BLOCK SIZE LIMIT DEBATE WORKING PAPER

A Transaction Fee Market Exists Without a Block Size Limit

Peter R[†]

August 4, 2015

Abstract. This paper shows how a rational Bitcoin miner should select transactions from his node's mempool, when creating a new block, in order to maximize his profit in the absence of a block size limit. To show this, the paper introduces the *block space supply curve* and the *mempool demand curve*. The former describes the cost for a miner to supply block space by accounting for orphaning risk. The latter represents the fees offered by the transactions in mempool, and is expressed versus the minimum block size required to claim a given portion of the fees. The paper explains how the supply and demand curves from classical economics are related to the derivatives of these two curves, and proves that producing the quantity of block space indicated by their intersection point maximizes the miner's profit. The paper then shows that an unhealthy fee market—where miners are incentivized to produce arbitrarily large blocks—cannot exist since it requires communicating information at an arbitrarily fast rate. The paper concludes by considering the conditions under which a rational miner would produce big, small or empty blocks, and by estimating the cost of a spam attack.

KEY WORDS

1. Bitcoin. 2. Block size limit. 3. Transaction fee market. 4. Blockchain spam.

1. Introduction

A pressing concern exists over the ramifications of changing (or not) a Bitcoin protocol rule called the *block size limit*. This rule sets an upper bound on the network's transactional capacity, or—more simply—the number of transactions the network can confirm per second. Its origins date back to the late summer of 2010, when Satoshi Nakamoto—worried about a spam attack on the fledgling Bitcoin network—modified the source code[1] to set a maximum permissible size for new blocks appended to the Blockchain. The limit was set at one megabyte, corresponding roughly to three transactions per second. Although this was only a sliver of Visa's transactional capacity,[2] it was over eight hundred times greater than what was required at the time.[3] Nakamoto said that the limit could be raised in the future when the need arrived.[4]

Between July 8 and July 15, 2015, a backlog cresting at over sixty thousand pending transactions formed.[5] Blocks were filled near capacity[6] and users experienced delays.[7] At the time of writing, the transaction rate is over three hundred times larger than when the block size limit was introduced,[8] and raising the limit is now being seriously considered. However, concerns regarding whether the network can support larger block sizes have been voiced. One of the concerns in particular is whether—in the absence of a limit or if the limit is far above the transactional demand—a healthy transaction fee market would develop which charges

[†] Peter R is from Vancouver, Canada and may be reached by email at peter_r@gmx.com or by personal message at bitcointalk.org.

The original PDF version of this document has been time-stamped in the Blockchain.
1BWZe6XkGLcf6DWC3TFXiEtZmcyAoNq5BW

users the full cost to post transactions (the term *healthy transaction fee market* is defined in Section 7). The fear—if this is not the case—is that the resulting subsidy to users would incentivize spamming and precipitate a "tragedy-of-the-commons"-type failure where network support costs spiral out of control. The object of this paper is to consider whether or not such a fee market is likely to emerge if miners, rather than the protocol, limit the block size.

Related efforts have been made. Houy showed that if the marginal cost to a miner to add a transaction to a block was zero, then a miner would "[include] all transactions whatever the fee attached." He concluded that either a minimum fee or a limited block size was required.[9] Andresen explained, however, that due to the increased chances of orphaning a block, the marginal cost was *not* zero; a rational miner should only include a given transaction if its fee is sufficient to cover the added risk of orphaning.[10] Extending on the work of Houy, we account for Andresen's orphaning factor and show that a rational miner will *not* in general include all fee-paying transactions, and that a healthy fee market is, in fact, the expected outcome of rational miner behavior, if block size is unconstrained by the protocol (and notwithstanding the assumptions stated explicitly in Section 10).

In Section 3, we derive the *miner's profit equation*—a simple analytical model for the expectation value of a miner's profit per block that accounts for orphaning risk. We then introduce two novel concepts called the *mempool demand curve* and the *block space supply curve*, in Sections 4 and 5, respectively. We illustrate how the demand curve can be constructed from the transactions in a node's mempool, while we derive the supply curve by differentiating the miner's profit equation with respect to block size, setting the result equal to zero, and then solving the ensuing differential equation. We find that the cost to supply block space *increases exponentially* with the size of the block. We explain that the supply curve is useful because it specifies the miner's cost of producing a given quantity of block space; and we suggest that the demand curve is useful because it represents the maximum fees that a miner can claim versus the block size he might consider producing.

In Section 6, we use the two curves to visualize the size of the block that maximizes the miner's profit. We also explain how the two curves relate to the more familiar supply and demand curves from economics. In Section 7, we show that an unhealthy fee market—one where a miner would be incentivized to produce an arbitrarily large block—is not possible because it requires communicating information over a channel at an arbitrarily high bit rate, thereby violating the Shannon-Hartley theorem.[11] This result applies whether block solutions are communicated in full, or first compressed (*e.g.*, using invertible bloom look-up tables). In Section 8, we consider the transaction fee market in more detail; and lastly, in Section 9, we estimate the cost of a spam attack. Let us begin by defining the symbols we use.

2. List of Symbols

For the remainder of this manuscript, the following symbols have the specified meanings.

B	bandwidth of a communication channel	$\mathbb{P}_{\text{orphan}}$	probability that a given block is orphaned
$\mathcal{B}$	the set of transactions included in a block	Q	block size or block space in bytes
b	number of transaction included in a block	Q^*	the block size that maximizes the miner's expected profit
$\langle C \rangle$	expectation value of a miner's hashing cost per block	R	block reward (presently 25 Ƀ)

C	channel capacity (bits per second)	$\frac{S}{N}$	signal-to-noise ratio of a communication channel
c	speed of light	T	expected block interval time (~10 min)
d	distance over which the block solution is communicated	$\langle V \rangle$	expectation value of a miner's revenue per block
H	total hash rate of Bitcoin network	γ	block solution coding gain
h	miner's individual hash rate	η	amortized cost per hash
i	index used to innumerate the transactions in mempool	$\langle \Pi \rangle$	expectation value of a miner's profit per block
M	money (bitcoins)	ρ	fee density, or the price per byte for block space
M_{demand}	partial sum of the transaction fees in mempool in order of descending fee density	ρ_{demand}	fee density bid by a given transaction in mempool
M_{supply}	miner's cost due to orphaning to produce a certain block size	ρ_{supply}	miner's cost per byte to produce additional block space
$\mathcal{N}$	the set of transactions in a miner's mempool	τ	block solution propagation time
n	number of transactions in a miner's mempool	$\Delta\tau$	block solution propagation time minus the time to communicate the block header

The symbol $ refers to *US dollars*; price conversions between bitcoin and US dollars assume that 1 Ƀ = $300.

