

# A Simple Bitcoin Market Model v1.1



Pascal Urien

December 2017

## Table of Content

Executive Summary .....	3
The bitcoin production rate .....	5
The hash rate .....	5
The production cost.....	5
Remark1: Defining the $\mu$ constant .....	6
Remark2: About the Bitcoin network constraint.....	7
Market Price and Valorization .....	7
Miners' gain and number of rigs.....	8
The Bitcoin Market .....	9
Growth Limit.....	10
Negative valorization .....	10
The Rig profit.....	10
The profit per rig in \$ .....	11
Estimation of the k factor .....	11
A miner keep bitcoin strategy .....	11
Non constant valorization.....	12
Checking the profit rig lemma .....	13

## Executive Summary

The network fixes the production price  $c(t)$  of the bitcoin (BTC)

$$c(t) \approx \mu H_{R(t)} / B_R \text{ in } \$ / BTC$$

$H_R$  is the quantity of hashes needed for the production of  $B_R$  (12,5 BTC in 2017) bitcoins.

$\mu$  is a physical factor (in  $\$/TH$ ) relying on the rig technology.

$$\mu = (R_A / \beta + 8.760 P_E E_C) / 31.536.000 \text{ in } \$ / TH$$

$R_A$ = Rig Amortization (in $\$/year/rig$ )	600
$P_E$ = Power Efficiency (in Joule per Giga Hash)	0,1
$E_C$ = Energy Cost (in $\$/KWh$ )	0,15
$B_R$ = Block Reward (in BTC)	12,5
$H_R$ = HashRate x 600s = $12 \cdot 10^6 \times 600$ (in Tera Hash)	$7,2 \cdot 10^9$
$\beta$ = The number of hashes produced by a rig (in THs)	14
$m$ = The <i>Market Valorization Factor</i>	1
$1/\lambda$ = The <i>Market Time Constant</i>	174 days
$1/k = 1/(\text{Market Incitement Factor}) = m \beta \mu$ = profit/ $\lambda$	1163 \$
$\mu$ = (in $\$/TH$ )	$5,53 \cdot 10^{-6}$

$$h(t) = \beta r(t) \text{ in Tera Hash per second} - THs$$

where  $r(t)$  is the number of rigs,  $h(t)$  the hashrate i.e. the number of hashes produced by the rigs' park every second. The market valorization  $v(t)$  is defined as:

$$v(t) = m c(t) , \text{ in } \$ / BTC$$

Where  $m$  is the *market valorization factor*. The market price is:

$$p(t) = c(t)(1 + m) , \text{ in } \$ / BTC \text{ with } m \geq -1$$

The rigs make money if the market valorization factor ( $m$ ) is positive. The profit in \$, per rig and per second is:

$$R_P = \text{rig profit} = m \beta \mu , \text{ in } \$ / s$$

We assume that the number of rigs  $r(t)$  increases with the miners' gain  $g(t)$  (expressed in \$) according to a constant  $k \geq 0$  factor .

$$r(t) - r(to) = k (g(t) - g(to)) , k \text{ in } \$^{-1}$$

Where  $k$  is the *market incitement factor*. We deduce from these hypothesizes that the number of rigs increases/decreases exponentially according to the sign of  $m$ .  $1/\lambda$  is the *market constant time*.

$$r(t) = r(to) e^{k\beta\mu \int_{to}^t m(t)dt}$$

$$r(t) = r(to) e^{\lambda (t-to)}$$

$$\text{with } \lambda = k m \beta \mu = k \text{ profit} , \text{ in } s^{-1}$$

Furthermore when the valorization  $m$  is positive the hashrate  $h(t)$ , the cost  $c(t)$ , the market price  $p(t)$ , and the valorization  $v(t)$  increase exponentially.

$$h(t) = h(to) e^{\lambda (t-to)}$$

$$c(t) = c(to) e^{\lambda (t-to)}$$

$$p(t) = (1 + m) c(to) e^{\lambda (t-to)}$$

$$v(t) = m c(to) e^{\lambda (t-to)}$$

When the valorization  $m$  is negative, the rigs lose money, their number decreases;  $\lambda$  is negative, and consequently the hashrate decreases. The network lowers the production price  $c(t)$ . The market price  $p(t)$  decreases until the valorization becomes positive again.

