ASIC Profitability and Bitcoin Price Forecast

Summary

p = ASIC price

c = annual mining cost

$€_0$ = annual mining reward in € at t = *0*

k = increase in bitcoin price / growth

Ω = end of ASIC profitability in years

b(t) = Bitcoin price in € as a function of time (t) in years

For every ASIC, Ω can be calculated by choosing the coefficient *k*

$$\Omega=\frac{\ln(€_0)-\ln(c)}{0.347-k}$$

while Ω has to satisfy

$$\frac{€_0}{-0.347}*(e^{-0.347*\Omega}-1)=(c*\Omega)+p$$

The lowest and highest *k* calculated using this method gives the upper and lower bounds of the bitcoin price at a specific point in time (t) in years.

$$b_{min}(t)=b(0)*e^{k_{min}*t} < \text{b(t)} < b_{max}(t)=b(0)*e^{k_{max}*t}$$

Variables:

p = ASIC price in €

c = annual mining cost

m = annual ASIC hashrate

Functions:

b(t) = Bitcoin price in € 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:

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

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

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

Determining the end of ASIC profitability (t = Ω)

The mining reward has to be bigger than the cost of mining, else mining would not be profitable. The end of ASIC profitability (t = *Ω*) is reached, when the cost of mining (*c*) is equal to the mining reward in €.

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*:*

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

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

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

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

b(0) * r(0) equals the mining reward in € at t = *0*. For simplification, it is defined as $€_{0.}$

(3) $$\Omega=\frac{\ln(c)-\ln(€_0)}{k+j}$$

Determining Mining Profitability

Mining is only profitable, if the sum of all bitcoin mined up until the end of ASIC profitability (t = *Ω*) 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

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

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

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

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

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

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

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

and (4) is solved to

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

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

(7) $$\frac{€_0}{j} * (e^{j*\Omega} - 1) = (c * \Omega) + p$$

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 (IC) doubles every two years.

$$e^{j*2} = 1/2$$

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

$$2j = -\ln(2)$$

$$j = \frac{-\ln(2)}{2}$$

which approximates to

$$j = -0.347$$

(3) can be solved to

$$\Omega = \frac{\ln(c) - \ln(€_0)}{k - 0.347}$$

(8) $$\Omega = \frac{\ln(€_0) - \ln(c)}{0.347 - k}$$

and (7) can be solved to

(9) $$\frac{€_0}{-0.347} * (e^{-0.347*\Omega} - 1) = (c * \Omega) + p$$

II: Estimating ASIC profitability and Bitcoin Price

For every ASIC, the constants p and c are known. When assuming Moore‘s Law (j is known), only the growth rate of the Bitcoin Price (k) is unknown. For every *k*, the end of ASIC profitability (t = Ω) of a specifiv ASIC can be calculated, using formula (8)

$$\Omega = \frac{\ln(€_0) - \ln(c)}{0.347 - k}$$

while Ω has to satisfy formula (9)

$$\frac{€_0}{-0.347} * (e^{-0.347*\Omega} - 1) = (c * \Omega) + p$$

Hence, *k* can be calculated for a specific ASIC.

By comparing different ASIC, an interval for a future Bitcoin price can be estimated. Less profitable ASIC would require a higher *k* compared to more profitable ASIC. This gives an interval:

$$b_{min}(t) = b(0) * e^{k_{min} * t} \ < \ b(t) \ < \ b_{max}(t) = b(0) * e^{k_{max} * t}$$