherum blockchain test network**



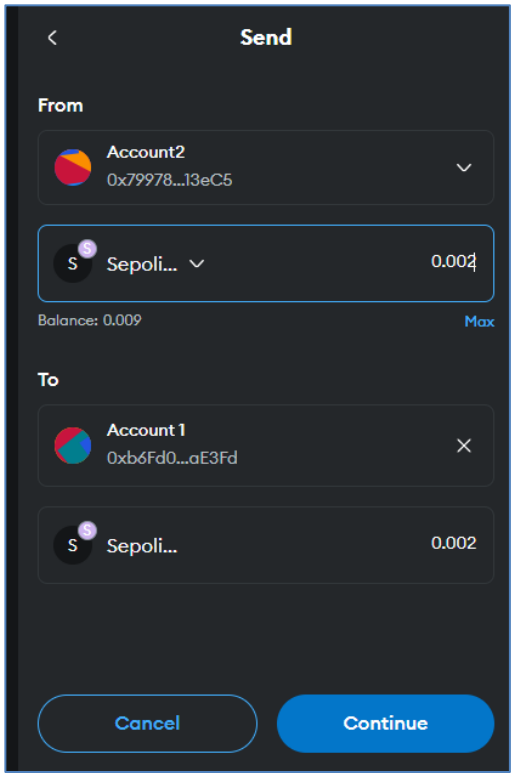
3. **Buy ethers.**

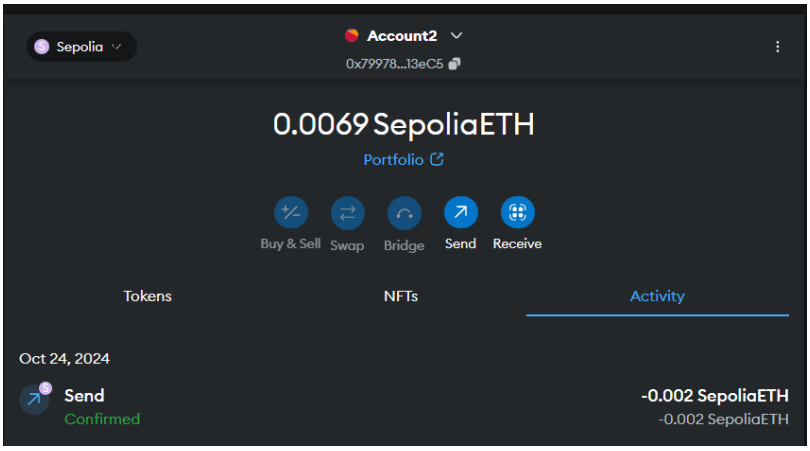






4. Send ethers.

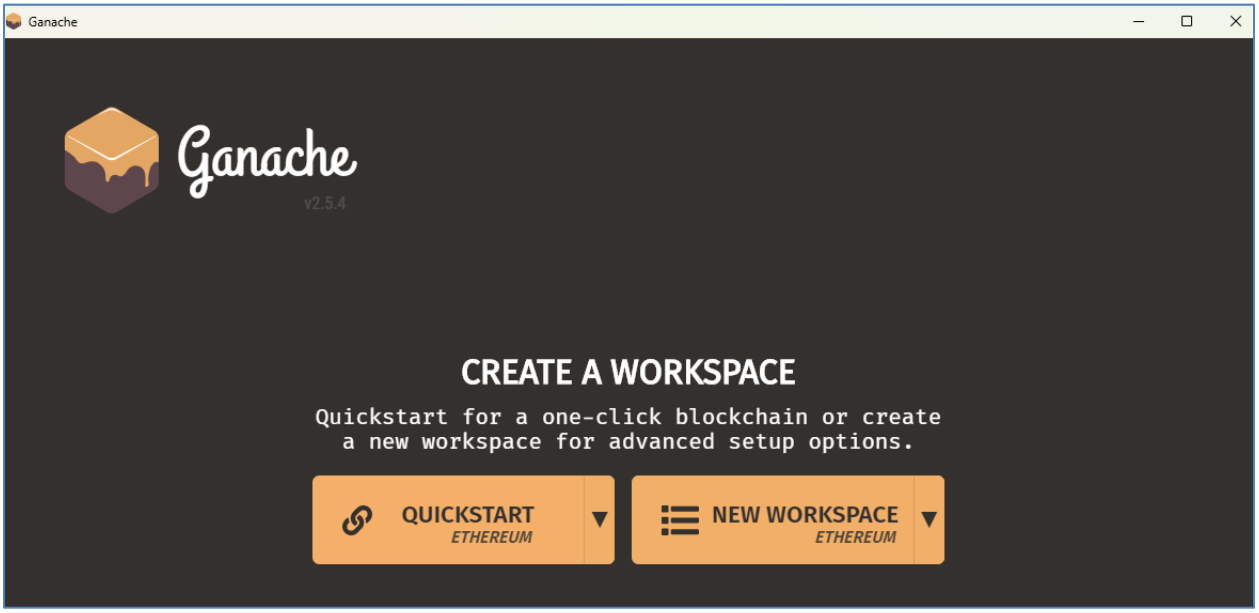




2. Start **Ganache** (your personal private blockchain network). Connect Ganache with **MetaMask** and import the account from Ganache to MetaMask. Transfer funds from imported account to other accountof MetaMask. Take the screenshots of created accounts, account assets and account transactions which showing the details of transaction from MetaMask and Ganache interface.

Output :

