Transaction-Confirmation Time for Bitcoin: A Queueing Analytical Approach to Blockchain Mechanism

Yoshiaki Kawase(✉) and Shoji Kasahara

Graduate School of Information Science, Nara Institute of Science and Technology, Takayama 8916-5, Ikoma, Nara 6300192, Japan
{kawase.yoshiaki.km3,kasahara}@is.naist.jp

Abstract. Bitcoin is a virtual currency based on a transaction-ledger database called blockchain. The blockchain is maintained and updated by mining process in which a number of nodes called miners compete for finding answers of very difficult puzzle-like problem. Transactions issued by users are grouped into a block, and the block is added to the blockchain when an algorithmic puzzle specialized for the block is solved. A recent study reveals that newly arriving transactions are not included in the block being under mining. In this paper, we model the mining process with a queueing system with batch service, analyzing the transaction-confirmation time. We consider an $M/\mathrm{G}^B/1$ with batch service, in which a newly arriving transaction cannot enter the service facility even when the number of transactions in the service facility does not reach the maximum batch size, i.e., the block-size limit. In this model, the sojourn time of a transaction corresponds to its confirmation time. We consider the joint distribution of the number of transactions in system and the elapsed service time, deriving the mean transaction-confirmation time. In numerical examples, we show how the block-size limit affects the transaction-confirmation time.

Keywords: Bitcoin · Blockchain · Transaction-confirmation time

1 Introduction

Bitcoin is an autonomous decentralized virtual currency that does not have a central server or administrator, and it succeeds to prevent fraud such as multiple payment and impersonation by encryption and peer-to-peer network technologies [1]. Bitcoin can provide immediate and secure service of international money transfer, and it is expected to be used for micropayment such as small amount remittance and billing of a piece of Internet content, due to its low fee [2]. Bitcoin demand grows rapidly in recent years, and the average number of transactions per day in 2016 is 226,000, which is about twice as much as the previous year's 125,000.

Bitcoin virtual-currency system is based on two data types: transaction and block. A transaction includes information indicating a specific amount of money

W. Yue et al. (Eds.): QTNA 2017, LNCS 10591, pp. 75–88, 2017.
https://doi.org/10.1007/978-3-319-68520-5_5

transferred from sender to recipient. On the other hand, a block consists of several transactions, and a newly generated block is confirmed by solving a puzzle-like problem. This confirmation process is called mining, and a number of nodes called miners compete for finding its answer. The difficulty of the puzzle-like problem is automatically adjusted so that mining finishes in 10 minutes on average [3]. A miner succeeds in mining, the miner receives reward called coinbase (currently 12.5 BTC in 2017) and transactions' remittance fees in the block. Note that miners keep mining work in order to get "coinbase" even when there are no transactions to be included into a block.

One of technical issues in Bitcoin is low transaction-processing speed due to the maximum block size [4]. In Bitcoin, newly arriving transactions are included in a block and confirmed by mining. Since the block size is limited to 1 MB and the time for mining is 10 min in average, the number of transactions processed per second is very small. In addition, Bitcoin system has transaction-priority mechanism, in which each transaction is prioritized according to its remittance amount, the elapsed time from previous approval, and the transaction-data size. A transaction is included in a block according to its priority value and the fee paid by user in advance [3]. Transactions with low remittance and/or low fee are likely not to be included in a block when the transaction arrival rate is high. It is reported in [5] that the recent block size is approaching the maximum block size, and therefore reducing the transaction size by separating part from transaction [6] have been proposed, however no agreement has been achieved for Bitcoin community.

In order to consider the scalability issue for Bitcoin, it is important to quantitatively characterize the transaction-confirmation process. Since transactions are processed in block basis, the transaction-confirmation process can be modeled as a single-server queueing system with batch service. In terms of the analysis for the single-server queue with batch service, the authors in [8] consider an $\mathrm{M}/\mathrm{G}^B/1$ queue and analyze the joint distribution of the number of customers in queue and the elapsed service time.

In [7], the authors consider an $\mathrm{M}/\mathrm{G}^B/1$ queue with priority mechanism, deriving the mean transaction-confirmation time for each transaction-priority class. In numerical experiments, they find quantitative difference between analysis and measured data. This results from the assumption based on default Bitcoin client mechanism, in which a newly arriving transaction is included in the block under mining if the number of transactions in the block is smaller than the block-size limit. They also find that the block-generation time follows an exponential distribution, conjecturing that a newly arriving transaction is not included in the block under mining.

