

ASICs and Decentralization FAQ

1 About this document.

1. What is the thesis of this document?

The main thrust of this document is that proof-of-work schemes ought to be as simple and dependent on raw computational power as possible. That is, a proof-of-work should tend toward the thermodynamic limit (see a later section for this term) as quickly and directly as possible.

2. Is Proof of Work interesting?

Not really ☹. Replacing or tweaking the proof-of-work algorithm is one of the most popular changes to Bitcoin done by copycat “alt” currencies, but it does not enable any new use cases or features for users of the currency. It is in effect a bikeshed painting¹ change, though as we will see it is not without its dangers.

3. Why did you write this document?

For two reasons:

- (a) to organize and lay out some folklore about proof-of-work which has not been written down in one place;
- (b) to answer some common questions and suggestions regarding Bitcoin’s proof-of-work and those of other currencies (which as established above, is not interesting and therefore no fun to answer repeatedly).

2 What is Proof of Work?

1. What is Proof of Work?

As it applies to Bitcoin, a *proof of work* is a computational proof that some scarce resource was consumed. Such a proof is possible because it appears that computational resources are physically bounded by available time, space and energy²

Further, a proof of work commits to some data, effectively "signing" it with some consumed resource.

2. How and why is it used?

¹See <http://bikeshed.com/> for a history of this phrase.

²See, for example, <http://arxiv.org/abs/quant-ph/0502072> for a discussion on the emergence of fundamental computational limits from physics.

Such proofs are useful because they ensure malicious actors are limited in their capacity to produce valid proofs of alternate histories, giving the remaining actors sufficient time and bandwidth to come to consensus on a single history, as long as they have more resources than the malicious ones.

Bitcoin's main innovation was aligning economic incentives to discourage resource-rich actors from becoming malicious.

Here a "history" is formed by a chain of proofs-of-work, each of which signs (a) a collection of valid Bitcoin transactions, and (b) the previous proof-of-work. Users are able to achieve consensus not only of the transactions, but of their order in time.

3. **How does the proof-of-work affect consensus?**

In order that all actors (including those not "mining" or generating proofs of work) can quickly reach consensus, the proof-of-work must be quickly verifiable. The greater the ratio of generation time to verification time, the better.

In order that all actors can reach consensus, the proof-of-work must require enough time that previously proven transaction history can propagate and be verified before the history is extended. Here "enough time" depends on both on the amount of data to be verified (the blocksize) as well as the speed at which the proof-of-work itself can be verified.

4. **How does the proof-of-work affect decentralization?**

In order that individual actors do not gain a disproportionate advantage — so that in the economic limit one actor has all the mining power and leases it out, obviating the proof-of-work since this is functionally identical (but ecologically trillions of trillions of times worse) to this actor simply digitally signing each transaction — the proof-of-work must be completely parallelizable and require no state. That is, one actor with $2N$ hashing power should have the same return as two actors each with N hashing power.

Bitcoin achieves this property by using a proof-of-work based on finding partial hash preimages. The work is accomplished by repeated hashing, and each attempt has a tiny i.i.d. chance of success (this is derived from the so-called *random oracle assumption* of the specific hash algorithm). This gives rise to a Poisson process, which is well-understood but in some ways unintuitive.

Another crucial way that the proof-of-work affects decentralization is in its physical attributes, which we cover in the next section.

5. **Why does the Poisson process matter?**

This is important enough to warrant its own question. To avoid centralization, it is important that miners can join or leave the network at any time without penalty. It is also important that miners with a lot of computational power should not achieve a disproportionate benefit.

These two requirements are related, because they effectively say that there should be no distinction between devoting more time to mining or devoting more computational power to mining.

To guarantee this, the computation of proof-of-work must be *progress free*, that is, the proof-of-work calculation at time T should not depend on any part of a calculation at time $T' < T$. This, along with the fact that successful proof-of-work calculation should be rare enough to limit block speed, implies that the probability of a proof-of-work being calculated in a time interval $[t_0, t_1]$ is proportional to $(t_1 - t_0)$ but independent of t_0 and t_1 .

