The economics of Bitcoin transaction fees

Nicolas Houy

GROUPE D'ANALYSE ET DE THÉORIE ÉCONOMIQUE LYON - ST ÉTIENNE

WP 1407

The economics of Bitcoin transaction fees

Nicolas Houy

February 2014

GATE Groupe d'Analyse et de Théorie Économique Lyon-St Étienne

93, chemin des Mouilles 69130 Ecully – France
Tel. +33 (0)4 72 86 60 60
Fax +33 (0)4 72 86 60 90

6, rue Basse des Rives 42023 Saint-Etienne cedex 02 – France
Tel. +33 (0)4 77 42 19 60
Fax. +33 (0)4 77 42 19 50

Messagerie électronique / Email : gate@gate.cnrs.fr
Téléchargement / Download : http://www.gate.cnrs.fr – Publications / Working Papers

The economics of Bitcoin transaction fees

v.0.1

Nicolas Houy*

February 24, 2014

Abstract

We study the economics of Bitcoin transaction fees in a simple static partial equilibrium model with the specificity that the system security is directly linked to the total computational power of miners. We show that any situation with a fixed fee is equivalent to another situation with a limited block size. In both cases, we give the optimal value of the transaction fee or of the block size. We also show that making the block size a non binding constraint and, in the same time, letting the fee be fixed as the outcome of a decentralized competitive market cannot guarantee the very existence of Bitcoin in the long-term.

JEL Classification: D23, E42.

Keywords: Bitcoin, transaction fee, mining, crypto-currency.

1 Introduction

Bitcoin[1] has been invented in 2008 ([Nakamoto, 2008]) but it really became popular and left the circle of strict early adopters in 2013[2]. It is usually described by laymen as an electronic or internet money even though this definition is much criticized by the computer science community that rather talks about a disruptive and revolutionary protocol. As a protocol, Bitcoin is still in its early stages of development and its specifications are still often modified. In order to reach the stage of implementation, a proposed modification goes through a whole process of validation. Some questions regarding some specifications are still more or less open and left undecided. Among those questions is the value and nature of the transaction fees in the Bitcoin network. In this paper, we intend to give an economist's point of view on this question.

*Université de Lyon, Lyon, F-69007, France; CNRS, GATE Lyon Saint-Etienne, Ecully, F-69130, France. E-mail: houy@gate.cnrs.fr.

[1]As the norm tends to be, we will write "Bitcoin" for the network or the protocol and "bitcoin" for each of the tokens that circulate on it.

[2]At the time this article is written, bitcoins can be bought and sold at about $630 apiece on some exchange markets. The monetary base is about $8,000,000,000.

In order to do that, we need to describe, even superficially, how Bitcoin actually works. When an individual sends some bitcoins to another individual, this information is broadcast to the peer-to-peer Bitcoin network. However, for technical purposes we won't address here, this transaction needs to be included, together with other transactions forming a *block*, in the *blockchain* in order to be confirmed and secured. The blockchain is a public ledger that contains the full history of all the transactions in bitcoins ever processed. It is the role of *miners* to do this work of confirming and securing transactions. Practically, this mining process consists in solving a mathematical problem and the first miner to do so can include a block of transactions in the blockchain. As it requires computational resources, the successful miner is rewarded in bitcoins for his useful work. This reward comes both from an *ex-nihilo* creation of some new bitcoins and from some fees that Bitcoin users can add to their transactions. In order to control the monetary base, mining is made more complex than it could be. And since the probability for each miner to solve the mining problem depends on his relative computational power, the complexity of mining is made dependent on the total computational power of all miners. Precisely, the complexity is dynamically adjusted so that a block solving and hence a creation of bitcoins occurs every ten minutes in expectation. Moreover, the amount of bitcoins newly created for each block solved is halved every 210,000 blocks (or about 4 years). Hence, the number of bitcoins ever created will asymptotically reach 21 millions[3]. The first amount created was 50 bitcoins, on January 3rd, 2009. This whole process is described as brilliant by some but it has been criticized for the inefficiency due to the loss of resources it induces (see [Krugman, 2013] for instance). Indeed, Bitcoin miners have engaged in an arm race to computational power and in the end, much hardware, engineering and energy are used to solve mathematical problems that are artificially made extremely complex. What is often forgotten or not known by people criticizing this aspect of Bitcoin is that Bitcoin security is directly depending on the total computational power of the miners. Then, the "lost" computational resource is the only determinant of Bitcoin security.

