Copied from: https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/pull/13

Blockchain Timestamps Unnecessary In Proof-of-Work?

Author: Greg Slepak - @taoeffect@mastodon.social

The Bitcoin blockchain has a 10-minute target blocktime that is achieved by a difficulty adjustment algorithm.

I assert, or rather, pose the hypothesis, that the use of timestamps in Bitcoin's blockchain may be unnecessary, and that Bitcoin can operate with the same security guarantees without it (except as noted in Risks and Mitigations), and therefore does not need miners to maintain global clock synchronization.

The alternative difficulty adjustment algorithm would work according to the following principles:

- The incentive for miners is and always has been to maximize profit.
- The block reward algorithm is now modified to issue coins into perpetuity (no maximum). Any given block can issue up to

X

number of coins per block.

- The number of coins issued per block is now tied directly to the difficulty of the block, and the concept of "epocs" or "block reward halving" is removed.
- The chain selection rule remains "chain with most proof of work"
- The difficulty can be modified by miners in an arbitrary direction (up or down), but is limited in magnitude by some maximum percentage (e.g. no more than 20% deviation from the previous block), we call this Y%

.

Observations

- Miners are free to mine blocks of whatever difficulty they choose, up to a maximum deviation
- The blockchain may at times produce blocks very quickly, and at other times produce blocks more slowly
- Powerful miners are incentivized to raise the difficulty to remove competitors (as is true today)
- Whether miners choose to produce blocks quickly or slowly is entirely up to them. If they produce blocks quickly, each block has a lower reward, but there are more of them. If they produce blocks slowly, each block has a higher reward, but there are fewer of them. So an equilibrium will be naturally reached to produce blocks at a rate that should minimize orphans.

A timestamp may still be included in blocks, but it no longer needs to be used for anything, or represent anything significant other than metadata about when the miner claims to have produced the block.

Risks and Mitigations

Such a system may introduce risks that require further modification of the protocol to mitigate.

The most straightforward risk comes from the potential increase in total transaction throughput that such a change would introduce (these are the same concerns that exist with respect to raising the blocksize). The removal of timestamps would allow a cartel of miners to produce high-difficulty blocks at a fast rate, potentially resulting in additional centralization pressures not only on miners but also on full nodes who then would have greater difficulty keeping up with the additional bandwidth and storage demands.

Two equally straightforward mitigations exist to address this if we are given the liberty of modifying the protocol as we wish:

1. Introducing state checkpoints into the chain itself could make it possible for full nodes to skip verification of large sections of historical data when booting up.
2. A sharded protocol, where each shard uses a "sufficiently different" PoW algorithm, would create an exit for users should the primary blockchain become captured by a cartel providing poor quality-of-service.