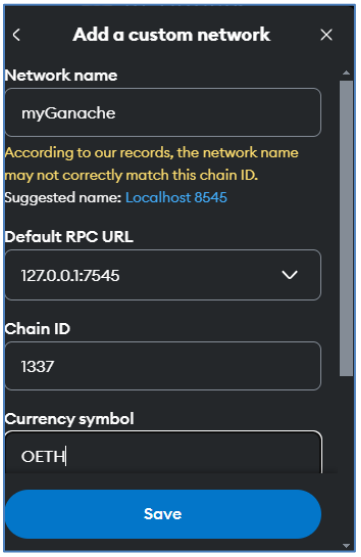
1. Start ganache

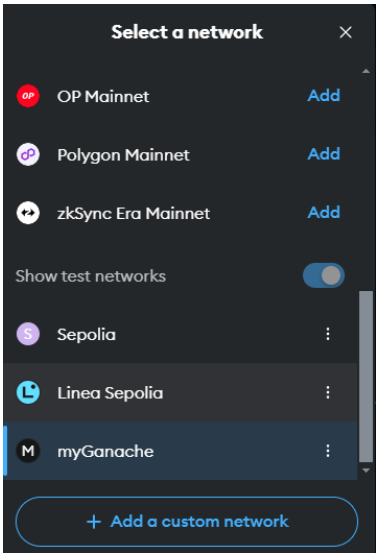


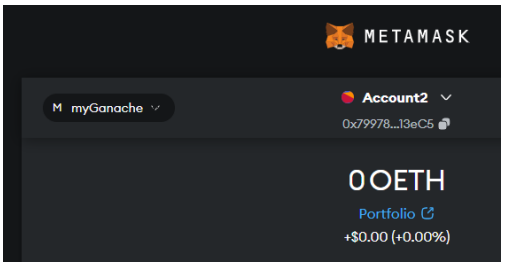
2. Connection of ganache with metamask

- **Copying the RPC server**

- **Connecting with metamask**

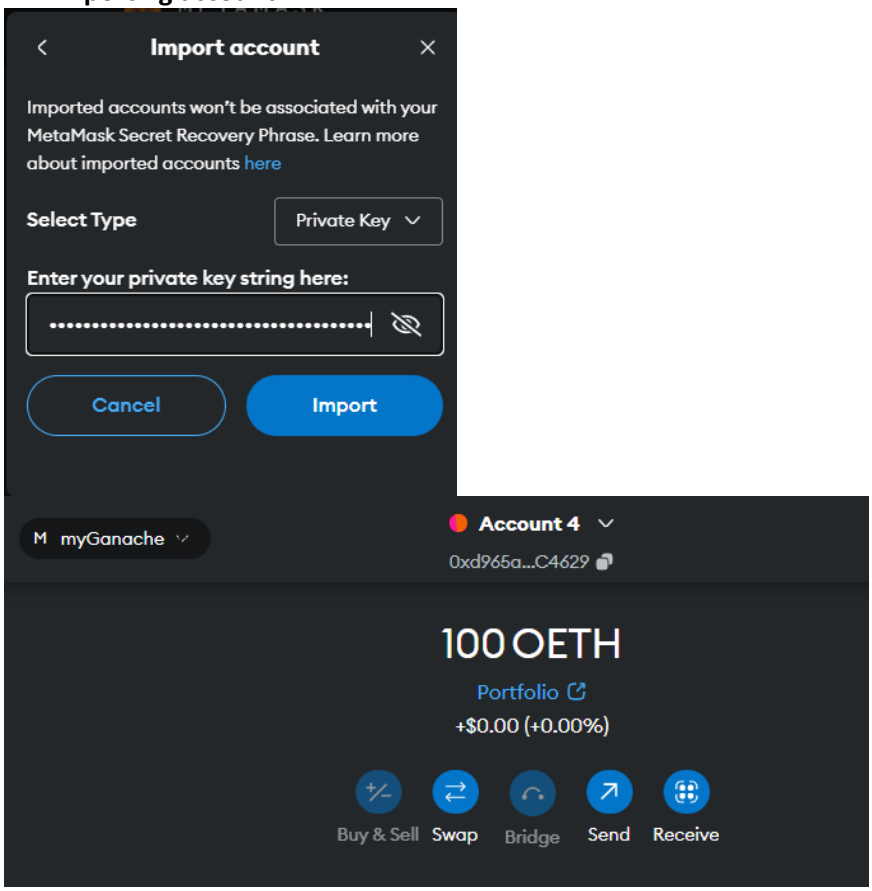




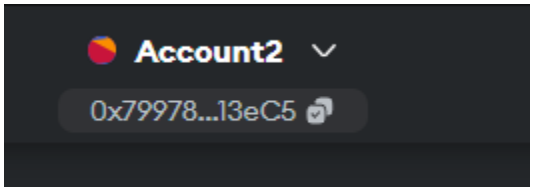


3. **Transfer funds from imported account to other account of MetaMask**

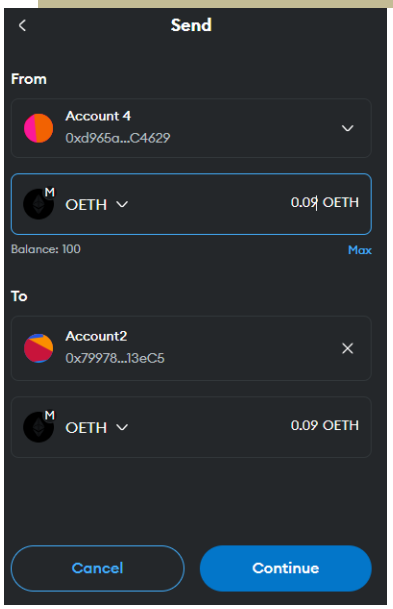
- **Importing account**

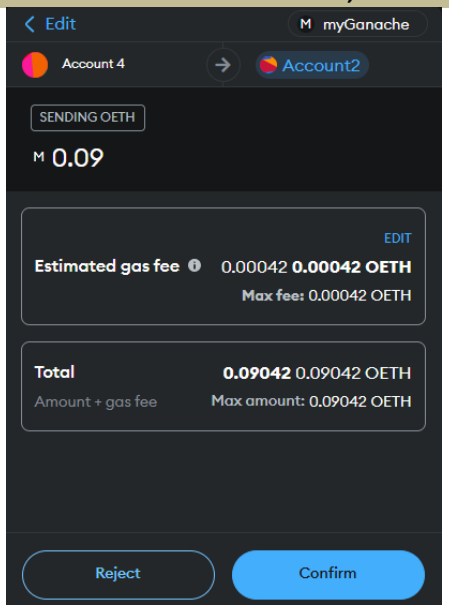


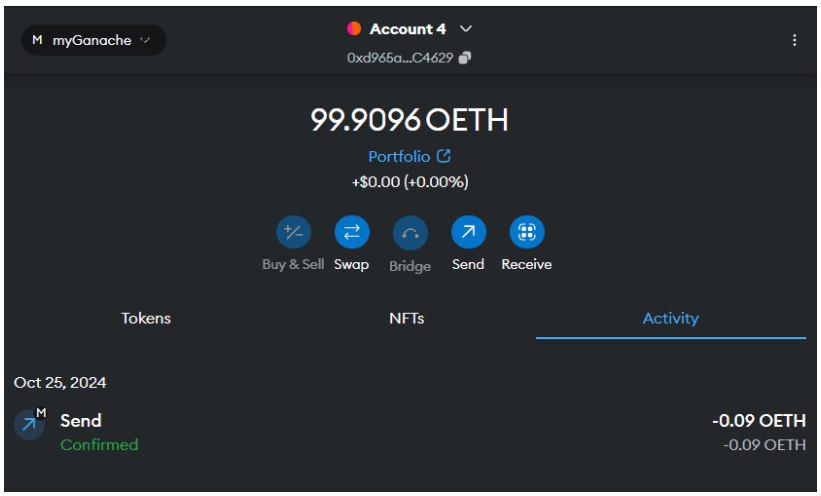
- **Address coied of account 2**

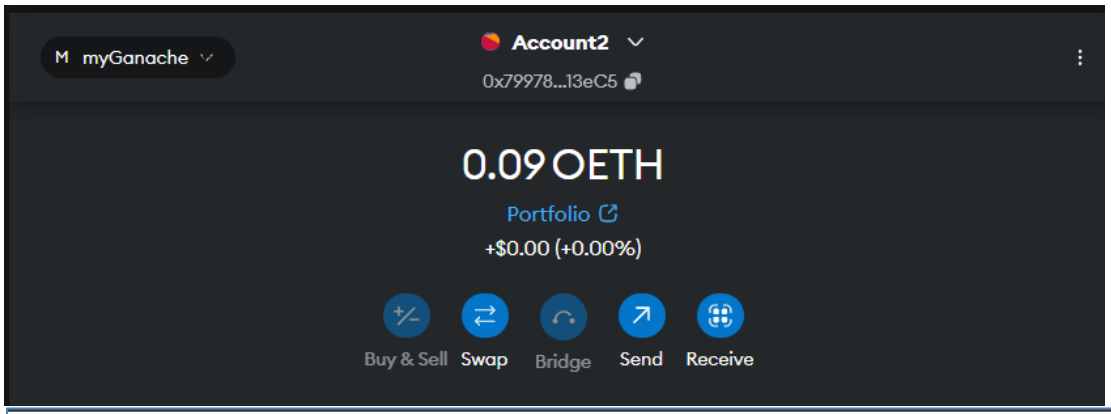


- **Transfer the funds**

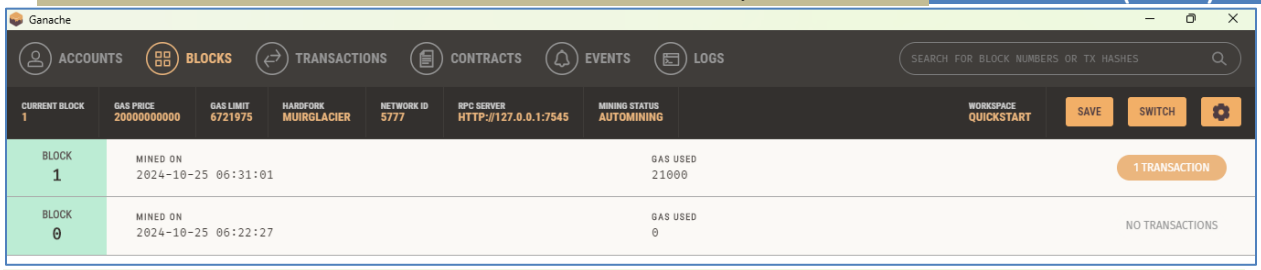

Send
From
Account 4
0xd965a...C4629
OETH
0.09 OETH
Balance: 100
Max
To
Account2
0x79978...13eC5
OETH
0.09 OETH
Cancel
Continue

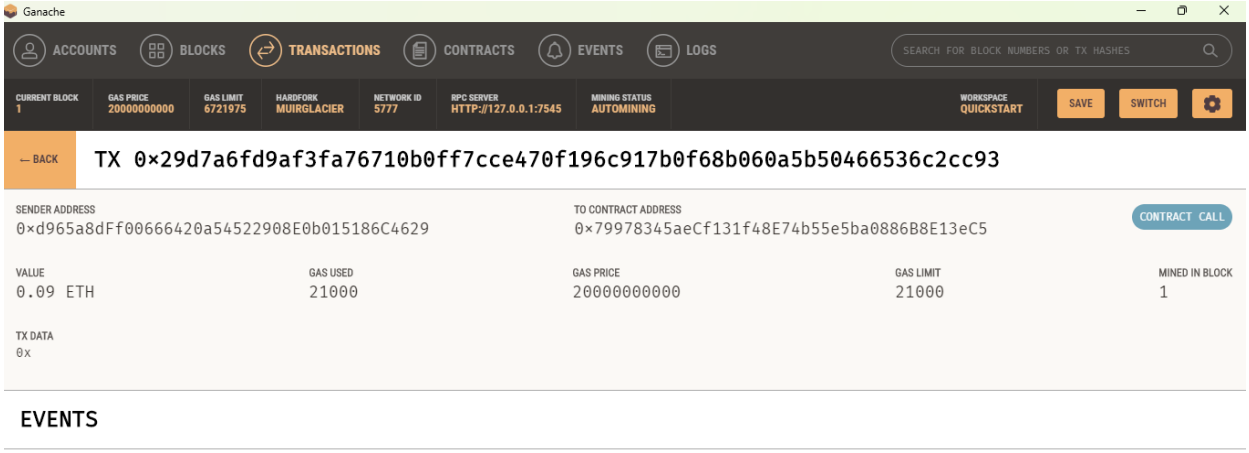

Edit
myGanache
Account 4
Account2
SENDING OETH
0.09
EDIT
Estimated gas fee
0.00042 0.00042 OETH
Max fee: 0.00042 OETH
Total
0.09042 0.09042 OETH
Amount + gas fee
