Just started reading about VDFs…

Noticed that Solana’s VDF is basically a recursive SHA256. A brief explanation of the model:

Medium – 4 Oct 19

Proof of History: A Clock for Blockchain

A high-level explanation of Solana’s core innovation

Reading time: 7 min read

The rationale is: " …thanks to Bitcoin there has been significant research in making this cryptographic hash function fast. This function is impossible to speed up by using a larger die area, like a Look Up Table, or unrolling it without impact to clock speed. Both Intel and AMD are releasing consumer chips that can do a full round of SHA256 in 1.75 cycles. Because of this, we have pretty good certainty that a custom ASIC will not be 100x faster, let alone 1000x, and most likey will be within 30% of what is available to the network. We can construct protocols that exploit this bound and only allow an attacker a very limited, easily detected and shortlived oportunity for a denial of service attack."

Any thoughts on this? Would it be worth considering for the Ethereum beacon chain? Thanks.