From the point of view of the existence of Bitcoin, if we need much and powerful mining for security reasons and miners have the incentive to mine through some rewards, all the better. In current days, this incentive is almost only due to new bitcoins creation[4]. As we said above, this process of bitcoin creation will slowly become insignificant. *Ceteris paribus*, when there is no new bitcoins created, the incentive to mine will decrease dramatically and the security of Bitcoin will not be achieved any longer. In fact, mining has strong positive externalities. It allows the very existence of Bitcoin. And transaction fees are, in the long-term, the only way Bitcoin users can make sure miners keep mining. Hence, the problem of how to deal with the transaction fees in the Bitcoin protocol becomes extremely important and is certainly one of the most determinant when looking at Bitcoin's future.

In this article, we study the economics of Bitcoin's transaction fees in a very simple partial equilibrium setting. We show that a fixed and imposed transaction fee can keep

[3]At the time this article is written, there are about 12,500,000 bitcoins in circulation.

[4]At the time this article is written, the transaction fees represent about 0.4% of the miners' rewards. The remainder is due to bitcoins creation.

Bitcoin secure enough if the transaction fee is high enough. We also show that any situation with a fixed transaction fee can be obtained equivalently by setting a maximum block size instead. However, if we let the transaction fee be the result of a decentralized market and have no constraint on the maximum block size, the transaction fee will eventually go to 0 and miners will not have the necessary incentives to keep mining, hence to keep Bitcoin alive.

As main recommendations, we support the view that the Bitcoin protocol should integrate a block size constraint effectively binding or equivalently a corresponding built-in transaction fee. Put the other way around, we warn for the risk of considering that the block size should be adapted so that Bitcoin can scale up for accepting all transactions and, in the same time, trust a decentralized and free market for space inside blocks that would set the transaction fee. Bitcoin mining is an activity with a strong positive externality (securing the network for other users) and economists know that, in this case, free markets are not efficient. Imposing a transaction fee implies tax revenues for miners and imposing a maximum block size creates a monopoly rent for miners. In both cases, it boils down to correcting a market inefficiency by introducing another one.

2 Model

The model we use is the simplest static model we can imagine of a partial equilibrium setting. It should be understood as modeling the situation that occurs between two inclusions of two following blocks of transactions in the blockchain. We consider an economy with two goods, a physical one and bitcoin to be used as means of exchange.

2.1 Without frictions due to the payment system

First, let us assume as is usually done in partial equilibrium that there is no friction due to the payment system. This case does not represent the situation with cash, debit/credit cards or checks since it assumes that there is no opportunity cost due to unearned interests, time wasting entering PIN codes or writing checks or even printing bills or minting coins ([Baumol, 1952, Tobin, 1956, Baumol and Tobin, 1989, Bounie and François, 2008]). It is rather written as a benchmark case.

The demand for physical good as a function of price is $Q^d(p) = d_0 - \alpha p$. The physical good is produced with a cost function depending on the quantity produced $C(q) = q^2/(2\beta)$ so that supply as a function of price is given by $Q^s(p) = \beta p$. Obviously, in a frictionless economy, the equilibrium price is

$$p^* = \frac{d_0}{\alpha + \beta},$$

the quantity exchanged at equilibrium is

$$q^* = \frac{\beta}{\alpha + \beta} d_0$$

and the profit of the supplier is

$$\Pi^* = \frac{\beta}{2(\alpha+\beta)^2} d_0^2.$$

We make the additional assumption that consumers have utility quasi-linear in bitcoin so that the consumer surplus is

$$CS^* = \frac{\beta^2}{2\alpha(\alpha+\beta)^2} d_0^2,$$

and the total surplus is

$$TS^* = \Pi^* + CS^* = \frac{\beta}{2\alpha(\alpha+\beta)} d_0^2.$$

Those results are standard. We will not interpret or comment them.