In this paper, we consider a modified $\mathrm{M}/\mathrm{G}^B/1$ queueing model in which newly arriving transactions wait in queue even when the number of transactions is smaller than the maximum batch size. Because mining is done even if there is no transaction in system, we also assume that the system is always busy when there is no transaction in system. We analyze the joint distribution of the number of transactions in system and the elapsed service time, deriving the mean transaction-confirmation time. In numerical examples, we quantitatively evaluate the effects of the block size on the transaction-confirmation time.

The rest of this paper is organized as follows. We describe our queueing model in Sect. 2. The analysis of the queueing model is presented in Sect. 3 and some numerical examples are shown in Sect. 4. Finally, we conclude the paper in Sect. 5.

2 Queueing Model

Transactions arrive at the system according to a Poisson process with rate λ. The transactions are grouped into a block, and the block is confirmed when one of miners finds the answer of the puzzle-like problem. We define the block-generation time as the time interval between consecutive block-confirmation time points. Note that the block-generation time can be regarded as the service time for our queueing model. Let S_i $(i = 1, 2, \ldots)$ denote the ith block-generation time. We assume $\{S_i\}$'s are independent and identically distributed (i.i.d) and follow a distribution function $G(x)$. Let $g(x)$ denote the probability density function of $G(x)$. The mean block-generation time $E[S]$ is given by

$$E[S] = \int_0^\infty x\, dG(x) = \int_0^\infty x g(x)\, dx.$$

Transactions arriving to the system are served in a batch manner, and the maximum batch size is b. When a transaction arrives at the system, the transaction enters the queue. The transaction cannot enter the server at its arrival point even when the batch size under service is smaller than b or when the number of transactions in system is zero. In other words, the arriving transaction is served in the next block-generation time or later. This service is regarded as the gated service with multiple vacations [9], in which vacation periods are i.i.d and follow the same distribution of the service time.

3 Analysis

Let $N_s(t)$ denote the number of transactions in the server at time t, $N_q(t)$ the number of transactions in the queue at time t, and $X(t)$ the elapsed service time at t. We define $P_{m,n}(x,t)(m = 0, 1 \ldots, b,\ n = 0, 1, \ldots,\ x, t \geq 0)$ as

$$P_{m,n}(x,t)\, dx = Pr\left\{N_s(t) = m, N_q(t) = n, x < X(t) \leq x + dx\right\}.$$

Let $\xi(x)$ denote the hazard rate of the service time S, which is given by

$$\xi(x) = \frac{g(x)}{1 - G(x)}.$$

When $\lambda E[S] < b$ holds, the system is stable and limiting probabilities exist. Letting $P_{m,n}(x) = \lim_{t\to\infty} P_{m,n}(x,t)$, and $x(t)$ denote the differentiation of elapsed service time, we obtain

$$\frac{d}{dx}P_{m,n}(x) = -\{\lambda + \xi(x)\}P_{m,n}(x) + \lambda P_{m,n-1}(x), \quad 0 \leq m \leq b, \quad n \geq 1, \tag{1}$$

$$\frac{d}{dx}P_{m,0}(x) = -\{\lambda + \xi(x)\}P_{m,0}(x), \qquad 0 \leq m \leq b. \tag{2}$$

We have the following boundary conditions at $x = 0$

$$\begin{aligned} P_{b,n}(0) &= \sum_{m=0}^{b} \int_0^\infty P_{m,n+b}(x)\xi(x)dx, \qquad n \geq 0, \\ P_{m,n}(0) &= 0, \quad m = 0, 1, \ldots, b-1, \quad n \geq 1, \\ P_{k,0}(0) &= \sum_{m=0}^{b} \int_0^\infty P_{m,k}(x)\xi(x)dx, \qquad k = 0, 1, \ldots, b. \end{aligned}$$

The normalizing condition is given by

$$\sum_{n=0}^{\infty} \sum_{m=0}^{b} \int_0^\infty P_{m,n}(x)dx = 1.$$

We define the following probability generating functions (pgf's)

$$P(z_1, z_2; x) = \sum_{n=0}^{\infty} \sum_{m=0}^{b} P_{m,n}(x) z_1^m z_2^n, \tag{3}$$

$$P(z_1, z_2) = \int_0^\infty P(z_1, z_2; x)\, dx. \tag{4}$$

From (1) and (2), we obtain

$$\begin{aligned} \sum_{n=0}^{\infty} \sum_{m=0}^{b} \frac{d}{dx} P_{m,n}(x)\, z_1^m z_2^n = \sum_{n=0}^{\infty} \sum_{m=0}^{b} &-\{\lambda + \xi(x)\} P_{m,n}(x)\, z_1^m z_2^n \\ &+ \lambda z_2 \sum_{n=0}^{\infty} \sum_{m=0}^{b} P_{m,n}(x)\, z_1^m z_2^n. \end{aligned}$$

