Proof of safety

Zihan

2022 年 8 月 21 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, 期望$\mathrm{E}(a_k(N)) = 2^k pN$~~.~~, 方差 $\mathrm{Var}(a_k(N)) = 2^k pN$.

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*

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

$$Var(W(N)) \le \frac{N}{p}$$

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

$$N = N_{\underline{1}0} + N_{\underline{2}1} + \cdots + N_{k_{\max}},$$

其中 ~~$N_k(1 \le k \le k_{\max})$~~ $N_k(0 \le k \le k_{\max})$ 表示在 2^k-block 上 ($\mathcal{B}_k$) 上的 Hash 次数. Analogously, 权重 $W(N)$ 亦有

$$W(N) = W_{\underline{1}0}(N_{\underline{1}0}) + W_{\underline{2}1}(N_{\underline{2}1}) + \cdots + W_{k_{\max}}(N_{k_{\max}}).$$

考虑 $\mathcal{B}_k$ 上的~~$W_k(N)$~~$W_k(N_k)$, 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

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

所以有

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

对方差也有

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

所以总权重期望有

$$\underline{E(W(N)) = E\left(\sum_{1 \le k \le k_{\max}} W_k(N_k)\right) = \sum_{1 \le k \le k_{\max}} E(W_k(N_k))}$$

$$\begin{aligned} E(W(N)) = E\left(\sum_{0 \le k \le k_{\max}} W_k(N_k)\right) &= \sum_{0 \le k \le k_{\max}} E(W_k(N_k)) \\ &= \sum_{0 \le k \le k_{\max}} N_k = N \end{aligned}$$

$$= \sum_{1 \le k \le k_{\max}} N_k = N$$

而且由于 $\{W_k(N_K)\}$ 相互独立，总权重方差

$$Var(W(N)) = Var\left(\sum_{0 \le k \le k_{\max}} W_k(N_k)\right) = \sum_{0 \le k \le k_{\max}} Var(W_k(N_k))$$

$$= \sum_{0 \le k \le k_{\max}} \frac{N_k}{2^k p} \le \sum_{0 \le k \le k_{\max}} \frac{N_k}{p} = \frac{N}{p}.$$

□

3 诚实者和攻击者

记事件攻击者篡夺成功为事件 F. 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. 即

$$F = \{W_a > W_h + W_0\}.$$

此时, 我们有如下的安全定理:

Theorem 2. $\forall \epsilon > 0, \exists T > 0,\ s.t.\ \forall t > T,$

$$\mathrm{P}(F) < \epsilon.$$

先证明一个引理:

Lemma 1. 若记 $\Delta = \mathrm{E}(W_h) - \mathrm{E}(W_a)$, 则进一步有

$$F \subseteq \{\mathrm{E}(W_h) - W_h > \frac{\Delta}{2}\} \cup \{W_a - \mathrm{E}(W_a) > \frac{\Delta}{2}\}.$$

证明. $\forall \omega \notin \{\mathrm{E}(W_h) - W_h > \frac{\Delta}{2}\} \cup \{W_a - \mathrm{E}(W_a) > \frac{\Delta}{2}\}$, 有

$$\omega \in \{\mathrm{E}(W_h) - W_h \le \frac{\Delta}{2}\} \cap \{W_a - \mathrm{E}(W_a) \le \frac{\Delta}{2}\}.$$

此时

$$\mathrm{E}(W_h) - W_h + W_a - \mathrm{E}(W_a) \le \Delta,$$

即

$$W_a - W_h \le \Delta - \mathrm{E}(W_h) - \mathrm{E}(W_a) = 0$$

于是

$$\omega \notin F,$$

也即

$$F \subseteq \{\mathrm{E}(W_h) - W_h > \frac{\Delta}{2}\} \cup \{W_a - \mathrm{E}(W_a) > \frac{\Delta}{2}\}.$$

□

下面我们证明 Theorem 2:

证明. 由 Lemma 1,

$$\begin{aligned} \mathrm{P}(A) &\le \mathrm{P}(\{\mathrm{E}(W_h) - W_h > \frac{\Delta}{2}\} \cup \{W_a - \mathrm{E}(W_a) > \frac{\Delta}{2}\}) \\ &\le \mathrm{P}(\mathrm{E}(W_h) - W_h > \frac{\Delta}{2}) + \mathrm{P}(W_a - \mathrm{E}(W_a) > \frac{\Delta}{2}) \\ &\le \mathrm{P}(|\mathrm{E}(W_h) - W_h| > \frac{\Delta}{2}) + \mathrm{P}(|W_a - \mathrm{E}(W_a)| > \frac{\Delta}{2}). \end{aligned}$$

由切比雪夫不等式,

$$\begin{aligned} \mathrm{P}(AF) &\le \frac{\mathrm{Var}(W_h)}{(\Delta/2)^2} + \frac{\mathrm{Var}(W_a)}{(\Delta/2)^2} \\ &= \frac{4(\mathrm{Var}(W_h) + \mathrm{Var}(W_a))}{\Delta^2} \end{aligned}$$

~~而对于 Δ,~~ 由 Theorem 1

$$\Delta = \mathrm{E}(W_h) - \mathrm{E}(W_a) = N_h - N_a = v_h t - q v_h t = (1-q) v_h t.$$

~~记 $f(t) = \frac{4(\mathrm{Var}(W_h) + \mathrm{Var}(W_a))}{[(1-q)v_h t]^2}$, 注意到~~

$$f\mathrm{Var}(tW_h) \simeq, + \mathrm{Var}(W_a) = \frac{N_h + N_a}{p} = \frac{(1+q)v_h t}{p}.$$

~~则显然有~~所以

$$\lim_{t\to\infty} f\mathrm{P}(tF) \leq \frac{4(1+q)v_h t}{p[(1-q)v_h t]^2} = 0. \frac{4(1+q)}{p(1-q)^2 v_h}\frac{1}{t}.$$

~~也即$\forall\epsilon > 0, \exists T > 0,$~~ 则$\forall\epsilon > 0$, select $T = \lceil \frac{4(1+q)}{p(1-q)^2}\frac{1}{v_h\epsilon} \rceil$, s.t. $\forall t > T$, 都有

$$\mathrm{P}(F) < f(T) \leq \frac{4(1+q)}{p(1-q)^2 v_h} \Big/ \frac{4(1+q)}{p(1-q)^2}\frac{1}{v_h\epsilon} = \epsilon.$$

~~此时~~

$$\mathrm{P}(F) < \epsilon,$$

□