Haym @SalomonCrypto

Oct 9 · 26 tweets · SalomonCrypto/status/1578941538607845376

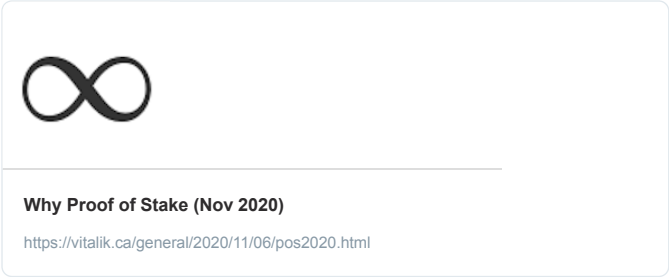
(1/25) "There are three key reasons why PoS is a superior blockchain security mechanism [for @ethereum] compared to PoW:

1) PoS offers more security for the same cost
2) Attacks are much easier to recover from in PoS
3) PoS is more decentralized than ASICs"

- @VitalikButerin

(2/25) The following thread is a summary of a November 2020 blog post by Vitalik.

Although 2 years is an entirety in crypto-years, the arguments still represent the best argument why Proof of Stake (PoS) > Proof of Work (PoW) I have seen (so far).



(3/25) 3 Reasons why PoS > PoW:

1) PoS offers more security for the same cost

Quick, back-of-napkin calculations can clearly illustrate the principle. We are going to evaluate the amount it would cost to attack a network who issues $1 of rewards per day.

(4/25) PoW comes in two flavors: vanilla or ASIC-resistant.

Vanilla PoW is a simple algorithm; you can build specialized machines that are only capable of solving that puzzle (Application Specific Integrated Circuit - ASIC).

ASIC-resistant PoW requires a general purpose GPU.

(5/25) GPU-based PoW

Attack method: rent GPUs to out-mine the existing miners; control the chain long enough to make changes.

Projected cost: ~$0.25

> **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

(6/25) ASIC-based PoW

Attack method: buy enough ASICs to produce enough mining power to control the chain

Projected cost: ~$500

> **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: $487 (ASICs) + $0.08 (electricity+maintenance) = $489**
>
> 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.

(7/25) Proof of Stake (PoS)

Attack method: provide enough stake to control enough validators to control the network.

Projected cost (2020): ~$2200

If you update the cacluation with today's $ETH staking rate (~5%):

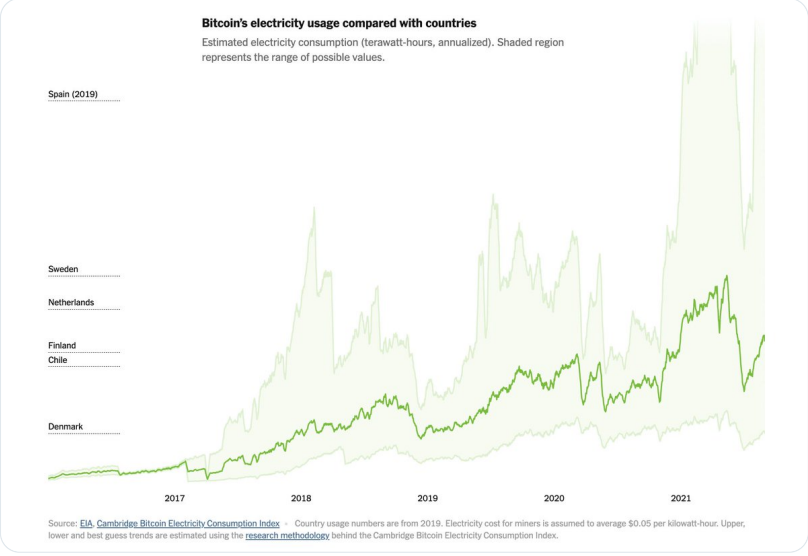
Projected cost (2022): ~$6600

> **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.

(8/25) Thus, PoS gives us AT LEAST an order of magnitude improvement over PoW.

Whats more, the only "cost" PoS imposes is the temporary loss of liquidity (addressed via liquid staking derivatives like $stETH).

In PoW, the cost is wasting an ABSURD amount of electricity.



(9/25) 3 Reasons why PoS > PoW:

2) Attacks are much easier to recover from in PoS

PoW is incredibly difficult to attack, but if the attack is able to gain control the network, it is (probably) entirely at the attackers mercy.

