Proof of safety

Zihan

2022 年 8 月 18 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。

1.1 一些定义和假设

Definition 1. Let $B \in G$ be a block. 称 B 为一个 2^k-block, 若其所在的 Sibling Group 有 2^k 个区块. 所有的 2^k-block 构成的集合记为 $\mathcal{B}_k$.

Assumption. 和其他文献一样, 我们把生成同一种区块的 Hash 过程视作一个 Poisson 过程. 具体来说, 若在 $\mathcal{B}_k$ 上进行 N 次 Hash, 记此时生成的 2^k-block 数目为 $a_k(N)$, 则 $a_k(N)$ 是一个强度为 $2^k p$ 的 Poisson 过程, 其中 p 是 Mining Difficulty.

Corollary. 由 Poisson 过程, $\mathrm{E}(a_k(N)) = 2^k pN$.

生成的每个 2^k-块的权重 W_k 设定为 $W_k = \dfrac{1}{2^k p}$, 且记诚实者算力为 v_h.

2 权重与 Hash 次数的关系

对于 Hash 次数和所生成的权重, 我们有以下定理:

Theorem 1. *给定 Hash 次数 N, 所生成的权重 $W(N)$, 作为一个随机变量, 其期望与具体生成区块的种类无关, 且有*

$$\mathrm{E}(W(N)) = N$$

证明. N 次的 Hash 是分配在各类区块上的. 由于 G 是有限大小的, $|\{\mathcal{B}_k\}| \in \mathbb{N}$, 记为 $k_{\max}$. 于是有

$$N = N_1 + N_2 + \cdots + N_{k_{\max}},$$

其中 $N_k (1 \leq k \leq k_{\max})$ 表示在 2^k-block 上 $(\mathcal{B}_k)$ 上的 Hash 次数. Analogously, 权重 $W(N)$ 亦有

$$W(N) = W_1(N_1) + W_2(N_2) + \cdots + W_{k_{\max}}(N_{k_{\max}}).$$

考虑 $\mathcal{B}_k$ 上的 $W_k(N)$, 由于所有生成的块, 根据算法, 都为首 sibling group 贡献了权重, 所以 $\mathcal{B}_k$ 上所提供的权重

$$W_k(N) = a_k(N) W_k = \frac{a_k(N)}{2^k p},$$

所以有

$$\mathrm{E}(W_k(N)) = \frac{\mathrm{E}(a_k(N))}{2^k p} = \frac{2^k p N}{2^k p} = N.$$

所以总权重期望有

$$\begin{aligned} \mathrm{E}(W(N)) &= \mathrm{E}\left(\sum_{1 \leq k \leq k_{\max}} W_k(N_k) \right) = \sum_{1 \leq k \leq k_{\max}} \mathrm{E}(W_k(N_k)) \\ &= \sum_{1 \leq k \leq k_{\max}} N_k = N \end{aligned}$$

□

3 诚实者和攻击者

攻击者若想篡夺主视图, 其首 sibling 权重应当大于主视图的首 sibling 权重.