TLDR: We have worked out a paper that shows trivial increase in block validation has leads to unfairness to miners with slow processing power. Also, it proposes a new mechanism to allow arbitrary computation in PoW blockchains. The core idea is to delay the validation of

transaction by up to \zeta

blocks to get block validation step off the critical path of PoW.

Abstract:

Proof-of-Work~(PoW) based blockchains typically allocate only a tiny fraction (e.g., less than 1% for Ethereum) of the average interarrival time~(mathbb{I}) between blocks for validating transactions. A trivial increase in validation time~(\tau

) introduces the popularly known Verifier's Dilemma, and as we demonstrate, causes more forking and increases unfairness. Large \tau

also reduces the tolerance for safety against a Byzantine adversary. Solutions that offload validation to a set of non-chain nodes (a.k.a. off-chain approaches) suffer from trust issues that are non-trivial to resolve.

In this paper, we present Tuxedo, the first on-chain protocol to theoretically scale \tau/\mathbb{I} \approx 1

in PoW blockchains. The key innovation in Tuxedo is to separate the consensus on the ordering of transactions from their execution. We achieve this by allowing miners to delay validation of transactions in a block by up to \zeta

blocks, where \zeta

is a system parameter. We perform security analysis of Tuxedo considering all possible adversarial strategies in a synchronous network with end-to-end delay \Delta

and demonstrate that Tuxedo achieves security equivalent to known results for longest chain PoW Nakamoto consensus. Additionally, we also suggest a principled approach for practical choices of parameter \zeta

as per the application requirement. Our prototype implementation of Tuxedo atop Ethereum demonstrates that it can scale \tau

without suffering the harmful effects of naive scaling in existing blockchains.

Paper link: https://arxiv.org/abs/2005.11791