

We know that a pure proof of stake must always solve the problem of who mints the next block. Traditionally, I have seen it proposed that a pseudo-random method is used either BFT or chain based - but this can lead to problems in grinding if more than just the next block creator is determined at once.

But what would be the merits of deciding next block creator via a secondary (slaved) consensus protocol instead of entropy?

As an idea... validators could nominate, subject to constraints, which block (by block height) they would forge during the next epoch and a secondary consensus method would be used to get agreement on validators proposals. The secondary consensus would have to front-run the main proof of stake blockchain (occur in advance) for the information generated to be useful. It would decide the order of block creation for the main blockchain only and not have an impact on economic return. The method for the secondary consensus could even be a proof of work method but without the burden of the security implications implicit in traditional POW it could be computationally less difficult or even decrease in computational complexity as each epoch gets closer (resetting as epochs pass).

The advantage are those that come with specifying block forger in advance and would presumably be an overall more coordinated flow of network traffic. In a moderate latency environment this could allow a faster block creation speed. It would also potentially allow validators to plan downtime without the consequent reduction in network security because their contributions end up concentrated into a single part of the epoch (of their own choosing).