I was thinking about a different approaches to POS and came up with something (maybe) interesting last night. All stuff about using VDFs for RNG has got me thinking about their utility recently.

If you have N

validators which each have

1. Staked some amount of eth (min staking required)
2. A VDF

Where the VDF takes time t

to evaluate (requires asic) and time << t

to validate (Does not require asic), where the block time \approx t

.

At the beginning of the block creation session…

1. Each Validator gathers up transactions from non-validator nodes, forming their own blocks. Previous block hash must be included in this block.
2. These blocks are then hashed/signed with the validator key and then run through the VDF.
3. The VDF outputs are then all collected by all validators, VDF outputs are arranged into a big block sorted by order with the previous block hash. Blocks are verified. Consensus is reached. Validators ensure no illegal transactions are present.
4. Slashing conditions apply. Validators are paid out based on their staked eth.
5. GOTO step 1

It's similar to POW, but instead of the resource being power it's time. In order to fabricate a blockchain of higher merit you would need time T to build from block height B.

T = t * B

For a 51% attack you need 51% of all the validators eth, if you were to pull it of the chain would probably just fork your wealth away.

Anyways, just a shower thought… might be interesting to some people, might not be. Digging the Tex formatting in this forum