From the above equation and (3), we obtain

$$\begin{aligned} \frac{d}{dx} P(z_1, z_2; x) &= -\{\lambda + \xi(x)\} P(z_1, z_2; x) + \lambda z_2 P(z_1, z_2; x) \\ &= -\{\lambda(1 - z_2) + \xi(x)\} P(z_1, z_2; x). \end{aligned}$$

From this differential equation, $P(z_1, z_2; x)$ is given by

$$P(z_1, z_2; x) = P(z_1, z_2; 0) e^{-\lambda(1-z_2)x} \{1 - G(x)\}. \tag{5}$$

Multiplying (5) by $\xi(x)$, and integrating the equation, we obtain

$$\begin{aligned} \int_0^\infty P(z_1, z_2; x)\xi(x)\, dx &= \int_0^\infty P(z_1, z_2; 0) e^{-\lambda(1-z_2)x} \{1 - G(x)\} \frac{dG(x)}{1 - G(x)} \\ &= P(z_1, z_2; 0) \int_0^\infty e^{-\lambda(1-z_2)x} dG(x) \\ &= P(z_1, z_2; 0) G^*(\lambda - \lambda z_2), \end{aligned} \tag{6}$$

where $G^*(s)$ is the Laplace-Stieljes transform (LST) of $G(x)$ and given by

$$G^*(s) = \int_0^\infty e^{-s} dG(x).$$

From (3) and (6), we obtain

$$P(z_1, z_2; 0)G^*(\lambda - \lambda z_2) = \int_0^\infty \sum_{n=0}^{\infty} \sum_{m=0}^{b} P_{m,n}(x)\xi(x)\, dx\, z_1^m z_2^n. \tag{7}$$

Substituting $x = 0$ into (3) yields

$$\begin{aligned} P(z_1, z_2; 0) &= \sum_{n=0}^{\infty} \sum_{m=0}^{b} P_{m,n}(0)\, z_1^m z_2^n \\ &= \sum_{n=0}^{\infty} \sum_{m=0}^{b} \int_0^\infty P_{m,n+b}(x)\xi(x)\, dx\, z_1^b z_2^n \\ &+ \sum_{n=0}^{b-1} \sum_{m=0}^{b} \int_0^\infty P_{m,n}(x)\xi(x)\, dx\, z_1^n. \end{aligned} \tag{8}$$

Using (7) and (8), we obtain

$$\begin{aligned} P(z_1, z_2; 0) = \left(\frac{z_1}{z_2}\right)^b &\left\{ P(1, z_2; 0)G^*(\lambda - \lambda z_2) - \sum_{n=0}^{b-1} \sum_{m=0}^{b} \int_0^\infty P_{m,n}(x)\xi(x)\, dx\, z_2^n \right\} \\ &+ \sum_{n=0}^{b-1} \sum_{m=0}^{b} \int_0^\infty P_{m,n}(x)\xi(x)\, dx\, z_1^n. \end{aligned} \tag{9}$$

Substituting $z_1 = 1$ into (9), we obtain

$$\begin{aligned} P(1, z_2; 0) = \left(\frac{1}{z_2}\right)^b &\left\{ P(1, z_2; 0)G^*(\lambda - \lambda z_2) - \sum_{n=0}^{b-1} \sum_{m=0}^{b} \int_0^\infty P_{m,n}(x)\xi(x)\, dx\, z_2^n \right\} \\ &+ \sum_{n=0}^{b-1} \sum_{m=0}^{b} \int_0^\infty P_{m,n}(x)\xi(x)\, dx. \end{aligned}$$

Multiplying the above equation by z_2^b yields

$$\left\{ z_2^b - G^*(\lambda - \lambda z_2) \right\} P(1, z_2; 0) = \sum_{n=0}^{b-1} (z_2^b - z_2^n) \sum_{m=0}^{b} \int_0^\infty P_{m,n}(x)\xi(x)\, dx.$$

