ASIC profitability and Bitcoin Price: Mathematical Derivation

Thomas Kocar

January 25, 2021

Summary

p = ASIC price
c = annual mining cost
f_0 = annual mining reward in Fiat currency (e.g. \$) at $t = 0$
k = increase in bitcoin price / growth
Ω = end of ASIC profitability in years
$b_{fair}(0)$ = Fair Bitcoin Price in Fiat currency (e.g. \$) at $t = 0$

For every ASIC, k can be calculated by solving

$$\Omega = \frac{\ln f_0 - \ln c}{0.347 - k}$$

with Ω satisfying:

$$\frac{f_0}{-0.347} * (e^{-0.347*\Omega} - 1) = (c * \Omega) + p$$

The lower the k, the more profitable ASIC.

For a gross estimation of the fair Bitcoin price $b_{fair}(0)$:

$$b_{fair}(0) = ln2 * b(0) * \frac{2c + p}{f_0}$$

Variables:
p = ASIC price in Fiat currency (e.g. $)
c = annual mining cost in Fiat currency (e.g. $)

Functions:
b(t) = Bitcoin price in Fiat currency (e.g. $) as a function of time t in years
r(t) = annual mining reward in ₿ as a function of time t in years
R(t) = $\int r(t)dt$ = Integral of r(t)

Assumptions:
We assume an annual incremental increase of Bitcoin price and hashrahte. Hence b(t) and r(t) are exponential functions:

$$r(t) = r(0) * e^{j*t} \tag{1}$$

$$b(t) = b(0) * e^{k*t} \tag{2}$$

with k and j being the growth coefficient of their respective function.

Determining the end of ASIC profitability

The mining reward has to be bigger than the cost of mining, else mining would not be profitable. The end of ASIC profitability ($t = \Omega$)) is reached, when the cost of mining c is equal to the mining reward in Fiat currency.

Hence,

$$b(\Omega) * r(\Omega) = c$$

given (1) and (2):

$$b(0) * e^{k*\Omega} * r(0) * e^{j*\Omega} = c$$

$$b(0) * r(0) * e^{(k+j)*\Omega} = c$$

solving for Ω:

$$e^{(k+j)*\Omega} = \frac{c}{b(0) * r(0)}$$

$$(k+j) * \Omega = \ln \frac{c}{b(0) * r(0)}$$

$$(k+j) * \Omega = \ln c - \ln \left(b(0) * r(0)\right)$$

$$\Omega = \frac{\ln c - \ln \left(b(0) * r(0)\right)}{k+j}$$

$b(0) * r(0)$ equals the mining reward in Fiat Currency at $t = 0$. For simplification, it is defined as f_0.

$$\Omega = \frac{\ln c - \ln f_0}{k+j} \tag{3}$$

Determining Mining Profitability

Mining is only profitable, if the sum of all bitcoin mined up until the end of ASIC profitability ($t = \Omega$) is no less then the bitcoin one would have gotten by simply buying Bitcoin at $t = 0$ on an exchange. Thus, mining is break even, when

$$R(\Omega) = \frac{(c * \Omega) + p}{b(0)} \tag{4}$$

where R(Ω) is the integer of r(t) from 0 to Ω:

$$R(\Omega) = \int_0^{\Omega} r(t)dt$$

$$R(\Omega) = \frac{r(0) * e^{j*\Omega}}{j} + C \tag{5}$$

As there is no mining reward at $t = 0$, R(0) has to be 0.

$$0 = \frac{r(0)}{j} + C$$

solving for C:

$$C = \frac{-r(0)}{j}$$

(5) is solved to

$$R(\Omega) = \frac{r(0) * e^{j*\Omega}}{j} - \frac{-r(0)}{j}$$

$$R(\Omega) = r(0) * \frac{e^{j*\Omega} - 1}{j} \tag{6}$$

and (4) is solved to

$$r(0) * \frac{e^{j*\Omega} - 1}{j} = \frac{(c * \Omega) + p}{b(0)}$$

$$r(0) * b(0) * \frac{e^{j*\Omega} - 1}{j} = (c * \Omega) + p$$

$$\frac{f_0}{j} * (e^{j*\Omega} - 1) = (c * \Omega) + p \tag{7}$$

Practical Application

I: Moores Law

For j we can apply Moore‘s Law. Moore‘s Law states, that the numbers of transistors in an Integrated Circuit doubles every two years.

$$e^{j*2} = \frac{1}{2}$$

$$2j = ln\frac{1}{2}$$

$$2j = -ln2$$

$$j = \frac{-ln2}{2}$$

which approximates to

$$j = -0.347$$

(3) can be solved to

$$\Omega = \frac{\ln c - \ln f_0}{k - 0.347}$$

$$\Omega = \frac{\ln f_0 - \ln c}{0.347 - k} \tag{8}$$

and (7) can be solved to

$$\frac{f_0}{-0.347} * (e^{-0.347*\Omega} - 1) = (c * \Omega) + p \tag{9}$$

II: Estimating ASIC profitability and Bitcoin Price

For every ASIC, the constants p and c are known. When assuming Moore's Law, j is also known and only the growth rate of the Bitcoin Price k has to be estimated. For every k, the end of ASIC profitability $t = \Omega$ of a specific ASIC can be calculated, using formula (8)

$$\Omega = \frac{\ln f_0 - \ln c}{0.347 - k}$$

Doing this, an Ω can be found that satisfies formula (9)

$$\frac{f_0}{-0.347} * (e^{-0.347*\Omega} - 1) = (c * \Omega) + p$$

By brute force iteration, k can be calculated for every ASIC. The lower the k, the more profitable the ASIC.

Most mining operations would assume a 2-3 year lifespan for an ASIC. For practical purposes we can assume $\Omega = 2$. Under these assumptions, mining at the hypothetical fair price $b_{fair}(0)$ has to be as profitable as buying Bitcoin at the current price $b(0)$.

given (7):

$$b_{fair}(0) * \frac{f_0}{j} * (e^{j*2} - 1) = b(0) * ((c * 2) + p)$$

solving for $b_{fair}(0)$:

$$b_{fair}(0) = b(0) * \frac{j}{(e^{2*j} - 1)} * \frac{2c + p}{f_0}$$

assuming Moore's Law:

$$b_{fair}(0) = b(0) * \frac{\frac{-ln2}{2}}{(e^{2*\frac{-ln2}{2}} - 1)} * \frac{2c + p}{f_0}$$

which simplifies to:

$$b_{fair}(0) = ln2 * b(0) * \frac{2c + p}{f_0} \tag{10}$$