These conditions are sufficient to give rise to a *Poisson process*³.

As an example of an unintuitive behaviour of Poisson processes, the expected time right now to the next Bitcoin block is ten minutes (plus or minus the difference between actual hashpower and the difficulty-targeted hashpower). This is independent of how long ago the last block was found, even though, on average, blocks are found every ten minutes.

6. What other algorithmic considerations are there?

Two additional requirements, from Greg Maxwell, are:

- (a) The proof-of-work must be *optimization free*; that is, there should not be any algorithmic speedups which would give an advantage over the standard algorithm. If a speedup exists and is found, there is strong motivation for the discoverer to use it secretly rather than publishing it, gaining an unfair advantage. This contributes to centralization.
- (b) The proof-of-work must be *approximation free*; that is, there should not be a defective variant of the proof-of-work which achieves a speedup in excess of its defect rate. (If this is done in software, it is a special case of the above; however it can be done in hardware as well *e.g.* by using a bad multiplexer which cannot demux certain bitstrings.)

3 The physics of Proof-of-Work.

1. What is (ir)reversible computing and why does it matter?

As this is not a physics paper, this section necessarily contains several claims with neither detail nor justification. The curious reader is encouraged to read the Wikipedia article⁴ and its references.

Reversible, or adiabatic computing, is a term for computing without increase in entropy. Such computations are reversible in time and therefore need to be injective as functions of their input, so a hash-based proof-of-work cannot be completely reversible. However, some components of the hash function may be reversibly computable, which is useful because reversible computations require no energy — more concretely, in the limit as computational speed goes to zero, the energy requirement of reversible computations also goes to zero.

Ordinary, non-reversible computations are subject to Landauer's principle⁵ which provides a lower bound on the energy required to flip a single bit.

³See https://en.wikipedia.org/wiki/Poisson_process.

⁴https://en.wikipedia.org/wiki/Reversible_computing

⁵https://en.wikipedia.org/wiki/Landauer%27s_principle

What this means is that ultimately, any irreversible proof of computational work is also a proof of physical work, *i.e.* energy dissipation.

2. What is the thermodynamic limit?

The thermodynamic limit describes the state at which proof-of-work is actually done at Landauer's lower bound for required energy dissipation. At this point, we are actually better off than the requirement that a single $2N$ -powered actor has the same advantage as two N -powered actors, because now N is proportional not only to hashing speed but also to heat dissipation requirements, and it is easier for two physically-separated actors to dissipate heat than for just one.

Therefore, in the thermodynamic limit we have a physical incentive for decentralization.

Fortunately, because the thermodynamic limit is also the limit of energy efficiency, Bitcoin's incentives for efficient proof-of-work are also incentives for miners to push toward the thermodynamic limit.

3. Who cares about heat dissipation? There are massive economies of scale in buying electricity.

A frequent claim in this document is that using thermodynamic limits to obtain a proof of work creates incentives against centralization because there are diseconomies of scale in cooling, since for any mining operation there are limits to (a) how much heat can be effectively dissipated and (b) how much waste heat can be used for other purposes. To increase heat dissipation capacity requires an engineering and construction outlay; as long as waste heat is useful mining is effectively free, while past that point it is not.

However, no matter what the economics of cooling are (and the above claims are hardly uncontroversial), several people have contacted me, most notably Tim Swanson⁶ and phantomcircuit⁷ to point out that there are massive economies of scale in electrical production, enough to dwarf any decentralization caused by cooling.

I have three responses to this:

- (a) First, these problems are made worse by using other physical limits (e.g. speed-of-light, as in a memory-hard PoW) which don't require miners to cool their equipment. So if Bitcoin's economics force centralization, it is an open problem what (if anything) doesn't.
- (b) In places where the waste heat is directly useful, the cost of mining is merely the difference between electric heat production and ordinary heat production (here in BC, this would be natural gas). Then electricity is effectively cheap even if not actually cheap. As capital costs come down (as ASIC manufacturers stop being backlogged) this will become a more important factor.