2.2 With a fixed transaction fee

Now, we consider that for each transaction, a fee c is required and is included in its payment by the buyer and is earned by a miner. In this case, the demand function becomes $Q^d(p,c) = d_0 - \alpha.(p+c)$. We will make the following assumption: $0 \leq c \leq d_0/\alpha$. Otherwise, the fee is so large that there is no physical good exchanged.

In this case, the equilibrium price is

$$p^f(c) = \frac{d_0 - \alpha c}{\alpha + \beta},$$

the quantity exchanged at equilibrium is

$$q^f(c) = \frac{\beta}{\alpha+\beta}(d_0 - \alpha c),$$

the profit of the supplier is

$$\Pi^f(c) = \frac{\beta}{2(\alpha+\beta)^2}(d_0 - \alpha c)^2,$$

the consumer surplus is

$$CS^f(c) = \frac{\beta^2}{2\alpha(\alpha+\beta)^2}(d_0 - \alpha c)^2,$$

and the total transaction fees transferred to the miner is

$$M^f(c) = \frac{\beta c}{(\alpha+\beta)}(d_0 - \alpha c).$$

Now, let us see what happens on the market for mining equipment. Any individual can buy some hashing power at a constant unit price k. If an individual has a hashing power h and the total network hashing power is H, he will earn, with a probability h/H,

a reward R plus the transaction fees given above. Considering risk-neutral miners, each of them makes his decision regarding his hashing power demand as a solution to

$$\max_h \frac{h}{H}(M^f(c)+R)-kh.$$

There is only one possible equilibrium with

$$H=\frac{M^f(c)+R}{k}.$$

Moreover, the profit of the miners is null.

Hence, the total surplus in this economy with a fixed transaction fee c is

$$TS^f(c)=\Pi^f(c)+CS^f(c)=\frac{\beta(d_0-\alpha c)^2}{2\alpha(\alpha+\beta)}.$$

Bitcoin, as a payment network, requires a sufficiently high degree of security. The level of security is directly linked to the hashing power of the network ([Eyal and Sirer, 2013, Kroll *et al.*, 2013, Houy, 2014]). Hence, we require for the exchanges to be possible that $H \geq \underline{H} > 0$. In this case, for Bitcoin to be sustainable, we need:

$$\frac{M^f(c)+R}{k} \geq \underline{H}.$$

Then, for normative reasons, the choice of c should be made as a solution to

$$\begin{array}{rl} \max_c & TS^f(c) \\ \text{st:} & \frac{M^f(c)+R}{k} \geq \underline{H} \\ & c \geq 0 \end{array}$$

If $k\underline{H}-R \leq 0$, obviously, we should have $\underline{c}=0$. Indeed, in this case, the reward is enough to give incentives for the miners to mine. Then, the distortive transaction fee can be set to 0. Otherwise, there exist no solution to this maximization problem if

$$k\underline{H}-R > \left(\frac{d_0}{2}\right)^2 \frac{\beta}{\alpha(\alpha+\beta)}.$$

Finally, when there is a non null solution, it is given by

$$\overline{c}=\frac{d_0-\sqrt{d_0^2-4(k\underline{H}-R)\frac{\alpha(\alpha+\beta)}{\beta}}}{2\alpha}. \quad (1)$$

A transaction fee higher than $\overline{c}$ implies a higher loss of efficiency that is not justified by an insufficient security level. A lower transaction fee implies that the minimal requirement in terms of security is not met, the miners having insufficient incentives.

Notice that this result suggests that the transaction cost should be depending on the reward R. When R is large enough, transaction fees can be insignificant. The optimal transaction is also increasing in the minimum level of security required. Indeed, the higher the level of security to be reached ($\underline{H}$), the higher the incentive to mine should be.

2.3 With a maximum block size

Assume now that there is no fixed transaction fee but instead the number of transactions that can be included in a block is limited.[5] Each individual can add to its transaction a fee for the miner. The amount of this fee can have any value. Then, this fee is fixed as a price on a market for space in blocks. Then, we need to consider the demand and supply for this space market. Supply is the inelastic fixed maximum number of transactions that can be included in a block and is denoted B. For this block size constraint to be weakly binding, we will assume that $0 \leq B \leq q^* = \frac{\beta}{\alpha+\beta} d_0$.

