**Blockchain Overview**

**Traditional Networks vs Blockchain:**

Traditionally, when you run an application be it a website or something that connects to a server you are interacting with a centralized entity. This is the oppositee of what you may recall from our distributed blockchain example, in that the server is controlled and run by a single centralized group.

Blockchains, as we saw, run on a network of independent nodes. In our previous example, each of the `Peers` was representative of an independent `node` operator. The term `node` typically refers to a single instance of a decentralized system, Peer A would be a `node`. This network, this combination of these nodes interacting with each other is what creates a blockchain. What makes these networks so potent, is that anybody can join. All anyone needs is a little bit of hardware and you can participate in securing a blockchain network. You could go to GitHub and start operating a node in a few seconds!

In the traditional world applications are run by centralized entities and if that entity goes down or is malicious or decides that they want to shut off – they just can. They’re the ones that control everything.

Blockchains, by contrast, don’t have this problem. If one node or one entity that runs several nodes goes down, since there are so many other independent nodes running, it doesn’t matter, the blockchain and the system will persist so long as there is at least one node always running. Luckily for us, the most popular chains like Bitcoin and Ethereum have thousands and thousands of nodes. Malicious nodes are kicked from the network, or even punished in some cases. Majority rules when it comes to the blockchain.

This gives blockchains this incredibly potent immutability trait where nothing can be changed or corrupted so in essence we can think of a blockchain as a decentralized database. In the case of Ethereum it has an extra additional feature where it also can do computation in a decentralized manner now.

**Consensus:**

Let’s talk consensus. This includes `Proof of Work` and `Proof of Stake`. You’ve probably heard these terms before and they’re really important to how these blockchains work.

The `mining` feature of our previous blockchain example was an example of `Proof of Work`

`Proof of Work` and `Proof of Stake` fall under this umbrella of `consensus`. And `consensus` is a really important topic when it comes to blockchains.

`Consensus` is defined as the mechanism used to reach an agreement on the state or a single value on the blockchain especially in a decentralized system.

Very roughly, a consensus protocol in a blockchain or decentralized system can be broken down into two pieces: a chain selection algorithm and a sybil resistance mechanism. Mining, or Proof of Work, is a sybil resistance mechanism. This is what Bitcoin currently uses.

`Proof of Work` is known as a sybil resistance mechanism because it defines a way to figure out who is the block author or which node did the work to mine a block. Sybil resistance is a blockchain’s ability to defend against users creating a large number of pseudo-anonymous identities to gain a disproportionately advantageous influence over said system.

As mentioned, there are two primary types of sybil resistance:

1. Proof of Work

2. Proof of Stake

We’ll look a little closer at `Proof of Work` first.

**Proof of Work:**

Proof of work is a system of sybil resistance used in many blockchains, in its essence a miner needs to go through a very computationally heavy process (mining) to find the block’s answer. As a result, it doesn’t matter how many additional nodes you’re running, each node is obligated to do this work in order to receive a reward. The playing field is kept fair.

**Note:** Some blockchains may make their riddle or their block answer intentionally hard, or intentionally easy to adjust the block time – which is the average time it takes to mine a block. Blocktime is proportional to how difficult these algorithms are.

Proof of Work needs to be combined with a `chain selection rule` to create `consensus`.

A `chain selection rule` is implemented as a means to determine which blockchain is the \_real\_ blockchain. Bitcoin (and prior to the merge, Ethereum), both use something called `Nakomoto Consensus`. This is a combination of Proof of Work (Etherum has since switched to Proof of Stake) and the `longest chain rule`.

In the `longest chain rule`, the decentralized network decides that whichever chain has the most number of blocks will be the valid, or \_real\_ blockchain. When we saw `block confirmations` in Etherscan earlier, this was representing the number of blocks ahead of our transaction in the longest chain.

You’ll sometimes hear people use \*\*Proof of Work\*\* to describe a consensus mechanism, but it’s a little bit inaccurate, it’s really the combination of sybil resistance \_and\_ chain selection that create consensus.

`Proof of Work` also serves as a means to determine who receives transaction fees as we discussed earlier. These transaction fees are paid by whomever initiates the transaction. In a Proof of Work system, every node is competing against eachother to solve the block problem first. The first node to solve the problem gets paid the transaction fees accumulated in the block they mine. In addition to this, miners are also paid a `block reward`, the `block reward` is given by the blockchain itself.

If you’ve previously heard of the Bitcoin Halving – this is the concept of the block reward being cut in half roughly every 4 years.

Block rewards are in the blockchains native currency – Bitcoin = BTC, Ethereum = ETH. This effectively increases the amount of that cryptocurrency in circulation.

**Blockchain Attacks:**

There are two major types of attacks that exist in the blockchain space.

* Sybil Attack – When a user creates a number of pseudo-anonymous accounts to try to influence a network.
* 51% attack – Occurs when a single entity possesses both the longest chain and majority network control. This would allow the entity to `fork` the chain and bring the network onto the entities record of events, effectively allowing them to validate anything.

Blockchains are very democratic. The bigger a blockchain is, the more decentralized, the more secure it becomes.

I encourage you to look into running a node yourself to increase the security of the network!

Proof of Work does come with drawbacks. For example, Proof of Work consumes a LOT of electricity. When you have thousands of nodes all working as hard as they can to solve a block problem the energy consumption is HUGE and as such, so is the potential environmental impact.

With the above in mind, many protocols are choosing the shift to a different consensus mechanism that is more environmentally friendly. The most popular of which is…

**Proof of Stake:**

In contrast to trying to solve a block problem, Proof of Stake nodes put up some collateral that they are going to behave honestly aka they `stake`. If a node is found to be misbehaving, it’s stake is slashed. This serves as a very effective sybil resistance mechanism because for each account, the validator needs to put up more stake and misbehaving risks losing all that collateral.

In a Proof of Stake system, `miners` are known as `validators`. They aren’t actually mining blocks, they’re validating other nodes.

Unlike in Proof of Work, where each node is racing to solve the block problem first, in Proof of Stake, validators are pseudo-randomly chosen to propose the next block and other nodes will validate it.

Proof of Stake of course comes with its own Pros and Cons.

Pros:

* great sybil resistance mechanism
* great for the environment, much less energy

Cons:

* Seen as less decentralized due to upfront staking costs

This raises the question of \_how decentralized is decentralized enough?\_ and I think I need to leave that to the community to decide.

**Layer 1 and Layer 2:**

I want to briefly touch on the concepts of Layer 1 and Layer 2 networks here as well.

1. `Layer 1` solutions: This refers to base layer blockchain implementations like Bitcoin or Ethereum.

2. `Layer 2` solutions: These are applications added on top of a layer one, like Chainlink or Arbitrum

Layer 2s like Arbitrum and Optimism are special in that they’re trying to solve the problem of scalability. These protocols leverage something called `rollups`. We won’t go too deep, but the idea is that the protocols bundle their transactions to be processed by a Layer 1.

**Wrap Up:**

This overview was huge. Amazing work, you now have a fundamental understanding of how blockchains work, how to interact with them and why they’re so secure and empowering.

Lets bring it all home in the final part!