From the above equation, we obtain

$$P(1, z_2; 0) = \frac{\sum_{n=0}^{b-1} (z_2^b - z_2^n)\alpha_n}{z_2^b - G^*(\lambda - \lambda z_2)}, \tag{10}$$

where α_n is given by

$$\alpha_n = \sum_{m=0}^{b} \int_0^\infty P_{m,n}(x)\xi(x)\,dx.$$

Applying Rouche's theorem [9] to (10), we can show that the equation

$$z_2^b - G^*(\lambda - \lambda z_2) = 0, \tag{11}$$

has b roots inside $|z_2| = 1 + \epsilon$ for a small real number $\epsilon > 0$. One of them is $z_2 = 1$. Let $z_{2,k}^*(k = 1, 2, ..., b-1)$ denote the root of (11). From (10), we have the following $b-1$ equations

$$\sum_{n=0}^{b-1} \left\{ \left(z_{2,k}^*\right)^b - \left(z_{2,k}^*\right)^n \right\} \alpha_n = 0, \qquad k = 1, 2, ..., b-1. \tag{12}$$

From (9) and (10), we have

$$P(z_1, z_2; 0) = \left(\frac{z_1}{z_2}\right)^b \left\{ \frac{\sum_{n=0}^{b-1} \left(z_2^b - z_2^n\right) \alpha_n}{z_2^b - G^*(\lambda - \lambda z_2)} G^*(\lambda - \lambda z_2) - \sum_{n=0}^{b-1} \alpha_n z_2^n \right\} + \sum_{n=0}^{b-1} \alpha_n z_1^n. \tag{13}$$

From (4) and (5), we obtain

$$\begin{aligned} P(z_1, z_2) &= P(z_1, z_2; 0) \int_0^\infty e^{-\lambda(1-z_2)x} \{1 - G(x)\}\,dx \\ &= P(z_1, z_2; 0) \frac{1 - G^*(\lambda - \lambda z_2)}{\lambda(1 - z_2)}. \end{aligned} \tag{14}$$

Multiplying (14) by $\lambda(1 - z_2)$ and partially differentiating it by z_2, we have

$$\begin{aligned} \frac{\partial P(z_1, z_2)}{\partial z_2} \lambda(1 - z_2) - P(z_1, z_2)\lambda = \frac{\partial P(z_1, z_2; 0)}{\partial z_2} \{1 - G^*(\lambda - \lambda z_2)\} \\ - P(z_1, z_2; 0) \frac{\partial G^*(\lambda - \lambda z_2)}{\partial z_2}. \end{aligned}$$

Substituting $z_1 = z_2 = 1$ into the above equation, and noting that $P(1, 1) = 1$, we have

$$P(1, 1) = P(1, 1; 0)E[S] = 1.$$

Multiplying (14) by $z_2^b(z_2^b - G^*(\lambda - \lambda z_2))$ in order to calculate $P(1,1;0)$, we have

$$\begin{aligned} P(z_1,z_2;0)\, z_2^b \left\{ z_2^b - G^*(\lambda - \lambda z_2) \right\} &= z_1^b \sum_{n=0}^{b-1} \left(z_2^b - z_2^n \right) \alpha_n G^*(\lambda - \lambda z_2) \\ &\quad - z_1^b \left\{ z_2^b - G^*(\lambda - \lambda z_2) \right\} \sum_{n=0}^{b-1} \alpha_n z_2^n \\ &\quad + z_2^b \left\{ z_2^b - G^*(\lambda - \lambda z_2) \right\} \left(\sum_{n=1}^{b-1} \alpha_n z_1^n + \alpha_0 z_1 \right). \end{aligned}$$

Partially differentiating the above equation by z_2 and substituting $z_1 = z_2 = 1$, we obtain under the stability condition of $b > \lambda E[S]$

$$P(1,1;0) = \frac{\sum_{n=0}^{b-1} (b-n)\, \alpha_n}{b - \lambda E[S]}.$$

Hence, the normalizing condition is given by

$$\frac{\sum_{n=0}^{b-1} (b-n)\, \alpha_n}{b - \lambda E[S]} E[S] = 1. \tag{15}$$

From (12) and (15), α_n's are uniquely determined. From (13) and (14), we have

$$\begin{aligned} P(z_1,z_2) = \Bigg\{ \left(\frac{z_1}{z_2} \right)^b \frac{\sum_{n=0}^{b-1} (z_2^b - z_2^n) \alpha_n}{z_2^b - G^*(\lambda - \lambda z_2)} G^*(\lambda - \lambda z_2) - \left(\frac{z_1}{z_2} \right)^b \sum_{n=0}^{b-1} \alpha_n z_2^n \\ + \sum_{n=0}^{b-1} \alpha_n z_1^n \Bigg\} \frac{1 - G^*(\lambda - \lambda z_2)}{\lambda (1 - z_2)}. \end{aligned} \tag{16}$$

