Coinweb L2 Reorgs analysis

1. At any point in time, given a specific node, we model the height of the observed last block l1-reorganization as a random variable $L1$ over a geometric probability distribution:

$$P(L1 = h) = Geo(h+1)$$

$$Geo(h) = (1-p)p^{h-1}$$

   where $P(L1 = 0)$ would indicate the block won't get l1-reorganized, p the chances single block gets l1-reorganized, and h the reorganization height.

2. Then under this model, the probability that a l1-reorganization will have at least height h is:

$$\begin{aligned} P(L1 >= h) &= \sum_{i=h}^{\infty}(1-p)p^i \\ &= (1-p)p^h \sum_{i=0}^{\infty}(1-p)p^i \\ &= (1-p)p^h \tfrac{1}{1-p} \\ &= p^h \end{aligned}$$

3. Now let's assume for the l2-network of blockchains that:

   - Each l2-blockchain is placed on a chess-like grid, each one connected to 8 adjacent blockchains (north, north-east,east, south-east, south,south-west, west and north-west).
   - To accept a transaction from a neighbor l2-blockchain, it waits for d confirmations.
   - **There are an infinite number of l2-blockchains**. Notice the actual network will be finite, but this shouldn't be a problem as a worst case scenario.

   This way, for every l2-blockchain, there are $8n$ blockchains at a n hop distance. An l2-reorganization will be triggered over l2-blockchain b iff:

   - its related l1-blockchain gets a h or deeper reorg.
   - any l2-blockchain at a minimal n hops distance gets a $h+dn$ reorg.

4. We model the random variable describing the height of the l2-reorganization on a l2-blockhain b as $L2_b$. As the probability of any independent pair of events is equal or greater than the sum of each events individual probability ($P(A\ or\ B) \geq P(A)+P(B)$) we get:

$$\begin{aligned} P(L2_b >= h) &\leq P(L1_b >= h) + \sum_{n=0}^{\infty} \sum_{\{k|distance(k)=n\}} P(L2_k >= h+dn) \\ &= P(L1_b >= h) + \sum_{i}^{\infty} 8iP(L2_k >= h+id) \\ &= P(L1_b >= h) + \sum_{i}^{\infty} 8iP(L1_k >= h+id) \\ &= p^h + \sum_{i=0}^{\infty} 8ip^{h+id} = p^h\big(1+8\sum_{i=0}^{\infty} ip^{di}\big) = p^h\big(1+8\sum_{i=0}^{\infty} iw^i\big) \\ &= p^h\big(1+\tfrac{8w}{(1-w)^2}\big) \\ &= p^h\big(1+\tfrac{8p^d}{(1-p^d)^2}\big) \end{aligned}$$

   Where we have used the fact that $p < 1$ and hence $p^d < 1$. As we can see, fixing p and d we get:

$$P(L2_b >= h) \leq k_{d,p}P(L1_b >= h)$$

   Meaning that probability distribution of the expected reorganization is bounded by the original distribution times a constant. In addition said constant quickly approximate to 1 as d increases.

5. Here we showed how the l2-reorganization expectation can be kept close to the l1-reorganization on a grid like topology even when the number of connected blockchains is arbitrarily large. A similar result can be obtained for more interesting topologies like random graphs, where the result remains true as long as $(k-1)p^d < 1$, where k is degree of each vertex.