**Blockchain Notes:**

**Smart Contracts:**

Smart contracts are self-executing pieces of code placed on the blockchain. They are paired with some type of oracle to get some information about the real world. A smart contract paired with an oracle is called a hybrid smart contract. Chain-link is a secure decentralized modular oracle network used to bring data into a smart contract and do some external computation.

**Advantages of Blockchain:**

1. Decentralized: They are not controlled by a single centralized entity but are managed by a network of independent users.
2. Transparency: Anything done can be verified by the other users, to ensure that everyone is playing by the same rules.
3. Speed: They are quick and efficient.
4. Immutable: Blockchains cannot be tampered or corrupted, hence they are extremely secure.
5. Removes Counterparty Risk: Smart contracts shift the traditional political brand-based agreements to math-based agreements.
6. Trust minimized agreements:

**DAO - Decentralized Autonomous Organization:**

/\* Need to write definition \*/

Mnemonic: all your accounts

/\* incomplete \*/

Faucet: It is an application that gives us free test tokens, like free test Rinkeby Ethereum.

Block Explorer: It is an application that allows us to see the details of transactions that happen on a blockchain.

**Gas:**

It is a unit of computational measure. Everytime we do something that changes the state of the blockchain, whether it be transferring some token or doing a transaction, we have to pay a fee (native token in nature) to the node operators.

Gas Price: The cost per unit of gas. It is based on the ‘demand’ of the blockchain. Only so many transactions can be processed and put into a node at once, so if there are more people, the gas prices will be higher to get your transaction executed faster.

Gas Limit: Max amount of gas that is permitted in a transaction.

Transaction Fee: Gas Used x Gas Price (21000 gas @ 1 Gwei per gas = 21000 Gwei)

**Hash:**

It is a unique string of fixed length that is used to identify keys or some piece of data. Ethereum uses Keccak-256 hash function.

**Block:**

It has 4 components:

1. Block Number
2. Nonce: A number used once to find the solution to the blockchain problem.
3. Data
4. Hash of Previous Block in the Chain

The hash of the current block is computed primarily using these 4 components, however, depending on the blockchain, it can vary.

**Mining:**

It is the process of finding the ‘solution’ to the blockchain ‘problem’. For example, let’s say the hash of the block must start with 4 zeroes, so, the miners have to brute force the nonce and find a corresponding hash that meets the requirement. The node operators are awarded by the blockchain itself and are paid some of the gas fees from the transactions for this mining.

**Keys and Signing:**

Private Key: A password or key only known to the entity holder.

Public Key: It is derived from a user’s private key using some digital signing algorithm and is used to verify the authenticity of transactions.

Signing a transaction: A person signs the transaction by their private key being hashed with their transaction data. It is verified using the same person’s public key which is known to everyone.

**Consensus:**

It is the mechanism which is used to agree on the state of the blockchain. Consensus protocols can be briefly broken into two elements:

1. Chain Selection: Selecting which blockchain is the actual and authentic blockchain.
2. Sybil Resistance: It is a mechanism by which we can decide the author of the block, which node is responsible for mining the block. Prevents someone from making pseudo anonymous nodes, so that they can earn lots of profit.

Block Time: The blockchain ‘problem’ is at times made intentionally harder or easier to manipulate what is known as block time. It is the time between two blocks being published and is proportional to the complexity of the problem.

Nakamoto Consensus: It is a combination of PoW and Longest Chain Selection Rule. This rule states that the chain with the most numbers of blocks is the one that we will use.

Block Confirmations: The number of blocks that the chain is ahead of our transaction.

**Attacks:**

Sybill attack: A user creates a lot of pseudo anonymous accounts to influence the network. This is very hard in PoW and PoS as the former requires a lot of work/computation to be done while the latter requires a lot of collateral.

51% attack: If some entity had the longest chain and could muster 51 percent of the nodes to agree with that chain, then they could essentially do a fork and change the state of the blockchain, being capable of leading it in any direction that they want to. ETH Classic is one of the best examples.

**Disadvantages of PoW:**

Environmental concerns as blocks require a lot of energy to mine and there is a race to solve the problem as fast as possible.

**Proof-of-Stake(PoS):**

The validators of the blockchain have to put up collateral that they will behave honestly. In case of some malpractice, they will lose all or some of that collateral.

In PoS, nodes are randomly chosen to propose the new block and then the rest of the validators verify the new block. The randomness with which the node is chosen is very essential, as the blockchains are deterministic entities.

**Scalability:**

When a lot of people want to use the blockchain, the gas prices skyrocket. This limits the number of people who can participate in the system due to the financial constraints imposed.

Sharding: A main chain will be coordinating amongst several chains that hook into it. This increases the number of chains, effectively increasing the block space that the people can use at any instant.

Layer1, layer2, rollups: kind of like a sharded chain.