Li *et al. Comput Soc Netw* (2019) 6:5
https://doi.org/10.1186/s40649-019-0066-1

Computational Social Networks

RESEARCH Open Access

Markov processes in blockchain systems

Quan-Lin Li[1*†], Jing-Yu Ma[2†], Yan-Xia Chang[3†], Fan-Qi Ma[2†] and Hai-Bo Yu[1†]

*Correspondence: liquanlin@tsinghua.edu.cn
†All authors contributed equally to this work.
[1] School of Economics and Management, Beijing University of Technology, Beijing 100124, China
Full list of author information is available at the end of the article

Abstract

In this paper, we develop a more general framework of block-structured Markov processes in the queueing study of blockchain systems, which can provide analysis both for the stationary performance measures and for the sojourn time of any transaction or block. In addition, an original aim of this paper is to generalize the two-stage batch-service queueing model studied in Li et al. (Blockchain queue theory. In: International conference on computational social networks. Springer: New York; 2018. p. 25–40) both "from exponential to phase-type" service times and "from Poisson to MAP" transaction arrivals. Note that the MAP transaction arrivals and the two stages of PH service times make our blockchain queue more suitable to various practical conditions of blockchain systems with crucial factors, for example, the mining processes, the block generations, the blockchain building and so forth. For such a more general blockchain queueing model, we focus on two basic research aspects: (1) using the matrix-geometric solution, we first obtain a sufficient stable condition of the blockchain system. Then, we provide simple expressions for the average stationary number of transactions in the queueing waiting room and the average stationary number of transactions in the block. (2) However, on comparing with Li et al. (2018), analysis of the transaction–confirmation time becomes very difficult and challenging due to the complicated blockchain structure. To overcome the difficulties, we develop a computational technique of the first passage times by means of both the PH distributions of infinite sizes and the *RG* factorizations. Finally, we hope that the methodology and results given in this paper will open a new avenue to queueing analysis of more general blockchain systems in practice and can motivate a series of promising future research on development of blockchain technologies.

Keywords: Blockchain, Bitcoin, Markovian arrival process (MAP), Phase type (PH) distribution, Matrix-geometric solution, Block-structured Markov process, *RG* factorization

Introduction

Background and motivation

Blockchain is one of the most popular issues discussed extensively in recent years, and it has already changed people's lifestyle in some real areas due to its great impact on finance, business, industry, transportation, healthcare and so forth. Since the introduction of Bitcoin by Nakamoto [1], blockchain technologies have obtained many important advances in both basic theory and real applications up to now. Readers may refer to, for example, excellent books by Wattenhofer [2], Prusty [3], Drescher [4], Bashir [5] and Parker [6]; and survey papers by Zheng et al. [7], Constantinides et al. [8], Yli-Huumo et al. [9], Plansky et al. [10], Lindman et al. [11] and Risius and Spohrer [12].

It may be necessary and useful to further remark several important directions and key research as follows: (1) smart contracts by Par [13], Bartoletti and Pompianu [14], Alharby and van Moorsel [15] and Magazzeni et al. [16]; (2) ethereum by Diedrich [17], Dannen [18], Atzei et al. [19] and Antonopoulos and Wood [20]; (3) consensus mechanisms by Wang et al. [21], Debus [22], Pass et al. [23], Pass and Shi [24] and Cachin and Vukolić [25]; (4) blockchain security by Karame and Androulaki [26], Lin and Liao [27] and Joshi et al. [28]; (5) blockchain economics by Swan [29], Catalini and Gans [30], Davidson et al. [31], Bheemaiah [32], Becket al. [33], Biais et al. [34], Kiayias et al. [35] and Abadi and Brunnermeier [36]. In addition, there are still some important topics including the mining management, the double spending, PoW, PoS, PBFT, withholding attacks, pegged sidechains and so on. Also, their investigations may be well understood from the references listed above.

