Chapter 14: Consensus.

Simply put, in the context of blockchains, consensus is about being able to arrive at a common state, while maintaining decentralization.

There are 2 most used Consensus algorithms:

1. Proof of Work (Mining):

The real purpose of mining (and all other consensus models) is to secure the blockchain, while keeping control over the system decentralized and diffused across as many participants as possible.

In PoW consensus there is also a corresponding “punishment,” which is the cost of energy required to participate in mining. If participants do not follow the rules and earn the reward, they risk the funds they have already spent on electricity to mine. Thus, PoW consensus is a careful balance of risk and reward that drives participants to behave honestly out of self-interest.

Ethereum’s PoW algorithm is slightly different than Bitcoin’s and is called Ethash.

2. Proof of Stake:

Historically, proof of work was not the first consensus algorithm proposed. Preceding the introduction of proof of work, many researchers had proposed variations of consensus algorithms based on financial stake, now called proof of stake (PoS).

In fact, there is a deliberate handicap on Ethereum’s proof of work called the difficulty bomb, intended to gradually make proof-of-work mining of Ethereum more and more difficult, thereby forcing the transition to proof of stake.

Ethereum’s planned PoS algorithm is called Casper. The introduction of Casper as a replacement for Ethash has been postponed several times over the past two years, necessitating interventions to defuse the difficulty bomb and postpone its forced obsolescence of proof of work.

Casper and Ethash.

In general, a PoS algorithm works as follows. The blockchain keeps track of a set of validators, and anyone who holds the blockchain's base cryptocurrency (in Ethereum's case, ether) can become a validator by sending a special type of transaction that locks up their ether into a deposit.

Importantly, a validator risks losing their deposit if the block they staked it on is rejected by the majority of validators. Conversely, validators earn a small reward, proportional to their deposited stake, for every block that is accepted by the majority. Thus, PoS forces validators to act honestly and follow the consensus rules, by a system of reward and punishment.

The major difference between PoS and PoW is that the punishment in PoS is intrinsic to the blockchain (e.g., loss of staked ether), whereas in PoW the punishment is extrinsic (e.g., loss of funds spent on electricity).

Ethash is the Ethereum PoW algorithm. It uses an evolution of the Dagger–Hashimoto algorithm, which is a combination of Vitalik Buterin's Dagger algorithm and Thaddeus Dryja's Hashimoto algorithm.

Application-Specific Integrated Circuits (ASIC).

Use of consumer-level GPUs for carrying out the PoW on the Ethereum network means that more people around the world can participate in the mining process. The more independent miners there are the more decentralized the mining power is, which means we can avoid a situation like in Bitcoin, where much of the mining power is concentrated in the hands of a few large industrial mining operations. The downside of the use of GPUs for mining is that it precipitated a worldwide shortage GPUs in 2017, causing their price to skyrocket and an outcry from gamers. This led to purchase restrictions at retailers, limiting buyers to one or two GPUs per customer.

Casper is the proposed name for Ethereum's PoS consensus algorithm. It is still under active research and development and is not implemented on the Ethereum blockchain.

Casper is being developed in two competing “flavors”:

Casper FFG: “The Friendly Finality Gadget”.
Casper CBC: “The Friendly GHOST/Correct-by-Construction”.

Vitalik Buterin, who was leading the research work on Casper FFG, decided to “scrap” the hybrid model in favor of a pure PoS algorithm. Now, Casper FFG and Casper CBC are both being developed in parallel.

The principles and assumptions of consensus algorithms can be more clearly understood by asking a few key questions:

- Who can change the past, and how? (This is also known as immutability.)
- Who can change the future, and how? (This is also known as finality.)
- What is the cost to make such changes?
- How decentralized is the power to make such changes?
- Who will know if something has changed, and how will they know?

So, which consensus algorithm is better?

It is likely that no algorithm can optimize across all dimensions of the problem of decentralized consensus.

Even if they were to be better, better at what?
Immutability? Finality? Decentralization? Cost?

In the end, there might not be a “correct” answer, just as there might be different answers for different applications.

The entire blockchain industry is one giant experiment where these questions will be tested under adversarial conditions, with enormous monetary value at stake. In the end, history will answer the controversy.