Hello,

These days I'm studying DPOS more closely, and it's a very scalable protocol. It can manage thousands of transactions per second.

Under DPOS, 1 node, chosen among elected witnesses, is building the next block.

For example, with the Bitshares client, block creation is showing up swiftly every few seconds. EOS will do the same in a few months.

Personally, I think the election of witnesses may create flaws, and additionally it leads to centralization, since this is nearly always the same nodes who build blocks.

An alternative would be to choose a random masternode to build the next block.

In a network of a few hundreds or thousands masternodes, choosing one random masternode would deliver the same scalability without the need of any election.

Every other masternodes would check the block produced.

If the chosen masternode fails to deliver the next block, he would receive no fee, and if he builds a bad block, he would get a penalty.

On its website, Bitshares explains : http://docs.bitshares.org/bitshares/dpos.html :

Reasons to not randomly select representatives from all users

High probability they are not online.

Attackers would gain control proportional to their stake, without any peer review.

But if only masternodes which are online are allowed to build blocks, and if each block is checked by other masternodes, these objections are no more relevant.

So why not considering this simple solution ?

Letting a random masternode build the next block.

It could deliver a very good scalability.

And it would be pretty safe, since it's close to the successful POS protocol of NXT, which uses a deterministic algorithm to select a random shareholder to generate the next block.