Max amount: 0.09042 OETH
Reject
Confirm


myGanache
Account 4
0xd965a...C4629
99.9096 OETH
Portfolio
+$0.00 (+0.00%)
Buy & Sell
Swap
Bridge
Send
Receive
Tokens
NFTs
Activity
Oct 25, 2024
Send
Confirmed
-0.09 OETH
-0.09 OETH


myGanache
Account2
0x79978...13eC5
0.09 OETH
Portfolio
+$0.00 (+0.00%)
Buy & Sell
Swap
Bridge
Send
Receive


MNEMONIC
crash armor forget dismiss march anxiety educate enroll audit write iron polar
HD PATH
m/44'/60'/0'/0/account_index
ADDRESS
0×d965a8dFf00666420a54522908E0b015186C4629
BALANCE
99.91 ETH
TX COUNT
1
INDEX
0



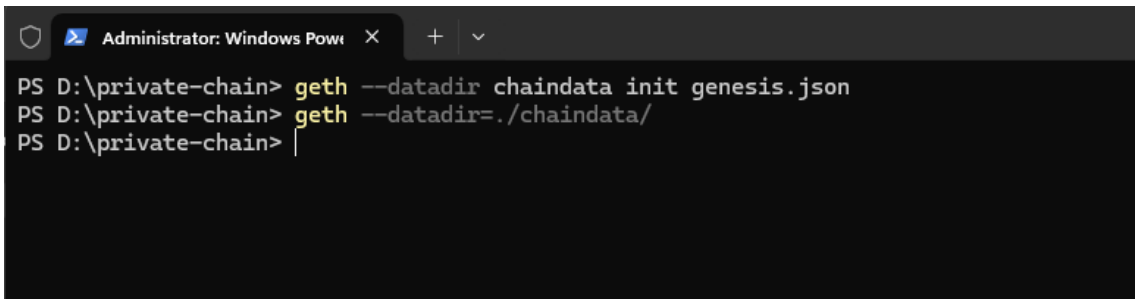


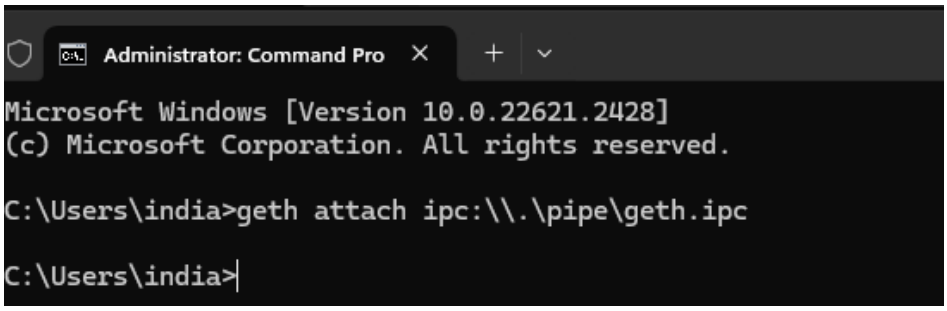
GoEthereum(Geth)

3. Create Ethereum node using **Geth (GoEthereum)** and create genesis block and create your personal private Ethereum blockchain. And use IPC to interact with Geth node to perform following task: create account, transfer funds using send transaction, mine the block, show the account balance before and after the mining the block, show the specific block details and access chain details.