3. The Miner's Profit Equation and the Effect of Orphaning

By attempting to mine a block, the miner expects to generate revenue $\langle V \rangle$ at hashing cost $\langle C \rangle$ to earn a profit per block

$$\langle \Pi \rangle = \langle V \rangle - \langle C \rangle. \quad (1)$$

The miner's expected hashing cost is equal to the product of his hardware's amortized price per hash,[12] η, his hash rate, h, and the length of time he expects to work on the block (typically the block time T). This can be expressed as the following equation:

$$\langle C \rangle = \eta h T. \quad (2)$$

The miner's expected revenue is equal to the amount he would earn if he won the block multiplied by his probability of winning. The amount he would earn is the sum of the block reward, R, and the transaction fees, M. His probability of winning, assuming all blocks propagate instantly, is equal to the ratio of his hash rate (h) to the total hash rate of the Bitcoin network (H). Putting this together, his expected revenue would be $\langle V \rangle = (R + M)\, h/H$.

The problem with this equation is that it does not reflect the miner's diminished chances of winning if he chooses to publish a block that propagates slowly to the other miners. Even though he may find the first valid block, if his solution is received after most miners are working on another, then his block will likely be discarded. This effect is called *orphaning*.

It makes including low-fee transactions unappealing if the added fee revenue is not sufficient to offset the increased risk. With this effect in mind, our equation for the miner's expected revenue gets discounted by the chances that his block is orphaned, $\mathbb{P}_{\text{orphan}}$, becoming

$$\langle V \rangle = (R + M)\frac{h}{H}\left(1 - \mathbb{P}_{\text{orphan}}\right). \tag{3}$$

It is intuitive that the chance of orphaning should be low if the propagation time is short, and should be high if the propagation time is long. Using the fact that block times follow a Poisson distribution, Andresen approximated[10] the orphaning probability as

$$\mathbb{P}_{\text{orphan}} = 1 - e^{-\frac{\tau}{T}}, \tag{4}$$

where τ is the block propagation time. Fig. 1 visualizes this effect. It must be emphasized that τ is the total time between when a miner has found a solution and when that solution has been communicated and accepted by his peers.[13]

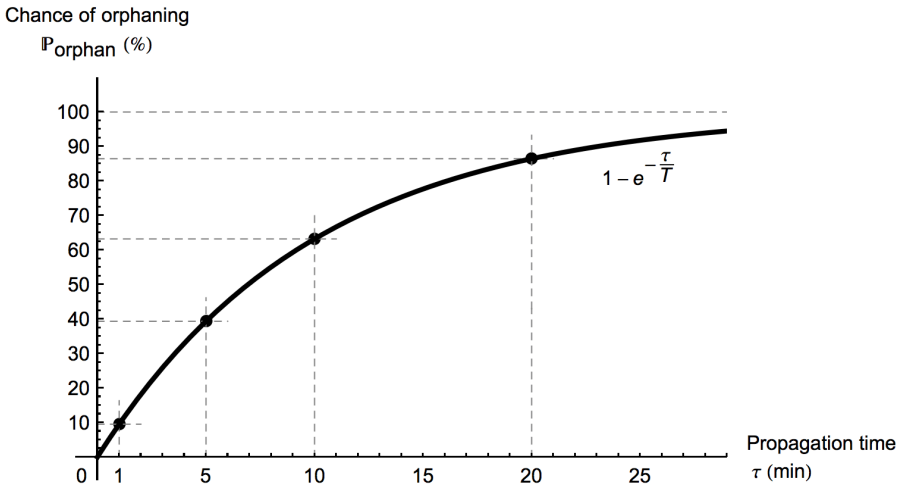

Fig. 1. The chance that a block gets orphaned increases with the amount of time it takes the block to propagate to the other miners.

By substituting Eqs. (2 - 4) into Eq. (1), we can now write the *miner's profit equation*:

$$\langle \Pi \rangle = (R + M)\frac{h}{H}e^{-\frac{\tau}{T}} - \eta h T. \tag{5}$$

A *rational miner* selects which transactions to include in his block in a manner that maximizes the expectation value of his profit. To better understand how he would make this selection, we will next introduce the concepts of the *mempool demand curve* and the *block space supply curve.*

4. The Mempool Demand Curve

Mempool is the name given to the set of valid transactions that the miner is aware of but that have not yet been included in a block. We denote this set as $\mathcal{N}$ and the number of transactions contained within it as n. In the absence of a block size limit, the miner is free to select $b \leq n$ transactions from $\mathcal{N}$ to create a new block $\mathcal{B} \subset \mathcal{N}$.

To construct the mempool demand curve, we first imagine sorting the mempool from greatest *fee density* (*i.e.*, the fee per size of the transaction in bytes) to least, and then associating an index $\{i : 1, 2, \ldots, n-1, n\}$ with each transaction in the resulting list. As illustrated in Fig. 2, each transaction can be thought of as a triangle whose height represents its fee, whose width represents its size in bytes, and whose slope represents its fee density.

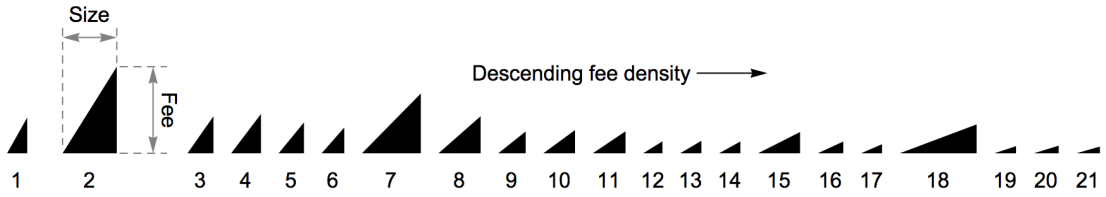

Fig. 2. A transaction can be visualized as a right triangle: its height represents its fee, its width represents its size in bytes, and its slope represents its fee density. To construct the mempool demand curve, we first sort the transactions in mempool in order of descending fee density.