Partially differentiating (16) by z_1 and substituting $z_1 = z_2 = 1$, we obtain the mean number of transactions in the server as

$$\begin{aligned} \left(\frac{\partial P(z_1,z_2)}{\partial z_1} \right)_{z_1=1, z_2=1} &= \left\{ \frac{\sum_{n=0}^{b-1} (b-n) \alpha_n}{b - \lambda E[S]} E[S] \right\} \lambda E[S] \\ &= \lambda E[S]. \end{aligned}$$

Similarly partially differentiating (16) by z_2, and substituting $z_1 = z_2 = 1$, we obtain the mean number of transactions in the queue as

$$\begin{aligned} \left(\frac{\partial}{\partial z_2} P(z_1,z_2) \right)_{z_1=1, z_2=1} &= \frac{1}{2(b - \lambda E[S])} \Bigg(\lambda^2 E[S^2] - 2b(b - \lambda E[S]) - b(b-1) \\ &\quad + \sum_{n=0}^{b-1} \Big\{ \lambda E[S^2](b-n) + E[S]\{b(b-1) - n(n-1)\} + 2bE[S](b-n) \Big\} \alpha_n \Bigg). \end{aligned}$$

Hence, the mean number of transactions in the system $E[N]$ is given by

$$E[N] = \frac{1}{2(b-\lambda E[S])}\left(\lambda^2 E[S^2] - b(b-1) - 2(b-\lambda E[S])^2 + \sum_{n=0}^{b-1}\left\{\lambda E[S^2](b-n) + E[S]\{b(b-1) - n(n-1)\} + 2bE[S](b-n)\right\}\alpha_n\right).$$

Let T denote the transaction-confirmation time, the time interval from the arrival time point of a transaction to its departure one. From Little's theorem, the transaction-confirmation time is given by

$$\begin{aligned} E[T] &= \frac{E[N]}{\lambda} \\ &= \frac{1}{2\lambda(b-\lambda E[S])}\left(\lambda^2 E[S^2] - b(b-1) - 2(b-\lambda E[S])^2 + \sum_{n=0}^{b-1}\left\{\lambda E[S^2](b-n) + E[S]\{b(b-1) - n(n-1)\} + 2bE[S](b-n)\right\}\alpha_n\right). \end{aligned} \tag{17}$$

4 Numerical Examples

4.1 Distribution of Block-Generation Time

It is reported in [7] that the distribution of the block-generation time $G(x)$ is the exponential one given by

$$G(x) = 1 - e^{-\mu x}, \qquad \text{where} \quad \mu = 0.0018378995.$$

Then, $E[S]$ and $E[S^2]$ are given by

$$E[S] = \frac{1}{\mu} = 544.0993884, \qquad E[S^2] = \frac{2}{\mu^2} = 592088.2889,$$

The Laplace-Stieltjes transform (LST) of $G(x)$ is given by

$$G^*(s) = \frac{\mu}{s+\mu}.$$

With these settings, we calculate the mean transaction-confirmation time $E[T]$.

4.2 Comparison of Analysis and Simulation

In order to confirm the validity of the results of analysis, we conduct the Monte-Carlo simulation of the same model as the analysis. Figure 1 shows the comparison of analysis and simulation model for the transaction-confirmation time. In this figure, the horizontal axis represents the transaction arrival rate λ and the vertical one is the mean transaction-confirmation time $E[T]$. The block size is fixed at $b = 1000$ in the numerical simulation. It is shown from Fig. 1 that the analytical result is the same as simulation, confirming the validity of analysis.

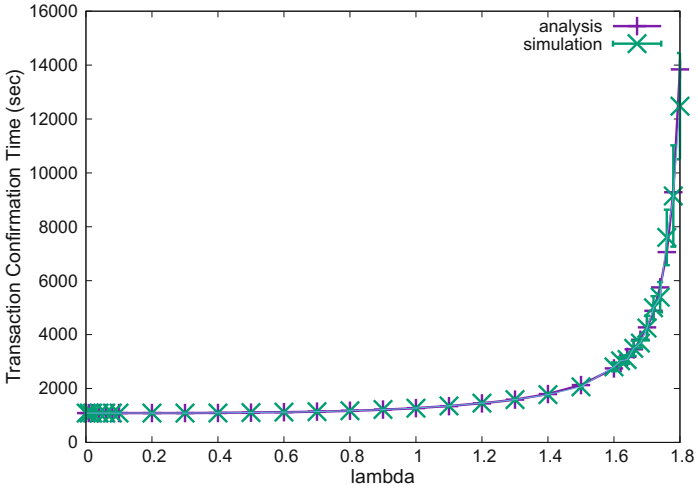

Fig. 1. Comparison of analysis and simulation model.