Output :

1. Geth account and genesis block :





2. Createaccount

```
d:\geth\geth.exe
Welcome to the Geth JavaScript console!

instance: Geth/v1.10.9-stable-eae3b194/windows-amd64/go1.17
at block: 0 (Thu Jan 01 1970 05:30:00 GMT+0530 (IST))
 datadir: D:\private-chain\chaindata
 modules: admin:1.0 debug:1.0 eth:1.0 ethash:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

To exit, press ctrl-d or type exit
> eth.Accounts
undefined
> eth.accounts
[]
> personal.newAccount()
Passphrase:
Repeat passphrase:
"0x141ecde52b4fc3bd9d2dfb157e83a09ca0c46963"
> eth.accounts
["0x141ecde52b4fc3bd9d2dfb157e83a09ca0c46963"]
```

3. Transfer funds using send transaction

```
d:\geth\geth.exe
> eth.accounts
["0x141ecde52b4fc3bd9d2dfb157e83a09ca0c46963", "0x40e2485221166c34ad2f2fad68e3276fa2aaa4e0"]
> eth.coinbase
"0x141ecde52b4fc3bd9d2dfb157e83a09ca0c46963"
> personal.unlockAccount(eth.accounts[0])
Unlock account 0x141ecde52b4fc3bd9d2dfb157e83a09ca0c46963
Passphrase:
true
> eth.sendTransaction({from:eth.coinbase,to:eth.accounts[1],value:web3.toWei(10,"ether")})
"0x3385777735c1ae8a86c2919a4c5562ced510ff614f127cd93618317cd96b37189"
```

4. Mine the block

```
> miner.start()
null
> miner.stop()
null
> eth.getBalance(eth.accounts[0])
80000000000000000000
```

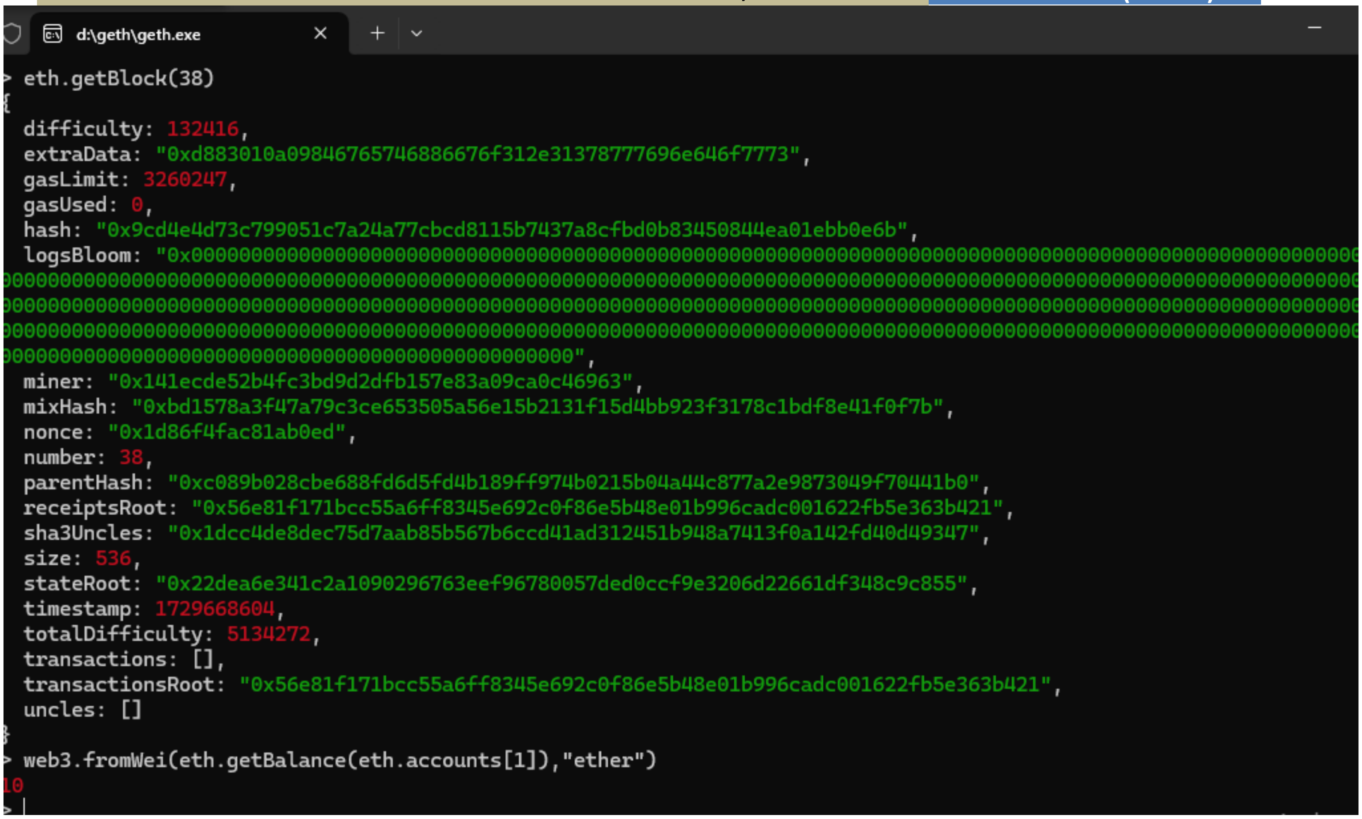
5. Show the account balance before and after the mining the block

```
d:\geth\geth.exe
null
> eth.getBalance(eth.accounts[0])
0
> miner.start()
null
> miner.stop()
null
> eth.getBalance(eth.accounts[0])
0
> eth.coinbaseeth.coinbase
TypeError: Cannot read property 'coinbase' of undefined
        at <eval>:1:1(2)

> eth.coinbase
"0x141ecde52b4fc3bd9d2dfb157e83a09ca0c46963"
> miner.start()
null
> miner.stop()
null
> eth.getBalance(eth.accounts[0])
80000000000000000000
```

6. Show the specific block details

```
> miner.start()
null
> miner.stop()
null
> eth.getBalance(eth.accounts[1])
1000000000000000000
> eth.getBlock("latest")
{
  difficulty: 132608,
  extraData: "0xd883010a0984676574686867 6f312e31378777696e646f7773",
  gasLimit: 3269803,
  gasUsed: 0,
  hash: "0xe991d5598d78883444246e7d9f3bf6f941e9b31235aa1252288929c331f72806",
  logsBloom: "0x0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
```

```
d:\geth\geth.exe
  extraData: "0xd883010a0984676574686867 6f312e31378777696e646f7773",
  gasLimit: 3269803,
  gasUsed: 0,
  hash: "0xe991d5598d78883444246e7d9f3bf6f941e9b31235aa1252288929c331f72806",
  logsBloom: "0x0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000",
  miner: "0x141ecde52b4fc3bd9d2dfb157e83a09ca0c46963",
  mixHash: "0xab32464ee9519e6aed119656f4d2768b7e1d7acd639cef72e8fe460c6619b938",
  nonce: "0x27b0370ee3549e0c",
  number: 41,
  parentHash: "0xaaa589813d38e1a49005d3cfbb3b8f5cc49715cff1bfbb4879f9b94b280f52c7",
  receiptsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
  sha3Uncles: "0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
  size: 536,
  stateRoot: "0xe4703aec776bb2dadf7dc5e93cdbbda2d23335b8b4231d35a64576da1eb1f529",
  timestamp: 1729668607,
  totalDifficulty: 5531904,
  transactions: [],
  transactionsRoot: "0x56e81f171bcc55a6ff8345e692c0f86e5b48e01b996cadc001622fb5e363b421",
  uncles: []
}
> eth.getBlock(38)
{
  difficulty: 132416,
  extraData: "0xd883010a0984676574686867 6f312e31378777696e646f7773",
  gasLimit: 3260247,
  gasUsed: 0,
```

