Disclaimer: This article probably requires basic knowledge about blockchain networks.

Introduction

In a public decentralized network, consensus between participants is arguably the most important element because there should only be one source of data considered truthy, and to actually communicate and perform meaningful actions with each other, nodes must agree on one state only. Consensus is also the reason why blockchain technologies was born - to make only one source of history public and unchangeable, thus giving out one agreed state.

If you don't understand what I have said, then here's a little bit simpler explanation: With centralized networks, there is only one source of information, and that's from the third party provider of the service you are using. But with decentralized networks, everyone can have their own opinions, and they can also lie, but truth is truth, and there should only be one source of truth, blockchain was designed to achieve this.

Going further

There are many consensus algorithms out there, but the two most popular would be proof of work and proof of stake.

PoW requires nodes to calculate one correct value called `nonce` to make a block's hash reach a requirement as proof, the first node to get the proof will be awarded with coins, and get to create the next block in the blockchain. This system keeps nodes honest as they can get rewards for being so, and it also helps nodes agree on one state because only the winner's block gets added to the chain. Furthermore, it is trustless and decentralized since every person's proof is random, and everyone has a chance to be the winner.

Proof of stake takes a different approach, rather than competing using computational power, nodes use staked money. The original idea is to have nodes stake their coins to become special nodes called `validators`. Like miners in PoW, validators are the ones who create new blocks. Nodes that have more money have more chance to be picked as the block creator, and cheating validators or offline validators must be punished by having their staked coin burned (this action is also called slashing). While this is a "workable" idea, there are still many caveats, you will see why in the next sections.

Both consensus algorithms are vulnerable to an attack famously called "the 51% attack", where one individual holds more than 51% (or 33% in some networks) voting power, he can then control the network and perform double-spending attacks however he likes. In PoW, one must have more than 51% computational power, while in PoS, one must have more than 51% of the token supply to attack.

The grand battle

Performance

There is an undeniable truth about proof of work is that it is slow and energy-inefficient since it needs big hardware to calculate complex proof. Proof of stake is usually considered to be a solution to replace proof of work, as it is indeed way faster and saves much more energy compared to proof of work since it doesn't rely on solving complicated problems using expensive hardware hoarding a ton of electricity, but relies on money and a few communication rounds between nodes.

Security

It is often argued that PoW is safer than PoS, however, this is untrue, because many mistake decentralization with security, which may/may not determine security.

Decentralization and trustlessness

This is debatably the most important part when it comes to blockchain networks, because the whole point of implementing all these fancy technology is to achieve decentralization.

The first thing I'm going to address is that many criticisms against PoS is often faulty. The most popular one is about PoS giving the rich all the power so PoW is better than PoS. This is often said in the blockchain community since PoS uses money to receive voting power, BUT, PoW also favors the rich indirectly through expensive hardware - one rich individual can buy better, more costly hardware to gain more power in the network. And technically, even if it is PoW or PoS, miners and validators don't often work individually, but rather work together, forming big pools, so we can say that this problem is irrelevant.

But do note that PoS has one devastating drawback, and I call this "gatekeeping". Gatekeeping is essentially the act of holding more than 51% (the network's threshold) tokens and staying that way forever. This is 100% doable, and there is probably no way around it. In PoW, it is better, but not much since it is just "kind of" solved because computational power is more flexible than money - when a person holds 51% computational power, other nodes can buy more expensive hardware and out-run that person. But there is still a bunch of "but" lying around here, what if that person does the same, I mean, if he has enough money to achieve 51%, how much money do you think he has, he just need to buy more hardware and everything goes in his way. And what if other nodes just give up, and what if other nodes side with the attacker, there are many edge cases that can't really be answered, but it is still fairly better than PoS.

To make the matter worse, proof of stake is poorly implemented in most if not all modern PoS networks. Most networks currently use delegated proof of stake, where you delegate others to be validators, because true proof of stake is actually pretty hard to implement (so yeah, you have been lied to by pretty much every blog and docs since the original proof of stake you hear don't exist). This leads to a ton of problems, and the biggest one is probably losing trustlessness. When you delegate someone, you are effectively trusting that person, and it kind of kills off one of the needed requirements for decentralized networks - to be trustless, to have truthiness without having to trust anybody. Also, DPoS doesn't slash faulty validators, yet another big problem in PoS. And the bad things haven't stopped there, there are also problems about bribery and centralization which I can't just cover up in one article, check this out instead: https://tr3y.io/articles/crypto/dpos-unsustainable.html. While some networks like Polkadot did implement slashing or Algorand where delegation is random, they still run into some problems of DPoS. Another problem is token distribution and staking requirement, in a PoS network, they are the most important parts yet managed poorly. For example, BSC gives 50% of the whole supply to the devs, which is already terrible, but to make matters worse they also set the staking requirement to 10000 BNB, aka 3 million dollars in the time of writing this article. there is also Cardano-the-VC-land and Polygon where 30% of the nodes come from Binance. The best PoS implementation is probably from Ethereum, where slashing is implemented and no delegation is involved. It is also not vulnerable to gatekeeping because of the fact that it used to be a PoW network, which means miners are the ones who hold tokens, not VCs, some rich individuals, or the devs. Still, it is not yet released.

Conclusion

Consensus mechanisms are still pretty young, and not really efficient, hopefully, in the future, a better algorithm can be thought of and used.

By: Nguyen Phu Minh