4.3 Comparison of Analysis and Measurement

In this subsection, we compare the analysis and measurement. In [7], the authors analyze two-year transaction data obtained from blockchain.info [5], reporting statistics such as the block-generation time, number of transactions in a block, and transaction-confirmation time. From the analysis of [7], the mean transaction size is 571.34 bytes, and hence the maximum block size b is set to 1750. Table 1 shows mean transaction-confirmation times of analysis and measurement. The analytical result is calculated with the mean transaction-arrival rate equal to 0.97091, which is obtained from measured data.

Table 1. Comparison of analysis and measurement.

Arrival rate	Measurement[s]	Analysis[s]
0.9709120529	1127.238651	1112.035745

Table 1 shows the results of measurement and analysis. We observe in this table that the analytical result is almost the same as the measurement value with relative error of 1.35%.

4.4 Comparison of Analysis and Trace-Driven Simulation

We conduct trace-driven simulation experiments for further validating our analytical model. We obtained two-year data of transaction-arrival time and block-generation time from [5], whose measurement period is from October 2013 to

September 2015. We perform simulation experiments driven by this data, investigating how the block size affects the transaction-confirmation time. Figure 2 shows the results of analysis and simulation. Here, we use two-year trace data for simulation, while the mean transaction-confirmation time of (17) is calculated with the mean arrival rate of two-year data. In Fig. 2, we observe a large discrepancy between analysis and simulation when the block size is small, while both results agree well with the increase in the block size.

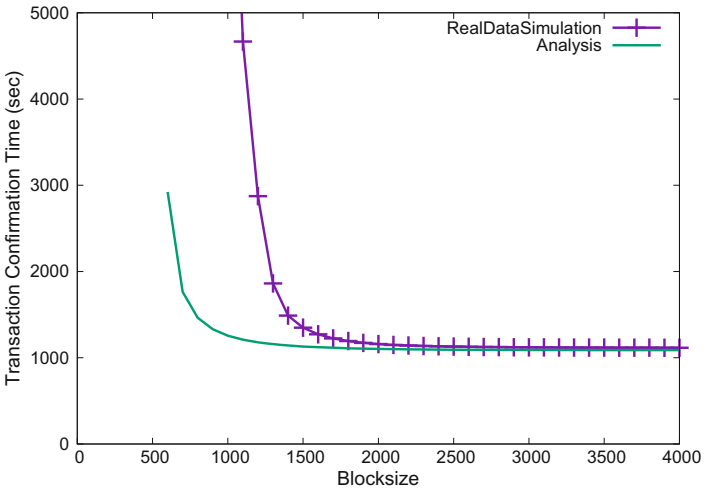

Fig. 2. Transaction-confirmation time vs. block size. The data measurement period is from October 2013 to September 2015, $\lambda = 0.9709120$, and $\mu = 0.0018378995$. The coefficient of variation of transaction inter-arrival time is 10.1789300.

Figures 3 and 4 represent the transaction-confirmation time against the block size. In Fig. 3, we use the trace data measured from October 2013 to September 2014, while the simulation result of Fig. 4 is based on the trace data measured from October 2014 to September 2015. Figure 3 shows a good agreement of analysis and simulation, however, we observe in Fig. 4 a discrepancy similar to Fig. 2.

In order to clarify the reason of these discrepancies, we investigate how the transaction arrival process evolves over time. Figure 5 shows the mean transaction-arrival rate per day. In this figure, we observe little variation during the first 12 months, while the mean transaction-arrival rate significantly varies for the last three months in the measured period.