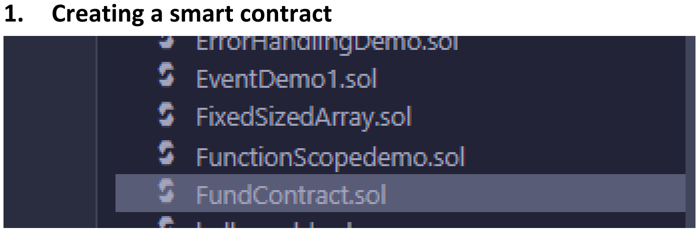


RemixIDE – Injected Provider - Public Test Network (Goerli, Sepolia) or Ganache

4. Write a solidity smart contract for performing following task using **remixIDE** and deployed it on **publictest network – Goerli / Sapolia** using **Injected provider** environment.
   a. To transfer funds (ethers) from user account to contract account.
   b. To withdraw funds (ethers) from contract account to user account.
   c. To apply restriction that only owner of the contract can withdraw funds (ethers) from contract account to his/her user account.

Output :

1. **Creating a smart contract**

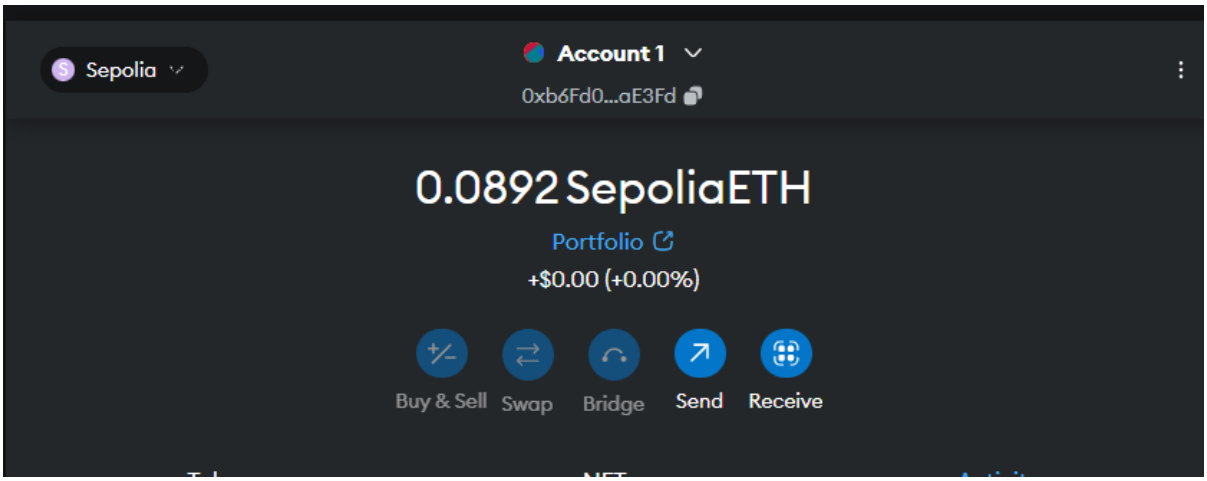


Code :

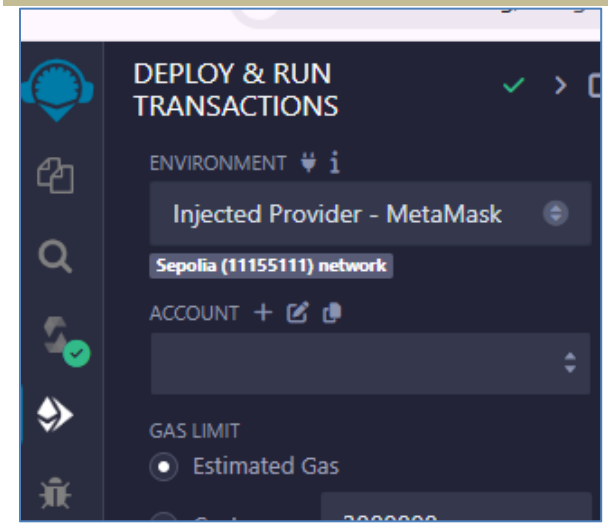
```
// SPDX-License-Identifier: MIT
pragma solidity >=0.5.0 <0.8.27;

contract FundContract {
    address public owner;

    // Event for logging deposits
    event Deposit(address indexed sender, uint256 amount);
```

```
    // Event for logging withdrawals
    event Withdraw(address indexed receiver, uint256 amount);

    // Set the contract deployer as the owner
    constructor() {
        owner = msg.sender;
    }

    // Function to deposit ether to the contract
    function deposit() public payable {
        require(msg.value > 0, "Deposit amount should be greater than zero");
        emit Deposit(msg.sender, msg.value);
    }

    // Function to withdraw ether from the contract
    function withdraw(uint256 _amount) public {
        require(msg.sender == owner, "Only owner can withdraw funds");
        require(_amount <= address(this).balance, "Insufficient contract balance");

        payable(owner).transfer(_amount);
        emit Withdraw(owner, _amount);
    }

    // Function to get contract balance
    function getBalance() public view returns (uint256) {
        return address(this).balance;
    }
}
```

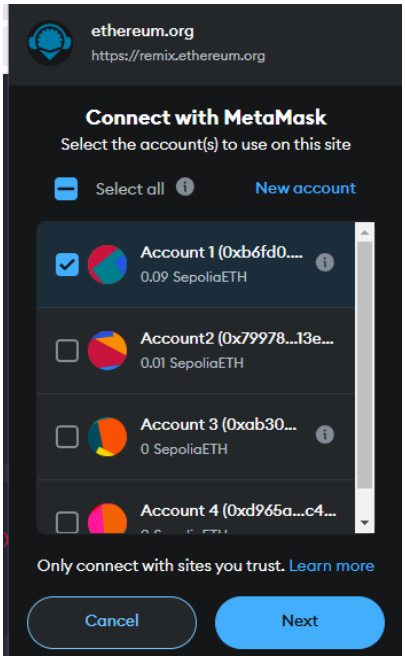
2. Metamask account and sepolia network :



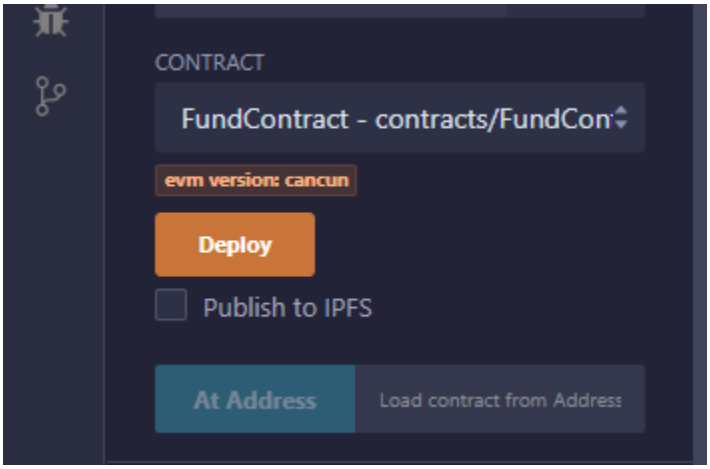
- **Injected Provider – metamask is Selectetd**