PoS gives @ethereum options.

(10/25) If PoW gets 51% attacked, PoW doesn't have the ability to react; the nature of PoW does not allow good-faith nodes to exclude bad-faith nodes.

(At least as of 2020) the PoW solution to a 51% is "wait until the attacker is done."

But what if they are never done?

> **What Is a 51% Attack?**
>
> A 51% attack is an attack on a cryptocurrency blockchain by a group of miners who control more than 50% of the network's mining hash rate. Owning 51% of the nodes on the network gives the controlling parties the power to alter the blockchain.
>
> The attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control. Reversing transactions could allow them to double-spend coins, one of the issues consensus mechanisms like proof-of-work were created to prevent.

(11/25) An ASIC-based system has a response available: they can deploy a hard fork and change the PoW algorithm, rendering the application-specific ASICs useless.

The chain would revert to the GPU case while the community tried to design, manufacture and distribute new ASICs.

(12/25) The GPU case is even bleaker; there's really nothing you can do.

If an attacker can gain control for even short time (a few days), most honest miners will drop out. Why bother mining if you aren't earning any block rewards?

(13/25) Don't be fooled, PoW is strong; the issue is that once attacked, its vulnerable. Even a small initial attack could permanently destroy the chain.

On the other hand, PoS provides a suite of tools that allows the network to continually extract huge costs from attackers.

(14/25) For some attacks (invalid blocks, reverting finalized blocks, etc) there is a built-in defense: slashing.

Slashing is the process by which an attacker's (and no one else's) stake is automatically destroyed. Slashing also removes the attacker from the validator set.

(15/25) PoS empowers the community to take further action if slashing is insufficient for warding off an attack.

The first line of defense it to activate a minority user-activated soft fork (UASF) and to trigger an inactivity leak.

(16/25) The inactivity leak is an emergency state that allows the @ethereum network to recover finality in the event that more than 1/3 of validators go offline.

This mechanism would largely destroy the attackers funds.

> - When the beacon chain is not finalising it enters a special "inactivity leak" mode.
> - Attesters receive no rewards. Non-participating validators receive increasingly large penalties based on their track records.
> - This is designed to restore finality in the event of the permanent failure of large numbers of validators.

(17/25) The beauty of the UASF defense is that no explicit "hard fork to delete coins" is required.

Once the community has coordinated around a UASF block, the protocol takes care of the rest.

(18/25) So not only does PoS provide more economic security and more tools to defend @ethereum, it can redeploy them over and over.

The first attack will burn billions... as will the second... as will every single attack.

And each time Ethereum will automatically recover.

(19/25) 3 Reasons why PoS > PoW:

3) PoS is more decentralized than ASICs

By this point we've recognized that GPU-based PoW isn't sufficiently secure; at least ASICs provide a reasonable amount of security.

Unfortunately, ASIC-based PoW is inherently centralizing.

(20/25) PoW derives its security from the operation of real computers (ASICs) consuming real electricity. Just like everything else in the real world, PoW is affected by the realities of economies of scale.

More mining = cheaper costs = more profits = more mining

(21/25) Economies of scale are the economic principle behind the idea of "the rich get richer." If costs are inversely proportionally to revenue, capital will eventually accrue to the largest and most competitive producers.

The logical conclusion: monopoly.

(22/25) In PoS, every staked $ETH earns the same yield REGARDLESS of how much is at stake

Bob's stake is growing at the same rate as @LidoFinance, even though Lido is running 115k validators and Bob is running just one

The rich aren't getting rich any faster than the little guy

(23/25) The logical conclusion of $ETH staking? On the surface: all validators grow at the same rate; no one validator captures stake any faster.

Dig a little deeper and you'll find that BOTH PoW and PoS have this problem in the form of MEV.

Fortunately, PoS has a fix for that!

(24/25) The best argument against PoS is about weak subjectivity.

Unlike PoW, a newly-online PoS node must find a third party source to determine the correct head of the chain.

However, PoW does require some implicit trust (eg developers). So, let's just call it a wash.

(25/25) Just under 2 years ago, Vitalik laid out the core argument for @ethereum Proof of Stake, long before we were confident that PoS would ever become a reality.

We are now in a post-Merge world; the deed is done!

Case closed.

Like what you read? Help me spread the word by retweeting the thread (linked below).

Follow me for more explainers and as much alpha as I can possibly serve.

• • •