⁶Private communication, largely based on data published at <http://bitcoinmagazine.com/12914/bitcoins-made-in-china/>.

⁷On #bitcoin, an unlogged IRC channel.

- (c) The main beneficiary of cheap-electricity centralization are a few well-connected businesses in China. This is something of an accident of history. Over the next few decades we will likely see this countered by
 - i. China's increasing wealth causing their regulatory and environmental costs to come in line with western nations; there will also be pressure against this sort of monopolistic behaviour.
 - ii. Highly centralized power production is inefficient because of line losses. As technology, such as solar power, matures, it will be possible to produce power more locally with lower startup costs and less dependence on geopolitical factors.

These comments reflect a very long-term view of Bitcoin; before Bitcoin can achieve its goals as a worldwide stateless currency where decentralization really matters, there are more pressing problems (usability, scalability, privacy) which need to be dealt with. My expectation is that by the time these problems are solved, these comments will be more immediate.

4 Actual frequently asked questions.

1. Are ASIC's evil?

No, dedicated hardware brings us closer to the thermodynamic limit, and is therefore eventually a good thing for mining decentralization. Also, because ASIC's produce more hashes for the same amount of energy, they produce stronger proofs-of-work with proportionally less environmental impact.

However, ASIC's bring with them a risk of manufacturer centralization, such as what we saw with Bitcoin in the early days of ASIC mining. Market forces eventually broke this monopoly⁸, and one thing which sped up the process is that Bitcoin uses the SHA2 hashing algorithm, which was designed for easy development of dedicated hardware. Therefore, relatively little startup capital is needed to develop Bitcoin ASIC's.

Further, regardless of one's personal feeling toward ASIC's, they are inevitable. Dedicated hardware will always be more efficient than general-purpose hardware (exactly because it is closer to the thermodynamic limit) and Bitcoin's incentives are aligned for ever-increasing efficiency.

2. Is ASIC resistance desirable?

No. ASIC resistance typically involves increasing algorithmic complexity to discourage ASIC developers. However, ASIC's are still inevitable; all ASIC resistance does is increase the startup capital required and therefore increase centralization of manufacturing.

⁸Well, this is a bit of a disingenuous statement. While there are many ASIC manufacturers on the market, these firms design IC's and outsource the actual IC fabrication. IC manufacturing is an extremely (and increasingly so) centralized industry. Thanks to Peter Todd for this observation.

Further, increasing the complexity of proof generation often means also increasing the complexity of proof validation, often disproportionately slow. This discourages (unpaid) non-mining validators, which also increases centralization.

3. Is ASIC resistance possible?

ASIC resistance, in the sense of making life difficult for ASIC manufacturers (and therefore reducing the number of distinct manufacturers) is possible. But it is impossible to create an algorithm which runs at the same speed on general-purpose and dedicated hardware (since general-purpose hardware contains many extraneous features, e.g. communication buses for peripherals), and so ultimately ASIC resistance is futile.

(Schemes such as “the developers will just change the proof-of-work algorithm if ASIC’s appear” do not even make sense — in a decentralized currency the developers have no such power, while in a centralized currency proof-of-work is a completely unnecessary waste of power.)

4. Is memory hardness desirable?

No. Memory hardness has the effect of increasing ASIC board footprint, weakening the heat-dissipation decentralization provided by the thermodynamic limit. Further, it increases the capital costs of mining equipment relative to the energy costs, which also encourages centralization (since established miners have amortized their equipment more than new miners). These effects are amplified by the fact that SRAM is both several times faster and several times more expensive than DRAM.

Also, memory hard proofs-of-work often require lots of memory on the part of the verifiers⁹, which is bad for decentralization as already discussed.

