Analysis on Unity Fork Choice Rule

Yulong Wu

May 23, 2019

1 Exclude Common Blocks

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 $p + q > 1$. One issue with this approach is the lack of canonical best chain. Different nodes in the network may have different views on what the best chain is, as shown in Figure 1.

2 Include Common Blocks

Essentially, the total mining difficulty is an integration of hash rate over time, while the total staking difficulty is an integration of sake over time.

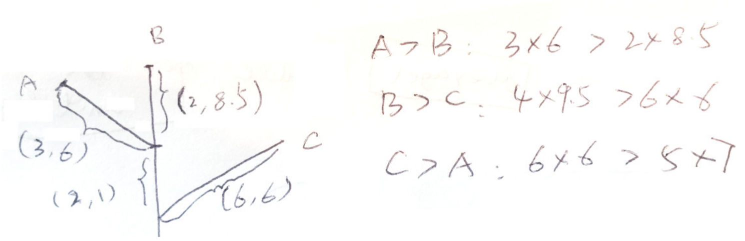

Figure 1: A counter example demonstrating where the network may have inconsistent views.

Assume an attacker has mining power and stake power (a, b) while the honest nodes have (c, d). Then the attacker's chain has an expected weight of

$$(td_w + a \cdot t) \cdot (td_s + b \cdot t)$$

and the honest nodes' chain has a weight of

$$(td_w + c \cdot t) \cdot (td_s + d \cdot t),$$

where td_w and td_s are the total mining difficulty and total staking difficulty of the common blocks, and t is the time elapsed since the fork.

For the attacker to overthrow the honest nodes' chain, the attacker's chain has to own a higher weight than the honest nodes' chain, which further leads to the following inequation:

$$td_s \cdot (a - c) + td_w \cdot (b - d) + (ab - cd) \cdot t \geq 0,$$

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