The growth limit is induced by the energy consumption, which relies on the rigs number. At this point the  $k$  factor will be null, implying a null value of  $\lambda$ , and therefore :

$$r(t) = r(to)$$

$$h(t) = h(to)$$

$$c(t) = c(to)$$

$$p(t) = (1 + m(t)) c(to)$$

$$v(t) = m(t) c(to)$$

## The bitcoin production rate

The bitcoin production rate is a constant (for example 12,5 BTC every 10 minutes), the number  $b(t)$  of bitcoins increases linearly with the time.

$$(1) \frac{db}{dt} = \alpha \text{ in BTC/s}$$

$$(1a) b(t) - b(t_0) = \int_{t_0}^t \alpha(t) dt, \alpha \approx \frac{B_R}{T_R}$$

$$(1c) b(t) - b(t_0) = \alpha(t - t_0)$$

For example:

$$B_R = 12,5 \text{ BTC}, T_R = 600s, \alpha = 12,5 \text{ BTC} / 600s = 2,083 \cdot 10^{-2} \text{ BTC/s}$$

## The hash rate



The hash rate  $h(t)$  (in THs = *Tera Hash per second*) is proportional to the number of rigs  $r(t)$ .

$$(2) h(t) = \beta r(t) \text{ in THs}$$

for example  $\beta = 14 \text{ THs}$  (figure from the AntminerS9 rig)

## The production cost

The production cost  $c(t)$  (in \$/BTC) is proportional to the hash rate  $h(t)$ .

$$(3) c(t) = \gamma h(t) \text{ in \$/BTC}$$

$$(3a) \gamma = (R_A / \beta + 8,76 \cdot 10^3 P_E E_C) / BTC\_Year \text{ in } \$/BTC /THs$$

$R_A$  = Rig amortization (\$/year/rig)

$P_E$  = Power Efficiency (Joule per Giga Hash)

$E_C$  = Energy Cost (\$/KWh)

$B_R$  = Block Reward (BTC)

$BTC\_year$  = number of bitcoins produced per year

$R_A$  = 600 \$/year, AntminerS9 1800 \$, with 3 years amortization,

$P_E$  = 0,1 J/GH, AntminerS9 (0,1 Joule per Giga Hash).

$E_C$  = 0,15 \$/KWh

$B_R$  = 12,5 BTC block reward every 10 minutes

$BTC\_year = B_R \times 144 \times 365 = 12.5 \times 144 \times 365$

$$\gamma = (600/144 + 8,76 \cdot 10^3 \times 0,1 \times 0,15) / (12.5 \times 144 \times 365)$$

$$\gamma = (42,9 + 131,4) / 657000 = 2,7 \cdot 10^{-4} \$/BTC /THs$$

For example with a hash rate of  $12 \cdot 10^6$  THs the cost per bitcoin is :

$$c(t) = 2,7 \cdot 10^{-4} \times 12 \cdot 10^6 = 3240 \$ / BTC$$

**Remark1: Defining the  $\mu$  constant**

$$(3b) \gamma = (R_A / \beta + 8,76 \cdot 10^3 P_E E_C) / (\alpha \cdot 31,536 \cdot 10^6)$$

$$(3c) \gamma = \mu / \alpha$$

$$(3d) \mu = (R_A / \beta + 8,76 \cdot 10^3 P_E E_C) / 31,536 \cdot 10^6$$

$$(3e) c(t) = \mu h(t) / \alpha$$

$$\text{For example: } \mu = (42,9 + 131,4) / 31,536 \cdot 10^6 = 5,53 \cdot 10^{-6}$$

The rig cost (\$/rig/s) is  $R_C = \mu \beta$ , remarking the  $\beta P_E = R_E$  is the energy (in KW) consumed by a rig we get:

$$(3f) R_C = \beta \mu = (R_A + 8.760 R_E E_C) / 31.536.000$$

### Remark2: About the Bitcoin network constraint

The network fixes a given quantity of hashes  $H_R$  in order to release  $B_R$  bitcoins.

When  $\int_{t_0}^t h(t) dt = H_R$  the network creates  $B_R$  bitcoins.

And the approximate  $\alpha$  value is :  $\alpha \approx B_R / (t - t_0) = B_R / \Delta T$

Let's assume a small variation of  $h(t)$  around  $t$  :

$$H_R \approx h(t) \Delta T$$

$$(3f) \quad c(t) \approx \mu H_R / B_R$$

$$(3g) \quad c(t) \approx \mu h(t) \Delta T / B_R \approx \mu h(t) / \alpha$$

For small variation of the hashrate, we assume the equation (3e) remains valid.

