Here's a weird VDF that came up as an idea when I was discussing VDFs with Ofer Grossman:

1. Fix some reasonable Turing Machine implementation.
2. Run some reasonably complicated f(x)

(in the language of the TM) for 2^n

time steps on the Turing machine. (we can e.g. get x from a RANDAO?)

1. Hash the 2^n

machine states with some H(x)

and Merklelize. The output of your computation is the Merkle root.

1. You verify by giving a Merkle branch to any node.

A few comments:

1. You already have a Turing Machine in Ethereum, so you can just use the specs for that

for this TM, which makes this both amusing (from a meta point of view) and good (from a reusability point of view).

1. This is very similar to TrueBit, which itself seems to kind of require some sort of TM. Might as well use the same implementation for engineering practices.

What are the tradeoffs of something like this in context of what Ethereum wants, compared to other solutions? Also, am I missing something obviously bad?

Good meeting many of you over the weekend!