Proof of safety

Zihan

2022 年 8 月 14 日

1 Preliminary

我们考察一种情形，攻击者的算力与诚实者算力之比为 $q \in [0, 1)$. 但是在此之前，我们先对算力与权重的关系进行一些分析。

期望 Hash 次数 和其他文献一样，我们把生成同质区块数目随 Hash 次数的变化视作一个参数为 p 的 Poisson 过程，其中 p 也是单次 Hash 生成区块的概率。则若记 N 为生成一个区块所进行的 Hash 次数，N 作为一个随机变量，满足参数为 p 的几何分布. 即

$$N \sim G(p).$$

对其期望与方差，我们有如下结论：

$$\mathrm{E}(N) = \frac{1}{p};$$

$$\mathrm{var}(N) = \frac{1-p}{p^2}.$$

特别地，对某一个单块，$p = 1/2^m$, 其中 m 代表 leading zero 的数目.

考察某 Block B, 若其所在的 Sibling Group 有 2^k 个区块，则我们称 B 为一个 2^k-block. 由于 2^k-block 的实际 leading zero 数目为 $m - k$, 所以其对应的 p 有

$$p = \frac{1}{2^{m-k}}.$$

于是，若记 N_k 为生成一个 2^k-block 所进行的 Hash 次数，我们有

$$n_k \equiv \mathrm{E}(N_k) = \frac{1}{\frac{1}{2^{m-k}}} = 2^{m-k}.$$

如前所述，我们定义了一个 2^k-block 的权重 W_k 为

$$W_k = 2^{m-k}.$$

因此我们可以定义