Proportional block reward as a price stabilization mechanism for peer-to-peer electronic cash system

Karol Trzeszczkowski

Licho

April 17, 2021

Abstract

A simple modification to Bitcoin reward system design, namely putting a function of mining difficulty as a block reward, creates a feedback loop regulating supply and stabilizing price of cryptocurrency around a certain equilibrium.

1 Introduction

As described in [1], Bitcoin was an attempt to create purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution. Bitcoin network is a distributed time stamp server, an immutable ledger of transactions transferring the the blockchain native currency between the network users. Immutability is ensured by the proof of work mechanism that makes it impossible to modify the ledger without redoing computational work previously done during an expensive mining process up to the point of time when the ledger entry was added to the blockchain. Mining is done by by guessing a solution to a cryptographic puzzle. An attempt to guess the solution is called a hash. The number of attempts in a period of time is called hash rate. The average number of guesses that has to be made to find the solution is called block difficulty.

Decentralized cryptocurrencies that aim to be peer to peer electronic cash such as Bitcoin Cash [1] Dash or Monero etc. rely on a very simple money supply model. New coins come into the system as a reward for finding a block of the blockchain. For Bitcoin, most of the time block reward is constant, until it is divided by half every four years, eventually going to zero. Others, like Doge coin and Monero have constant reward forever. More complicated predetermined schedule is used by zero-zed [3]. Having supply as a predetermined function of time means that the relative currency price changes are driven purely by ongoing exchange. Supply does not react to the changes in the environment. The entire prediction is ruined if the currency adoption won't meet the schedule.

Raise of multiple payment processors that offer automatic conversion to fiat currencies defeats the purpose of peer-to-peer electronic cash by introducing a trusted third party in the middle. Raise of so called stable coins is a strong signal, that the initial economic assumptions of Bitcoin might have been wrong. Lack of shelling point value for short term stabilization, as well as 17% deflation per year that have to occur for Bitcoin to replace fiat money in 100 years [2], might be harmful to Bitcoin economy.

2 Proportional reward supply system

Key proposition of this paper is a system of supply for a cryptocurrency that would ensure long term stability of purchasing power, by adjusting the supply to match the demand for the currency.

To achieve it, block reward shall be a linear function of the current block mining difficulty.

This modification will peg the price to the expenses of miners working on the new blocks of the blockchain. Keeping the halving mechanism of Bitcoin protocol will adjust for improving efficiency of mining hardware. Detailed parameters of halving shall be approximated from the current hardware efficiency trend. Any long term, averaged changes in the purchasing power will depend on the quality of this prediction.

3 Mathematical model

To evaluate this proposition and prove that putting a block reward as a function of difficulty will in fact stabilize the price, let us present our assumptions and build a model.

The strongest assumption made here is dealing only with averaged quantities and changes that are slow enough to not interfere with the internal equilibrium of the system. Second assumption is that there exists sufficient capacity of large cryptocurrencies with the same hashing algorithm as a buffer for miners, reducing delays in setting up new mining farms and producing new mining equipment.

The law of supply and demand

Relative price of a currency with no other utility than being a unit of exchange is expressed as follows:

$$p(t) = \frac{z(t)}{N(t)} \tag{1}$$

Where N is the number of units of the currency, and z is the value accumulated in the economy of the currency. It is defined as:

$$z(t) = \int_0^t (d(\tau) - s(\tau))p(\tau)d\tau$$

where d is market demand and s is market supply counted in the units of the currency in consideration. Formula (1) is in fact integral equation, not a definition. To get some intuitive understanding of eq. (1)behind let's consider that doubling the amount of currency units in circulation in a quasi-static process while having fixed z is equivalent to changing all the prices and amounts in people pockets by the factor of two. Such change would reduce the relative price of a currency by half. This consideration works for any factor.

Similarly, with the fixed N the price p is proportional to the difference between supply and demand integrated over time.