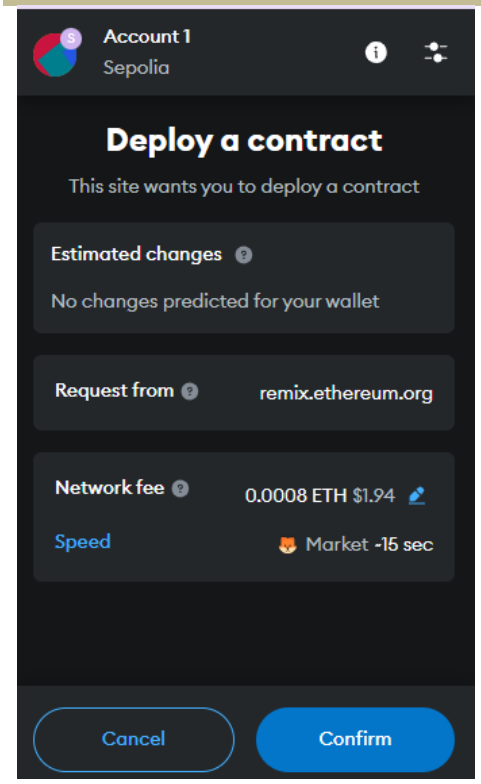
- **Connect with metamask**



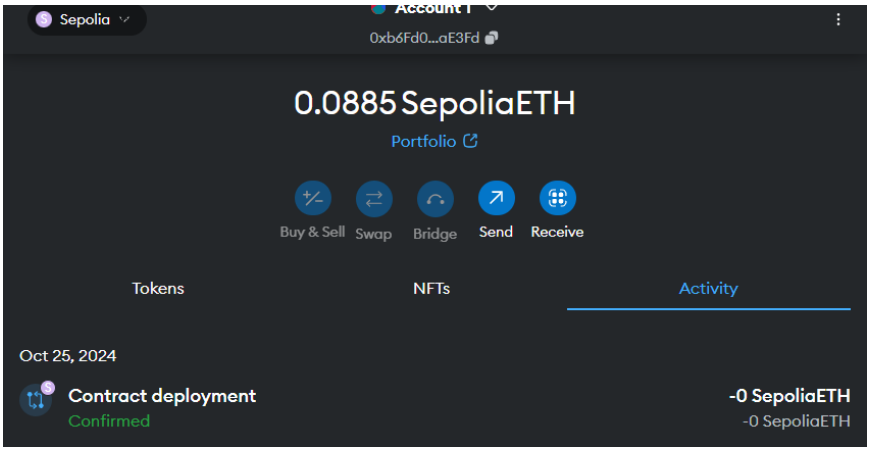
- **Connected with contract**



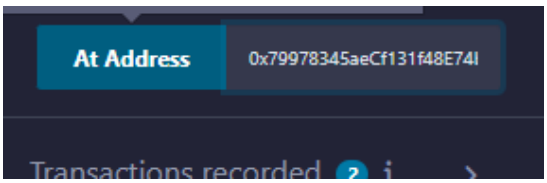
- **After clicking deploy**

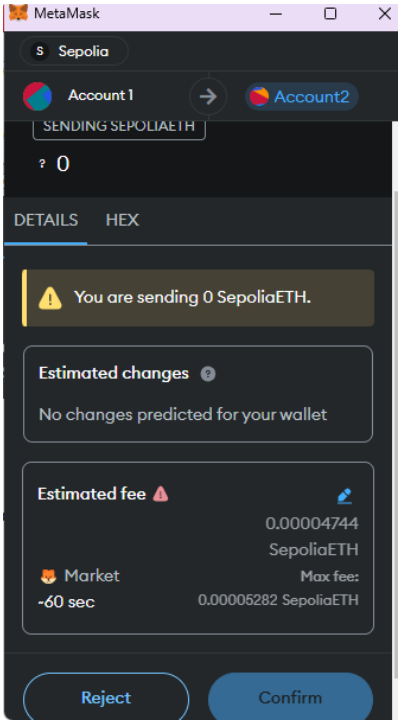

Account 1
Sepolia
Deploy a contract
This site wants you to deploy a contract
Estimated changes
No changes predicted for your wallet
Request from
remix.ethereum.org
Network fee
0.0008 ETH $1.94
Speed
Market -15 sec
Cancel
Confirm


Deployed Contracts 1
FUNDCONTRACT AT 0X844...0

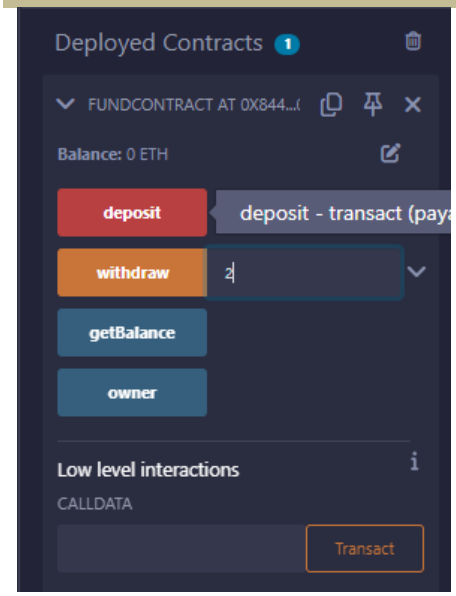

Sepolia
0xb6Fd0...aE3Fd
0.0885 SepoliaETH
Portfolio
Buy & Sell
Swap
Bridge
Send
Receive
Tokens
NFTs
Activity
Oct 25, 2024
Contract deployment
Confirmed
-0 SepoliaETH
-0 SepoliaETH

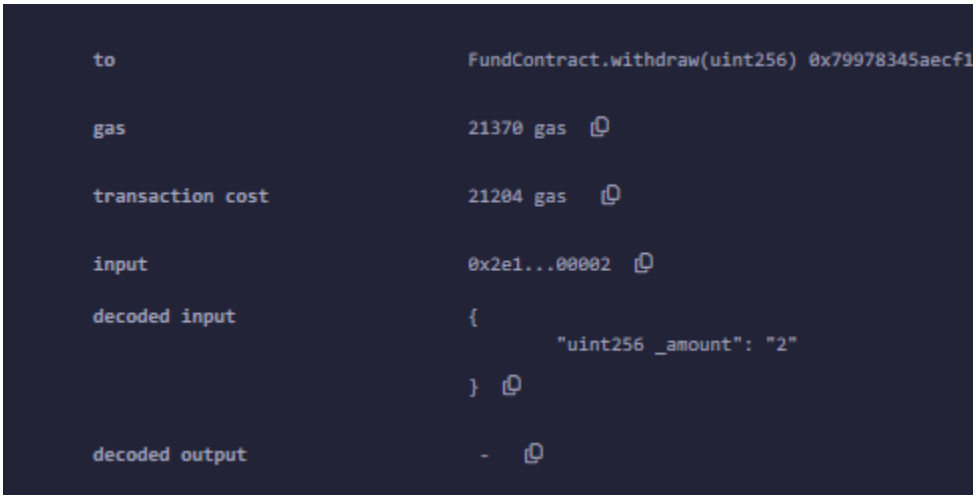
a. To transfer funds (ethers) from user account to contract account

