Why Proof of Stake (Nov 2020)

2020 Nov 06 See all posts

There are three key reasons why PoS is a superior blockchain security mechanism compared to PoW.

PoS offers more security for the same cost

The easiest way to see this is to put proof of stake and proof of work side by side, and **look at how much it costs to attack a network per $1 per day in block rewards**.

GPU-based proof of work

You can rent GPUs cheaply, so the cost of attacking the network is simply the cost of renting enough GPU power to outrun the existing miners. For every $1 of block rewards, the existing miners should be spending close to $1 in costs (if they're spending more, miners will drop out due to being unprofitable, if they're spending less, new miners can join in and take high profits). Hence, attacking the network just requires temporarily spending more than $1 per day, and only for a few hours.

Total cost of attack: ~$0.26 (assuming 6-hour attack), potentially reduced to zero as the attacker receives block rewards

ASIC-based proof of work

ASICs are a capital cost: you buy an ASIC once and you can expect it to be useful for ~2 years before it wears out and/or is obsoleted by newer and better hardware. If a chain gets 51% attacked, the community will likely respond by changing the PoW algorithm and your ASIC will lose its value. On average, mining is ~1/3 ongoing costs and ~2/3 capital costs (see here for some sources). Hence, per $1 per day in reward, miners will be spending ~$0.33 per day on electricity+maintenance and ~$0.67 per day on their ASIC. Assuming an ASIC lasts ~2 years, that's $486.67 that a miner would need to spend on that quantity of ASIC hardware.

Total cost of attack: $486.67 (ASICs) + $0.08 (electricity+maintenance) = $486.75

That said, it's worth noting that ASICs provide this heightened level of security against attacks at a high cost of centralization, as the barriers to entry to joining become very high.

Proof of stake

Proof of stake is almost entirely capital costs (the coins being deposited); the only operating costs are the cost of running a node. Now, how much capital are people willing to lock up to get $1 per day of rewards? **Unlike ASICs, deposited coins do not depreciate, and when you're done staking you get your coins back after a short delay. Hence, participants should be willing to pay much higher capital costs for the same quantity of rewards**.

Let's assume that a ~15% rate of return is enough to motivate people to stake (that is the expected eth2 rate of return). Then, $1 per day of rewards will attract 6.667 years' worth of returns in deposits, or $2433. Hardware and electricity costs of a node are small; a thousand-dollar computer can stake for hundreds of thousands of dollars in deposits, and ~$100 per months in electricity and internet is sufficient for such an amount. But conservatively, we can say these ongoing costs are ~10% of the total cost of staking, so we only have $0.90 per day of rewards that end up corresponding to capital costs, so we do need to cut the above figure by ~10%.

Total cost of attack: $0.90/day * 6.667 years = $2189

In the long run, this cost is expected to go even higher, as staking becomes more efficient and people become comfortable with lower rates of return. I personally expect this number to eventually rise to something like $10000.

Note that the only "cost" being incurred to get this high level of security is just the inconvenience of not being able to move your coins around at will while you are staking. It may even be the case that

the public knowledge that all these coins are locked up causes the value of the coin to rise, so the total amount of money floating around in the community, ready to make productive investments etc, remains the same! Whereas **in PoW, the "cost" of maintaining consensus is real electricity being burned in insanely large quantities.**

Higher security or lower costs?

Note that there are two ways to use this 5-20x gain in security-per-cost. One is to keep block rewards the same but benefit from increased security. The other is to massively reduce block rewards (and hence the "waste" of the consensus mechanism) and keep the security level the same.

Either way is okay. I personally prefer the latter, because as we will see below, in proof of stake even a successful attack is much less harmful and much easier to recover from than an attack on proof of work!

Attacks are much easier to recover from in proof of stake

In a proof of work system, if your chain gets 51% attacked, what do you even do? So far, the only response in practice has been "wait it out until the attacker gets bored". But this misses the possibility of a much more dangerous kind of attack called a **spawn camping attack**, where the attacker attacks the chain over and over again with the explicit goal of rendering it useless.

In a GPU-based system, there is no defense, and a persistent attacker may quite easily render a chain permanently useless (or more realistically, switches to proof of stake or proof of authority). In fact, after the first few days, the attacker's costs may become very low, as honest miners will drop out since they have no way to get rewards while the attack is going on.

