TLDR: We present a VDF difficulty scheme that significantly reduces the RNG lookahead, i.e. the amount of time random numbers are made public before they are used.

Context

In a previous post Vitalik exposed a DoS attack on a naive VDF-based RNG where an attacker, assumed to have a hardware advantage up to A_{max}, can ramp up the VDF difficulty and then under-perform (e.g. by going offline). This would cause the randomness beacon to pause for an extended period of time, hence stalling the beacon chain and shards.

One way to address the DoS vector is to have a lookahead quadratic in A_{max}, as presented in Vitalik's post. In this post we achieve a lookahead linear in A_{max} with a difficulty scheme strengthened against DoS attacks.

Construction

Notice that when an attacker ramps up the VDF difficulty versus the capabilities of honest players and then under-performs he is revealing two pieces of information:

1. an upper bound on the VDF speed of honest players
2. a lower bound on the VDF speed of the attacker

Let's call the range between these two bounds the "DoS zone" and let:

- s_i be the fastest observed VDF speed in epoch i
- t_i be the target VDF speed (the difficulty) in epoch i
- s_{max} be the historically fastest observed VDF speed prior to epoch i

The difficulty adjustment works as follows:

- If $s_i \le t_i$ then set $t_{i+1} = \max{s_i, s_{max}/A_{max}}$. That is, downward difficulty adjustments are maximally steep up to the safe minimum s_{max}/A_{max}.
- If $s_i > t_i$ and $s_{max} > t_i$ then set $t_{i+1} = t_i * c$ where c is the smallest constant that safely accounts for organic improvements to VDF speeds. That is, upward difficulty adjustments in the DoS zone are slow.
- If $s_i > t_i$ and $s_{max} = t_i$ then set $t_{i+1} = s_i$. That is, upward difficulty adjustments outside the DoS zone are maximally steep.

Discussion

By setting the lookahead to be linear in A_{max}

the attacker can do a large DoS attack, but only rarely. For example if the lookahead is set to the expected VDF computation time, A_{max}=10

, and c

is set to target a maximum of 2x VDF speedup in 1 year then DoS attacks only become viable once per few years.