Thoughts on modeling -coin as a resource

Akhil Rao

January 7, 2018

Overview

This memo builds on Sean's 1/1/2018 memo. I agree with its premise that there is a lot of low-hanging fruit in modeling -coin mining decisions. For context, the model from the earlier memo is below:

Each period miners invest in new processing power, with capital costs per gigahash/sec (Gh/s) of $k(t)$ - better technology likely means $\dot{k} < 0$. The dollar price of bitcoin is $B(t)$, which is a random variable .The flow of bitcoins per Gh/s is $\frac{X(t)}{M(t)}$, where $X(t)$ is the flow of new coin and transaction fee payments and $M(t)$ is the total number of miners in terms of total Gh/s. Finally, the electricity and other variable costs is $c(t)$ and the processor breaks down after a period of T. Assuming risk neutral miners and free entry we get the equilibrium where miners invest until

$$k(t) = E\left[\int_0^T e^{-rt}B(t)\left(\frac{X(t)}{M(t)}\right) - c(t)dt\right]. \tag{1}$$

Building up

I have three lines of thought, mainly theoretical, to add to the earlier memo.

The first (perhaps most obvious) line of thought is that there isn't much that is special about Bitcoin from a math-econ perspective, expect perhaps the form of the reward function. So, any model developed for Bitcoin should be generalizable to many other -coins, with some minor modifications such as replacing $X(t)/M(t)$ with a general reward function $\mathcal{M}(t, X(t), M(t))$. More substantively, this suggests that the relevant alternate option for an agent who has decided to become a miner may not be "mine nothing", but rather "mine some other coin". I don't have a prior over whether this is a first-order modeling concern or not, or for which questions it would be relevant. My first attempt to argue the irrelevance of the point would be along the lines, "if a prospective Bitcoin miner chooses to mine dogecoin[1], their decision was in a sense 'do not enter Bitcoin' so their specific choice of alternate coin is irrelevant to a Bitcoin model". My first attempt to counter that would be along the lines, "perhaps the effects of switching between coins in equilibrium would yield more conditions

---

[1]For example.

we could use".

The second line of thought is related to how salient the end of a processor's life is to mining versus the obsolescence of a particular processor. The model as it currently stands seems like it would have the end of a processor's life playing a large role in the investment decision, though my prior is that obsolescence is a bigger factor than breakdown. I think obsolescence is likely to be a more important modeling concern than other coins, since it gets to the "arms race" nature of mining investments. There may be some interaction between the two if miners allocate hardware across coins based on relative processing power. Formally, I think the arms race aspect could be incorporated by expanding out the $M(t)$ term in equation 1 along the following lines: assuming $n(t)$ miners at instant t, denoting an individual miner by i, and the amount of Gh/s owned by miner i as $o_i(t)$, $M(t) \equiv \int_0^{n(t)} o_i(t)di$. Assuming the processor lasts for T periods as before, the gross return (ignoring capital costs) to a single miner's setup is

$$E\left[\int_0^T e^{-rt}B(t)\left(\frac{o_i(t)X(t)}{M(t)}\right) - c(t)dt\right].$$

An individual miner's instantaneous capital costs here would be $k(t)\dot{o}_i(t)$. In this setup, we can consider the effect of time trends in $M(t)$ on investment decisions in more detail. We can also use this setup to consider the incentives of mounting a 51% attack, though I think that might be a project for a later date. It seems to increase the analytical complexity of the model, as a miner's choice is no longer just "enter/don't" but also "how much to invest". $M(t)$ is still the endogenous equilibrator, but now through two channels: $n(t)$ and $o_i(t)$. This setup could also connect to Ali's model of the externalities of mining investments.

The third line of thought is that it may be worthwhile to consider the underlying maximization problems that yields the equilibrium conditions. This may let us model the option value of waiting to enter in more detail. I think it would look something like

$$V_i^E(t) = \max_{y_i(t)\in\{0,1\}}\{(1-y_i(t))V_i^E(t) + y_i(t)V_i^M(t)\} \tag{2}$$

$$V_i^M(t) = \max_{o_i(t)}\{E\left[\int_0^T e^{-rt}B(t)\left(\frac{o_i(t)X(t)}{M(t)}\right) - c(t)dt\right] - k(t)o_i(t)\} \tag{3}$$

Equation 2 is the entry decision, and equation 3 is the investment decision, with $y_i(t) = 1$ meaning the miner has decided to enter[2]. Free entry should pin down $n(t)$ through equation 2, while profit maximization should pin down $o_i(t)$ through equation 3. Practically, I think we would solve equation 3 for the optimal amount of investment first, then equation 2. There is an implicit assumption of a perfect resale market in processors. I think assuming that miners do not treat each other strategically is how we would want to start down this path.

---

[2]I am more familiar with these equations in discrete time, so I may have the form wrong in continuous time. I think continuous time is the appropriate framework for this question since lags in entry aren't really relevant here. This is probably a minor modeling concern at best.

I want to stress that, given how little has been done in this space, we should probably work with the model in equation 1 first, for which equation 2 may be a reasonable depiction of the underlying decision problem.

Lastly, I think another question worth considering is a miner's choice of which pool to enter. I think this would add some more structure along the lines of equation 2, but is something to do after we've fully characterized the model in equation 1.