In an ASIC-based system, the community can respond to the first attack, but continuing the attack from there once again becomes trivial. The community would meet the first attack by hard-forking to change the PoW algorithm, thereby "bricking" all ASICs (the attacker's *and* honest miners'!). But if the attacker is willing to suffer that initial expense, after that point the situation reverts to the GPU case (as there is not enough time to build and distribute ASICs for the new algorithm), and so from there the attacker can cheaply continue the spawn camp inevitably.

In the PoS case, however, things are much brighter. For certain kinds of 51% attacks (particularly, reverting finalized blocks), there is a built-in "slashing" mechanism in the proof of stake consensus by which a large portion of the attacker's stake (and no one else's stake) can get automatically destroyed. For other, harder-to-detect attacks (notably, a 51% coalition censoring everyone else), the community can coordinate on a **minority user-activated soft fork (UASF)** in which the attacker's funds are once again largely destroyed (in Ethereum, this is done via the "inactivity leak mechanism"). **No explicit "hard fork to delete coins" is required; with the exception of the requirement to coordinate on the UASF to select a minority block, everything else is automated and simply following the execution of the protocol rules**.

Hence, attacking the chain the first time will cost the attacker many millions of dollars, and the community will be back on their feet within days. Attacking the chain the second time will still cost the attacker many millions of dollars, as they would need to buy new coins to replace their old coins that were burned. And the third time will... cost even more millions of dollars. **The game is very asymmetric, and not in the attacker's favor**.

Proof of stake is more decentralized than ASICs

GPU-based proof of work is reasonably decentralized; it is not too hard to get a GPU. But GPU-based mining largely fails on the "security against attacks" criterion that we mentioned above. ASIC-based mining, on the other hand, requires millions of dollars of capital to get into (and if you buy an ASIC from someone else, most of the time, the manufacturing company gets the far better end of the deal).

This is also the correct answer to the common "proof of stake means the rich get richer" argument: ASIC mining *also* means the rich get richer, and that game is *even more* tilted in favor of the rich. At least in PoS the minimum needed to stake is quite low and within reach of many regular people.

Additionally, proof of stake is more censorship resistant. GPU mining and ASIC mining are both very easy to detect: they require huge amounts of electricity consumption, expensive hardware purchases and large warehouses. PoS staking, on the other hand, can be done on an unassuming laptop and even over a VPN.

Possible advantages of proof of work

There are two primary genuine advantages of PoW that I see, though I see these advantages as being fairly limited.

Proof of stake is more like a "closed system", leading to higher wealth concentration over the long term

In proof of stake, if you have some coin you can stake that coin and get more of that coin. In proof of work, you can always earn more coins, but you need some outside resource to do so. Hence, one could argue that over the long term, proof of stake coin distributions risk becoming more and more concentrated.

The main response to this that I see is simply that in PoS, the rewards in general (and hence validator revenues) will be quite low; in eth2, we are expecting annual validator rewards to equal ~0.5-2% of the total ETH supply. And the more validators are staking, the lower interest rates get. Hence, it would likely take over a century for the level of concentration to double, and on such time scales other pressures (people wanting to spend their money, distributing their money to charity or among their children, etc.) are likely to dominate.

Proof of stake requires "weak subjectivity", proof of work does not

See here for the original intro to the concept of "weak subjectivity". Essentially, the first time a node comes online, and any subsequent time a node comes online after being offline for a very long duration (ie. multiple months), that node must find some third-party source to determine the correct head of the chain. This could be their friend, it could be exchanges and block explorer sites, the client developers themselves, or many other actors. PoW does not have this requirement.

However, arguably this is a very weak requirement; in fact, users need to trust client developers and/or "the community" to about this extent already. At the very least, users need to trust someone (usually client developers) to tell them what the protocol is and what any updates to the protocol have been. This is unavoidable in any software application. Hence, the marginal additional trust requirement that PoS imposes is still quite low.

But even if these risks do turn out to be significant, they seem to me to be much lower than the immense gains that PoS sytems get from their far greater efficiency and their better ability to handle and recover from attacks.

See also: my previous pieces on proof of stake.

- Proof of Stake FAQ
- A Proof of Stake Design Philosophy