Define $M_{\text{demand}}(b)$ as the sum of the fees offered by each transaction in this sorted list: $M_{\text{demand}}(b) \equiv \sum_{i=1}^{b} \text{fee}_i$; and define $Q(b)$ as the sum of each transaction's size in bytes: $Q(b) \equiv \sum_{i=1}^{b} \text{size}_i$. The mempool demand curve is then described parametrically as the sequence of points in the MQ-plane, $[Q(b),\ M_{\text{demand}}(b)]$, as b is incremented from 1 to n. It can be visualized by stacking the triangles from Fig. 2 corner-to-corner as shown in Fig. 3. A point on the curve represents the *maximum* fees a miner can claim by producing a given quantity of block space. This mempool demand curve helps us reduce a multi-dimensional selection problem into a one-dimensional one.

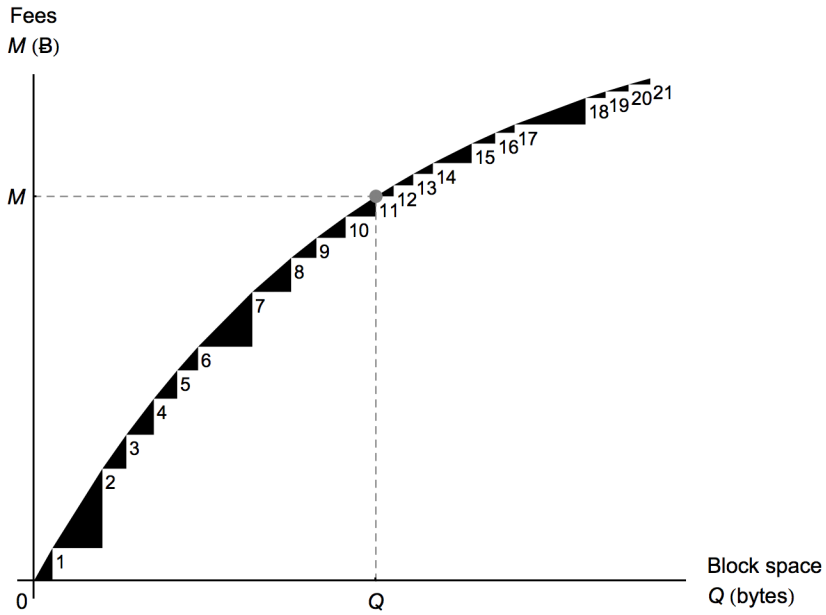

Fig. 3. The mempool demand curve describes the *maximum* fees a miner can claim from his mempool, M, as a function of the quantity of block space, Q, he might produce. To construct this curve, the triangles representing the sorted transactions in mempool are stacked vertex-to-vertex as shown.

5. The Block Space Supply Curve

The size of the block a miner elects to produce controls the fees he attempts to claim, $M(Q)$, and the propagation time he chooses to risk, $\tau(Q)$. Both these variables affect the expectation value of his profit.

To investigate this in more detail, we define the *neutral profit* as the profit (or loss) the miner would earn by publishing an empty block. We can construct a fee curve, $M_{\text{supply}}(Q)$, in the MQ-plane where all points on the curve return the neutral profit by requiring that the miner's profit (*cf.* Eq. 5) remain constant for any block size:

$$\frac{d}{dQ}\langle \Pi \rangle = \frac{d}{dQ}\left\{\left[R + M_{\text{supply}}(Q)\right]\frac{h}{H}e^{-\frac{\tau(Q)}{T}} - \eta h T\right\} = 0. \tag{6}$$

Eq. (6) is an ordinary differential equation that we show in the Appendix has solution

$$M_{\text{supply}}(Q) = R\left(e^{\frac{\Delta\tau(Q)}{T}} - 1\right), \tag{7}$$

where $\Delta\tau(Q) \equiv \tau(Q) - \tau(0)$. We call this the *block space supply curve*. It represents the fees a miner requires to cover the additional cost of supplying block space Q (Fig. 4); these costs grow *exponentially* with the propagation time. If a block can be constructed with MQ-coordinates above the curve, the miner has a *surplus*; if not, he has a *deficit* and would be better off mining an empty block. We next consider how he can use this curve, along with the mempool demand curve, to maximize his profit.

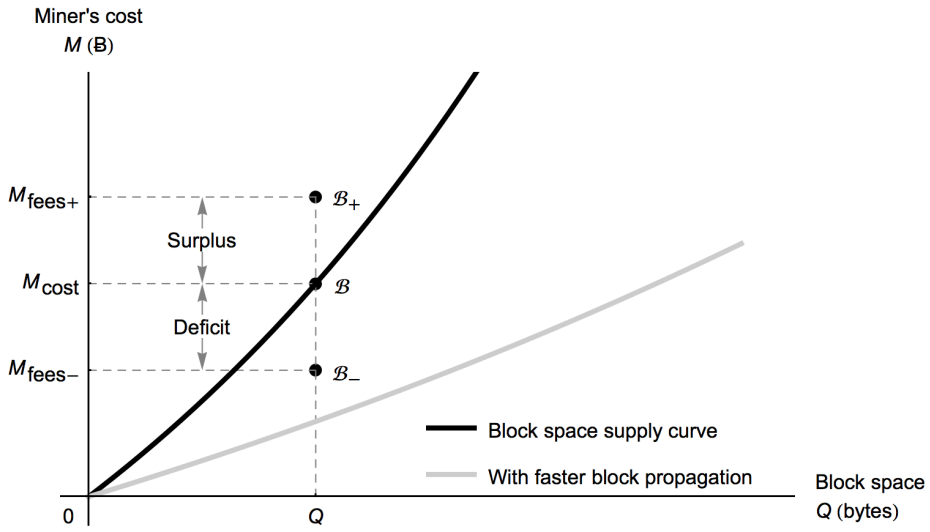

Fig. 4. The block space supply curve describes the cost for a miner to produce a block of a certain size. Consider the three blocks of size Q shown: $\mathcal{B}_+$, $\mathcal{B}$ and $\mathcal{B}_-$. Since $\mathcal{B}_+$ lies *above* the curve, the miner would expect a surplus equal to $M_{\text{fees+}} - M_{\text{cost}}$ by mining it. The block $\mathcal{B}$ lies *on* the curve, and hence the miner would be indifferent to mining that block over an empty block. The block $\mathcal{B}_-$, on the other hand, lies below the curve and the miner would expect to incur a deficit if he mined it (and thus would prefer to mine an empty block). Note that the block $\mathcal{B}_-$ would result in a surplus with faster block propagation.