Recently, blockchain has become widely adopted in many real applications. Readers may refer to, for example, Foroglou and Tsilidou [37], Bahga and Madisetti [38] and Xu et al. [39]. At the same time, we also provide a detailed observation on some specific perspectives, for instance, (1) blockchain finance by Tsai et al. [40], Nguyen [41], Tapscott and Tapscott [42], Treleaven et al. [43] and Casey et al. [44]; (2) blockchain business by Mougayar [45], Morabito [46], Fleming [47], Beck et al. [48], Nowiński and Kozma [49] and Mendling et al. [50]; (3) supply chains under blockchain by Hofmann et al. [51], Korpela et al. [52], Kim and Laskowski [53], Saberi et al. [54], Petersen et al. [55], Sternberg and Baruffaldi [56] and Dujak and Sajter [57]; (4) internet of things under blockchain by Conoscenti et al. [58], Bahga and Madisetti [59], Dorri et al. [60], Christidis and Devetsikiotis [61] and Zhang and Wen [62]; (5) sharing economy under blockchain by Huckle et al. [63], Hawlitschek et al. [64], De Filippi [65], and Pazaitis et al. [66]; (6) healthcare under blockchain by Mettler [67], Rabah [68], Griggs et al. [69] and Wang et al. [70]; (7) energy under blockchain by Oh et al. [71], Aitzhan and Svetinovic [72], Noor et al. [73] and Wu and Tran [74].

Based on the above discussion, whether it is theoretical research or real applications, we always hope to know how performance of the blockchain system is obtained, and whether there is still some room to be able to further improve performance of the blockchain system. For this, it is a key to find solution of such a performance issue in the study of blockchain systems. Thus, we need to provide mathematical modeling and analysis for blockchain performance evaluation by means of, for example, Markov processes, Markov decision processes, queueing networks, Petri networks, game models and so on. Unfortunately, so far only a little work has been on performance modeling of blockchain systems. Therefore, this motivates us in this paper to develop Markov processes and queueing models for a more general blockchain system. We hope that the methodology and results given in this paper will open a new avenue to Markov processes of blockchain systems and can motivate a series of promising future research on development of blockchain technologies.

Related work

Now, we provide several different classes of related work for Markov processes in blockchain systems, for example, queueing models, Markov processes, Markov decision processes, random walks, fluid limit and so on.

Queueing models

To use queueing theory to model a blockchain system, we need to observer some key factors, for example, transaction arrivals, block generation, blockchain-building, block size, transaction fee, mining pools, mining reward, solving difficulty of crypto mathematical puzzle, throughput and so forth. As shown in Fig. 1, we design a two-stage, Service-In-Random-Order and batch service queueing system by means of two stages of asynchronous processes: block generation and blockchain building. Li et al. [75] is the first one to provide a detailed analysis for such a blockchain queue by means of the matrix-geometric solution. Kasahara and Kawahara [76] and Kawase and Kasahara [77] discussed the blockchain queue with general service times through an incompletely solving idea, which has still been for dealing with an interesting open problem up to now. In addition, they also gave some useful numerical experiments for performance observation. Ricci et al. [78] proposed a framework encompassing machine learning and a queueing model, which is used to identify which transactions will be confirmed and to characterize the confirmation time of a confirmed transaction. Memon et al. [79] proposed a simulation model for the blockchain systems by means of queuing theory.

Bowden et al. [80] discussed time-inhomogeneous behavior of the block arrivals in the bitcoin blockchain because the block-generation process is influenced by several key factors such as the solving difficulty level of crypto mathematical puzzle, transaction fee, mining reward, and mining pools. Papadis et al. [81] applied the time-inhomogeneous block arrivals to set up some Markov processes to study evolution and dynamics of blockchain networks and discussed key blockchain characteristics