To transition from integral equation to differential equation we make a first derivative of $p(t)$:

$$p'(t) = \frac{d(t) - s(t) - N'(t)}{N(t)}p(t) \tag{2}$$

In Bitcoin protocol $N'(t)$ is defined by the block reward and most of the time it's fixed so the long term price is driven purely by demand due to the bitcoin economy growth.

3.1 Hash rate and difficulty

Hash rate is the amount of work being done on the proof of work blockchain per unit of time. Changes in hash rate are driven by the reward ($N'p$) and the cost of finding a block, which depends

on electricity cost and difficulty. Miners profit is considered constant and and included in electricity cost.

$$h'(t) = \alpha(N'(t)p(t) - D(t)\varepsilon), \tag{3}$$

The parameter α describes how fast new hash rate can be added or moved to the system. The assumption that there exists a large cryptocurrency of the same hashing algorithm makes this value high.

$D(t)$ is the difficulty. On average, block difficulty is equal to the current hash rate. It is adjusted by a moving average to reflect what work is being done on it and keep the block production steady.

Remark 1 *The relationship between difficulty and block solve time is linear.*

In further consideration we will be using the following, averaged version of eq. (3) and use words hash rate and difficulty interchangeably when it's not confusing.

$$h'(t) = \alpha(N'(t)p(t) - h(t)\varepsilon). \tag{4}$$

4 Modeling Bitcoin

For Bitcoin with the constant money supply $N'(t) = R = const.$ and $N(t) = Rt$. The resulting system of equations reads:

$$\begin{cases} p' = p\frac{d-s}{Rt} - p\frac{R}{Rt}, \\ h' = \alpha(Rp - h\varepsilon). \end{cases} \tag{5}$$

The two equations are separate. The first equation does not depend on the solution of the second one and $\varepsilon = const.$, the second equation can also be solved using Green's function method with $p(t)$ as a boundary. The fundamental solution of the equation reads:

$$G_h(t) = R\alpha\Theta(t)e^{-\varepsilon\alpha t}$$

For constant positive demand $d - s$ exceeding money production the price growth would be linear. For demand $d - s \sim p$, meaning that Bitcoin is getting more popular proportionally to the price growth, the solution of the first equation is a hyperbola. Indeed between 2016 and 2018 Bitcoin BTC price chart is shaped like one.

When the reward is constant, the hash rate follows the price with a delay measured with α. The hash rate function is just $h = G_h * p$.

5 Proportional reward supply model

Proportional reward system is a postulate to put a function of the current block difficulty as the current block reward. For now, let's assume $\varepsilon = \varepsilon_0 = const$, meaning that the cost of making a single hash does not change over time.

We put

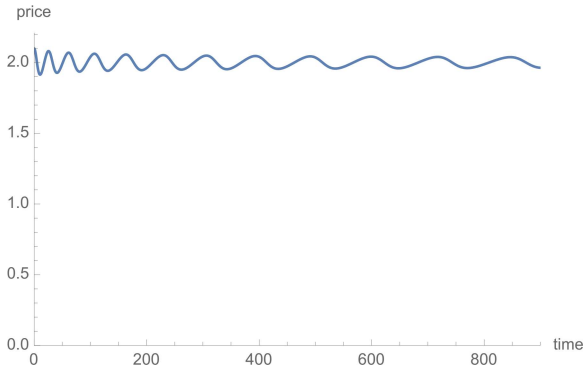
$$f(h(t)) = N'(t) \tag{6}$$

to the equations (2) and (4) forming the system of equations:

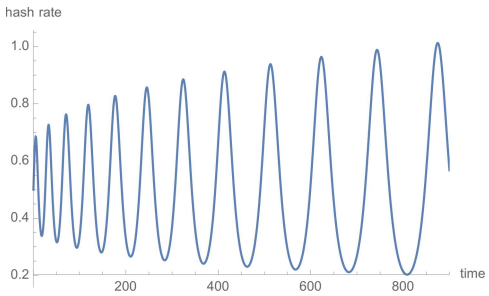
$$\begin{cases} p' = p\frac{d-s}{N} - p\frac{N'}{N}, \\ h' = \alpha(N'p - h\varepsilon), \\ f(h) = N'. \end{cases} \tag{7}$$

For convenience we dropped the time argument.