For a price p_m for block space and a price of the physical good p, the demand for block space is given by the number of individuals who are willing to pay more than $p + p_m$ for the good, *i.e.*

$$\mathcal{Q}^d(p, p_m) = d_0 - \alpha(p + p_m).$$

Equilibrium on the market for block space is reached when $\mathcal{Q}^d(p, p_m) = B$, hence, for space price

$$p_m = \frac{d_0 - B}{\alpha} - p.$$

Then, when we combine both the market for block space and for physical good, we get a physical good equilibrium price

$$p^b(B) = \frac{B}{\beta},$$

and a physical good quantity exchanged at equilibrium

$$q^b(B) = B,$$

the profit of the supplier is

$$\Pi^b(B) = \frac{B^2}{2\beta},$$

the consumer surplus is

$$CS^b(B) = \frac{B^2}{2\alpha},$$

and the total transaction fees transferred to the miner is

$$M^b(B) = \frac{B}{\alpha}\left(d_0 - B\frac{\alpha+\beta}{\beta}\right).$$

Notice that we have full equivalence between a fixed transaction fee c and a maximum block size $B(c)$ whenever

$$B(c) = \frac{\beta}{\alpha+\beta}(d_0 - \alpha c).$$

[5] In reality, the maximum size of a block is given in bytes. Transactions can have different sizes in bytes. The size of a transaction depends on many parameters (number of inputs and outputs mainly) but not directly on the amount paid in the transaction. We will make the simplifying assumption that each transaction has size 1.

Indeed, it is straightforward to check that

$$\begin{aligned} p^f(c) &= p^b(B(c)), \\ q^f(c) &= q^b(B(c)), \\ CS^f(c) &= CS^b(B(c)), \\ \Pi^f(c) &= \Pi^b(B(c)), \\ M^f(c) &= M^b(B(c)). \end{aligned}$$

Hence, having a fixed transaction fee in the Bitcoin protocol and having a binding fixed maximum block size are equivalent. In the first case, the fee should be imposed in the Bitcoin protocol. In the second case, the fee will be set as an equilibrium price on a market for block space. Then, it is the maximum block size that is imposed by the protocol. And by making the maximum block size smaller than it could be, the artificially imposed scarcity of the total block space creates the reward for the miner.

Notice that if $B = \frac{\beta}{\alpha+\beta} d_0$, *i.e.* the maximum block size is not constraining, we have $p_m = 0$ which leads to a situation equivalent to a case with a fixed transaction fee $c = 0$. Then, the revenue of the miners is only the creation of new bitcoins. The security of the system is guaranteed only as long as $R/k > \underline{H}$ which cannot hold in the long-term, when R tends to 0, whenever $\underline{H} > 0$. Then, making sure that the maximum block size is large enough to handle all transactions and in the same time, letting the transaction fee floating, will lead to a situation where transaction fees will go to 0 and hence, the security of Bitcoin cannot be guaranteed.

Now, the optimal block size is given as $\overline{B} = B(\overline{c})$ where $\overline{c}$ is given by Equation 1:

$$\overline{B} = \frac{\beta}{\alpha+\beta} \left(\frac{d_0 + \sqrt{d_0^2 - 4(k\underline{H} - R)\frac{\alpha(\alpha+\beta)}{\beta}}}{2} \right).$$

2.4 The cost of Bitcoin

Let us finish by an estimation of the cost of Bitcoin as a payment system. We only consider the sum of private costs here. In particular, externalities due to the environmental damage caused by mining activities are not estimated. Assume that Bitcoin is run at its maximum efficiency point, *i.e.* with transaction fee, $\overline{c}$, given in Equation 1. Then, the total surplus cost of Bitcoin is

$$TS^* - TS^f(\overline{c}) = \frac{\beta}{2(\alpha+\beta)} \overline{c}(2d_0 - \alpha\overline{c}).$$

This evaluation is to be compared with the estimations of costs for other payment systems ([Schmiedel *et al.*, 2012, Hayashi and Keeton, 2012]) and is left for future studies.

3 Conclusion

In this article, we have led a simple study on the economics of Bitcoin transaction fees. In order to do that, we have used a very simple partial equilibrium setting with a market for a physical good with bitcoins used as means of exchange. As a specificity of our study, we introduced the market for mining equipment in order to check for the security of the system. Indeed, the security of Bitcoin depends on the computational power of miners. Finally, when we studied the possibility to have a limit on the block size, we introduced the market for block space.

