In a new paper with Minghao Pan and Christoph Schlegel [2407.14485] On sibyl-proof mechanisms), we consider Sybil-proof mechanisms. We show that the only non-wasteful, incentive compatible and Sybil-proof mechanism is a second price auction. This can be viewed as a negative result as well, if you see lotteries to be leading to more decentralization than auctions do.

The generic setting is a single-parameter mechanism design environment, where there is a single item to allocate to bidders. In blockchain context, this could be giving proposing right for the next block. Assigning proposing rights to network nodes using lottery is assumed to make a chain more decentralized and censorship resistant. Both proof of stake and proof of work are examples of a (proportional) lottery.

We define multiple suitable properties allocation rule should satisfy.

First is “non-wastefulness” – item is always given to someone.

Second is incentive compatibility, which means that payments are designed so that it is the best strategy to report true private value of having an item.

Third is sibyl-proofness, which is a desirable property, especially in a decentralized environment where creating sybils is cheap and easy.

Thus, if there is private information, lotteries or other mechanisms that do not always allocate to a highest-value bidder are not sibyl-proof or not incentive compatible.

Any feedback is welcome.