Let's put $f = id$ for simplicity. A proportionality factor can be added here. This system of equations can't be solved analytically therefore we will present numerical solution for some different

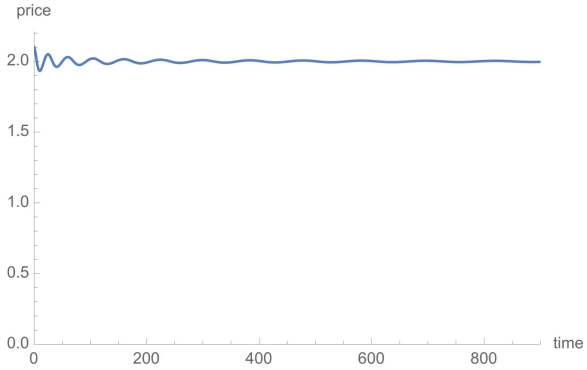


(a) Numerical solution of system (7) for p.

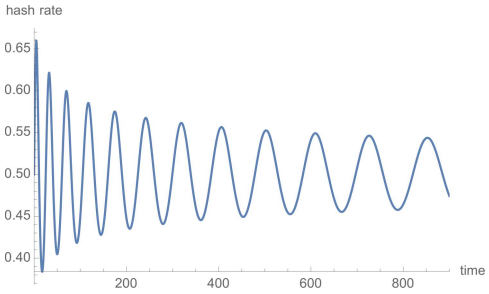


(b) Numerical solution of system (7) for h.

Figure 1: Numerical solution for $\varepsilon_0 = 2$, $C = 0.5$, $p(0) = 2.1$, $h(0) = 0.5$, $N(0) = 10$.



(a) Numerical solution of system (7) for p.



(b) Numerical solution of system (7) for h.

Figure 2: Numerical solution for $\gamma = 0.6$ and the rest of parameters are the same as before.

initial conditions and assumptions on $(d-s)$. For $d-s = C, C = const., C > 0$ The plot is presented on figure 1.

The price oscillates around the point of equilibrium, which is ε_0 and hash rate oscillates around C. We can see that although price oscillations are stable, the amplitude of of hash rate oscillations is growing.

Any predictable market behavior can be exploited for profit, therefore we may introduce damping force around the equilibrium $-\gamma(p-\varepsilon_0)$in the first equation of (7) due to speculation. It means that the more the price is below equilibrium, the more people buy it, knowing the price will grow and the more the price is above equilibrium, the more people sell, knowing the price will soon fall.

$$p' = \frac{p(d-s) - \gamma(p-\varepsilon_0)}{N} - p\frac{N'}{N}.$$

After introducing damping factor $\gamma > C$ (fig. 4), not only the price oscillations decrease in time, but also the hash rate stabilizes. In reality the damping factor may turn out to be very large because any predictability is a big opportunity for making money. In fact it should always be sufficient to extinguish the oscillatory behavior.

In this simple model, as it is intuitively expected, the currency unit value is close to the value of electricity used for work and money supply is equal to the demand for new coins. Mining becomes direct, one way exchange of electricity for coins.

