

Cornell researchers have proposed Continuous VDFs.

In a nutshell (if I understood everything right

), continuous VDF enable efficient verification of “sequences of VDFs”, which was not possible before.

The authors demonstrate three potential applications, the most interesting one probably being the construction of public randomness beacons that only require an initial random seed (and no further unpredictable sources of randomness).

Was wondering if someone looked into this in the context of blockchains/beacon chains...

<https://eprint.iacr.org/2019/619>

cc [@JustinDrake](#)