ASSIGNMENT 03

1) **Write one liner explainer for ethereum signature data v,r and s?**
   v, r, s are the values for the transaction's signature. They can be used as in Get public key of any ethereum account. r and s are outputs of an ECDSA signature, and v is the recovery id.

2) **How to delete a branch github from both local as well as remote repo?**

   Delete a local Git branch, follow these steps:

   - Open a Git BASH window or Command Window in the root of your Git repository
   - If necessary, use the git switch or checkout command to move off the branch you wish to delete
   - Issue the
     git branch --delete <branchname>
     command to delete the local branch

   - Run the git branch -a command to verify the local Git branch is deleted

   Delete a remote branch is:

   - git push remote_name -d remote_branch_name
   - Instead of using the git branch command that you use for local branches, you can delete a remote branche with the git push command.
   - Then you specify the name of the remote, which in most cases is origin.
   - -d is the flag for deleting, an alias for --delete.
   - remote_branch_name is the remote branch you want to delete.

3) **Why Ethereum is called the world computer?**

As a relatively new development utilizing bitcoin technology, Ethereum aims to implement a globally decentralized, un-ownable, digital computer for executing peer-to-peer contracts. Put more simply, Ethereum is a world computer you can't shut down. Ethereum's combination of features allow it to provide users smart contracts and decentralized applications. It is an extension of the blockchain concept of data, which validates, stores, and replicates transaction data on many computers around the world.

4) **What is CryptoKitty in Ethereum blockchain?**

CryptoKitties is a blockchain game on Ethereum developed by Canadian[1] studio Dapper Labs that allows players to purchase, collect, breed and sell virtual cats.

A CryptoKitty's ownership is tracked via a smart contract on the Ethereum blockchain. Each CryptoKitty is represented as a non-fungible token using the ERC-721 token standard on Ethereum.

5) **Write a short not on the DAO hack and explain it simply.**

DAO stands for Decentralized Autonomous Organization. It is a decentralized organization to facilitates cryptocurrency transactions without any managers or board. It made use of the Ethereum network.

The DAO was developed in such a way that it allowed investors to invest their money. In return, the organization would provide them with tokens that allowed the investors to vote rights on many projects.

DAO hack: Hackers attacked DAO because it was vulnerable. It allowed the hackers to drain almost one-third of ether. There was a token sale for 28 days. Many investors invested money and DAO raised 15 million ethers, But before the end of the token sale, one of the onlookers was concerned about vulnerability. There was a bug in smart contract wallets. While the programmers were fixing the bug issue, the attacker exploited other loopholes in the code and started to steal funds. He attacked by making a small contribution and requested withdrawal using a recursive function. In this way, the attacker was able to draw almost 3.6 million ether.

6) **What is the name of Ethereum's PoS algorithm?**

The algorithm used in proof-of-stake Ethereum is called LMD-GHOST, and it works by identifying the fork that has the greatest weight of attestations in its history.

7) **What is the name of Ethereum's PoW algorithm?**

Ethereum mining used an algorithm known as Ethash. The fundamental idea of the algorithm is that a miner tries to find a nonce input using brute force computation so that the resulting hash is smaller than a threshold determined by the calculated difficulty. This difficulty level can be dynamically adjusted, allowing block production to happen at a regular interval.

8) **Go through the Ethereum Yellow Paper and White Paper.**

Ethereum Yellow Paper:

https://ethereum.github.io/yellowpaper/paper.pdf

A yellow paper is a more technical version of the white paper. It presents the scientific details of the technology in a very concise way. If you think of a white paper as a proposal, the yellow paper can be a part two where all the specific details are.

Ethereum White Paper:

https://ethereum.org/en/whitepaper/

A white paper is a marketing document used to persuade potential customers to learn more or use the service or technology. It should contain a problem, the solution, how the token works to create the solution, the team, and the deployment plan. Think of it like a proposal.

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

The EVM will execute the contract code. The EVM just executes the bytecode and does not know anything about functions. Solidity, Serpent and web3.js implement the same Application Binary Interface, which is how functions and data are encoded. An EVM compiler produces contract code that simulates functions according to the ABI.

10) What is the major difference between HTTP and IPFS?