As a result, we showed that having a mandatory transaction fee or limiting the block size and letting the price for block space be determined on a decentralized market are equivalent. However, letting the transaction fee be the outcome of a market *and* make the block size irrelevant or not binding would lead to a too low level of security for Bitcoin. The reason why the market is not an answer in this case is that mining has a private value different from its social one. Privately, it represents rewards for the miners. Socially, it allows the system to be secure. This is a perfect case of externality that implies the inefficiency of a free market. The transaction fee is a way to bring closer the private and social benefits of mining. So is the limited size of blocks that allows the miner to sell a scarce resource.

In the latter case a question arises: why don't miners limit the size of what they include in the blocks themselves? The reason is the following. When a miner tries to solve a block, the transactions are already in the network. In this case, he is a Stackelberg follower and he has an incentive to include all transactions in the limitless block he tries to solve. He could announce before solving a block that if he indeed solves a block, he will not include all transactions. But this announcement would not be credible. Indeed, since miners are in competition with distributed hashing power, the transactions a miner would not include would certainly be included just ten minutes later by another miner. Including all transactions whatever the fee attached is the only subgame perfect Nash equilibrium of the game we described.

Let us finish our study by mentioning its weaknesses. First, with a static setting we could not consider the dynamic aspects of mining. In addition to what we said above about the competition between miners, it is obvious that mining power purchase decisions are ones that are tightly linked with dynamic aspects. Indeed, buying hashing power is mainly buying a very expensive ASIC machine to be used at almost no marginal cost for a long time with total hashing power highly variable. Second, we did not consider the price volatility of Bitcoin that is huge. Third and related, we did not consider the inflation that should be linked with new bitcoins creation as rewards. Since we did not, it would be optimal in our setting to always have R sufficiently high in order to have a level of security high enough. However, this would create inflation and should have social costs that we cannot capture in our model. Fourth, we did not consider variable or unknown levels of demands and supply for the physical good. This could be problematic especially if we had to set a maximum block size. Finally, our model cannot capture ideas almost philosophical but that are very important for the community of people currently using

Bitcoin like "Bitcoin neutrality": our study is limited to the economic aspects of Bitcoin transaction fees.

References

[Baumol, 1952] Baumol W.J. (1952) "The transactions demand for cash: an inventory theoretic approach", Quarterly Journal of Economics, 66: 545-556.

[Baumol and Tobin, 1989] Baumol W.J. and Tobin J. (1989) "The optimal cash balance proposition: Maurice Allais' priority", Journal of Economic Literature, 27(3): 116-1162.

[Bounie and François, 2008] Bounie D. and François A. (2008) "The economics of bill payments: an empirical analysis", Applied Economics Letters, 18(10): 961-966.

[Eyal and Sirer, 2013] Eyal I. and Sirer E.G. (2013) "Majority is not enough: Bitcoin mining is vulnerable", arXiv: 1311.0243.

[Hayashi and Keeton, 2012] Hayashi F. and Keeton W.R. (2012) "Measuring the costs of retail payment methods", Federal Reserve Bank of Kansas City Economic Review, 2012 QII: 37-77.

[Houy, 2014] Houy N. (2014) "It will cost you nothing to 'kill' a proof-of-stake crypto-currency", Working paper GATE 2014-04.

[Kroll *et al.*, 2013] Kroll J.A., Davey I.C. and Felten E.W. (2013) "The economics of Bitcoin mining, or Bitcoin in the presence of adversaries", *Mimeo.*

[Krugman, 2013] Krugman P. (2013) "Adam Smith hates Bitcoin". NYTimes blog. http://krugman.blogs.nytimes.com/2013/04/12/adam-smith-hates-bitcoin/

[Nakamoto, 2008] Nakamoto S. (2009) "Bitcoin: A peer-to-peer electronic cash system".

[Schmiedel *et al.*, 2012] Schmiedel H., Kostova G. and Ruttenberg W. (2012) "The social and private costs of retail payment instruments", ECB Occasional Paper 137.

[Tobin, 1956] Tobin J. (1956) "The interest elasticity of the transactions demand for cash", Review of Economics and Statistics, 38(3): 241-247.