6. Maximizing the Miner's Profit

To maximize his profit, the miner constructs a mempool demand curve from the real transactions pending in his mempool, and constructs a block space supply curve from empirical data he has on propagation delay versus block size (to estimate τ). The block size Q^* where the miner's surplus, $M_{\text{demand}} - M_{\text{supply}}$, is largest represents the point of maximum profit (Fig. 5a). This is the size of the block a rational miner should create.

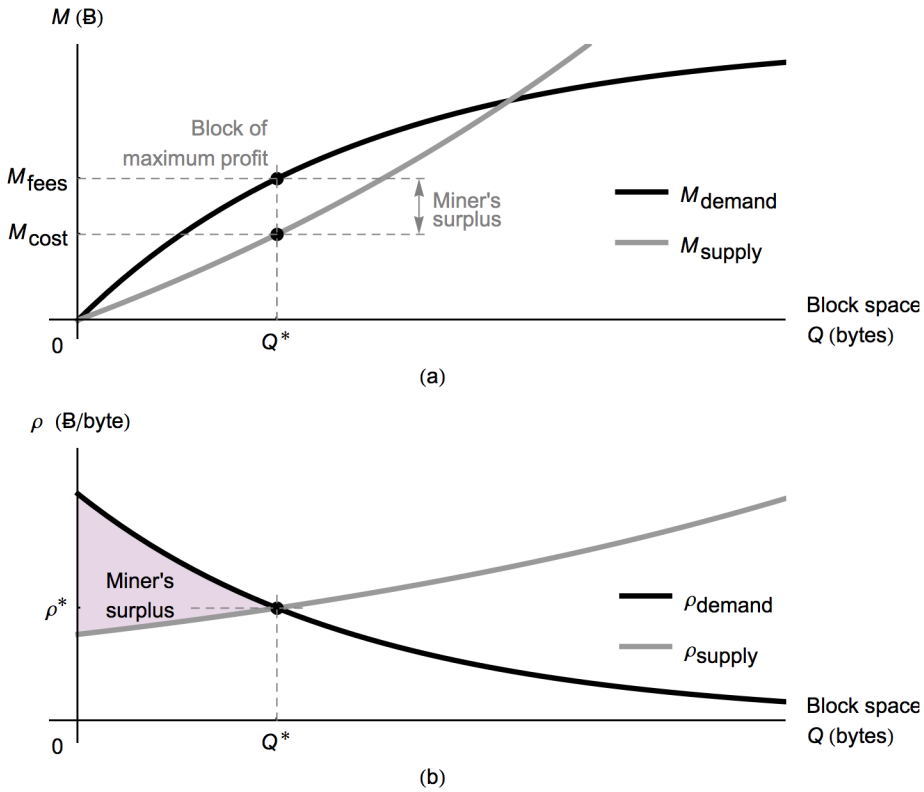

Fig. 5. The miner's surplus is greatest when the gap between M_{demand} and M_{supply} is a maximum. This occurs when the derivatives of the curves intersect at Q^*; or, in other words, when supply meets demand. Producing a smaller block than Q^* leaves profitable fee-paying transactions behind, while producing a larger block results in too high an orphan rate.

We can draw a parallel to the traditional economic supply and demand curves[14] with only a bit more work. The traditional supply curve represents the *unit price* of a commodity at a given level of production Q. However, so far our analysis has considered the price *per complete block*. The price *per byte*, ρ,[15] for the miner to produce a given quantity of block space follows by differentiating M_{supply} with respect to Q:

$$\rho_{\text{supply}}(Q) \equiv \frac{d}{dQ} M_{\text{supply}} = \frac{R}{T} \frac{d\tau}{dQ} e^{\frac{\tau(Q)}{T}}. \tag{8}$$

We can construct something similar to the traditional demand curve by differentiating M_{demand} with respect to Q:

$$\rho_{\text{demand}}(Q) \equiv \frac{d}{dQ} M_{\text{demand}}.$$

As illustrated in Fig. 5 (b), the block size Q^* where the miner's profit is greatest occurs when

$$\rho_{\text{supply}}(Q^*) = \rho_{\text{demand}}(Q^*).$$

We can think of ρ_{supply} and ρ_{demand} as the *differentiated curves* and M_{supply} and M_{demand} as the *integrated curves*. Both are useful. Armed with these results, let us now consider the conditions under which a healthy fee market should emerge.

7. Conditions for a Healthy Fee Market

We consider three market conditions for Bitcoin transaction fees: *healthy*, *unhealthy* and *non-existent*. In a healthy fee market, the miner's surplus is maximized at a finite quantity of block space, and thus the miner is incentivized to produce a finite block (Fig. 6a). In an unhealthy market, the miner's surplus continually increases with block space, and therefore a rational miner should produce an arbitrarily large block (Fig. 6b). In a non-existent market, including *any* transactions results in a deficit to the miner, and so the miner is better off producing an empty block (Fig. 6c).

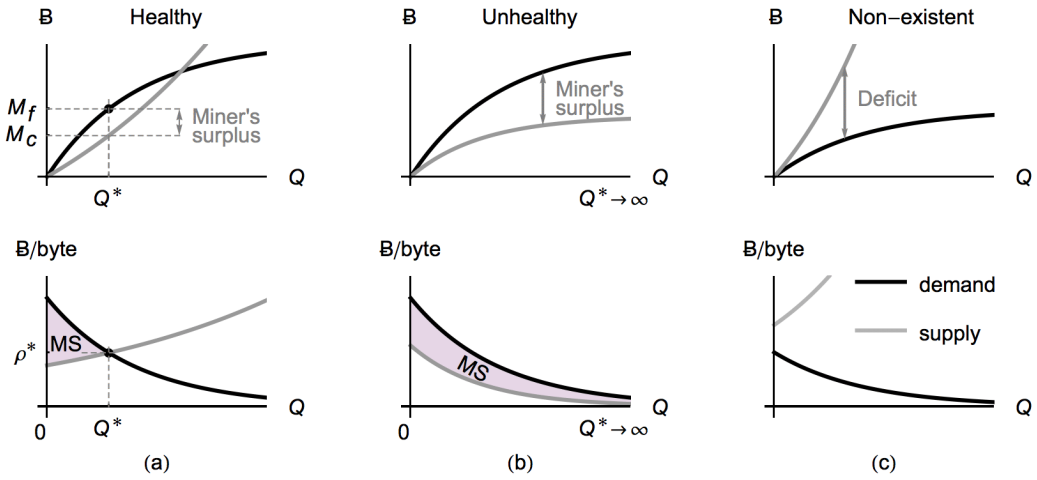

Fig. 6. This chart illustrates healthy, unhealthy and non-existent transaction fee markets. In a healthy market, the miner's surplus is maximized at a finite block size (a). In an unhealthy market, the miner's surplus continually increases with block space suggesting that he should produce an infinite block (b). In a non-existent market, the miner cannot earn a surplus by including transactions and is thus better off producing an empty block (c).

