When Ethereum debuted I was a fan. I put money in The DAO expecting to lose (after all, more things could fail than succeed!) and was fascinated to watch the unfolding hack and fork.

While that fork was low risk and only contentious on philosophical grounds, it sparked a schism in the community. We survived it and the ecosystem is flourishing. Now, as we near another serious fork that is not sparked by necessity, I am not excited. The upcoming fork is motivated with two assumptions: that PoW is inefficient, and that it is slow, and so must be replaced with something that provides cheaper security and is faster. You might say, “Surely, you don’t mean to say it’s an assumption? How can something so energy hungry and with 15s block times (not fast enough for payments) not be improved??”

Over the past few years I have convinced myself of two things:

1. That PoW is the most secure consensus protocol possible, because it introduces a measure of security that is fundamental to the concept of security itself. When the situation is considered in the context of reality, there is no simple mechanism in nature that would require less energy to defend than to attack, which suggests that any proposal that makes such a claim is not likely to be correct.

2. That PoW is the fastest consensus protocol possible, because it does not require voting or any form of chatter around the agreement. Any limitation on speed stems purely from physical limitations of latency and the community’s appetite for storing the transaction history.

For point 1 I have even asked Vitalik to weigh in, and he has. He proposed that hide and seek is a simple game where it costs less to defend than to attack. This is not true, since a hider must also be active and activity (communication or physical) reveals position. An inactive hider is a dead hider. To put it in more base terms, in the realm of security the map is the territory and no trickery or violence is off the table.

For point 2 I hope the argument is easier to understand. See point 2 below.

Both points are explained in two articles:

1. On security: https://medium.com/coinmonks/blockchain-myth-5-proof-of-work-wastes-energy-a848000aea9a

Read just the TLDR to get the picture.

1. On speed: https://medium.com/@brrabski/blockchain-myth-6-proof-of-work-is-slow-8f0a4e0bca2b

I was encouraged to post this by someone. I do not expect to be able to change the minds of everyone here… Most of you are probably staking, which puts you at a conflict of interest in taking an objective look. This post is to warn of the inevitable and perhaps help explain, when things inevitably will not turn out as expected.

Feel free to challenge the propositions on their merits. Many have tried.