### Market Price and Valorization

The market price  $p(t)$  is equal to the sum of production cost ( $c(t)$ ) and the market valorization  $v(t)$ .

$$(4) \quad p(t) = c(t) + v(t) \text{ in } \$/\text{BTC}$$

We assume that the market valorization  $v(t)$  is proportional to the cost  $c(t)$ :

$$(5) \quad v(t) = m c(t) \text{ in } \$/\text{BTC}$$

Where  $m$  is the *market valorization factor*. From(4)(5)

$$(5a) \quad p(t) = c(t) (1 + m) \text{ in } \$/\text{BTC}$$

m is usually positive, but a negative value could be possible with the constraint  $m \geq -1$

From the bitcoin price history let's assume  $m=1$  (i.e. the valorization is equal to the cost).

For example with a hash rate of  $12 \cdot 10^6$  THs the valorization per bitcoin is :

$$v(t) = m c(t) = 3240 \$ / \text{BTC}, \text{ and } p(t) = 6480\$$$

## Miners' gain and number of rigs

We can write the miners' gain  $dg$  (\$) during a time  $dt$  as :

$$(6) dg = v(t) db \quad \text{in \$}$$

Or:

$$(6a) g(t) - g(to) = \int_{b(to)}^{b(t)} v(t) db$$

And therefore :

$$(7) \frac{dg}{dt} = v(t) \frac{db}{dt} = \alpha v(t)$$

We assume that the interest for mining is proportional to the miners' gain  $g(t)$ , which implies an increase of rigs.

$$(7a) r(t) - r(to) = k(g(t) - g(to))$$

$$(8) \frac{dr}{dg} = k \quad \text{in } \$^{-1}$$

Where  $k$  is a positive constant, the *market incitement factor* ( $k \geq 0$ ).

The variation of  $r$  is negative if the variation of  $g$  is negative.

When  $\Delta g = 1/k$  \$, a new rig ( $\Delta r = 1$ ) is added to the bitcoin network.



From (8) and (7) we get

$$(9) \frac{dr}{dt} = k \frac{dg}{dt} = k \alpha v(t)$$

and thereafter from (5) (3) (2)

$$(10) \frac{dr}{dt} = k \alpha \beta \gamma m r(t)$$

## The Bitcoin Market

This relation (9) works even if  $\alpha$  is not constant :

$$(10a) \frac{dr}{dt} = k \beta \alpha(t) \gamma(t) m r(t) = k \beta \mu m r(t)$$

let's define:

$$(10b) \lambda = k \alpha \beta \gamma m \quad \text{in s}^{-1}$$

$$(10c) \lambda = m k \beta \mu \quad \text{in s}^{-1}$$

$$(10e) \frac{dr}{dt} = \lambda r(t)$$

The  $\lambda$  parameter is not dependant from  $\alpha$  (bitcoin rate production, i.e. the block mining rate).

Therefore :

$$(11) r(t) = r(to) e^{\lambda (t-to)}$$

$$(12) h(t) = h(to) e^{\lambda (t-to)}$$

$$(13) c(t) = c(to) e^{\lambda (t-to)}$$

$$(14) p(t) = (1 + m) c(to) e^{\lambda (t-to)}$$

$$(15) v(t) = m c(to) e^{\lambda (t-to)}$$

## Growth Limit

We believe that the growth limit is induced by the energy consumption, which relies on the rigs number.

At this point the  $k$  factor will be null, implying a null value of  $\lambda$ , and therefore :

$$\begin{aligned}r(t) &= r(to) \\h(t) &= h(to) \\c(t) &= c(to) \\p(t) &= (1 + m(t)) c(to) \\v(t) &= m(t) c(to)\end{aligned}$$

## Negative valorization

$$(16) \ v(t) = m \ c(to) \ e^{\lambda (t-to)}$$

When the valorization  $v(t)$  is negative ( $m < 0$ ) the  $\lambda$  parameter is negative. The number of working rigs decreases, and so the mining costs. The block mining rate decreases. Therefore after a few  $1/\lambda$  the valorization reaches a null value, the system crashes. Likely the bitcoin network will fix a difficulty and therefore a hash rate leading to a null valorization ( $m=0$ ) before the crash.