We can define the conditions for each type of market more rigorously if we make the assumption that block space is a normal economic commodity that obeys the *law of demand* (*i.e.*, the quantity of block space demanded increases monotonically as the unit price per byte decreases).[16] Although we will not prove it, it is straightforward to calculate the constraints on the supply curve and the propagation time for each type of market (Table 1).

Table 1. Healthy, unhealthy and non-existent fee markets (positive inflation)

Market type	Block size (maximizes profit)	Demand constraint[17]	Supply constraint	Propagation time asymptote	Physically possible?
Healthy	Finite	$\frac{d\bar{\rho}_{\text{demand}}}{dQ} < 0$	$\frac{d\rho_{\text{supply}}}{dQ} > 0$	$\tau(Q) > O(\log Q)$	Yes
Unhealthy	Infinite		$\frac{d\rho_{\text{supply}}}{dQ} < 0$	$\tau(Q) < O(\log Q)$	No
Non-existent	Zero		$\rho_{\text{supply}} > \bar{\rho}_{\text{demand}}$	-	Yes

As described in Table 1, an unhealthy fee market requires a propagation time that grows asymptotically with block size *slower* than $\log Q$. Using physical arguments, we can show that this is not possible. To proceed, expand $\tau(Q)$ in a power series around $Q = 0$ to get

$$\tau(Q) = \tau(0) + \left.\frac{d\tau}{dQ}\right|_{Q=0} Q + O(Q^2).$$

The first term represents the communication channel's *lag*: for the purposes of this paper, it is the time it takes to communicate the block header across the channel. It has a physical lower bound due to the speed of light constraint $\tau(0) \geq d/c$, where d is the distance over which the information is communicated and c is the speed of light.

The second term partially relates to the channel's *carrying capacity* and has a lower bound described by the *Shannon-Hartley theorem*.[11] We can see this more clearly by setting

$$\frac{1}{\gamma C} = \left.\frac{d\tau}{dQ}\right|_{Q=0} \quad \rightarrow \quad C = \frac{1}{\gamma}\left.\frac{dQ}{d\tau}\right|_{Q=0}$$

where γ is the coding gain and C is the channel capacity (with units of bits of information per second). The carrying capacity of a communication channel is limited to $C = B\log_2\left(1 + \frac{S}{N}\right)$, where B is the channel's bandwidth, S is the signal power and N is the channel's noise power.

The third term lumps together all the terms of order Q^2 and greater. In any practical implementation these terms will exist simply due to the messiness of the real world; however, the author is not aware of any physical reason they *must* exist. *For the remainder of the paper, we will assume these terms are negligible compared to the constant and linear terms*, in which case we can make the approximation

$$\Delta\tau(Q) = \tau(Q) - \tau(0) \approx \frac{Q/\gamma}{C}. \tag{9}$$

This equation states that the extra propagation time is approximately equal to the size of the block produced, divided by the coding gain with which the block solution can be transmitted, and divided by the effective capacity of the communication channel. Since neither C nor γ can be infinite, this term must be finite. Furthermore, there is no reason to expect C or γ to be functions of Q to any appreciable extent, since C is a physical property of the channel and since γ is the degree to which the transactional information within a block can be compressed. This means that no physical communication channel should have a block propagation time that grows asymptotically slower than $O(Q)$. Since this is faster than the $O(\log Q)$ requirement to achieve a healthy fee market (assuming $R > 0$), *an unhealthy fee market is not physically possible.*

8. Big Blocks, Small Blocks and Empty Blocks

To put numbers to our analysis, we express Eq. (8) in terms of the coding gain and channel capacity (*cf.* Eq. 9):

$$\rho_{\text{supply}}(Q) \approx \frac{1}{\gamma C}\frac{R}{T}e^{\frac{Q}{\gamma CT}}. \tag{10}$$

This equation describes the marginal fee density required for a miner to profitably add *another* transaction to a block of size Q. It is plotted in Fig. 7 (for $\frac{R}{T} = \frac{25\text{Ƀ}}{10\text{ min}}$) and illustrates the fee density required to incentivize a miner to produce big, small and empty blocks, at various block solution propagation rates. The important relationships to note are (1) that fees become exponentially more expensive if more transactions bid for space in a block, (2) that fees (measured in Ƀ) become cheaper with improvements in propagation rates, and (3) that a minimum fee density, below which rational miners will produce empty blocks, exists.

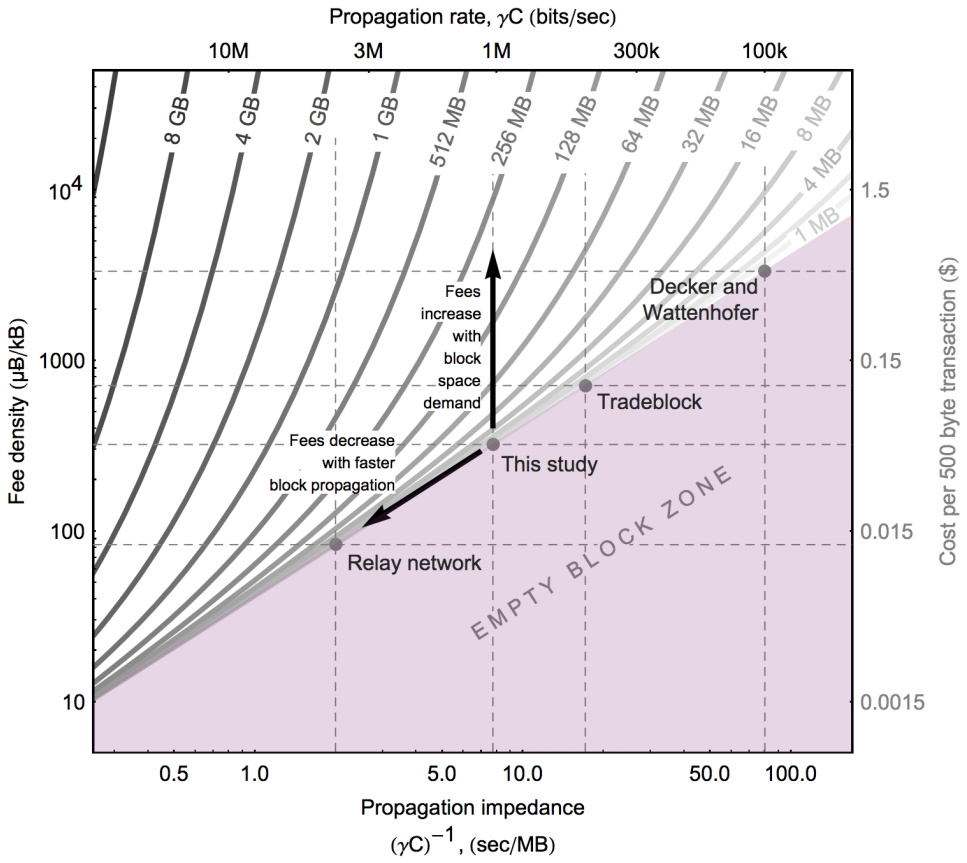

Fig. 7. A rational miner will produce a big block if his mempool is full of high fee density transactions, and will produce an empty block if no transactions pay a fee sufficient to offset the orphaning risk. Transaction fees decline with improvements to the rate at which block solutions propagate across the network.

The fee density is sensitive to the assumed value for the block propagation impedance. Table 2 summarizes four different estimates for the propagation impedance, along with the

minimum fee density associated with each. In the next section, and for each of these four estimates, we calculate the cost to fill a block with 128 MB of spam.

Table 2. Estimates for the Block Solution Propagation Impedance and the Associated Minimum Fee Density

Estimate name	Propagation impedance, $1/\gamma C$ (sec/MB)	Method	Year	Ref.	Min. fee density $R/\gamma CT$ (μB/kB)
Decker and Wattenhofer	80	Direct measurement	2013	10	3,333
Tradeblock	17.1	Direct measurement	2015	18	713
This study	7.6	Defined[a] as $\frac{1}{\gamma C} = \frac{TM}{RQ}$	2015	19	318
Relay network	2.0	Taken as T5 time to 99%	2015	20	83

[a] The estimate shown in the table used *M* and *Q* values taken from the Blockchain over Q2 2015. Refer to note 19 for more details.

9. Cost of a Spam Attack

We can interpret the block space supply curve as a minimum bound on the cost an attacker must bear to produce a significant quantity of blockchain spam. In the case where the attacker is a miner, it represents the cost imposed by orphaning risk (*e.g.*, he may lose the block rewards for several spam blocks before one "sticks"). In the case where the attacker is not a miner, it represents the minimum fees necessary to entice a rational miner to publish a large block. The spam cost (*cf.* Eqs. 7 and 9) is approximately

$$M_{\text{spam}}(Q) \approx R\left(e^{\frac{Q}{\gamma CT}} - 1\right). \tag{11}$$

The cost increases exponentially with the quantity Q of spam stuffed into a block.

Fig. 8 plots contours of constant spam quantity; it illustrates how the cost to produce spam increases as an attacker attempts to fill a block with additional bytes of transactional data, and how the spam cost decreases as network interconnectivity improves. Table 3 lists the estimated spam costs, along with a comparison to the minimum fee densities calculated in Section 8. Due to the exponential in Eq. (10), producing an exceptionally large spam block requires an attacker to pay an effective fee significantly greater than the minimum fee.

Table 3. Cost to Produce a Block That Contains 128 MB of Spam

Estimate name	Propagation impedance $1/\gamma C$ (sec/MB)	Quantity of spam Q (MB)	Cost of spam M (B)	Eff. fee density M/Q (μB/kB)	Min. fee density $R/\gamma CT$ (μB/kB)	Eff. fee divided by min. fee
Decker and Wattenhofer	80	128	646×10^6	$5{,}043\times10^6$	3,333	1.51×10^6
Tradeblock	17.1		935	7,304	713	10.3
This study	7.6		101	793	318	2.50
Relay network	2.0		13	104	83	1.25

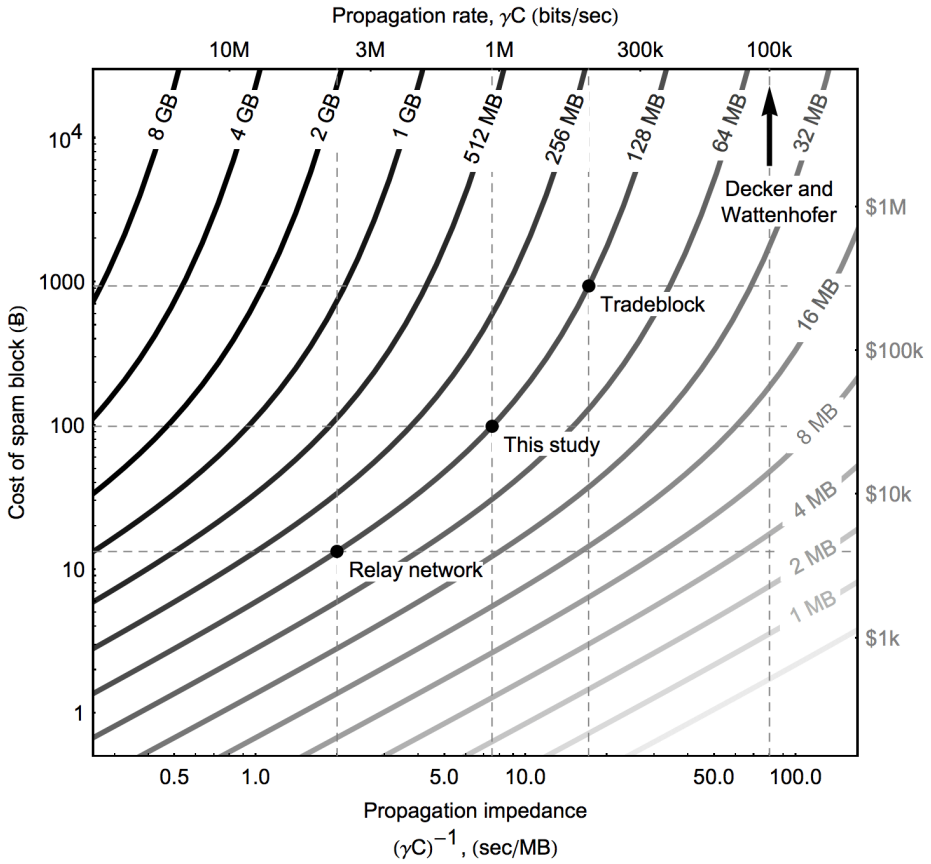

Fig. 8. This chart illustrates the cost to publish spam blocks of various sizes under past, current and future network conditions (labeled points refer to 128 MB blocks at various propagation speeds). The cost of a spam attack increases exponentially with the size of the spam block; however, improvements in the rate at which block solutions can be communicated to the other miners significantly decrease the cost of the attack.

It is interesting to note that the four-week moving average for the price of one bitcoin at the time when the block size limit was introduced (September 6, 2010) was $0.068. The cost to add gigabytes of blockchain spam was thus measured in thousands of dollars, rather than millions as it is today. Since the spam cost is measured in *bitcoins*, a high market value for a bitcoin is an effective anti-spam measure.

10. Conclusion

We showed that a transaction fee market should emerge without a block size limit if miners include transactions in a manner that maximizes the expectation value of their profit. A critical step in establishing this result was our calculation of the miner's cost to supply additional block space by accounting for orphaning risk. Not unexpectedly, we showed that the cost of block space was proportional to both Bitcoin's inflation rate, $\frac{R}{T}$, and the amount of time it takes per uncompressed megabyte to propagate block solutions to the other miners, $\frac{1}{\gamma C}$. More interestingly, however, we showed that the orphan cost is not static, but rather increases exponentially with the block size, Q, demanded:

$$\rho_{\text{supply}}(Q) \approx \underbrace{\frac{1}{\gamma C}\frac{R}{T}}_{\substack{\text{Static} \\ \text{approximation}}} \overbrace{e^{\frac{Q}{\gamma C T}}}^{\text{Correction}} .$$

Not only is there a minimum fee density below which no rational miner should include *any* transactions as Andresen observed,[10] but the required fee density also naturally increases if demand for space within a block is elevated.[21] Indeed, a rational miner will not include all fee-paying transactions, as urgent higher-paying transactions necessarily bump lower-fee transactions out, thereby bidding up the minimum fee density exponentially with demand. Analogously, an attacker who wishes to produce a large spam block—whether the attacker is the miner or a user—must pay an effective fee density significantly greater than the cost per byte he would pay for a modest amount of block space. A fee market naturally emerges.

We made three important simplifying assumptions in this paper: (1) we assumed the probability of orphaning a block was well characterized by a single parameter that represented the time between when a miner had solved a block and when his solution had been communicated and accepted by his peers, (2) in Sections 7 to 9, we assumed that this time parameter had a lower bound, in part, due to the capacity of the channels used to communicate the solutions and by the coding gain with which they could be compressed, as described by the Shannon-Hartley theorem, and (3) we ignored the costs a miner bears when he commits transactions to a block beyond those due to orphaning. These simplifications bring up questions that deserve further study:

(1) The time it takes to propagate information to the other miners is not in general constant across the network,[22] while the mempool is largely homogenous. This suggests that, assuming equal hashing costs, miners who can propagate their block solutions faster will earn a larger surplus. Relatedly, recent evidence also suggests that miners may begin mining prior to fully receiving and validating new blocks.[23] How do these phenomena affect the current analysis?

(2) Imagine the existence of a mining cartel, interconnected with high-capacity relay channels and committed to standardized mempool policies (to facilitate dense compression of block solutions). Such a cartel could greatly reduce the time required to propagate solutions to its other members. Do we expect such cartels to form and what might be their effect?

(3) When a miner accepts a transaction that increases the set of unspent outputs (UTXO), he takes on a liability equal to the present value of the cost of storing those new outputs indefinitely far into the future. Is a healthy fee market expected to emerge that charges users the true cost of expanding Bitcoin's UTXO set?

We conclude by noting that the analysis presented in this paper breaks down when the block reward falls to zero. It suggests that the cost of block space is zero; however, this would suggest zero hash power, which in turn would suggest that transactions would never be mined and, paradoxically, that no block space would be produced. Happily, questions about the post-block reward future can be explored at a leisurely pace, as we have a quarter-century before it begins to become a reality. Into the distant future then, a healthy transaction fee market is expected to exist without a block size limit.

Appendix

The block space supply curve can be derived by finding the function of block size, $M_{\text{supply}}(Q)$, that describes the fees required to precisely compensate for orphaning risk. Mathematically, we require that the miner's profit (*cf.* Eq. 5) remain constant for any quantity of block space, Q:

$$\frac{d}{dQ}\langle \Pi \rangle = \frac{d}{dQ}\left\{\left[R + M_{\text{supply}}(Q)\right]\frac{h}{H}e^{-\frac{\tau(Q)}{T}} - \eta h T\right\} = 0. \tag{A1}$$

Eq. (A1) can be re-written

$$\frac{h}{H}\frac{d}{dQ}\left\{\left[R + M_{\text{supply}}(Q)\right]e^{-\frac{\tau(Q)}{T}}\right\} - \frac{d}{dQ}\{\eta h T\} = 0,$$

and then the terms that do not depend on Q eliminated:

$$\frac{d}{dQ}\left\{\left[R + M_{\text{supply}}(Q)\right]e^{-\frac{\tau(Q)}{T}}\right\} = 0.$$

By the fundamental theorem of calculus

$$\int_0^Q \frac{d}{dq}\left\{\left[R + M_{\text{supply}}(q)\right]e^{-\frac{\tau(q)}{T}}\right\}dq$$
$$= \left[R + M_{\text{supply}}(Q)\right]e^{-\frac{\tau(Q)}{T}} - \left[R + M_{\text{supply}}(0)\right]e^{-\frac{\tau(0)}{T}} = 0$$

and since by definition $M_{\text{supply}}(0) = 0$

$$M_{\text{supply}}(Q)e^{-\frac{\tau(Q)}{T}} + Re^{-\frac{\tau(Q)}{T}} = Re^{-\frac{\tau(0)}{T}}$$

so

$$M_{\text{supply}}(Q) = R\left(e^{\frac{\Delta\tau(Q)}{T}} - 1\right), \tag{A2}$$

where $\Delta\tau(Q) \equiv \tau(Q) - \tau(0)$. Eq. (A2) thus describes the cost to produce block space Q accounting for orphaning risk. For the purposes of this paper, $\tau(0)$ should be interpreted as the time it takes to propagate the block header.

Acknowledgement

The author gratefully acknowledges the kind review and suggestions of Dr. Christopher E. Wilmer. The author also wishes to thank the many thoughtful individuals from the Bitcoin Forum, whose ideas helped form the basis of this work, as well as the community of r/bitcoin for their encouragement and enthusiasm.

Notes

[1] The block size limit was implemented with two Git commits. The first, on 14-Jul-2010, prevented clients from mining blocks larger than 1 MB (commit a30b56e), while the second, on 06-Sep-2010, prevented the network from accepting blocks larger than 1 MB (commit 8c9479c). *Source: Github.*

[2] In 2010, the Visa network processed 2,000 transactions per second on average. *Source: https://en.bitcoin.it/wiki/Scalability*.

[3] On September 6, 2010, the 4-week moving average for daily transactions was 354 per day. A 1 MB block size would permit 144 MB of transactional data per day. At an average transaction size of 500 bytes, this would allow 288,000 transactions per day to be logged to the Blockchain, or 288,000 / 354 = 814 times more than the demand at that time. *Source: blockchain.info.*

[4] Satoshi Nakamoto commented on 4-Oct-2010 on the Bitcoin Forum that a larger blocksize limit "can be phased in, like: if (blocknumber > 115000) maxblocksize = largerlimit." *Source: bitcointalk.org.*

[5] The transaction backlog peaked at over 64,000 unconfirmed transactions on July 14, 2015. *Source: statoshi.com.*

[6] The author has been tracking the moving seven-day average of the block size, and recorded a surge to over 70% capacity the seven days beginning 08-Jul-2014. *Source: https://bitcointalk.org /index.php?topic=68655.msg11982079.*

[7] J. Donnelly. "Bitcoin Network Still Backlogged With Tens of Thousands of Unconfirmed Transactions, Causing Delays." *Bitcoin Magazine.* 07-Jul-2015.

[8] The average number of transactions per day (4 week moving average) centered on September 6, 2010 was 335. The 4-week moving average centered on 01-Jul-2015 was 133,225: 376x times greater. *Source: blockchain.info.*

[9] Nicolas Houy. "The economics of Bitcoin transaction fees." Self published 24-Feb-2014 (v0.1). The quote from Houy in the main text is taken from page 8, paragraph 3, last sentence. It is clear that he does not consider the orphan cost when he writes on p. 4 that "if an individual has 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."

[10] In the winter of 2013, Gavin Andresen wrote a Gist "to come up with a back-of-the-envelope estimate for how much it costs a miner to create larger, rather than smaller, blocks" where he presented the orphaning factor used in this paper. *Source: https://gist.github.com/gavinandresen/5044482.*

[11] Claude E. Shannon. "Communication in the presence of noise." *Proc. Institute of Radio Engineers* **37** (1): 10–21, January 1949.

[12] The hardware's amortized price per hash, η, includes its fully amortized cost as well as electricity, maintenance and the cost of supporting infrastructure.

[13] We leave the precise definition of the propagation time "fuzzy" with regards to its homogeneity across the network or exactly what fraction of the hash power the solution should have reached in this time period.

[14] Usually attributed to Alfred Marshall, Principles of Economics, 1890.

[15] We use the symbol ρ because it is visually similar to the symbol *P* often used to denote the traditional supply and demand curves, while still reflecting that fact that what it is describing is the *fee density* (ρ is often used for density in physics and engineering).

[16] In economics, the law of demand states that, all else being equal, as the price of a product increases (↑), quantity demanded falls (↓); likewise, as the price of a product decreases (↓), quantity demanded increases (↑). *Source: https://en.wikipedia.org/wiki/Law_of_demand.*

[17] The curve $\bar{\rho}_{\text{demand}}$ differs slightly from the curve ρ_{demand}. The latter represents the empirical demand measureable from a miner's mempool, while the former represents the traditional demand curve that is less quantifiable (the demand that would exist if the price was different).

[18] Tradeblock performed a careful study where they measured the time it takes on average for new block solutions to be accepted by 50% of the nodes they were connected to. For our purposes, the time to reach 50% of the hashing power would be preferable; however, this number was not available. *Source: https://tradeblock.com/blog/bitcoin-network-capacity-analysis-part-6-data-propagation.*

[19] Between 1-Apr-2015 and 30-Jun-2015, the Blockchain grew by $Q = 5{,}100$ MB while the total fees earned by miners over the same period averaged 17.82 Ƀ/day × 91 days → $M = 1{,}621$ Ƀ. An estimate for the propagation impedance can be made as $\frac{1}{\gamma C} = \frac{TM}{RQ} = (600\text{ s})(1621\text{ Ƀ})/[(25\text{ Ƀ})(5100\text{ MB})] = 7.62$ s/MB. *Source: blockchain.info.*

[20] Matt Corallo's Relay Network Statistics. *Source: http://bitcoinrelaynetwork.org/stats.html.*

[21] It makes perfect sense that the cost to supply a kilobyte of block space increases with block size. Imagine that at some very large block size the probability that a miner's block was orphaned was exactly 100%. If this is true, then just before this point, the cost of *a bit more* block size would be infinite: there is no transaction fee a miner would rationally accept in exchange for including an extra transaction because he would be guaranteed to have his block orphaned if he did. From this view point, then it is intuitive that as the probability of orphaning increases, the cost of adding another transaction must increase too.

[22] Peter Wuille showed via simulation that miners connected with fast channels can earn a greater profit per hash than miners connected over slower channels. This is in-line with the results presented in this paper, as a miner with faster communication channels would have a lower cost of production yet select transactions from the essentially the same mempool demand curve, thereby earning a greater surplus. *Source: http://www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg08161.html.*

[23] For example, F2Pool was observed mining on invalid blocks on 3-Jul-2015, due to their use of SPV mining. *Source: https://www.reddit.com/r/Bitcoin/comments/3c2cfd/psa_f2pool_is_mining_invalid_blocks/*