MONERO RESEARCH LAB

TECHNICAL NOTE MRL-00XX

Framework for assessing safe lock times based on worst case plausible scenario

Isthmus
Monero Research Lab, Noncesense Research Lab
October 2019

Abstract

This note describes a framework for assessing and discussing the depth that constitutes a safe lock time. The principle is intuitive: the lock time is derived from the worst case plausible scenario. Phenomena that produce alternative blocks are exhaustively enumerated, the expected maximum length is estimated for each. The appropriate lock time is determined by the greatest element and a safety term.

1 Theory

Let T_i represent a phenomenon that creates alternative blocks, with expected maximum alternative chain length L_i. An appropriate lock depth (D) is calculated from the set of lengths and a safety term, S. Generally,

$$D = \text{fxn}(\max(\{L_1, L_2, ...L_n\}), S). \tag{1}$$

One simple form is:

$$D = S \cdot \max(\{L_1, L_2, ...L_n\}). \tag{2}$$

2 Phenomena

Phenomena that could produce alternative blocks include:

- T_1: Latency
- T_2: 51% attack
- T_3: Selfish* & stubborn† mining

This list must be as comprehensive as possible, so please contribute your ideas.

3 Techniques for length estimation

For each phenomenon, we take an individualized approach to selecting our maximum length expectation L_i, since there is no one-size-fit-all algorithm for different physical phenomena.

3.1 Latency

For T_1 (latency), Noncesense archival network data can be compared across multiple nodes to put an experimental upper bound on length of reorgs experienced globally (i.e. by more than 15% of nodes). Archival network data from early 2019 showed no global reorganizations greater than depth of two, so $L_1 = 2$. Note that more recent data should be reviewed, and latency-induced forks will increase with block size.

*Ittay Eyal and Emin Gün Sire *Majority is not Enough: Bitcoin Mining is Vulnerable*, 2013, https://arxiv.org/abs/1311.0243

†Kartik Nayak, Srijan Kumar, Andrew Miller, Elaine Shi *Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack*, 2016, IEEE, DOI: 10.1109/EuroSP.2016.32

3.2 51% attack

For T_2 (51% attack), we cannot safely derive L_2 from empirical data, since one should always assume that an adversary may control significant hash power not contributing to the main chain. For example, there may currently exist an entity with enough hashrate to mine competitive alternative chains 7 or 8 blocks deep, which are never broadcasted, in order to avoid revealing their existence until one of their alternative chains exceeds common lock depth (at time of writing, $D = 10$ for most software).

Here is one possible approach for assessing L_2. Consider P, the probability of mining a winning chain n blocks long, over t time window, with h fraction of the hash rate.

$$P = \text{fxn}(n, t, h) \tag{3}$$

First, we determine comfortable values for P, t, and h. For example, it could be highly disruptive if an entity mining with 20% of the hashrate can cause a reorganization deeper than lock time on a week timescale. However, it may be acceptable for an entity with $h = 20\%$ of the hash rate to have a $P = 0.0001\%$ chance of producing a winning alternative chain in $t = 10000$ years. With P, t, and h determined, equation 3 can be inverted to solve for the only unknown, $n = L_2$.

3.3 Stubborn and selfish mining

T_3 encompasses alternative blocks produced by selfish and stubborn miners, which has parallels with principles discussed in the previous section. I expect $L_3 < L_2$, so it is not explored further here.

4 Alternative forms

In §1, equation 2 was suggested as a specific form of the general equation 1, however alternative forms can be constructed.

While the safety term was a multiplicative factor in equation 1, it could be an additive term S' instead

$$D = \max(\{L_1, L_2, ...L_n\}) + S'. \tag{4}$$

Instead of a single safety term, a phenomenon-specific buffer s_i could be estimated for each T_i

$$D = \max(\{s_1 L_1, s_2 L_2, ...s_n L_n\}). \tag{5}$$

I recommend against this approach of multiple safety modifiers, since it introduces more degrees of freedom, more room for error, and complicates community discussion. Suppose evidence starts to suggest that specialized mining equipment (e.g. ASICs) is being used on the Monero network again - this change in available information may need to be reflected in the lock depth. The direct way to take this into account is adjusting h in equation 3 to its new worst case scenario, rather than modifying the s_2 confidence.

5 Conclusions

This framework is designed to facilitate and focus discussion around selecting an appropriate lock time, based on exhaustive risk analysis. Community members are encouraged to contribute to the list of possible phenomena, suggest ways to estimate plausible lengths, and consider an appropriate safety term.

Note: I suspect that an analytical solution for equation 3 is available in literature; please direct me towards the result.