Recently, I've been exploring new ideas related to PoW systems and how we can use ideas from PoS to build new protocol mechanisms. While this doesn't have to do with PoS or Ethereum specifically, I thought it's worth sharing the research. Attached you can find the paper: Delayed_Blockchain_Protocols (1).pdf (230.8 KB)

TL;DR

We can simulate "staking" mechanisms in Proof of Work systems by delaying the issuance of miner rewards. That is, miner's earn rewards for blocks they mine at some arbitrarily tuned, future date/round. In this manner, if a miner attempts to double-spend (or other malicious actions), proof of this behavior can lead to slashing their future rewards. The range of additional functions that can be utilized on top of delayed rewards, such as decaying rewards for short-lived miners, is vast. If we combine what we know from infinitely repeated games with punishment phases and that of staking mechanisms, we can incentivize long-lived, honest behavior by forcing miners to wait for their rewards. In doing so, these miners have stake in the future payouts and are less incentivized to deviate from the protocol (the cost of an attack is at least as much as their delayed payments for arbitrary delay rates).

I'd like to hear people's thoughts on this idea and whether it holds up. I know Bitcoin delays rewards by 100 blocks for other reasons than incentive compatibility, but this method is strictly for increasing the security of the underlying protocol by increasing the cost of successful deviations from the protocol.

As it relates to Ethereum, delayed rewards on top of a PoS system could provide additional incentives for validators to stick around. Although I focus on PoW, it can easily be extended to PoS since delayed rewards are agnostic to the PoX and underlying protocol (thought being implemented on said protocol).

Thanks to @nate for comments on the idea.