As an aside, since memory is far away and expensive to access on general purpose computers, memory hardness actually increases the benefit provided by ASIC’s! This is contrary to the goals of most memory-hard advocates, and as we have seen above, memory-hardness worsens the centralizing effects of ASIC’s while weakening the decentralizing effects¹⁰.

One more thing worth mentioning is time-memory tradeoff (TMTO). This is a property of an algorithm which allows higher memory usage to be traded for a heavier computational load. An algorithm which is highly susceptible to TMTO has poorly defined memory hardness, which at the very least complicates analysis. It may also cause an algorithm to fail to be optimization free.

5. Is scrypt better than SHA2?

No, for a few reasons:

- (a) It is much slower to validate, reducing scalability and discouraging non-mining validation.

⁹Though not necessarily — see for example John Tromp’s “cuckoo cycle” scheme at <https://bitcointalk.org/index.php?topic=451177.0>.

¹⁰In fact, at the time of this writing, scrypt ASIC’s are just appearing on the market, and do indeed provide a proportionally greater gain in hashpower than did SHA2 ASIC’s.

- (b) It is a more complex “ASIC-resistant” algorithm. See above.
- (c) It is more memory-hard than SHA2 (though depending on parameters, it can hardly be considered “memory-hard” — see Litecoin’s settings, for example). See above.

6. **Is Primecoin better than SHA2?** No, for a few reasons:

- (a) It is much slower to validate, reducing scalability and discouraging non-mining validation.
- (b) It is a more complex “ASIC-resistant” algorithm. See above.
- (c) It is an ad-hoc algorithm with no reason to believe that it is progress-free, approximation-free or optimization-free.

7. **What about “useful” proofs-of-work?**

These are typically bad ideas for all the same reasons that Primecoin is, and also bad for a new reason: from the network’s perspective, the purpose of mining is to secure the currency, but from the miner’s perspective, the purpose of mining is to gain the block reward. These two motivations complement each other, since a block reward is worth more in a secure currency than in a sham one, so the miner is incentivized to secure the network rather than attacking it. However, if the miner is motivated not by the block reward, but by some social or scientific purpose related to the proof-of-work evaluation, then these incentives are no longer aligned (and may in fact be opposed, if the miner wants to discourage others from encroaching on his work), weakening the security of the network.

5 Proof of Stake

1. **What is Proof of Stake?**

Proof of stake is the idea that rather than consuming some physical resource, perhaps miners should consume the cryptocurrency itself, thus “bootstrapping” the security of the system from its own value, rather than requiring expensive and energy-intensive mining operations.

However, it does not appear that there is a viable way to achieve consensus through proof of stake, due to the so-called “nothing at stake” problem¹¹.

2. **In principle, how does Proof of Stake work?**

The typical way that proof of stake is accomplished is by associating “votes” to individual coins, and to require blocks to be voted highly in order to be valid. To improve scalability and prevent “tyranny of the rich” scenarios, each block is voted on by a small set of coin holders, who are determined as part of the currency’s consensus algorithm.

3. **What is the “nothing at stake” problem?**

¹¹Thanks to Andrew Miller for this name.

The problem here is that ultimately, there is no cost for users to vote on multiple forks of the blockchain, but there is some benefit. Therefore, the idea that miners will behave honestly to protect their own coins' value is actually a tragedy of the commons.

The benefit of mining on multiple forks is that the blocks themselves determine the distribution of coins and therefore the distribution of future votes. In fact, the exact voters of future blocks must be deterministic, perhaps chosen by a PRF on the contents of past blocks, so by choosing which blocks to vote on, a miner can skew the distribution of future votes in his favour. As an extreme case, the miner could simply do a proof-of-work, where the "work" is finding new blocks which give him every future vote.

This is fatal for centralization, and because each miner is individually incentivized to act this way, it is also fatal for consensus.

4. Is Proof of Stake good for anything?

Certainly. The ability to cryptographically prove one's stake in a system is an exciting feature which is unique to cryptographic goods. It can be used to construct new and innovative protocols which I have no understanding of ☺. It just can't be used to create distributed consensus.