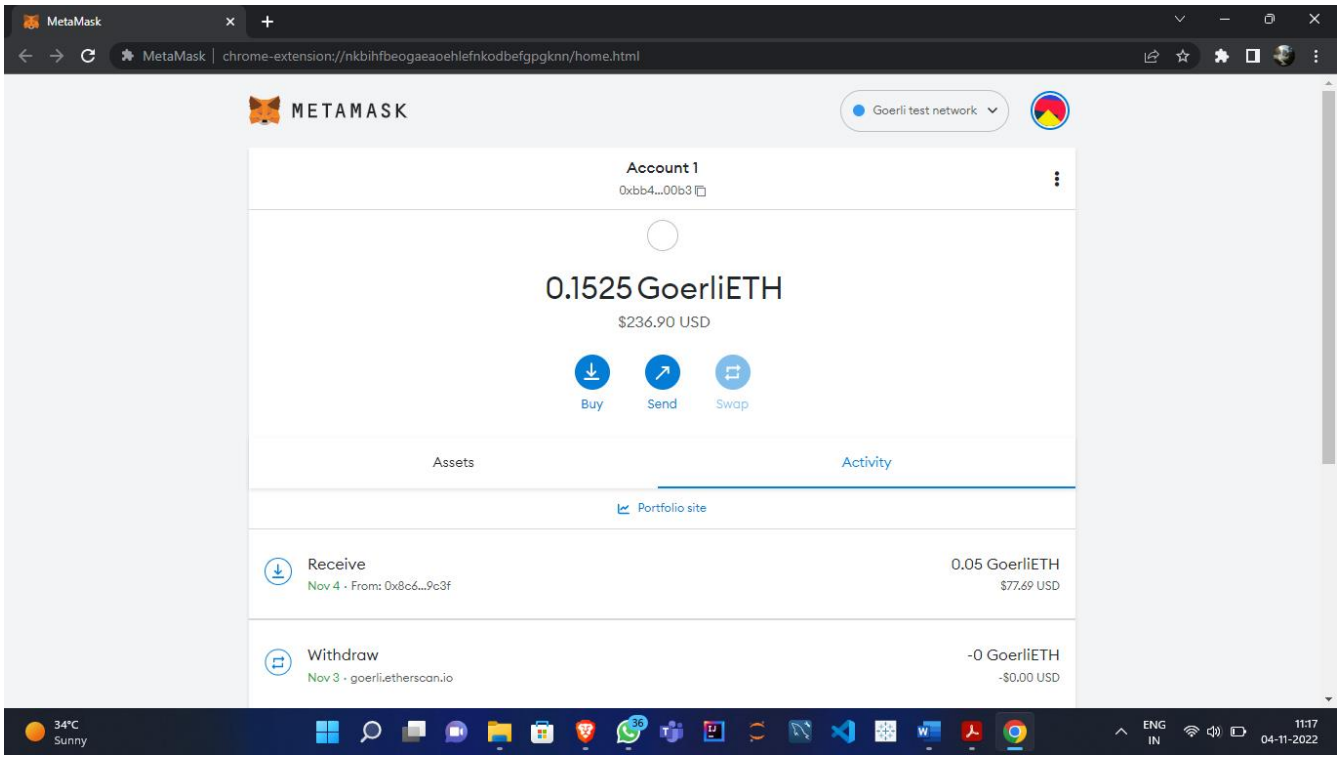
HTTP	IPFS
HTTP stands for HyperText Transfer Protocol.	IPFS stands for InterPlanetary File System.
Data is not persistent in HTTP.	Data persistent in IPFS.
HTTP is not efficient.	IPFS efficient compare to HTTP.
It uses a centralised client server approach.	It uses a decentralised peer to peer approach.
Data is requested using the address on which data is hosted.	Data is requested using the cryptographic hash of that data.
Data cannot be accessed if the server is down or fails or any link gets broken.	Data is copied to multiple nodes, hence it can be accessed whenever needed.
The bandwidth provided is low, as multiple clients request from a single server at the same time.	Bandwidth is high, as data is requested from the closest peer who has the copy of that data.
One has to set up a hosting server or pay for one, in order to make content publicly available.	Uploading content on the IPFS network does not require a host server, every node hosts the data on the network.
HTTP is well established as an industry standard, this is where HTTP has an upper hand.	IPFS is relatively newer and is not yet as popular as HTTP.
HTTP support is inbuilt on almost all machines.	To run IPFS you need to access it using the HTTP to IPFS portal or manually setup up an IPFS node on your machine.
HTTP is used by almost everyone to access the web.	Currently, there is a shortage of IPFS nodes due to it’s low popularity among the laymen.

11) Read about location based addressing and content based addressing,

Location-based addressing: dentifying data by its physical address. Location-based addressing in a computer is a file in a folder; for example, a PowerPoint presentation in a Windows computer might be addressed as c:\users\maria\documents\crypto.ppsx. On a website, that file might be found at www.computerlanguage.com/crypto.ppsx.

Content based addressing: Content-addressable storage (CAS), also referred to as content-addressed storage or fixed-content storage, is a way to store information so it can be retrieved based on its content, not its name or location. It has been used for high-speed storage and retrieval of fixed content, such as documents stored for compliance with government regulations.

12) **Make sure you have Goerli ETH in your Metamask wallet** .



13) How does metamask stores private keys in browser?

Centralized exchanges like Coinbase store your private keys on their servers, while for modern self-custodial wallets like MetaMask that are browser-based, the private keys are kept in the browser's data store. MetaMask stores the Secret Recovery Phrase, passwords, and private keys in an encrypted format locally on the device where it's installed. MetaMask will never share your public address with a website unless you give it permission. This means you are always browsing privately and control the data you share with an application. It also makes it easy to browse between different applications without creating a new account each time.

Metamask is a Chrome extension (or is directly integrated with Brave), and it stores its private keys in the browser -- not on a remote server. It's as secure as running a wallet that you haven't yourself audited the source code of (so, as secure as Exodus, Parity, MyEtherWallet, or Mist).