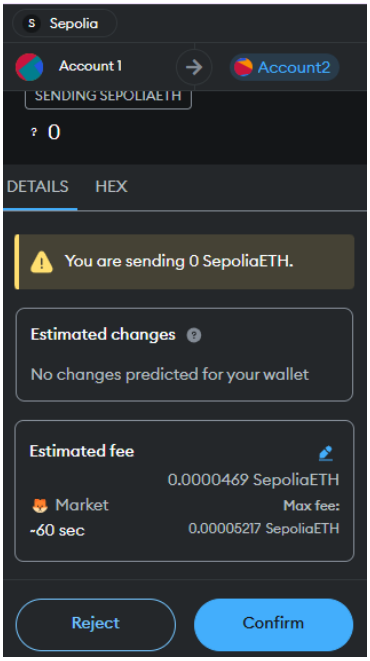


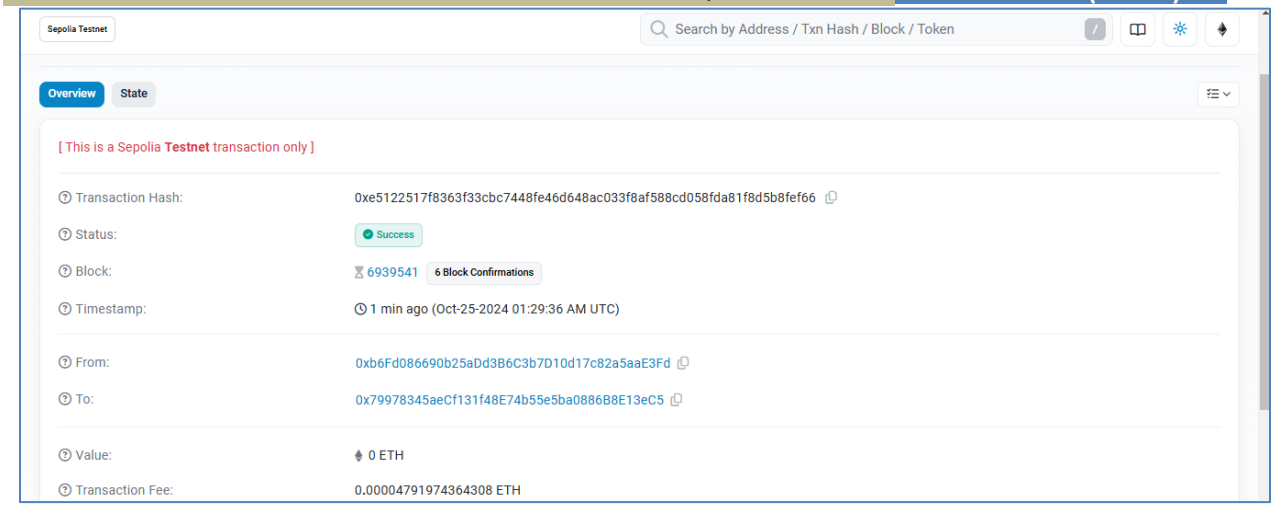


b. To withdraw and deposite funds (ethers) from contract account to user account.

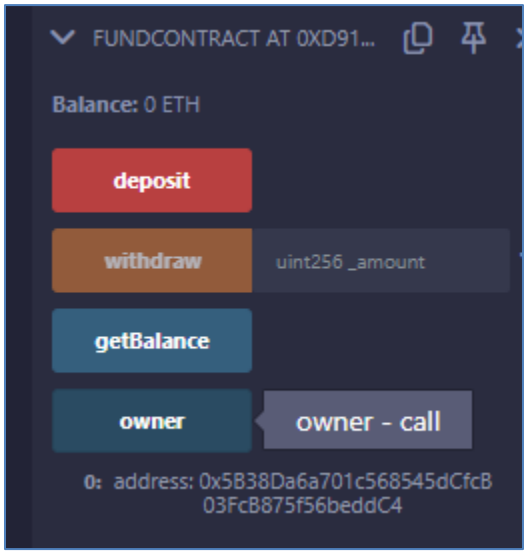

Deployed Contracts 1
FUNDCONTRACT AT 0X844...(
Balance: 0 ETH
deposit
deposit - transact (pay
withdraw
2
getBalance
owner
Low level interactions
CALLDATA
Transact

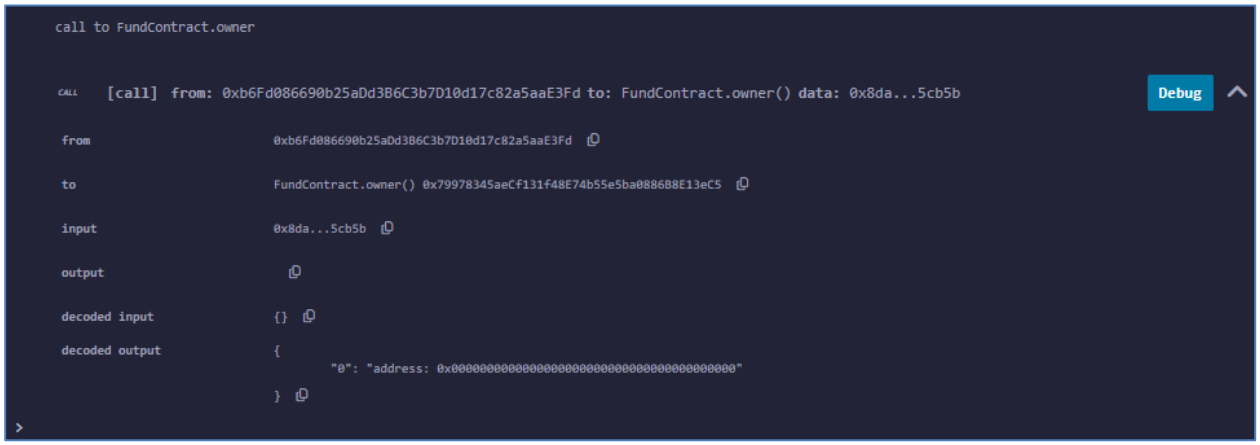

to
FundContract.withdraw(uint256) 0x79978345aecf1
gas
21370 gas
transaction cost
21204 gas
input
0x2e1...00002
decoded input
{
"uint256 _amount": "2"
}
decoded output
-


Sepolia
Account 1
Account2
SENDING SEPOLIAETH
? 0
DETAILS
HEX
You are sending 0 SepoliaETH.
Estimated changes
No changes predicted for your wallet
Estimated fee
0.0000469 SepoliaETH
Market
-60 sec
Max fee:
0.00005217 SepoliaETH
Reject
Confirm



c. To apply restriction that only owner of the contract can withdraw funds (ethers) from contractaccount to his/her user account.