Table 2 shows coefficients of variation for the three measurement periods: October 2013 to September 2014 (1st period), October 2014 to September 2015 (2nd period), and October 2013 to September 2015 (overall period). In this table, the coefficient of variation of the 2nd period is larger than that of 1st period. This large coefficient of variation of the 2nd period results in a large

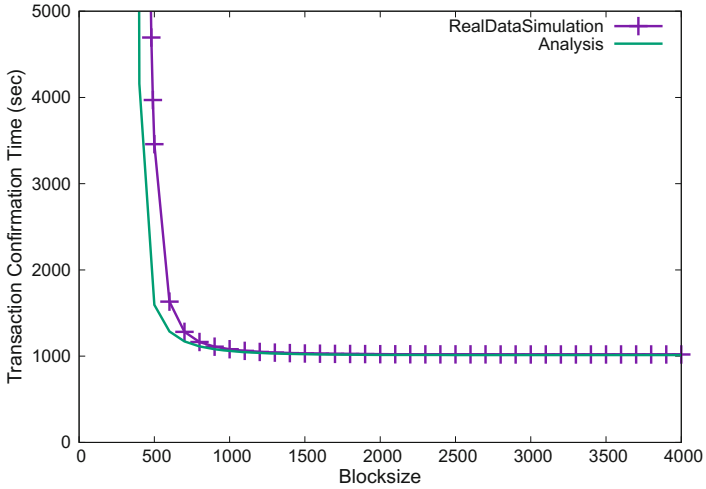

Fig. 3. Transaction-confirmation time vs. block size. The data measurement period is from October 2013 to September 2014, $\lambda = 0.7336929$, and $\mu = 0.0019748858$. The coefficient of variation of transaction inter-arrival time is 3.72401599.

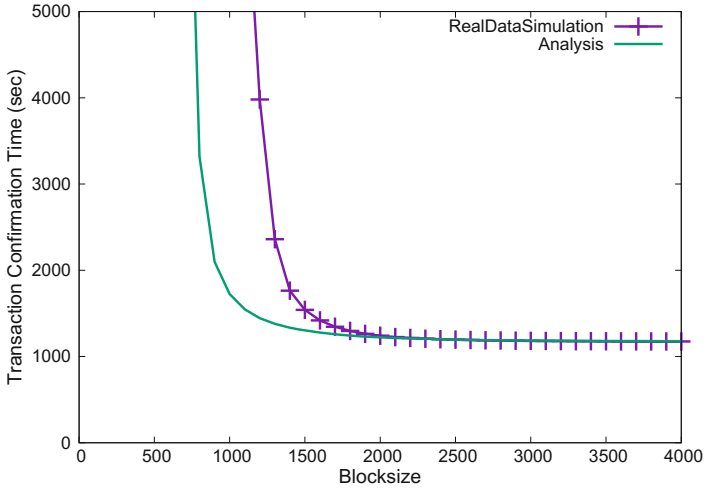

Fig. 4. Transaction-confirmation time vs. block size. The data measurement period is from October 2014 to September 2015, $\lambda = 1.2081311$, and $\mu = 0.0017009449$. The coefficient of variation of transaction inter-arrival time is 15.3250509.

coefficient of variation of the overall period, causing the discrepancy between analysis and simulation. When the block size is large, there is enough space to include transactions in the next block, and hence burst transaction arrivals are likely to be served in the next block. This causes little difference between analysis and simulation. On the other hand, when the block size is small, the system is

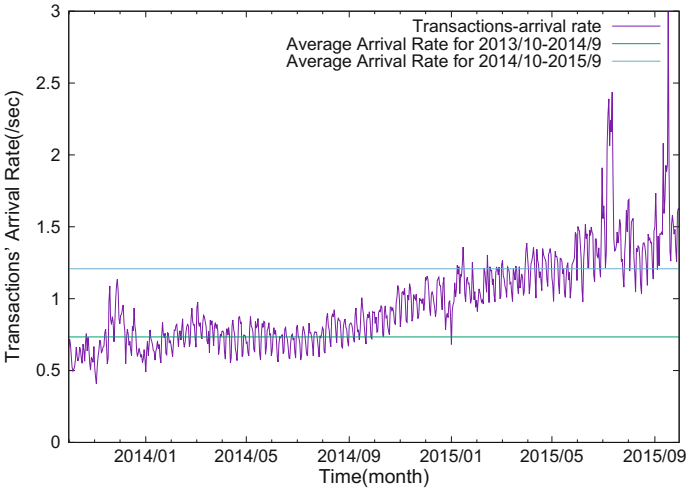

Fig. 5. The mean transaction-arrival rate.

likely to be congested due to the bursty nature of the transaction-arrival process. This results in a larger transaction-confirmation time for simulation than that for analysis.

Table 2. Coefficients of variation.

