PG_DFBD

Programming for FinTech and Blockchain_Solidity

1. Clone the repository git clone https://github.com/balajipachai/pg-dfbd.git

2. Read this and make sure you follow it. Git Commit Style Guide

3. Create a branch using your name Example: git checkout -b balaji-shetty-pachai

4. Create PDF files of the assignments.

5. Commit the PDF files on your respective branches and push those to the repository.

6. Faucet link:

   o https://goerli-faucet.mudit.blog/

   o https://faucet.paradigm.xyz/

Assignment 1

- Difference between public and private and consortium blockchain.

- Read about Merkle Trees w.r.t. Blockchain

- Merkle Tree Openzeppelin smart contract

- Double spending in blockchain

- Difference between PoS & PoW

Assignment 2

- Using Github

  o How to clone repo?

  o How to create a branch in github?

  o How to make a commit?

  o How to push changes to the remote repository?

- What are ommers block in blockchain?

- What is hard fork and soft fork in blockchain?

- What is difficulty bomb?

- What is Re-entrancy attack?

- Difference between ERC721 and ERC20.

- Install and run ganache and attach the screenshot in the pdf that will be pushed to GitHub.

- Write a short note on your understanding of HD wallet.

- Characteristics of IPFS.

- What is a rainbow table attack?

- What is the payable function in solidity?

- How library contract is different with other contract in solidity?

- Create a mist wallet and add the address to the pdf that will be pushed to github.

- What is opensea with respect to NFT?

- What is RLP encoding in ethereum?

- Read about solidity assembly from solidity read the docs.

- Characteristics of a decentralized storage network.

- What is meant by turing complete?

Assignment 3

Assignment 3:

- Write one liner explainer for ethereum signature data v,r and s?

- How to delete a branch github from both local as well as remote repo?

- Why Ethereum is called the world computer?

- What is CryptoKitty in Ethereum blockchain?

- Do the summation of 132 transaction gas usage and ensure it is <= 30 Million in block https://goerli.etherscan.io/block/7842712

- Write a short not on the DAO hack and explain it simply.

- What is the name of Ethereum's PoS algorithm?

- What is the name of Ethereum's PoW algorithm?

- Go through the Ethereum Yellow Paper and Jellow Paper and White Paper.

- How does the EVM knows which function to execute of a smart contract? Since everything is bytecode. (Method IDs of smart contracts)

- What is the major difference between HTTP and IPFS?

- Read about location based addressing and content based addressing.

- Make sure you have Goerli ETH in your Metamask wallet.

- How does metamask stores private keys in browser?

Assignment 4

- What is a full node in blockchain?

- Difference between remote client and light client?

- When should a full node be run?

- If I want to mine new blocks then I should run a full node. True or False.

- From the clients mentioned in

  o Choose any ethereum client and run a single node as we have done for 3 nodes using Geth client

  o Document the steps that you follow to achieve the goal.

- Get command line options

- What are upgradeable smart contracts?

Assignment 5

- Why do we need a Personal Blockchain even though we have Testnet OR Private Network?

- [Read about Ethereum Opcodes](#)

- How to form mainnet or testnet using Ganache?

- What is snapshot in ganache?

- How to fast forward time in ganache?

- How to impersonate an account using ganache?

- What is the difference between quick start workspace and already saved workspace in Ganache?

- Activity:

  - Launch Ganache

  - Connect Metamask to localhost 8545

  - Open Remix IDE

    - Environment - Injected Provider

    - Create HelloWorld contract

    - Deploy the contract

    - Create Counter contract

    - Deploy the coutner contract

      - Perform Increment & Decrement Transactions

Assignment 6

- Are Ommer blocks included in the blockchain?

- Deploy Counter contract on the **private n/w** and perform Increment & Decrement Transactions.

- What is CREATE2 in Solidity or EVM or Ethereum?

- What happens if you try to store 256 using uint8?

- What is the difference between **address** & **address payable**?

- Apart from msg.sender & block.timestamp, list all the global variables of Solidity.

- What is the difference between **view** & **pure** functions in Solidity?

- selfdestruct in Solidity?

- Why **memory** keyword is used in case of arrays, strings & bytes in Solidity in function arguments or return statements?

- How to call **external functions** from within the same contract in Solidity?

- *COMPLETE SOLIDITY BEGINNER COURSE FROM [LEARNETH FROM REMIX IDE](#)*

- SOLIDITY BEGINNER COURSE SOLUTION CONTRACT SHOULD BE ADDED IN THE FOLLOWING ORDER

  - CHAPTER NAME

  - Assignment

    - Details of the Assignment

  - SOLUTION CONTRACT [ENTIRE SMART CONTRACT CODE]

- ▪ Deployed Address on Ganache

Assignment 8

- Read Blockchain Basics from Solidity Read The Docs PDF and create notes on each topic
- Read The EVM from Solidity Read The Docs PDF and create notes on each topic
- What is the gas usage of SLOAD, SSTORE, MLOAD, MSTORE?
- selfdestruct in Solidity?
- The contracts that we will cover from read the docs must be Verified and Published on the Goerli Testnet. - You have to add the contract URL of Etherscan

Assignment 9

- What are the different ways in which import can be used in Solidity?
- How to use Openzeppelin's SafeMath library?
- Can we use multiple SPDX licenses? Yes/No, Give reason. (Try out in Remix)
- Develop a Smart Contract called MyFriends OR PGDFBD_Batchmates
- What is the largest number that can be represented using 256 bits?
- Try assigning a value to Fixed Point Number in Solidity using Remix
- What are contract types & integer literals in Solidity?
- Perform conversion from address to address payable.
    - o address to uint160
    - o address to bytes20
- What is the difference between transfer & send when it comes to addresses?
- Difference between call, staticcall & delegatecall
- Check does your address passes the Checksum test.
- What is address checksum test?
- Deploy Enums Test Contract on Goerli Testnet

Assignment 10

- Why does Solidity has memory/storage/calldata data location?
- Understand array slice operator [:]
- Why memory array cannot be dynamic?
- Try to deploy Array Literal Example, wherein function g() is public view instead of public pure [Explain whether you get an error or warning or can you deploy the contract?]
- What is the exception for accessing non-existing index of an array in Solidity?
- Try to use array slices in either memory or storage arrays and report your findings.
- Deploy Crowdfunding contract on Goerli Testnet, Verify and Publish the contract, Perform Txs and add those to the PDF

Assignment 11

- What is the gas passed by .send() & .transfer() in Solidity?

- Deploy SendContract from readthe docs on Goerli Testnet.

  - Trap this contract into an Unusable state, i.e. no one should be able to call becomeRichest() [In simple words txs involving becomeRichest must fail]

Assignment 12

- Where does npm installs packages (package location)?

- Create an NFT contract and deploy on Goerli. Instead of MyNFT use the name YourNameNFT

- Create a list of functions of OZ's Ownable, AccessControl, Pausable contract

- What is MultiSigWallet contract?

- What are the different types of ERC20 provided by OZ? (Define and its usage)

- Creae and deploy ERC20, ERC721, ERC777 & ERC1155 contracts on Goerli Testnet

- List differences between ERC20, ERC721, ERC777 & ERC1155