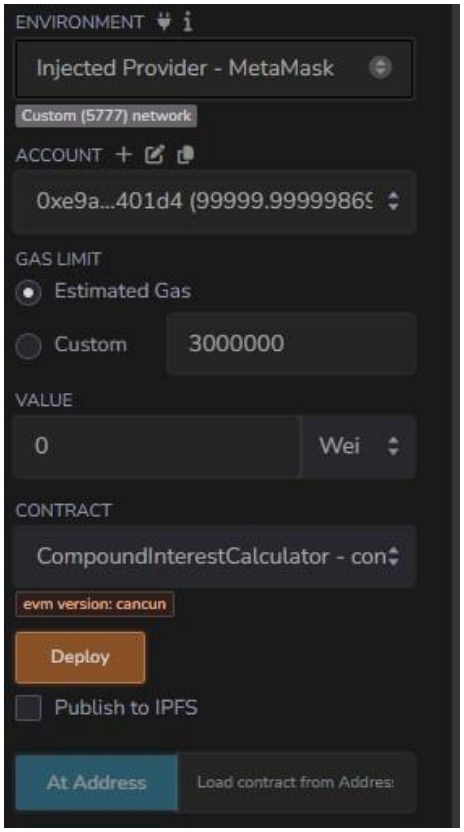
5. Write a smart contract to calculate the compound interest and deploy it on **Ganache** using **injected provider**.

Output :

CompoundIntrest.sol:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract CompoundInterestCalculator {
function calculateCompoundInterest(uint256 _principal, uint256 _rate, uint256 _time, uint256 _n)
public pure returns (uint256) {
require(_principal > 0, "Principal must be greater than 0");
require(_rate > 0, "Rate must be greater than 0");
require(_time > 0, "Time must be greater than 0");
require(_n > 0, "Number of times interest applied must be greater than 0");
uint256 base = (1e18 + (_rate * 1e18 / (100 * _n)));
uint256 exponent = _n * _time;
uint256 amount = (_principal * power(base, exponent)) / 1e18;
uint256 compoundInterest = amount - _principal;
return compoundInterest;
}
function power(uint256 base, uint256 exponent) public pure returns (uint256) {
uint256 result = 1e18; // Start with 1 (in 18 decimal precision)
while (exponent > 0) {
if (exponent % 2 == 1) {
result = (result * base) / 1e18; // Multiply and maintain precision
}
base = (base * base) / 1e18; // Square the base and maintain precision exponent /= 2; // Divide exponent by 2
}
return result;
}
}
```

- Deploy the contract



- Transactions on Ganache

- Transaction

Truffle - Ganache

6. Build and test decentralized application **(Dapp) for Election Voting System** on the local Ethereum Blockchain Network **Ganache** using **truffle suite**.

Output :

Code :

- **VotingSystem.sol**

```
//SPDX-License-Identifier: MIT
pragma solidity >=0.5.0 <0.8.27;
contract VotingSystem {
   struct Candidate {
      uint256 id;
      string name;
      uint256 voteCount;
   }
   mapping(address => bool) public voters;
   mapping(uint256 => Candidate) public candidates;
   uint256 public candidateCount;
   event votedEvent(uint256 indexed _candidateId);
   constructor() public {
      addCandidate("Candidate 1");
      addCandidate("Candidate 2");
      addCandidate("Candidate 3");
   }
   function addCandidate(string memory _name) public {
      candidateCount++;
      candidates[candidateCount] = Candidate(candidateCount, _name, 0);
   }
   function vote(uint256 _candidateId) public {
      require(!voters[msg.sender], "You already voted");
      require(_candidateId > 0 && _candidateId <= candidateCount);
      voters[msg.sender] = true;
      candidates[_candidateId].voteCount++;
      emit votedEvent(_candidateId);
   }
   function getCandidateDetails(uint _candidateId) public view returns (uint,string memory,uint) {
     return (candidates[_candidateId].id, candidates[_candidateId].name, candidates[_candidateId].voteCount);
   }
}
```

- **2_delpoy_contracts.js**

```
var VotingSystem = artifacts.require("./VotingSystem.sol");
module.exports = function(deployer)
{
deployer.deploy(VotingSystem);
};
```

- **Open Terminal and type truffle migrate**

```
Compiling your contracts...
===========================
> Compiling .\contracts\VotingSystem.sol
> Artifacts written to C:\Users\dhruv\OneDrive\Desktop\blockchain-toolkit\build\contracts
> Compiled successfully using:
   - solc: 0.5.16+commit.9c3226ce.Emscripten.clang


Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


2_deploy_contracts.js
=====================

   Deploying 'VotingSystem'
   ------------------------
   > transaction hash:    0x38112f2c9c024b2d8124f7d1726d477436b2415caa5f419188594933ec6327e2
   > Blocks: 0            Seconds: 0
   > contract address:    0x2Ae052232B70e9E5Bf8b9f97BFcd550b6F5E6776
   > block number:        1
   > block timestamp:     1729942291
   > account:             0x3C0BF12BDf9B792e3E309152B47427f5C6E33226
   > balance:             99.999998040997
   > gas used:            653001 (0x9f6c9)
   > gas price:           0.003 gwei
   > value sent:          0 ETH
   > total cost:          0.000001959003 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:      0.000001959003 ETH

Summary
=======
> Total deployments:   1
> Final cost:          0.000001959003 ETH
```

7. Build and test decentralized application, **(Dapp) for Banking System** on the local Ethereum Blockchain Network **Ganache** using **truffle suite**.

- **BankingSystem.sol:**

```
pragma solidity >=0.5.16;
contract SimpleBank {
   // State variable to store the balance
   uint256 private balance;
   // Constructor to ini alize balance
   constructor () public {
      balance = 0;
   }
   // Func on to add (deposit) amount to the balance
   function addAmount(uint256 amount) public {
      balance += amount;
   }
   // Func on to withdraw amount from the balance
   function withdrawAmount(uint256 amount) public {
      require(amount <= balance, "Insufficient balance");
      balance -= amount;
   }
   // Func on to check the remaining balance
   function checkBalance() public view returns (uint256) {
      return balance;
   }
}
```

- **2_deploy_contracts.js**

```
const SimpleBank = artifacts.require("SimpleBank");
module.exports = function (deployer) {
   deployer.deploy(SimpleBank);
};
```

```
Compiling your contracts...
===========================
> Compiling .\contracts\BankingSystem.sol
> Artifacts written to C:\Users\dhruv\OneDrive\Desktop\blockchain-toolkit\build\contracts
> Compiled successfully using:
   - solc: 0.5.16+commit.9c3226ce.Emscripten.clang


Starting migrations...
======================
> Network name:    'development'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


2_deploy_contracts.js
=====================

   Deploying 'SimpleBank'
   ----------------------
   > transaction hash:    0x0866874b64a469b2a3b7ffba5b9681e1dc2942d156c9781c20cedd4be2608ae6
   > Blocks: 0            Seconds: 0
   > contract address:    0x0346Bb526acEBB459a88549285E6610B65438e37
   > block number:        1
   > block timestamp:     1730023929
   > account:             0xe8b670Ee7D3Ab9C1A8b61aA17cbF776f98705ffA
   > balance:             99.999999573139
   > gas used:            142287 (0x22bcf)
   > gas price:           0.003 gwei
   > value sent:          0 ETH
   > total cost:          0.000000426861 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:      0.000000426861 ETH

Summary
=======
> Total deployments:   1
> Final cost:          0.000000426861 ETH
```

Conclusion: Developed and deployed Dapp in Ethereum.