

# 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。

**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 过程视为一个 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  $E(a_k(N)) = 2^k p N$ , 方差  $\text{Var}(a_k(N)) = 2^k p N$ .

生成的每个  $2^k$ -块的权重  $W_k$  设定为  $W_k = \frac{1}{2^k p}$ , 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

$$E(W(N)) = N$$

$$\text{Var}(W(N)) \leq \frac{N}{p}$$

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

$$N = N_0 + N_1 + \cdots + N_{k_{\max}},$$

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

$$W(N) = W_0(N_0) + W_1(N_1) + \cdots + W_{k_{\max}}(N_{k_{\max}}).$$

考虑  $\mathcal{B}_k$  上的  $W_k(N_k)$ , 由于所有生成的块, 根据算法, 都为 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

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

对方差也有

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

所以总权重期望有

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

而且由于  $\{W_k(N_k)\}$  相互独立, 总权重方差

$$\begin{aligned} \text{Var}(W(N)) &= \text{Var}\left(\sum_{0 \leq k \leq k_{\max}} W_k(N_k)\right) = \sum_{0 \leq k \leq k_{\max}} \text{Var}(W_k(N_k)) \\ &= \sum_{0 \leq k \leq k_{\max}} \frac{N_k}{2^k p} \leq \sum_{0 \leq k \leq k_{\max}} \frac{N_k}{p} = \frac{N}{p}. \end{aligned}$$

□

### 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.**  $\forall \epsilon > 0, \exists T > 0, s.t. \forall t > T,$

$$P(F) < \epsilon.$$

先证明一个引理:

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

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

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

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

此时

$$E(W_h) - W_h + W_a - E(W_a) \leq \Delta,$$

即

$$W_a - W_h \leq \Delta - E(W_h) - E(W_a) = 0$$

于是

$$\omega \notin F,$$

也即

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

□

下面我们证明 Theorem 2:

证明. 由 Lemma 1,

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

由切比雪夫不等式,

$$\begin{aligned} P(F) &\leq \frac{\text{Var}(W_h)}{(\Delta/2)^2} + \frac{\text{Var}(W_a)}{(\Delta/2)^2} \\ &= \frac{4(\text{Var}(W_h) + \text{Var}(W_a))}{\Delta^2} \end{aligned}$$

由 Theorem 1

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

$$\text{Var}(W_h) + \text{Var}(W_a) = \frac{N_h + N_a}{p} = \frac{(1 + q) v_h t}{p}.$$

所以

$$P(F) \leq \frac{4(1 + q) v_h t}{p[(1 - q) v_h t]^2} = \frac{4(1 + q)}{p(1 - q)^2 v_h t}.$$

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

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

□