We obviously believe that  $m$  is not a constant over the time,  $m(t) = f(t)$ .

## The Rig profit

Given  $h(t)$  and  $p(t)$  we can retrieve:

$$\begin{aligned}c(t) &= \gamma \ h(t) \\v(t) &= p(t) - \gamma \ h(t) = m \ c(t) \\r(t) &= \frac{1}{\beta} \ h(t)\end{aligned}$$

**The profit per rig remains constant  $v(t)/r(t) = \text{constant}$  (in \$/BTC).**

$$(17) v(t)/r(t) = m \beta \gamma$$

### The profit per rig in \$

The profit in \$ per rig and per year is written as:

$$(18) BTC\_Year v(t)/r(t) = m \beta (R_A/\beta + 8,76 \cdot 10^3 P_E E_C)$$

For example :

$$BTC\_Year v(t)/r(t) = 14 \times (42,9 + 131,4) = 2440 \$ / \text{rig/year}$$

### Estimation of the k factor

Every  $\tau = \ln(2) / \lambda$  the profit doubles

Let's assume  $\tau = 4 \text{ months}$  (x8 every year)

$$\lambda = 0,7 / (3600 \times 24 \times 365/3) = 6,66 \cdot 10^{-8}$$

$$k = \frac{\lambda}{\alpha \beta \gamma m} = 6,66 \cdot 10^{-8} / (2,083 \cdot 10^{-2} \times 14 \times 2,7 \cdot 10^{-4} \times 1)$$

$$k = 8,46 \cdot 10^{-4} \$^{-1}$$

One rig is added to the bitcoin network every  $(1/k)$  1182 \$ profit

If we assume k is a constant

$$1/\lambda = 1 / m k \alpha \beta \gamma = 174 \text{ days} / m$$

### A miner keep bitcoin strategy

A rig produces  $\alpha/r(t)$  bitcoin per second.

The benefit (in \$/s) is  $m/(1+m) p(t) \alpha/r(t)$

The benefit in BTC/s is  $m/(1+m) \alpha/r(t)$

If the miner keeps the benefit in bitcoin, it will benefit from the market price increase. His benefit after a time T is therefore :

$$(19) \ b(T) = p(t) \frac{m}{m+1} \alpha \int_0^T 1/r(t) dt$$

$$(20) \ b(T) = \frac{p(to)}{r(to)} \frac{m}{1+m} \alpha \lambda^{-1} (e^{\lambda T} - 1)$$

For example :

$$r(to) = h(to)/14 = 12 \cdot 10^6 / 14 = 860,000 \text{ rigs}$$

$$p(to) = 6480 \$$$

$$1/\lambda = 174 \text{ days}$$

$$\alpha = 657000/365 \text{ days}$$

$$b(T(\text{days})) = p(to) \frac{m}{1+m} 0,37 (e^{T/174} - 1)$$

## Non constant valorization

From (10):

$$(21) \ \frac{dr}{r(t)} = k \beta \mu m(t)$$

And therefore:

(22)

$$\frac{r(t)}{r(to)} = e^{\int_{to}^t \beta \mu k(t) m(t) dt}, m(t) \geq -1, k\beta\mu \text{ constant}$$

$$(22a) \ r(t) = r(to) e^{\int_{to}^t \beta \mu k(t) m(t) dt}$$

## Checking the profit rig lemma

From (7) and (15), we get:

$$\int_{t_0}^t dg = g(t) - g(t_0) = \alpha \int_{t_0}^t v(t) dt$$

$$g(t) - g(t_0) = \frac{\alpha}{\lambda} v(t_0) (e^{\lambda(t-t_0)} - 1)$$

From (11) :

$$g(t) - g(t_0) = \frac{\alpha}{\lambda} \frac{v(t_0)}{r(t_0)} (r(t) - r(t_0))$$

From (5) (3) (2)

$$v(t_0) = m \beta \gamma r(t_0)$$

Therefore from (10)

$$g(t) - g(t_0) = \frac{m \alpha \beta \gamma}{\lambda} (r(t) - r(t_0))$$

$$g(t) - g(t_0) = \frac{1}{k} (r(t) - r(t_0))$$

$$r(t) - r(t_0) = k (g(t) - g(t_0))$$

Which gives again (8)