New paper Formal Barriers to Longest-Chain Proof-of-Stake Protocols from Arvind Narayanan of Princeton.

Not sure if these papers should be posted to this forum (my instinct is that they should!), but trying it as an experiment (instead of just discussing on Twitter).

Key idea:

At a conceptual level, the barriers stem from the following: all cryptocurrencies require some source of (pseudo)randomness. In Proof-of-Work, this pseudorandomness is in some sense external to the cryptocurrency: the first miner to successfully find a good nonce produces the next block, and this miner is selected completely independently of the current state of the cryptocurrency. In Proof-of-Stake, it is highly desirable that the pseudorandomness comes from within the cryptocurrency itself, versus an external source (due to network security concerns discussed in Section 2). One might initially suspect that with sufficiently many hashes or digital signatures of past blocks, this can indeed serve as a good source of pseudorandomness for future blocks. However, we formalize surprising barriers showing a fundamental difference between external pseudorandomness and pseudorandomness coming from the cryptocurrency itself.