Unity Fork Choice Rule

Yulong Wu

May 21, 2019

1 Analysis

Based on the analysis in [1], the PoW block generation rate $\lambda_w = \sum_{m \in M} \frac{m}{d_w}$. In a period of unit time, the number of blocks will be produced is a random variable $X \sim Pois(\lambda_w)$, and $E(X) = \lambda_w$. Let Y_w be the total mining difficulty, then $E(Y_w) = E(X) * d_w$. Thus,

$$E(Y_w) = \sum_{m \in M} \frac{m}{d_w} * d_w = \sum_{m \in M} m.$$

Similarly, the PoS block generation rate $\lambda_w = \sum_{s \in S} \frac{s}{d_s}$. Let Y_s be the total mining difficulty, then

$$E(Y_s) = \sum_{s \in S} \frac{s}{d_s} * d_s = \sum_{s \in S} s.$$

If the final weight of a chain is $W = Y_w \cdot Y_s$ and **the common blocks in a fork are not counted**, the wining chain will be the one with the highest $s \cdot m$ bound to it. Assume an attacker has a mining power $p \cdot M$ and a stake power $q \cdot S$, the honest nodes have $(1-p) \cdot M$ and $(1-q) \cdot S$, then the expected weight of the attacker's chain C_a, in unit time, is

$$E(C_a) = (p \cdot M) \cdot (q \cdot S) = pq \cdot MS.$$

Similarly, the expected weight of the honest nodes' chain C_h is

$$E(C_h) = ((1-p) \cdot M) \cdot ((1-q) \cdot S) = (1 - p - q + pq) \cdot MS.$$

Therefore, the attacker is expected to win if $p + q > 1$.

References

[1] B. Group, "Proof of stake versus proof of work," 2015. [Online]. Available: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf