

Incentive Mechanisms for Securing the Bitcoin Blockchain

White Paper

BitFury Group

Dec 07, 2015 (Version 1.0)

Abstract

This white paper studies the two major incentive mechanisms which provide for the security and immutability of the Bitcoin blockchain: block rewards and transaction fees. We examine the role such incentives play in providing the resilience of the Bitcoin blockchain to blockchain reorganization and denial of service attacks, and the sources of blockchain security in the context of emerging off-chain payment methods. Machine-to-machine / Internet of Things payments are also examined due to the enabling impact blockchain technology could have in organizing the decentralized economy. Lastly, we present a methodology for estimating the aggregate transaction fees over the Bitcoin network in the medium term based on existing and emerging Bitcoin applications.

© 2015 Bitfury Group Limited

Without permission, anyone may use, reproduce or distribute any material in this paper for noncommercial and educational use (i.e., other than for a fee or for commercial purposes) provided that the original source and the applicable copyright notice are cited.

Legal Disclaimer

This white paper is based on various publicly available information sourced from third parties which has not been independently verified by us and on certain methodologies and assumptions as stated in the white paper. This white paper is for information purposes only. Bitfury Group Limited does not guarantee the accuracy of the conclusions reached in this paper, and the white paper is provided “as is” with no representations and warranties, express or implied, whatsoever, including, but not limited to (i) warranties of merchantability, fitness for a particular purpose, title or non-infringement; (ii) that the contents of this white paper are free from error or suitable for any purpose; and (iii) that such contents will not infringe third-party rights. All warranties are expressly disclaimed. Bitfury Group Limited and its affiliates expressly disclaim all liability for, damages of any kind arising out of use, reference to, or reliance on any information contained in this white paper, even if advised of the possibility of such damages. In no event will Bitfury Group Limited or its affiliates be liable to any party for any direct, indirect, special or consequential damages for any use of or reliance on this white paper. The user of this white paper assumes the full risk of using the information in this white paper.

The Bitcoin blockchain possesses an append-only property: once a transaction is added into the chain of blocks, it is economically very costly to remove it (that is, to *reverse* a transaction in order to perform a *double-spend*). The cost to remove a transaction from the blockchain increases with the number of transaction confirmations [1, 2]. (The number of confirmations for a transaction is the number of blocks on the blockchain including the block containing the transaction and all later blocks. For transactions not yet included into a block, the number of confirmations is 0.) In order to perform a double-spend, an attacker needs to reorganize the blockchain by replacing all blocks including and after the block containing the transaction that the attacker attempts to reverse. However, adding blocks is made computationally expensive by using the proof of work consensus algorithm, which secures the blockchain from reorganizations.

In the paper, we use the term *mining* to refer to the process of solving computationally expensive puzzles associated with the proof of work consensus algorithm. The role of mining in the Bitcoin ecosystem is providing security of the blockchain and notarizing users' transactions according to the predefined set of rules (the Bitcoin protocol) in exchange for a fee. Thus, Bitcoin miners could be called *Bitcoin notaries*. Notaries on the Bitcoin blockchain perform two tasks: mining and transaction processing. Neither of these tasks depends on the other one:

- transaction processing is performed by all full nodes in the Bitcoin network, of which miners constitute a small part
- mining could be performed without transaction processing in a subtype of *SPV mining* [3] (this type of mining is inherently dangerous, as the miner cannot fully validate the contents of received blocks).

Therefore, “notary” is a more specific term than “miner” or “transaction processor”.

Since 2013, bitcoin mining is performed with specialized hardware (utilizing application-specific integrated circuits or ASICs), with individual miners aggregated into large mining pools. Bitcoin notaries are incentivized with two revenue streams:

- block rewards – each new block contains an algorithmically determined reward (25 bitcoins as of time of the writing), which is collected by the miner of the block
- transaction fees associated with transactions in the block.

In the long term, these revenue streams are aligned with the value of bitcoins. Therefore, according to game theory, long-term notaries' goals are aligned with the users' goals to increase or maintain bitcoin value.

We examine the sources of the notaries' incentives in Section 1. In Section 2, we consider off-chain transactions and the manner in which they may influence the Bitcoin ecosystem. We estimate the transaction volumes and fees in the short to medium term (by 2020–2025) in Section 3.

1 Sources of Notarial Incentives

1.1 Block Rewards

A fixed amount of bitcoins (*block reward*) is created with each new block of transactions. This amount is claimed in the first transaction of a block and is determined algorithmically based on the height of the block in the blockchain [4]. The reward halves every 210,000 blocks (approximately 4 years), which assures the limited total supply of bitcoins of 21 million. Initially, the block reward was 50 bitcoins; it was halved to 25 bitcoins on November 28, 2012. The next halving is expected to occur in July 2016 [5].

Block rewards can be viewed as a (controlled) inflation subsidy paid by Bitcoin users to Bitcoin notaries (Fig. 1). As of 2015, the annual inflation of the Bitcoin monetary supply is approximately 9%. By 2025, the annual Bitcoin inflation will be below 1%. Although the monetary base of Bitcoin is increasing, the demand for bitcoins is growing faster as evidenced by the increasing velocity of bitcoins. Thus, the growth of the Bitcoin supply is not excessive.

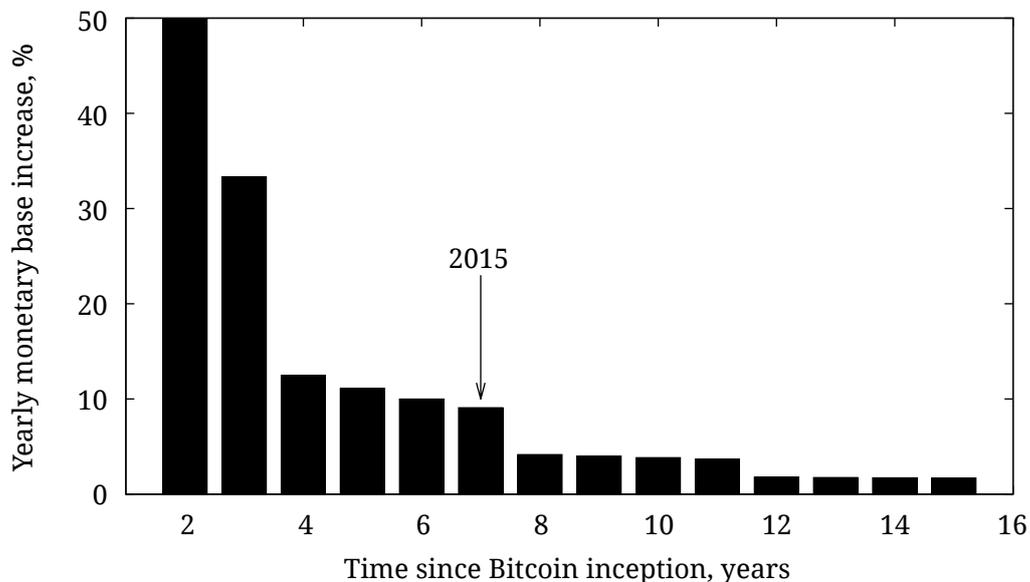


Figure 1: Increase of the Bitcoin’s monetary supply. The rate of increase is defined as the increase of the Bitcoin supply per year divided by the Bitcoin supply at the beginning of the year.

With the role of block rewards steadily diminishing, transaction fees are expected to play an increasing role in incentivizing Bitcoin notaries to continue mining and transaction processing in order to provide network security.

1.2 Transaction Fees

A transaction fee can be included into any Bitcoin transaction; the fee provides an incentive to Bitcoin notaries to include the transaction in a block [6]. If a user wants the transaction to be confirmed (i.e., included into a block) faster, he would need to pay a higher fee.

Each Bitcoin transaction consists of inputs and outputs. Each input references an unspent output of a previous transaction recorded on the blockchain. From a technical standpoint, a transaction fee is the sum of values of all inputs of the transaction minus the sum of values of all outputs created by the transaction. For example, if a transaction has a single input with the value of 1 bitcoin and creates two outputs with the values of 0.6 bitcoins and 0.3998 bitcoins, then the transaction fee is

$$1 - 0.6 - 0.3998 = 0.0002 \text{ bitcoins.}$$

Transaction fees influence how transactions propagate across the Bitcoin network. There is a tunable parameter **minrelaytxfee** of the default Bitcoin client (Bitcoin Core), which determines the minimum possible fee amount per kilobyte of transaction size; transactions with lower fee are considered spam and are not propagated by a Bitcoin node. The threshold is determined by rounding the transaction size in thousands of bytes up to the nearest integer:

$$\langle \text{Fee threshold} \rangle = \lceil \langle \text{Size in bytes} \rangle / 1000 \rceil \cdot \langle \text{minrelaytxfee} \rangle.$$

By default, **minrelaytxfee** equals 0.01 millibitcoins, or 1000 satoshis (1 satoshi = 10^{-8} bitcoins; it is the atomic unit of Bitcoin value). This value can be changed by the user operating the node. If the size of a transaction is 999 bytes, then the minimum transaction fee with the default **minrelaytxfee** is 1000 satoshis; if its size is 1001 bytes, then the threshold is 2000 satoshis. Most Bitcoin wallets currently set the default transaction fee to 10000 satoshis per kilobyte; usually, the fee value can be changed by the user. Several Bitcoin-related websites, such as BlockTrail [7], provide a service allowing Bitcoin users to estimate the necessary fee to include a transaction into the next block. As a typical transaction does not exceed 1000 bytes in size, the default fee implies an extra payment for a single transaction of about 3 cents based on a bitcoin exchange rate of \$300 per 1 bitcoin. In the future, most wallets are expected to implement smart transaction fee logic similar to the **estimatefee** RPC method in Bitcoin Core [8]; the method estimates the optimal transaction fee based on transactions recently removed from the pool of unconfirmed transactions.

The transaction fee per thousand bytes plays a crucial role in determining the order in which transactions are included into a block by Bitcoin notaries. When creating a block, the notary sorts all unconfirmed transactions he has verified and placed into his transaction pool (*mempool*) by decreasing transaction fee per kilobyte and includes into the block the transactions with the highest value of this parameter. Thus, transaction fees help mitigate denial of service attacks on the Bitcoin network.

The Bitcoin notary can reserve a certain space in a block for high-priority transactions, i.e. transactions with a large amount of transferred bitcoins (or, more specifically, their *coin age*) normalized for the transaction size. Coin age of a transaction input is calculated as its value multiplied by the age (the number of confirmations) of an unspent output that the input is referencing [6]. (For example, if a transaction input references the unspent output that has been created by a transaction with 10 confirmations, the age of the input is 10.) Coin age of a transaction is the sum of coin ages of its inputs. Thus, the priority of a transaction is

$$\text{Priority}(T) = \frac{1}{\text{Size}(T)} \sum_{In \in T} \text{Value}(In) \cdot \text{Confirmations}(In)$$

Consider a transaction T with the size of 500 bytes and two inputs:

- 1 bitcoin with 10 confirmations
- 0.5 bitcoins with 30 confirmations.

The priority of T is

$$\text{Priority}(T) = (1 \cdot 10 + 0.5 \cdot 30) / 500 = 0.05 \text{ BTC / byte.}$$

The threshold for high priority values is 0.576 BTC / byte, which corresponds to a transaction with a single day-old 1 BTC input and a size of 250 bytes.

Reserving the space for high-priority transactions is optional, and the default amount of allocated space is quite small (50 kilobytes out of 1 MB block space [9]), so we can with reasonable certainty conclude that transactions are included into a block based solely on their transaction fee per kilobyte.

In order to prevent double-spends, most Bitcoin payments are considered final when a corresponding transaction gains a necessary number of confirmations, e.g. 6. Thus, the less the transaction fee, the longer it takes to confirm the payment. Transactions with no fee or with a fee substantially lower than average can still be included into a block; however, there may be an unpredictable delay. Furthermore, if the transaction fee per kilobyte is lower than the **minrelaytxfee** setting of some nodes in the network, the transaction may not be relayed at all. If a more restricting **minrelaytxfee** value is set by a mining node, the transaction would not be included into any blocks created by the corresponding Bitcoin notary, as it would never enter the pool of transactions eligible for inclusion into a block. Thus, increasing **minrelaytxfee** is a natural way to make spam attacks on the Bitcoin network more expensive. In light of spam attacks in 2015, changes have been made to Bitcoin Core in order to regulate the minimum acceptable transaction fee dynamically depending on the number of unconfirmed transactions [10].

2 Off-chain Transactions

An off-chain transaction is the movement of value in bitcoins, which is not recorded on the Bitcoin blockchain [11]. This type of transactions is already widely utilized by Bitcoin wallet services and exchanges such as Coinbase [12], Circle [13] and ChangeTip [14]. Some estimates are that off-chain transactions constitute as many as 90–99% of all Bitcoin transactions as of June 2015 [15]. Off-chain transactions have several advantages compared to ordinary Bitcoin transactions recorded directly on the blockchain:

- immediate confirmation instead of an approximately 1 hour wait for on-chain transactions
- lower transaction fees, which makes off-chain transactions more suitable for micropayments
- better scalability for a high volume of transactions.

Some transactions are driven off-chain because of the limitations placed on transactions by the Bitcoin protocol (e.g., by rules defining standard transaction types). These transactions could be secured on-chain by establishing agreements between the off-chain services and Bitcoin notaries.

The main drawback of existing off-chain payment services is their centralization; the users of such services have no guarantee their funds are safe in the service. Two major efforts to launch decentralized or federated¹ off-chain payment infrastructure are

- pegged sidechains [16]
- Lightning [17].

Lightning (Fig. 2) could become a crucial development in the Bitcoin ecosystem, as it would provide a means for decentralized, peer-to-peer instant payments among Bitcoin users, the security of which would still be guaranteed by the Bitcoin network. The core idea behind Lightning is the following: if there exists a stable stream of blockchain-based payments between two parties (e.g., an online streaming content provider and its user), intermediate transactions do not need to be recorded on the blockchain. The only transactions that need to be recorded are the initial funding transaction and the transaction closing the payment channel (either by agreement of the parties or forced by uncooperative behavior of one of the parties). Lightning provides a high degree of scalability in the form of hashed timelock contracts (HTLCs). HTLCs allow parties to trustlessly use intermediate network nodes in payment channels, which would make it unnecessary to establish a direct payment channel between each pair of parties.

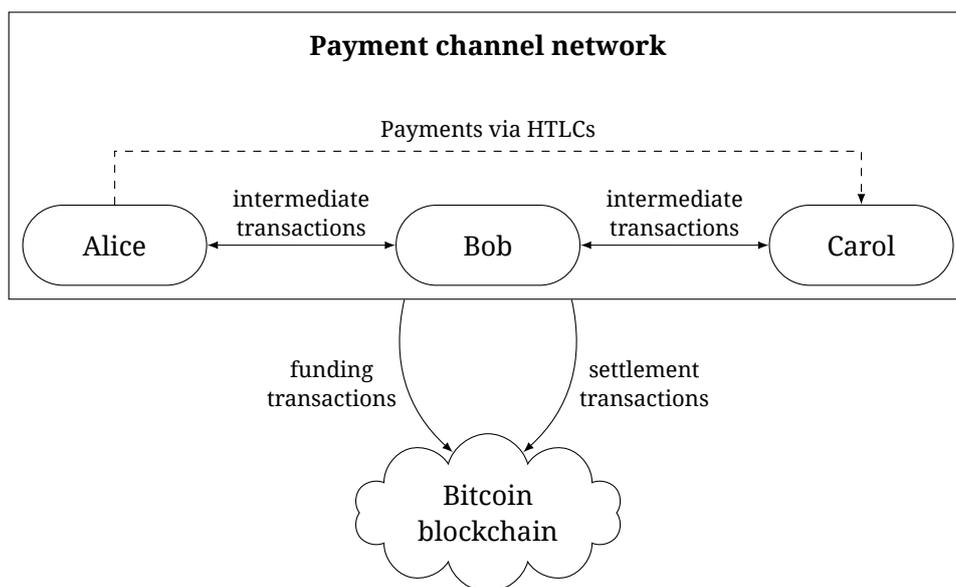


Figure 2: Organization of a payment channel network on top of the Bitcoin blockchain

To ensure security, off-chain solutions would still need to be pegged to the Bitcoin blockchain; thus, the security of off-chain payments depends on the security of the underlying blockchain. As off-chain transactions do not pay fees directly, several other ways to fund network security have been proposed [18] in the case that most transactions are performed off the blockchain, including:

¹Federated system in this context is understood as a system operated cooperatively by several independent, mutually distrusting entities [16].

- high fees for pegging on-chain transactions
- in the case of payment channels: forced channel close-out periods related to the due date of refund transactions
- direct payments to known Bitcoin notaries
- assurance contracts [19] in the form of collective donations.

As Bitcoin is presently a system for consumer-to-consumer and, to a lesser degree, consumer-to-business payments, it has an opportunity to capture the emerging market of decentralized peer-to-peer services among consumers and small businesses. In this context, the Bitcoin network and protocols built on top of it could provide the technological basis for the following opportunities:

- online payments, micropayments and ubiquitous payments
- machine-to-machine payments / Internet of Things innovations
- services for unbanked
- international money transfer and remittances.

As consumer-to-business and especially consumer-to-consumer markets necessitate decentralization of payment processing and trustlessness to achieve global scale, Bitcoin could be a vital technology with regards to these markets. Besides largely eliminating the need for trusted intermediaries, Bitcoin could also provide these markets with greater divisibility suitable for micropayments and availability of permissioned environments on top of the Bitcoin infrastructure (e.g., colored coin protocols or permissioned sidechains).

Expansion of Internet of Things and advent of machine-to-machine payments could become a major force behind the adoption of blockchain technology [20]. Bitcoin infrastructure in this context could provide a neutral, permissionless, tested, fully open and transparent blockchain. According to various estimates, there will be 20–50 billion devices connected to the Internet by 2020, which would generate on the order of \$100 billion annual revenue (Table 1). By the 2020s, blockchain integration could become a simple and inexpensive process given the present trend of replacing single-purpose embedded systems with multi-purpose system-on-chip architectures and single-board computers. In these systems, blockchain support could be added *after* the device is delivered to a customer, e.g. in an over-the-air update or with a dedicated application. Most blockchain-enabled devices would use the simplified payment verification mode [1], which requires little computational and storage resources; more powerful systems could run the full blockchain node stack, e.g. for mining or providing infrastructure.

Blockchain technology would provide the medium for two categories of device transactions [30]:

- **Asset transfer and value transactions**, which would provide monetization services for the Internet of Things (rental, sharing, insurance, lending / borrowing, etc.)
- **Asset operations transactions**, which would establish connectivity and management services (authorization, management, reporting, etc.).

Table 1: Numerical estimates of Internet of Things

Author	Year	Indicator	Value	Link
Gartner	2020	number of devices	25 billion	[21]
Gartner	2020	incremental revenue	\$300 billion	[22]
ABI Research	2020	number of devices	40.9 billion	[23]
Cisco	2020	number of devices	50 billion	[24]
Cisco	2024	incremental revenue	\$19 trillion	[24]
IDC	2020	spending	\$1.7 trillion	[25]
Accenture	2019	coverage	69%	[26]
Machina Research	2023	annual revenue	\$700 billion	[27]
IHS Automotive	2020	number of devices	18 billion	[28]
IHS Automotive	2020	number of connected cars	152 million	[28]
Navigant Research	2022	number of smart meters	1 billion	[29]

Blockchains would provide capabilities that are difficult to achieve with a centralized approach, such as direct customer-to-customer rental and lending services, decentralized authorization, automated location-based payments, etc. Most IoT transactions could be performed off-chain in a peer-to-peer fashion using Lightning or a similar mesh network built on top of the Bitcoin blockchain. For data transactions, the use of anchored document-based sidechains would be more appropriate (these kinds of blockchains are currently being explored e.g. by Factom [31]).

Another potential use case of off-chain transactions is financial services. Financial institutions have shown interest in using blockchains in their infrastructure. While they have shown interest primarily to build permissioned blockchains (i.e., blockchains, in which there is a limited list of transaction processors with known identities), there are several potential ways to integrate these blockchains with Bitcoin, including

- colored coin protocols for digital asset transfer on top of the Bitcoin blockchain
- usage of known transaction processors for Bitcoin transactions
- merged mining [32] and blockchain anchoring [33] to secure permissioned chains via Bitcoin mining
- pegged sidechains enabling the use of Bitcoin as a monetary transfer service or as a medium for clearing operations among permissioned sidechains.

Because financial institutions require security of their transactions, financial applications could become a valuable source of transaction fees as Bitcoin is adopted for use in these applications.

3 Estimating Aggregate Transaction Fees

3.1 Lower Bound for Transaction Fees

Transaction fees have been steadily rising since June 2015 [34]. Currently, the amount of transaction fees collected per day is approximately 25 bitcoins (Fig. 3), or about 0.17 bitcoins per block (Fig. 4), which constitutes less than 1% of the overall incentives being earned by Bitcoin notaries. Transaction fees in the future could be estimated using a mathematical model proposed in the paper, *A transaction fee market exists without a block size limit* [35]. According to the model, a rational Bitcoin notary maximizing his profit would include transactions based on their marginal fee (i.e., approximately the same algorithm as used now in mining). Including more transactions into a block is offset by the risk that the block would propagate slower because of its size and become stale², as there is a risk that another block would be discovered at the same time and adopted by more network nodes. Thus, if transaction fees are lower than a certain limit, a rational Bitcoin notary would not include them into a block.

Let M denote an amount of transaction fees, and Q denote the block size. To determine transactions which would be included into a block, a rational Bitcoin notary builds two curves in the MQ plane.

Definition 1. The *mempool demand curve* $M_d(Q)$ determines the maximum amount of fees that can be added into a block with the size Q based on transactions from the mempool. This curve is built by sorting transactions by decreasing fee density (fee per transaction size in bytes) and calculating cumulative size and fees.

Let $\{f_i\}_{i=1}^n$ and $\{s_i\}_{i=1}^n$ denote fees and sizes of transactions in the mempool respectively. Assume transactions are sorted by decreasing fee density:

$$\frac{f_1}{s_1} \geq \frac{f_2}{s_2} \geq \dots \geq \frac{f_n}{s_n}.$$

Let

$$\forall i = 1, \dots, n \quad S_i = \sum_{j=1}^i s_j; \quad S_0 = 0.$$

Then the mempool demand curve is defined as

$$M_d(0) = 0; \quad \forall i = 1, \dots, n \quad M_d(S_i) = \sum_{j=1}^i f_j.$$

The curve is linearly interpolated on intervals (S_i, S_{i+1}) , $i = 0, \dots, n - 1$.

Definition 2. The *block space supply curve* $M_s(Q)$ determines the amount of fees a miner requires to be compensated for the increased risk of orphaning associated with larger block sizes.

²Stale blocks [36] are valid Bitcoin blocks not included into the consensus Bitcoin blockchain. The miner of a stale block essentially wastes his resources, as he cannot not spend the reward for that block on the consensus blockchain. Stale blocks are different from orphaned blocks, which are blocks with no known parent.

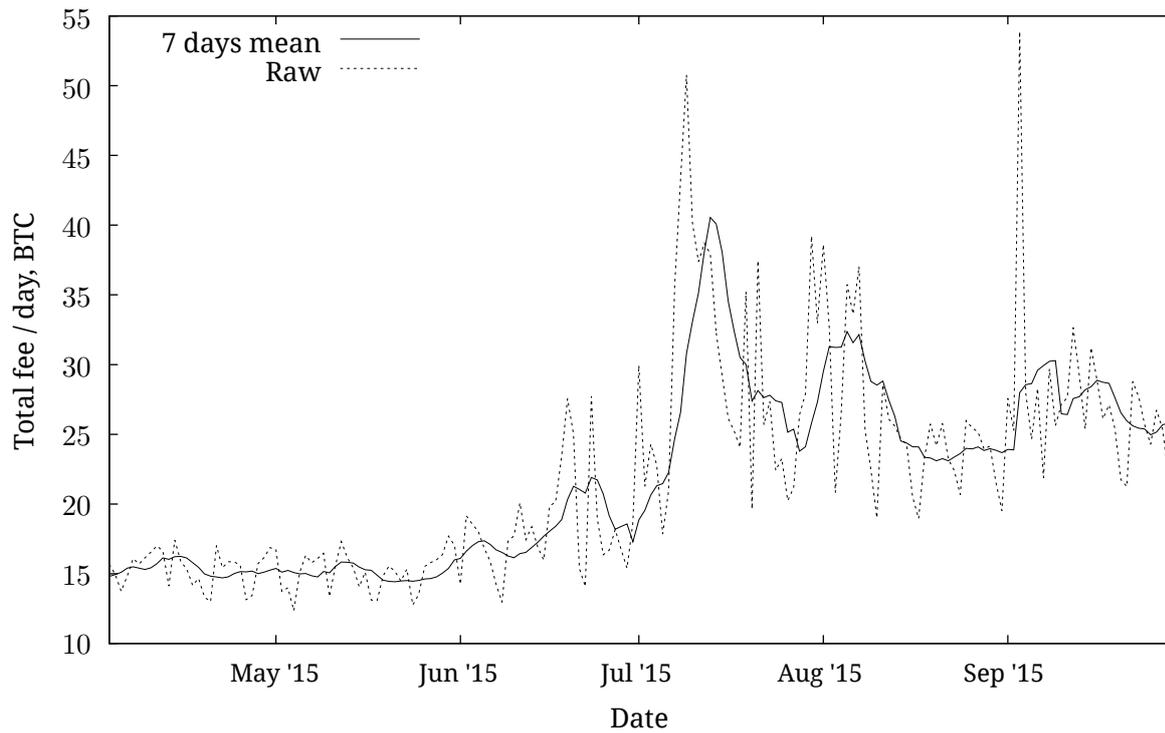


Figure 3: Total transaction fees per day. In this and the following charts, we ignore blocks with total fee of more than 2 bitcoins, as such fees only arise as a result of a mistake

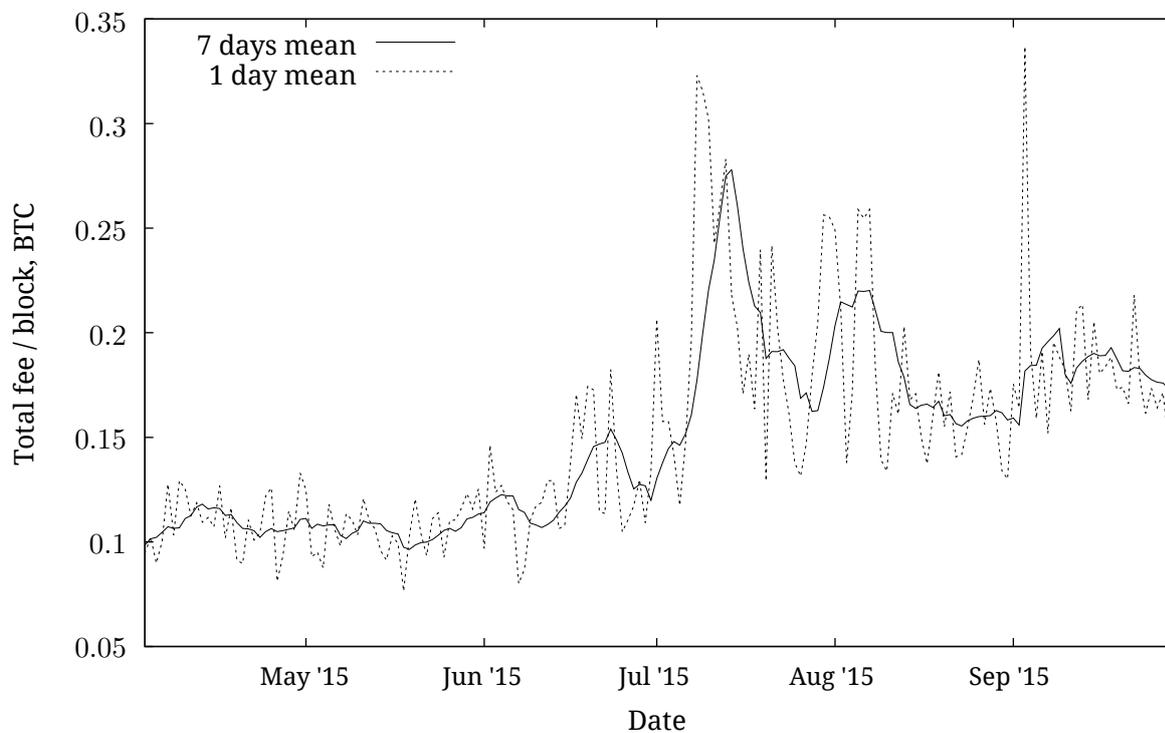


Figure 4: Total transaction fees per block, averaged on a daily and weekly basis

The block space supply curve can be approximated [35] as

$$M_s(Q) = R \left(\exp\left(\frac{IQ}{T}\right) - 1 \right), \quad (1)$$

where

- R is the block reward (currently, 25 bitcoins)
- I is the impedance of the block propagation over the Bitcoin network (estimated in [35] to be approximately 7.6 seconds / megabyte)
- T is the expected time between blocks (10 minutes)

This results in the current estimate $M_s \approx 0.16$ bitcoins for 0.5 megabyte blocks, which is close to the observed value (Fig. 5). Note that the causes of network impedance are not limited to the bandwidth of Internet channels. As blocks become larger, validating the contents of the block (e.g., the block's Merkle root [38] and digital signatures of transactions) also takes more time.

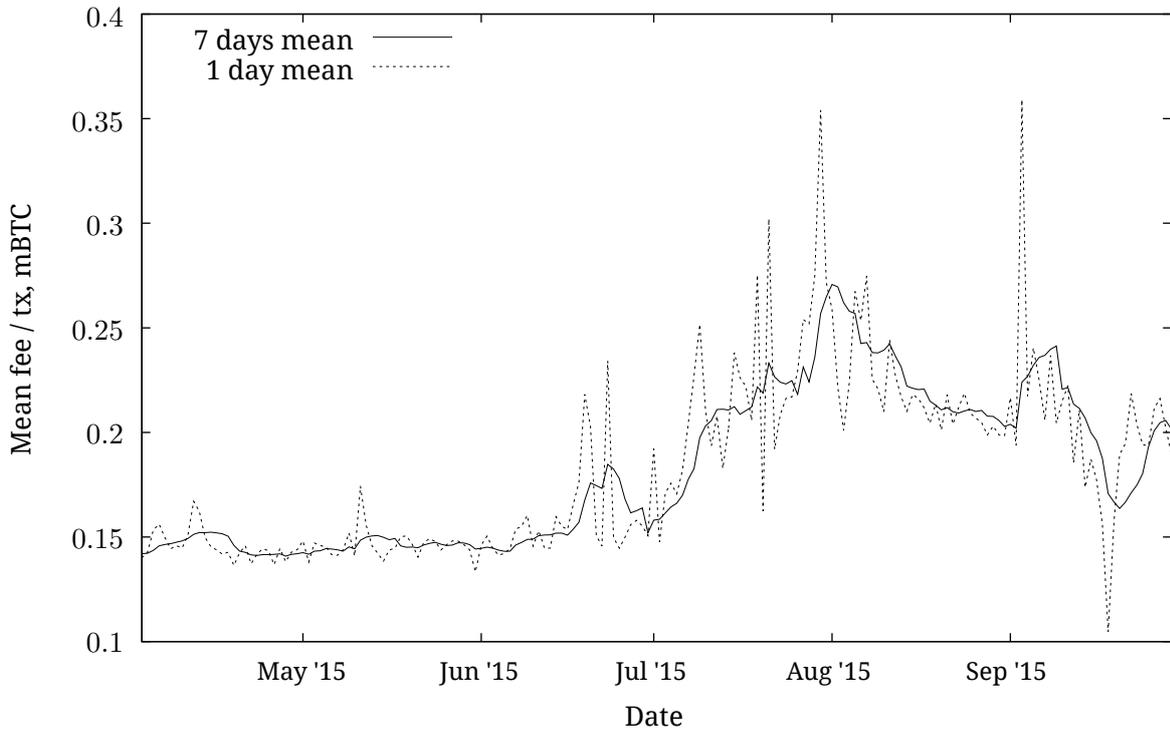


Figure 5: Transaction fee, averaged on a daily and weekly basis

The optimal size of a block Q^* can be calculated by solving the optimization problem

$$Q^* = \arg \max_Q (M_d(Q) - M_s(Q)) \Leftrightarrow \frac{\partial M_d}{\partial Q}(Q^*) = \frac{\partial M_s}{\partial Q}(Q^*).$$

Together with (1), this gives us the number of transactions that should be accepted into the block:

$$i^* = \max \left\{ i : \frac{f_i}{s_i} > \frac{IR}{T} \exp\left(\frac{IS_i}{T}\right) \right\}. \quad (2)$$

As $\{f_i/s_i\}$ is non-increasing and the marginal supply strictly increases with i , the equation (2) has no more than one solution. In the case the set in the right part of the equation is empty, a rational Bitcoin notary should create a block with no transactions ($i^* = 0$).

Supply and demand curves built based on blockchain data (Fig. 6, 7) show that the current behavior of Bitcoin notaries is partially altruistic, as they include into blocks transactions with lesser fee density than specified by Equation (2). As for small blocks

$$\frac{IR}{T} \exp\left(\frac{IS_i}{T}\right) \approx \frac{IR}{T},$$

the current default fee density $d_0 = 10$ satoshis / byte corresponds to the block propagation impedance $I_0 \approx Td_0/R \approx 2.5$ s / MB, which is significantly lower than the observed value. On the other hand, the fee density implied by (2) (≈ 30 satoshis per byte) is already satisfied for most small transactions.

Figure 7 shows that the transaction fees market is actively developing: although most transactions are still included into blocks altruistically, the percentage of transactions paying a market fee has increased from 22% to 37% in the last 6 months.

Block space supply (1) can be used to estimate absolute minimum transaction fees based on the average block size and block propagation impedance (Table 2; actual amount of fees could be substantially higher as we show in the following sections). Consider the following values for a medium-term estimation of the fee amount in the beginning of 2020:

- The block reward is planned to be cut in half in July 2016: $R = 12.5$ bitcoins.
- The expected time between the blocks will remain the same.
- Network impedance is expected to decrease 17.7% per year [39], which implies $I \approx 7.6/1.17^5 \approx 3.47$ seconds per megabyte. Although faster block relay can be implemented with various techniques (such as Bitcoin Relay Network [40] or invertible Bloom lookup tables [41]), we do not consider them in the fee calculations, as their adoption would change the incentives of Bitcoin notaries.

Table 2: Estimated minimum transaction fees that would compensate orphaning risks by the beginning of 2020 (the impedance $I \approx 3.5$ s / MB)

Block size, MB	Size growth per year, %	Fee / block, BTC	Fee, % of block reward	Orphan rate, %
1.1	17.1	0.08	0.64	0.63
2.2	34.5	0.16	2.76	1.26
6.4	66.5	0.47	5.86	3.63
16	100	1.21	9.79	8.83
32	130	2.54	14.0	16.9

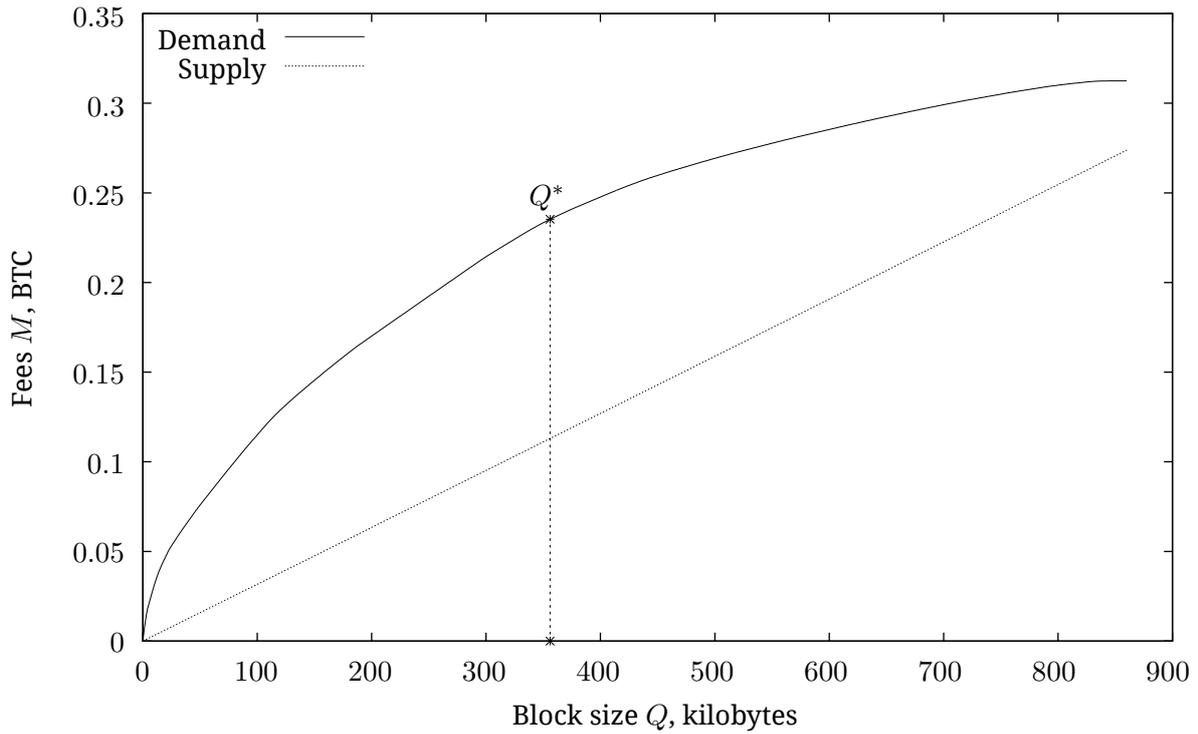


Figure 6: Supply and demand curves for transactions in the block #380,025. The optimal block size for the impedance $I = 7.6 \text{ s / MB}$ is $Q^* \approx 356$ kilobytes, i.e., about 40% of the actual block size (860 kB).

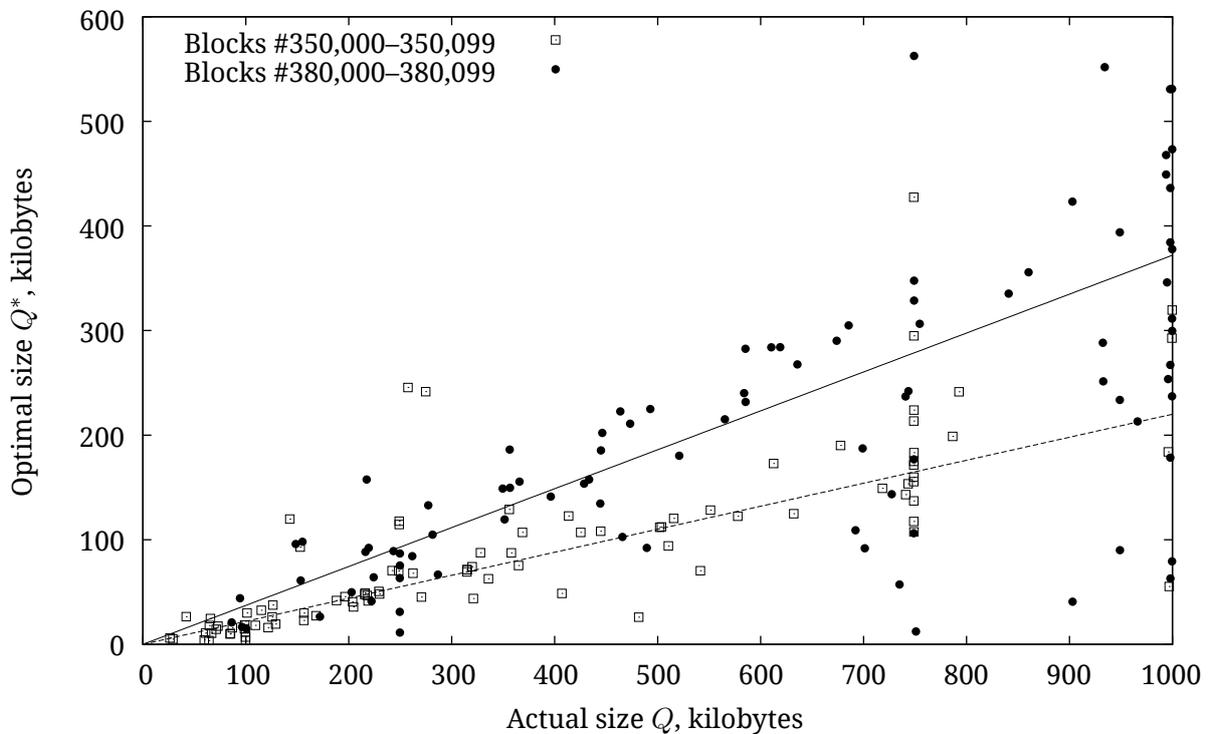


Figure 7: Actual and optimal block sizes for the impedance $I = 7.6 \text{ s / MB}$ calculated for two groups of blocks: created on March 31, 2015 (block heights 350,000–350,099) and on October 22, 2015 (block heights 380,000–380,099). Median ratios of the optimal size to the actual block size for these two groups (22% and 37%, respectively) are shown as lines.

We consider the following values of the block size Q :

- $Q = 1.17^5 \approx 2.2$ megabytes is the maximum block size in 2020 according to Peter Wuille's block size regulation proposal [39].
- $Q = 2.2/2 = 1.1$ megabytes is the average block size according to the same proposal under the assumption that it would be equal to approximately half of the maximum, as it is the case currently.
- Similarly, $Q = 32$ MB and $Q = 16$ MB are the maximum and the estimated average block sizes in 2020 set by Gavin Andresen's BIP 101 [42]. 32 megabytes is also the maximum size of a block that could be relayed in a single message according to the peer-to-peer protocol utilized in Bitcoin.
- $Q = 0.5 \cdot (0.5/0.3)^5 \approx 6.4$ megabytes corresponds to the observed increase of the average block size [37] from 0.3 megabytes to 0.5 megabytes in a span of 1 year (September 2014 – September 2015), provided that the trend continues for the next five years.

Table 2 includes the estimated orphan rate $1 - \exp(-IQ/T)$. The orphan rate becomes too high for 16 MB and 32 MB blocks; blocks of this size would necessitate changes to the Bitcoin protocol in order to diminish network impedance I . Invertible Bloom lookup tables, Bitcoin Relay Network and other Bitcoin scalability efforts could be capable of reducing the block relay impedance to $I \leq 0.1$ s / MB. This would mean an acceptable orphan rate of 2–3% for 100–200 MB blocks, which correspond to the global adoption of Lightning [17]. Acceptable transaction throughput capacity could also be partially achieved by processing a portion of transactions on sidechains pegged to the Bitcoin blockchain and / or by scalability efforts (the GHOST protocol [43], treechains [44]) diminishing the role of block orphaning in miners' risks.

The model described above is based on the assumption that Bitcoin notaries can vary the size of transaction blocks within a sufficiently wide interval. If this is not the case (e.g., if the maximum allowable block size is significantly lower than the demand created by transactions), transaction fees will be growing until excessive transactions are pushed off-chain and the transaction throughput reaches the supply of blockchain space provided by Bitcoin notaries. This scenario is difficult to analyze quantitatively, as, excluding short spikes in transaction volume caused by "stress tests" conducted in June, July and September of 2015 [45], the supply of blockchain space has always been higher than the demand placed on it.

The other factor not considered by the model is the marginal cost of maintaining the blockchain, which depends on the blockchain size and, thus, on the block size Q . As the block size has remained relatively small since Bitcoin's inception, it is difficult to draw any conclusion as to how much the growth of the block size would influence the cost of mining operations; however, it is quite clear that in the case of growth of transaction throughput, transaction fees would need to be raised to compensate for Bitcoin notaries' expenses. Whether or not the block size is limited by the protocol, blockchain space is a scarce resource, which facilitates the development of the transaction fee market.

Similarly, the above analysis would not apply if Bitcoin transactions are largely performed off-

chain as described in Section 2. In this case, fees on the remaining transactions would need to be raised in order to diminish the possibility of spam attacks on the network. In all off-chain payment methods pegged to the Bitcoin blockchain, spam attacks would constitute a major security issue, as they would complicate timely settlement of financial contracts between parties.

3.2 Bitcoin Exchange Rate

The Bitcoin exchange rate can be modeled on the proposition that the value of a network system depends on the number of its users. We use the version of the network value law [46] stating that the network value is proportional to $n \log n$, with n denoting the number of users. (The original law formulated by R. Metcalfe [47] states that the network value is proportional to n^2 ; our estimate is based on assumptions that more closely match empirical data). In the case of Bitcoin,

- the value of the network can be measured by the market capitalization of Bitcoin [48]. The capitalization translates into exchange rate as the amount of the currency is defined algorithmically (see Section 1.1).
- the measure of network participation n is the number of unique Bitcoin addresses [49] used during a certain time interval.

For both the market capitalization and the number of unique addresses, we use daily values averaged over calendar months.

The network participation can be estimated using quadratic function depending on time (Fig. 8). The estimate yields approximately 1.2 million addresses in use per day in 2020, i.e., 4.7 times the present value.

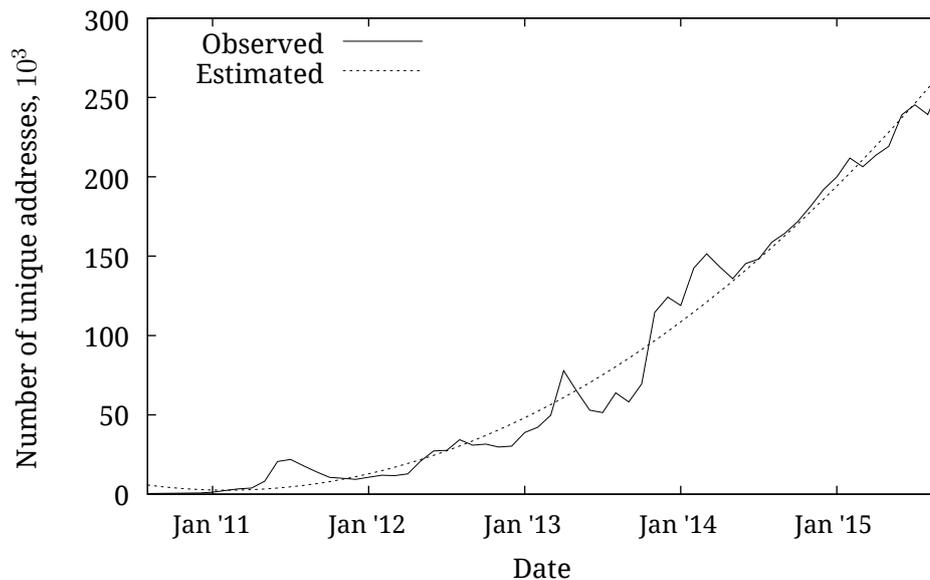


Figure 8: Network participation and the fitted quadratic approximation. The coefficient of determination of the fit is $r^2 = 98.1\%$.

Next, we use linear regression to determine the relationship between network effect factor $n \log n$ and the market capitalization. We use values since August 2010 to May 2013 as the training set; we believe that the values of market capitalization since the second half of 2013 until the beginning of 2015 have a speculative nature and do not reflect the value of the network. The resulting model (Fig. 9) has a satisfactory coefficient of determination $r^2 \approx 76\%$ on the training set. The Bitcoin market capitalization is estimated to be \$23.5 billion in December 2020, which corresponds to the exchange rate of \$1,270 per bitcoin. This estimate together with the lower bound estimate of transaction fees (0.5 bitcoins per block) yields the minimum amount of Bitcoin notaries' incentives at

$$(12.5 + 0.5) \cdot 144 \cdot \$1267 \approx \$2.4 \text{ million per day.}$$

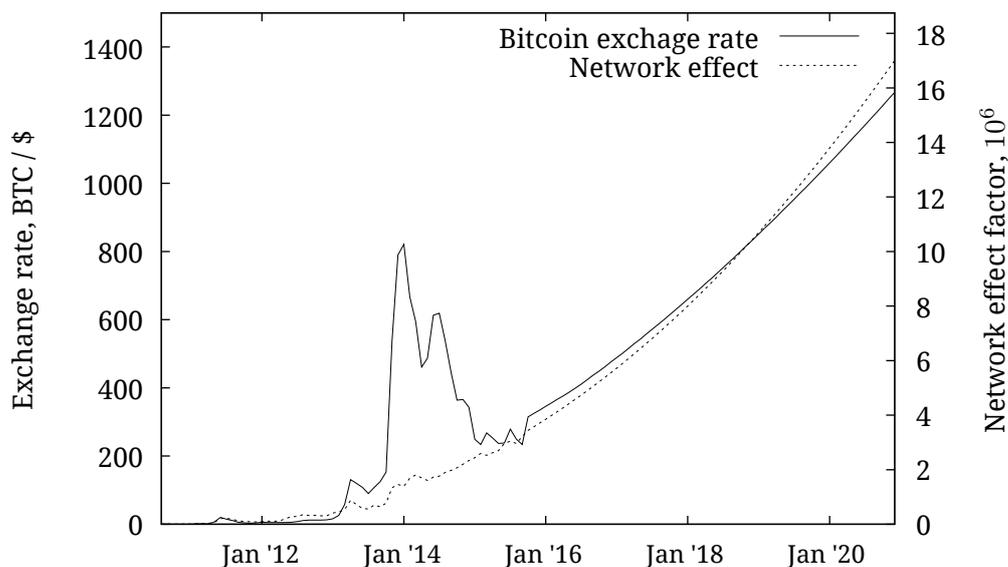


Figure 9: Network effect factor $n \log n$ and the Bitcoin exchange rate. Values up to October 2015 are actual; later values are based on the quadratic estimation of the network participation factor n and on the linear relationship between market capitalization and the network effect factor. As the Bitcoin supply grows with time, the estimated exchange rate is not precisely proportional to the estimated network effect factor.

The estimate above does not take into account innovative uses of the Bitcoin blockchain, e.g. in IoT applications; we consider these applications in the following sections. Arguably, the number of blockchain-enabled IoT devices would not correspond to the effective number of network users n one-to-one, as the devices form a more closed subsystem. Assuming that the effective Bitcoin participation factor would reach $n = 10^7$ in as soon as 2020, the estimated Bitcoin exchange rate would rise to \$12,100 / BTC; this value corresponds to the minimum aggregate amount of notarial incentives of \$22.6 million per day.

3.3 Emerging Bitcoin Applications

In all estimates below, we assume that the amount of notarial incentives [50] is approximately proportional to the transaction volume [51] and that this correlation is maintained when transaction volume

is partially performed off-chain. The ratio of the notarial incentives to the value of the transaction volume currently equals $\approx 1\%$; it will likely remain the same or slightly decrease to 0.8–0.9% in the medium term.

Assume there would be 25 billion devices constituting the Internet of Things in 2020, close to the lower bound of estimates referenced in Section 2. If 80% of these devices would be capable of blockchain support (i.e., they would be based on multi-purpose programmable platforms such as ARM chips), and 5% of these devices would actually use the Bitcoin blockchain or related infrastructure for transactions, there would be $25 \cdot 0.8 \cdot 0.05 = 1$ billion of blockchain-enabled devices by 2020. Additionally, we use the following assumptions [30]:

- Each device performs a value transaction each month (i.e., 12 transactions per year). Average transaction value would be quite small, as the emerging consumer-to-consumer market brings more small opportunities than centralized markets. We use the average value of \$5 per value transaction.
- Each device performs an operational transaction each day (i.e., 365 transactions per year). The average value of a single operational transaction is lower than for value transactions; we use the average value of \$0.1 per operational transaction.

Thus, the total value of the annual transaction volume of blockchain-enabled devices is

$$10^9 \cdot (12 \cdot \$5 + 365 \cdot \$0.1) \approx \$100 \text{ billion.}$$

With the notarial incentives equal to 1% of the value of the transaction volume, this implies notarial incentives of \$2.7 million daily.

Another estimate corresponds to the wide adoption of blockchain technology in IoT, which could be achieved by 2025–2030:

- There would be at least 10 billion blockchain-aware devices
- Each device would perform 1 value transaction per week (i.e., 52 transactions per year).

These assumptions yield the value of the annual transaction volume

$$10^{10} \cdot (52 \cdot \$5 + 365 \cdot \$0.1) \approx \$3 \text{ trillion,}$$

which translates to the notarial incentives of approximately \$81 million daily.

Similar estimates could be obtained using the amount of consumer-to-consumer payments estimated by a Wedbush Securities report on Bitcoin [52]. These kinds of Bitcoin payments are estimated to be \$125 billion in 2020, which equates to approximately \$3.4 million daily notarial incentives. By using the same methodology, the daily amount of notarial incentives related to consumer-to-consumer transactions is estimated to rise to \$65 million by 2025.

Although financial institutions currently are cautious about the use of the Bitcoin and other permissionless blockchains in financial applications, the development of a sizable consumer-to-consumer

market with high revenue opportunities would help them embrace the technology. If the value of the transaction volume generated by financial institutions adopting Bitcoin is equal to \$1 billion per day by 2020–2025 (which is 13 times the present volume and is equal to 7.8% of daily payments volume processed by Visa [53]), the notarial incentives associated with these transactions would be equal to \$11.5 million. \$1 billion per day of Bitcoin transactions can be viewed as conservative, as the World Economic Forum report [54] estimates that by 2027, transactions representing 10% of the global gross domestic product (i.e., order of \$10 trillion) will be stored using blockchain technology.

3.4 Role of Transaction Fees in Bitcoin Security

According to the previously discussed estimates of the bitcoin exchange rate and the value of Bitcoin transaction volume, transaction fees are estimated to play the increasing role in the notarial incentives (Table 3). Current transaction velocity [55] of Bitcoin is approximately 6 / year, which is consistent with the values in Table 3. The sources of the transaction fee growth would be

- growing number of applications using the Bitcoin blockchain or related blockchain technologies, which would also support an increasing bitcoin value
- increasing Bitcoin velocity, provided by the growing role of consumer-to-consumer and IoT-related applications.

Table 3: Role of transaction fees in the notarial incentives according to various plausible values of Bitcoin transaction velocity, which agree with estimations of the incentives from Section 3.3. The calculations are based on the ratio of the notarial incentives to the value of the transaction volume of 1%.

Year	Base assumptions	Velocity of Bitcoin, year ⁻¹	Annual tx volume, \$ billion	Daily notarial incentives, \$ million	Daily tx fees, \$ million	Fees, % of incentives
2020	1 BTC = \$1,270;	4.7	110	3	0.7	24
	12.5 BTC	6.3	146	4	1.7	43
	block reward	7.8	183	5	2.7	54
2025–2028	1 BTC = \$12,100;	3.8	913	25	19	78
	3.125 BTC	6.1	1,460	40	34	86
	block reward	7.6	1,825	50	44	89
		11.4	2,738	75	69	93

While in the short term, growth of the notarial incentives would be primarily the result of the increasing bitcoin exchange rate (caused by expanding Bitcoin applications and increasing the value stored on the Bitcoin blockchain), this link should diminish with the stabilization of Bitcoin ecosystem and dominance of transaction fees in the total notarial incentives. Under these assumptions, the incentives would chiefly depend on supply and demand of payment methods provided by Bitcoin and its competitors.

4 Conclusion

The incentives in the form of block rewards and transaction fees play an important role in maintaining the security of the Bitcoin network and preventing blockchain reorganization attacks. Transaction fees provide a means to prioritize inclusion of transactions into the blockchain, as well as an unobtrusive mechanism to contribute to the security of the Bitcoin network for Bitcoin users (i.e., to its protection against blockchain reorganizations and denial of service attacks).

While the focus on consumer-centric payments is likely to persist for Bitcoin in the short term, due to the limited supply of bitcoins and inadequacy of blockchains for real-time transaction processing, the Bitcoin blockchain could eventually be used as a means for settlement and clearing among permissionless (e.g. payment channels) and permissioned (e.g. sidechains) applications operating on top of it. That is, Bitcoin and other permissionless blockchains could act as the base layer of the next-generation financial ecosystem. With the advent of high-level trustless real-time infrastructure on top of the Bitcoin blockchain, fees on the remaining transactions could be substantially raised in order to prevent transaction spam attacks and to facilitate the transition of end customers to new services. Transaction fees would increase due to the growing demand on the limited blockchain space.

Machine-to-machine / Internet of Things payments could become a major driver of the value of the Bitcoin network, as blockchain technology provides opportunities to establish a ubiquitous payment infrastructure and an immutable data store for the Internet of Things. Decentralized consumer-to-consumer markets powered by the Bitcoin blockchain and related technologies could grow to trillions of US dollars.

The trajectory of growth of notarial incentives in Bitcoin is difficult to estimate. Emerging decentralized payment mechanisms (e.g., sidechains and Lightning) could push most current Bitcoin transactions off-chain, with remaining transactions representing high-value operations such as contract funding, settlement and clearing. Both consumer-to-consumer payments and use of Bitcoin in financial applications could provide substantial sources of the notarial incentives in the medium term. The notarial incentives are estimated at \$5–10 million daily by 2020 (which is five to ten times more than the present value) and at \$50–100 million daily by 2025. By 2020, transaction fees could constitute 50% or more of the notarial incentives due to increasing velocity of Bitcoin and the increased value secured with the Bitcoin blockchain; the amount of transaction fees as a percentage of total incentives could grow to 80–90% by 2025. The growth would be achieved due to both the increase in transaction fees and the growing Bitcoin exchange rate. With the stabilization of Bitcoin markets and the increasing role of transaction fees in notarial incentives, the role of the Bitcoin exchange rate is expected to diminish.

