Edit 2018.08.16: I am from now on going to use “immediate message driven GHOST” to refer to what I previously referred to as “recursive proximity to justification” or “RPJ”.

There are two desirable goals for fork choice rules that the current proposed fork choice rules[1] [2] fail to satisfy:

1. Bad proposer resistance

: if there is a medium-length run of bad proposers (possible because of RNG manipulation), then this could lead to damaging the chain’s guarantees with relatively small coalitions (eg. censorship attacks with much less than 50% participating)

1. Stability

: the fork choice should be a good prediction of the future fork choice

As an example of (1), consider the following case:

[

%5BG%5D%20-%3E%20%5BA1%5D%2C%5BG%5D%20-
%3E%20%5BB1%7Bbg%3Ared%7D%5D%2C%5BB1%7Bbg%3Ared%7D%5D%20-
%3E%20%5BB2%7Bbg%3Ared%7D%5D%2C%5BB2%7Bbg%3Ared%7D%5D%20-
%3E%20%5BB3%7Bbg%3Ared%7D%5D%2C%5BB3%7Bbg%3Ared%7D%5D%20-
%3E%20%5B.....%7Bbg%3Ared%7D%5D

168×735

](https://yuml.me/diagram/scruffy/class/%5BG%5D%20-%3E%20%5BA1%5D%2C%5BG%5D%20-
%3E%20%5BB1%7Bbg%3Ared%7D%5D%2C%5BB1%7Bbg%3Ared%7D%5D%20-
%3E%20%5BB2%7Bbg%3Ared%7D%5D%2C%5BB2%7Bbg%3Ared%7D%5D%20-
%3E%20%5BB3%7Bbg%3Ared%7D%5D%2C%5BB3%7Bbg%3Ared%7D%5D%20-
%3E%20%5B.....%7Bbg%3Ared%7D%5D)

Suppose the red chain consists of only malicious proposers and attesters, and is published after the fact. In the grey “chain” (really not a chain at all), the proposers are malicious, but the attesters are honest. Suppose the fraction of malicious attesters is, say, 1/4. The attacker publishes A1, waits, and then after some time reveals the chain with B1…

In this model, the attacker’s chain clearly wins in the longest chain rule. The solution to these kinds of attacks is a GHOST scoring rule (see [2]), which would keep increasing the weight of A1 as more honest validators attest to it, ensuring that it continues to overtake the attacker’s chain.

However, GHOST has one weakness in the context of FFG, which is lack of stability. For example, consider this case, where each box represents a checkpoint and the number inside of it is the percentage of validators voting for that checkpoint.

[

%5BG%5D%20-%3E%20%5B55%7Bbg%3Agreen%7D%5D%2C%5B55%7Bbg%3Agreen%7D%5D%20-
%3E%20%5B56%7Bbg%3Agreen%7D%5D%2C%5BG%5D%20-
%3E%20%5B15%7Bbg%3Ayellow%7D%5D%2C%5B15%7Bbg%3Ayellow%7D%5D%20-
%3E%20%5B16%7Bbg%3Ayellow%7D%5D%2C%5B16%7Bbg%3Ayellow%7D%5D%20-
%3E%20%5B65%7Bbg%3Ayellow%7D%5D

168×568

](https://yuml.me/diagram/scruffy/class/%5BG%5D%20-
%3E%20%5B55%7Bbg%3Agreen%7D%5D%2C%5B55%7Bbg%3Agreen%7D%5D%20-
%3E%20%5B56%7Bbg%3Agreen%7D%5D%2C%5BG%5D%20-
%3E%20%5B15%7Bbg%3Ayellow%7D%5D%2C%5B15%7Bbg%3Ayellow%7D%5D%20-
%3E%20%5B16%7Bbg%3Ayellow%7D%5D%2C%5B16%7Bbg%3Ayellow%7D%5D%20-
%3E%20%5B65%7Bbg%3Ayellow%7D%5D)

A GHOST implementation that tries to naively replicate GHOST in PoW would add up all votes in the subtree, and the green subtree would get 111 votes relative to 96 on the yellow subtree, so the green subtree would win, even though the yellow tree is clearly much closer to getting a justified checkpoint.

One could try to change this by instead only looking at most recent votes. But this would break in a different case:

Here, yellow would win, even though the green subtree is clearly only 2% attestations away from being justified. This is dangerous because an attacker with 2% of stake could wait for such a scenario to arise (realistically, trigger it by forcing high network latency), then wait until the opportune moment to release their attestations, suddenly flipping over the chain.

Our fork choice rule will start from the first version of GHOST above, but make one modification: instead of adding

the votes for the checkpoints in a subtree, we take the maximum

. The philosophy here is that if a block is justified, that implicitly justifies its ancestors as well, so the distance of a block to being justified is really the minimum of the distances of any of its descendants, and so the proximity

to being justified is the maximum

.

Hence, in the first example, yellow is preferred over green because max(15, 16, 65) > max(55, 56), and in the second example, green is preferred over yellow because max(65, 20) > max(15, 51).

(As a historical note, I'll add that this exact algorithm was considered for hybrid Casper FFG, but was ultimately rejected because there was no proof that some chain closer to justification had a longer PoW chain, and epoch numbers were tied to PoW lengths, but in the latest protocol epoch numbers are tied to slots, ie. timestamps, which resolves this issue).

Within an epoch, the GHOST rule can be used to find the preferred head to improve safety against bad proposers, though from the point of view of stability it does not theoretically matter as much which fork choice rule is used inside an epoch.

It is worth noting that there is

one weakness of this fork choice rule:

Here, even though the green chain is "closer" to justification according to the fork choice rule (60 > 51), it is "further away" in practice because getting it justified would require 7% equivocation, whereas the yellow chain could be justified with no equivocation. However, this kind of scenario could only arise in a fairly extreme circumstance with either a majority attacker or very high network latency.