This week was more alternative consensus, with two chains presented as alternatives to more established / lindy-consensus mechanisms.

Bitcoin NG And Blockene

Bitcoin NG is a proposal to change the block structure we use in traditional Bitcoin. Bitcoin NG (next generation) primarily differs from Bitcoin separating between two block types: key blocks and micro blocks. The miner of the key block becomes the leader, allowed to mine a certain amount of micro blocks until a new leader mine a key block. The incentive mechanism is supposed to make it attractive to act in a trusted way according to the protocol. According to the paper, Bitcoin NG is a proposed protocol to solve Bitcoins bottlenecks without making any meaningful trade-offs. Too good to be true?

Blockene is an interesting protocol based on a split-trust architecture where we have two types of nodes. citizens and politicians. Politicians are powerful but few in number (100s). They are not trusted by the other set of nodes - citizens. According to the paper, up to 80% of politicians might be corrupt. Exactly how the mechanisms work in practice is unclear to me, but a main point is that politicians can only execute citizens' decisions, they can not propose or alter decisions. Citizens are poor in power compared to politicians but many in numbers (millions). They are able to run the decision-making and their job as nodes on mobile devices. The paper assumes more than 70% honest nodes for the chain to function. They claim this assumption to be valid because of the law of large numbers. Citizens take all decisions by a majority, meaning which transactions are valid, and which should be appended to blocks. The only data trusted on-chain is from the majority of votes from the citizens. Citizens gossip thru politicians. Politicians can't fabricate messages. They might however reply to old signed messages and forget blocks. The paper proposes that TEE (Trusted Execution Environment) prevent cybil attacks - with hardware functions from phones. Struggle to see negatives from reading this paper as well…