**Week 4 Seminar Solutions**

1. Check your private key and address in your Metamask.

2. Send 0.01 TEST ETH via Sepolia Test Netwok to me.

0xE704dA48a0156c20D9ea99CB497E6F970Cacdc3A

3. How does proof of stake (PoS) differ from proof of work (PoW)? And the advantages of PoS.

With blockchains such as Ethereum, there is a need to validate transactions in a decentralized way. Ethereum, like other cryptocurrencies, previous used a consensus mechanism known as proof of work (PoW).

In this system, miners use computer hardware processing power to solve complex mathematical puzzles and verify new transactions. The first miner to solve a puzzle adds a new transaction to the record of all transactions that make up the blockchain. They are then rewarded with cryptocoins. However, this process can be energy-intensive.

Proof of stake (PoS) differs in that instead of miners, transaction validators stake crypto for the right to verify a transaction. These validators are selected to propose a block based on how much crypto they hold, and how long they’ve held it for.

Other validators can then attest that they have seen a block. When there are enough attestations, a block can be added to the blockchain. Validators then are rewarded for the successful block proposition. This process is known as “forging” or “minting”.

The main advantage of PoS is that it is far more energy-efficient than PoW, as it decouples energy-intensive computer processing from the consensus algorithm. It also means that you don’t need a lot of computing power to secure the blockchain.

4. Explain the difference between Externally Owned Accounts (EOAs) and Contracts (contract account).

The type of account you created in the MetaMask wallet is called an externally owned account (EOA). Externally owned accounts are those that have a private key; having the private key means control over access to funds or contracts.

That other type of account is a contract account. A contract account has smart contract code, which a simple EOA can’t have. Furthermore, a contract account does not have a private key. Instead, it is owned (and controlled) by the logic of its smart contract code: the software program recorded on the Ethereum blockchain at the contract account’s creation and executed by the EVM.

Contracts have addresses, just like EOAs. Contracts can also send and receive ether, just like EOAs. However, when a transaction destination is a contract address, it causes that contract to run in the EVM, using the transaction, and the transaction’s data, as its input. In addition to ether, transactions can contain data indicating which specific function in the contract to run and what parameters to pass to that function. In this way, transactions can call functions within contracts.

**Note that because a contract account does not have a private key, it cannot initiate a transaction.** Only EOAs can initiate transactions, but contracts can react to transactions by calling other contracts, building complex execution paths. One typical use of this is an EOA sending a request transaction to a multisignature smart contract wallet to send some ETH on to another address. A typical DApp programming pattern is to have Contract A calling Contract B in order to maintain a shared state across users of Contract A.

5. Explain the following Ethereum components.

* P2P network

Ethereum runs on the Ethereum main network, which is addressable on TCP port

30303, and runs a protocol called ÐΞVp2p.

* Transactions

Ethereum transactions are network messages that include (among other things) a

sender, recipient, value, and data payload.

* State machine

Ethereum state transitions are processed by the Ethereum Virtual Machine

(EVM), a stack-based virtual machine that executes bytecode (machine-language

instructions). EVM programs, called “smart contracts,” are written in high-level

languages (e.g., Solidity) and compiled to bytecode for execution on the EVM.

* Data structures

Ethereum’s state is stored locally on each node as a database (usually Google’s LevelDB), which contains the transactions and system state in a serialized hashed data structure called a Merkle Patricia Tree.

* Consensus algorithm

Ethereum uses Bitcoin’s consensus model, Nakamoto Consensus, which uses

sequential single-signature blocks weighted in importance by PoW to determine

the longest chain and therefore the current state. However, they already moved to a PoS weighted voting system codenamed Casper, 15 Sept 2022.

* Economic security

PoS.

* Clients

Ethereum has several interoperable implementations of the client software, the

most prominent of which are Go-Ethereum (Geth) and Parity.

6. What is the DAO? Why make an organization like the DAO?

The DAO was an organization that was designed to be automated and decentralized. It acted as a form of venture capital fund, based on open-source code and without a typical management structure or board of directors. To be fully decentralized, the DAO was unaffiliated with any particular nation-state, though it made use of the ethereum network.

The developers of the DAO believed they could eliminate human error or manipulation of investor funds by placing decision-making power into the hands of an automated system and a crowdsourced process. Fueled by ether, the DAO was designed to allow investors to send money from anywhere in the world anonymously. The DAO would then provide those owners tokens, allowing them voting rights on possible projects.

The DAO launched in late April 2016 thanks to a month-long crowdsale of tokens that raised more than $150 million in funds. At the time, the launch was the largest crowdfunding fundraising campaign of all time.