Period	2013/10–2014/09	2014/10–2015/09	2013/10–2015/09
Value	3.72401599	15.3250509	10.1789300

4.5 Impact of the Block Size on the Transaction-Confirmation Time

In this section, we investigate the effect of the block size on the transaction-confirmation time.

Figure 6 shows the analytical results with block size $b = 1000$, 2000, 4000, and 8000. We observe that the transaction-confirmation time grows with the increase in the arrival rate. From [7], the maximum number of transactions included in the current maximum block size 1MB is approximately given by $b = 1750$. This value is close to $b = 2000$, diverging around $\lambda = 3.6$.

We also observe that enlarging the block size results in a small transaction-confirmation time. However, the transaction-confirmation time for $b = 8000$ rapidly increases when λ is greater than 13 transaction per second. This implies that enlarging the block size does not solve the scalability issue fundamentaly.

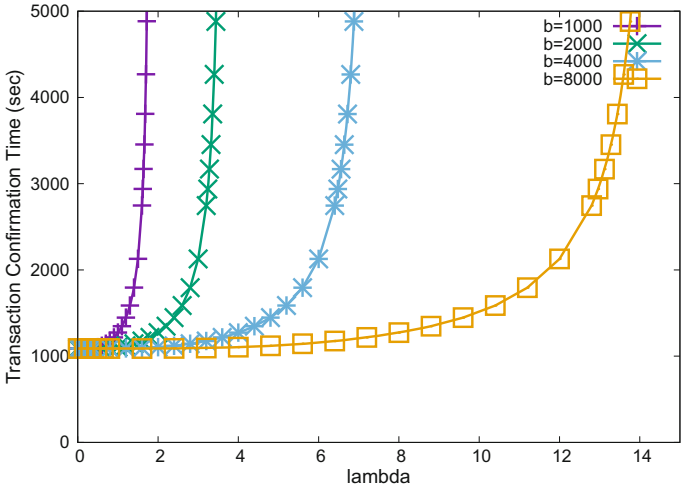

Fig. 6. The effects of the block size on the transaction-confirmation time.

5 Conclusion and Future Work

In this paper, we analyzed the transaction-confirmation time for Bitcoin using a single-server queue model with batch service $M/G^B/1$. In this queuing model, newly arriving transactions are temporarily stored in the queue first even when the number of transactions in the server is smaller than the batch size. We analyzed the mean transaction-confirmation time, and validated it by comparing simulation, and evaluated effects of the block size and transaction-arrival rate on the transaction-confirmation time. We found that the transaction-confirmation time can be decreased by changing the maximum block size. However, its improvement is not effective enough to increase the number of transactions processed per unit time.

In Bitcoin system, priority mechanism is implemented, in which the priority value of a transaction is determined according to transaction attributes such as remittance amount, data size, coin age and fee. It is important to analyze the transaction-confirmation time for the model in which the priority mechanism is taken into consideration. Other topic recently focused on in Bitcoin community is lightening network, which provides a channel dedicated to micropayment transactions [11]. The lightening network is expected to mitigate the overloaded block-generation process, however, it is not clear how the lightening network decreases the transaction-confirmation time. Developing analytical models for the above issues is also our future work.

Acknowledgments. This research was supported in part by SCAT Foundation, and Japan Society for the Promotion of Science under Grant-in-Aid for Scientific Research (B) No. 15H04008.

References

1. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008). https://bitcoin.org/bitcoin.pdf
2. http://www.meti.go.jp/committee/kenkyukai/sansei/fintech_kadai/pdf/003_02_00.pdf
3. Antonopoulos, A.M.: Mastering Bitcoin. O'Reilly (2014)
4. http://www.coindesk.com/1mb-block-size-today-bitcoin/
5. https://blockchain.info/
6. http://www.coindesk.com/segregated-witness-bitcoin-block-size-debate/
7. Kasahara, S., Kawahara, J.: Effect of Bitcoin fee on transaction-confirmation process. arXiv:1604.00103 [cs.CR]
8. Chaudhry, M.L., Templeton, J.G.C.: The queing system $M/G^B/1$ and its ramifications. Eur. J. Oper. Res. **6**, 56–60 (1981)
9. Takagi, H.: Queueing Analysis: A Foundation of Performance Evaluation vol. 1, Vacation and Priority Systems, Part 1, North-Holland (1991)
10. https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki
11. Poon, J., Dryja, T.: The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments (2016). https://lightning.network/lightning-network-paper.pdf