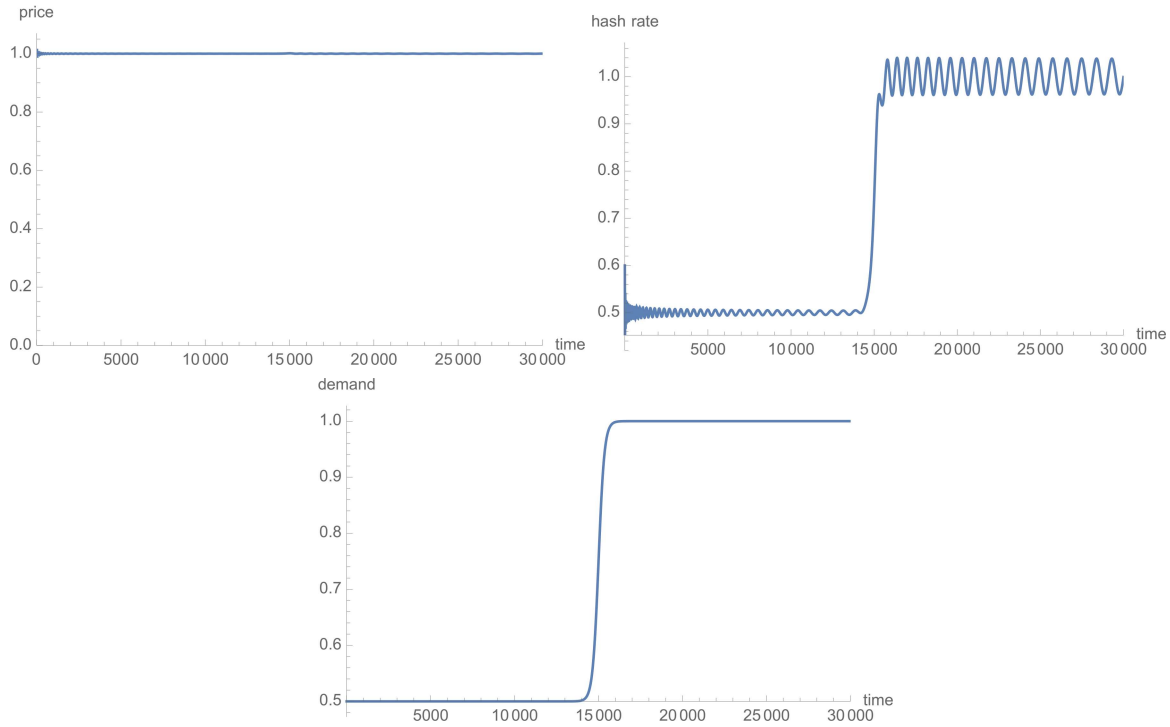


Figure 3: Numerical solution for s-curve 2x increase in demand at $t = 1500$ with the smoothness parameter $t_0 = 350$.

5.1 Arbitrary function of demand

With the proportional reward system, the supply adjusts to the demand. A simulation of demand doubling is presented on the figure 3. The hash rate changes to reflect the demand.

5.2 The choice of function considerations

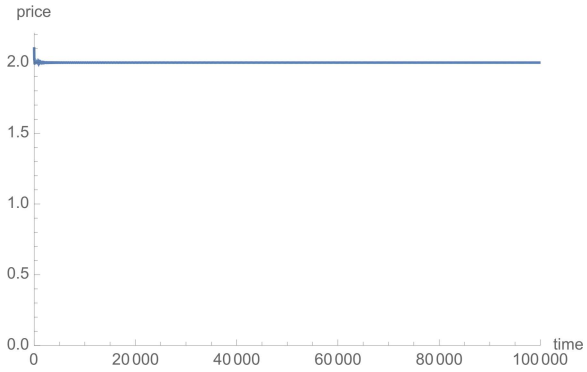
The simple identity used for the function of difficulty sheds some light on the problem of hashrate oscillations [5].

As mentioned in the remark 1, the average block solve time depends linearly on the difficulty. If a difficulty adjustment algorithm (DAA) is not responsive enough, the blocks come out at a different rate than the target for a while, proportionally to the DAA mistake. A sudden change in the hash rate might cause a series of very fast blocks or no blocks for a long time.