References

- [1] *Satoshi Nakamoto* (2008). Bitcoin: A peer-to-peer electronic cash system
URL: <https://bitcoin.org/bitcoin.pdf>
- [2] *Meni Rosenfeld* (2012). Analysis of hashrate-based double-spending
URL: <https://bitcoil.co.il/Doublespend.pdf>
- [3] (2015). Some miners generating invalid blocks
URL: <https://bitcoin.org/en/alert/2015-07-04-spv-mining>
- [4] Controlled supply. In: Bitcoin wiki
URL: https://en.bitcoin.it/wiki/Controlled_supply
- [5] Bitcoin clock
URL: <http://bitcoinclock.com/>
- [6] Transaction fees. In: Bitcoin Wiki
URL: https://en.bitcoin.it/wiki/Transaction_fees
- [7] BlockTrail: Bitcoin API and block explorer
URL: <https://www.blocktrail.com/BTC>
- [8] `src/rpcmining.cpp`. In: Bitcoin Core Github repository
URL: <https://github.com/bitcoin/bitcoin/blob/master/src/rpcmining.cpp>
- [9] `src/policy/policy.h`. In: Bitcoin Core Github repository
URL: <https://github.com/bitcoin/bitcoin/blob/master/src/policy/policy.h>
- [10] (2015). Limit mempool by throwing away the cheapest txn and setting min relay fee to it. In: Bitcoin Core Pull Requests
URL: <https://github.com/bitcoin/bitcoin/pull/6722>
- [11] Off-chain transactions. In: Bitcoin Wiki
URL: https://en.bitcoin.it/wiki/Off-Chain_Transactions
- [12] Coinbase
URL: <https://www.coinbase.com/>
- [13] Circle
URL: <https://www.circle.com/en>
- [14] ChangeTip
URL: <https://www.changetip.com/>
- [15] *Adam Back* (2015). improving development model
URL: <http://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-June/008844.html>
- [16] *Adam Back, Matt Corallo, Luke Dashjr et al.* (2014). Enabling blockchain innovations with pegged sidechains
URL: <https://www.blockstream.com/sidechains.pdf>
- [17] *Joseph Poon, Thaddeus Dryja* (2015). The Bitcoin Lightning Network: scalable off-chain instant payments
URL: <http://lightning.network/lightning-network-paper.pdf>
- [18] Funding network security. In: Bitcoin Wiki
URL: https://en.bitcoin.it/wiki/Funding_network_security
- [19] Assurance contract. In: English Wikipedia
URL: https://en.wikipedia.org/wiki/Assurance_contract
- [20] (2015) EB75 – Paul Brody: Internet of Things and the democracy of devices. In: Epicenter Bitcoin
URL: <https://letstalkbitcoin.com/blog/post/epicenter-bitcoin-75-paul-brody-internet-of-things-and-the-democracy-of-devices>

- [21] *Gartner* (2014). Gartner says 4.9 billion connected "things" will be in use in 2015
URL: <http://www.gartner.com/newsroom/id/2905717>
- [22] *Gartner* (2014). Gartner says the Internet of Things will transform the data center
URL: <http://www.gartner.com/newsroom/id/2684616>
- [23] *ABI Research* (2014). The Internet of Things will drive wireless connected devices to 40.9 billion in 2020
URL: <https://www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect/>
- [24] *John Chambers* (2014). Are you ready for the Internet of everything? In: World Economic Forum Agenda
URL: <https://agenda.weforum.org/2014/01/are-you-ready-for-the-internet-of-everything/>
- [25] *IDC* (2015). Explosive Internet of Things spending to reach \$1.7 trillion in 2020, according to IDC
URL: <http://www.idc.com/getdoc.jsp?containerId=prUS25658015>
- [26] *Accenture* (2014). 2014 state of the Internet of Things study from Accenture Interactive predicts 69 percent of consumers will own an in-home IoT device by 2019
URL: <https://newsroom.accenture.com/industries/systems-integration-technology/2014-state-of-the-internet-of-things-study-from-accenture-interactive-predicts-69-percent-of-consumers-will-own-an-in-home-iot-device-by-2019.htm>
- [27] *Machina Research* (2014). Consumer electronics M2M connections will top 7 billion in 2023, generating USD700 billion in annual revenue
URL: <https://machinaresearch.com/news/press-release-consumer-electronics-m2m-connections-will-top-7-billion-in-2023-generating-usd700-billion-in-annual-revenue/>
- [28] *IHS* (2013). Big Data in the driver's seat of connected car technological advances
URL: <http://press.ihs.com/press-release/country-industry-forecasting/big-data-drivers-seat-connected-car-technological-advance>
- [29] *Navigant Research* (2013). The installed base of smart meters will surpass 1 billion by 2022
URL: <http://www.navigantresearch.com/newsroom/the-installed-base-of-smart-meters-will-surpass-1-billion-by-2022>
- [30] Consultations by *Paul Brody* on the Internet of Things.
- [31] *Paul Snow, Brian Deery, Jack Lu, David Johnston, Peter Kirby* (2014). Factom: business processes secured by immutable audit trails on the blockchain
URL: https://github.com/FactomProject/FactomDocs/blob/master/Factom_Whitepaper.pdf
- [32] Merged mining specification. In: Bitcoin Wiki
URL: https://en.bitcoin.it/wiki/Merged_mining_specification
- [33] *Paul Snow, Brian Deery, Jack Lu, David Johnston, Peter Kirby* (2014). Factom: business processes secured by immutable audit trails on the blockchain
URL: https://github.com/FactomProject/FactomDocs/blob/master/Factom_Whitepaper.pdf
- [34] Total transaction fees. Blockchain.info
URL: <https://blockchain.info/charts/transaction-fees>
- [35] *Peter R* (2015). A transaction fee market exists without a block size limit
URL: <https://scalingbitcoin.org/papers/feemarket.pdf>
- [36] Orphan block. In: Bitcoin Wiki
URL: https://en.bitcoin.it/wiki/Orphan_Block
- [37] Average block size. Blockchain.info (retrieved on Oct 02, 2015)
URL: <https://blockchain.info/charts/avg-block-size?timespan=1year>
- [38] *Ralph Merkle* (1988). A digital signature based on a conventional encryption function. In: *Advances in Cryptology – CRYPTO '87* (Lecture Notes in Computer Science), Vol. 293, pp. 369–378
URL: http://link.springer.com/chapter/10.1007%2F3-540-48184-2_32

- [39] *Pieter Wuille* (2015). Block size following technological growth
URL: <https://gist.github.com/sipa/c65665fc360ca7a176a6>
- [40] The Bitcoin Relay Network
URL: <http://bitcoinrelaynetwork.org/>
- [41] *Gavin Andresen* (2014). O(1) block propagation
URL: <https://gist.github.com/gavinandresen/e20c3b5a1d4b97f79ac2>
- [42] *Gavin Andresen* (2015). Increase maximum block size (BIP 101)
URL: <https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki>
- [43] *Yonatan Sompolinsky, Aviv Zohar* (2013). Accelerating Bitcoin's transaction processing: fast money grows on trees, not chains
URL: <https://eprint.iacr.org/2013/881.pdf>
- [44] *Peter Todd* (2014). Tree-chains preliminary summary
URL: <http://www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg04388.html>
- [45] July 2015 flood attack. In: Bitcoin Wiki
URL: https://en.bitcoin.it/wiki/July_2015_flood_attack
- [46] *Bob Briscoe, Andrew Odlyzko, Benjamin Tilly* (2006). Metcalfe's law is wrong. In: IEEE Spectrum
URL: <http://spectrum.ieee.org/computing/networks/metcalfe-s-law-is-wrong>
- [47] Metcalfe's law. In: English Wikipedia
URL: https://en.wikipedia.org/wiki/Metcalfe's_law
- [48] Bitcoin (BTC) price, charts, and info. Crypto-Currency Market Capitalizations
URL: <http://coinmarketcap.com/currencies/bitcoin/>
- [49] Number of unique bitcoin addresses used. Blockchain.info
URL: <https://blockchain.info/charts/n-unique-addresses>
- [50] Miners revenue. Blockchain.info
URL: <https://blockchain.info/charts/miners-revenue?timespan=all>
- [51] Estimated USD transaction volume. Blockchain.info
URL: <https://blockchain.info/charts/estimated-transaction-volume-usd?timespan=all>
- [52] *Gil Luria, Aaron Turner* (2015). Bitcoin Investment Trust: equity research
URL: <http://scribd.com/doc/271095696/GBTC-Initiation-2015-07-09>
- [53] (2015) Visa: annual report 2014
URL: http://investor.visa.com/files/doc_downloads/annual%20meeting/2014/817762_BMK1.pdf
- [54] *Global Agenda Council on the Future of Software & Society* (2015). Deep shift: technology tipping points and societal impact
URL: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf
- [55] Velocity of money. In: English Wikipedia
URL: https://en.wikipedia.org/wiki/Velocity_of_money