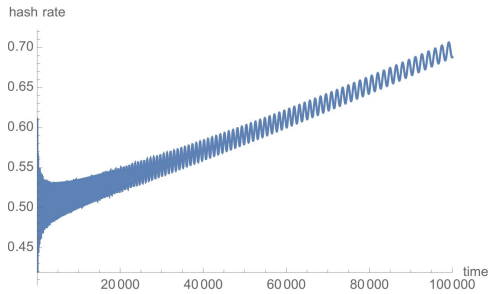
If, however, the reward is a linear function of the difficulty, the amount of coins minted over time does not change during the periods of adjustment, ultimately removing incentive behind DAA oscillations. For example, two times faster blocks will reward the miners with only half the reward as the normally spaced blocks after the difficulty is adjusted. The step of replacing $D(t)$ with $h(t)$ in the section 3.1 is justified and in the case of the linear reward it is an equivalence.

Nonlinear function

A a choice of the function f of the form x^a, with $0 < a < 1$, offers an interesting middle-ground between the proportional reward system and the constant reward, with Bitcoin being at the limit of $a \to 0$ and proportional reward at $a \to 1$. For an a very close to 1 the system has an equilibrium that moves with the changes in the demand and doesn't require the introduction of the market damping force.



(a) Numerical solution of system (7) for p.



(b) Numerical solution of 7 for h.

Figure 4: Numerical solution for $a = a_{estim.} = 1/300000$ and the rest of parameters are the same as before.

5.3 Mining efficiency

Mining equipment, namely ASICs, are getting better over time. There is a clear trend in hashes per Joul of new generations. At this point is impossible to tell whether the trend is exponential, going to infinity or, more likely, hyperbolic tangent, approaching some limit. At early stages those trends are indistinguishable. Even if the trend is in fact hyperbolic tangent, it's too early stage to predict with any satisfactory certainty what the actual limit is. To actually keep the value of the currency pegged to the real value of electricity, not falling against it over time, it's necessary to take the technological advances in account. Lets assume

$$\varepsilon(t) = \varepsilon_0 e^{-at},$$

which reflects exponential growth of efficiency of ASIC miners. In this case, to achieve stable price it's necessary to put

$$f(h) = e^{-a_{estim.}t} h(t).$$

The resulting price depends on the quality of $a_{estim.}$ parameter estimation. Overestimation results in inflationary currency and underestimation results in deflationary currency. The effects take place at large timescales. If the advancements of the technology is around doubling every 3 years and it was overestimated by 10%, the currency will experience doubling of the value in almost 30 years, which is around 2% deflation every year. While doing estimation the uncertainty can be assessed so the future price can be known up to some range, although planning for growth or fall might interfere with the damping force and make the hash rate unstable.

6 Related concepts

The article [4] describes the idea of using hash rate as an oracle for the price. The brief analysis does not reveal that hash rate is only directly related to the price in a constant reward system, as shown in the section 4.

The model investigated here shows that the variables are interlocking in a system of equations. With the proportional reward in place the hash rate is proportional to the demand, not the price. When the reward becomes dependent on the hash rate, difficulty stops being a price estimator. In the case from the simulation of demand doubling (fig. 3) the price estimator would mistakenly interpret the jump in demand as a jump in the price and keep increasing the supply until the currency collapse.

7 Conclusions

Proportional reward supply system may unlock possibility of creating a stable peer-to-peer electronic cash, reflecting average cost of electricity in the world. A bitcoin equipped with the proportional supply system won't be an investment, but will serve only its original, fundamental purpose of getting rid of trusted third party from electronic transactions. The theoretical model can be tested experimentally by creating a blockchain and cryptocurrency utilizing this system.

References

[1] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system,

[2] The World Bank data, https://data.worldbank.org/indicator/FM.LBL.BMNY.GD.ZS?view=chart

[3] Janez Trobevsek, Calem Smith, Federico De Gonzalez-Soler, DoI-SMS: A Diffusion of Innovations based Subsidy Minting Schedule for Proof-of-Work Cryptocurrencies, October 2018

[4] Vitalik Buterin, The Search for a Stable Cryptocurrency, November 11, 2014,

[5] Sam M. Werner, Dragos I. Ilie, Iain Stewart and William J. Knottenbel, Unstable Throughput: When the DifficultyAlgorithm Breaks, November 22, 2020