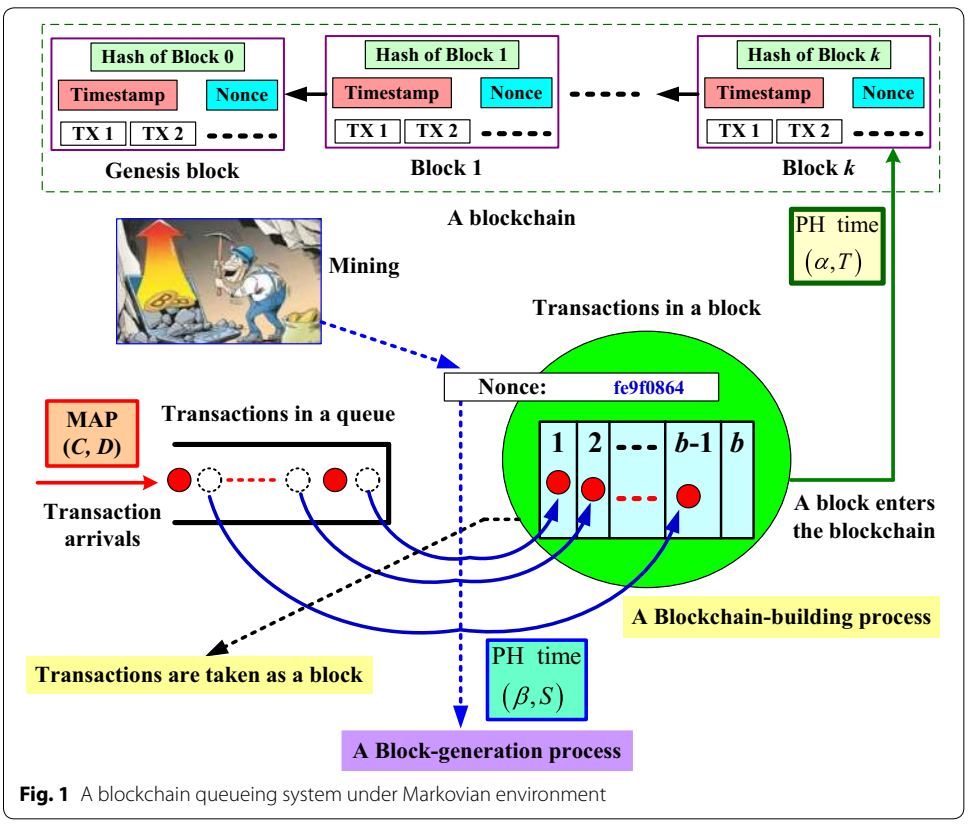

Fig. 1 A blockchain queueing system under Markovian environment

such as the number of miners, the hashing power (block completion rates), block dissemination delays, and block confirmation rules. Further, Jourdan et al. [82] proposed a probabilistic model of the bitcoin blockchain by means of a transaction and block graph and formulated some conditional dependencies induced by the bitcoin protocol at the block level. Based on analysis in the two papers, it is clear that when the block-generation arrivals are a time-inhomogeneous Poisson process, we believe that the blockchain queue analyzed in this paper will become very difficult and challenging and, thus, it will be an interesting topic in our future study.

Markov processes

To evaluate performance of a blockchain system, Markov processes are a basic mathematical tool, e.g., see Bolch et al. [83] for more details. As an early key work to apply Markov processes to blockchain performance issues, Eyal and Sirer [84] established a simple Markov process to analyze the vulnerability of Nakamoto protocols through studying the block-forking behavior of blockchain. Note that some selfish miners may get higher payoffs by violating the information propagation protocols and postponing their mined blocks such that such selfish miners exploits the inherent block forking phenomenon of Nakamoto protocols. Nayak et al. [85] extended the work by Eyal and Sirer [84] through introducing a new mining strategy: stubborn mining strategy. They used three improved Markov processes to further study the stubborn mining strategy and two extensions: the Equal-Fork Stubborn (EFS) and the Trail Stubborn (TS) mining strategies. Carlsten [86] used the Markov process to study the impact of transaction fees on the selfish mining strategies in the bitcoin network. Göbel et al. [87] further considered the mining competition between a selfish mining pool and the honest community by means of a two-dimensional Markov process, in which they extended the Markov model of selfish mining by considering the propagation delay between the selfish mining pool and the honest community.

Kiffer and Rajaraman [88] provided a simple framework of Markov processes for analyzing consistency properties of the blockchain protocols and used some numerical experiments to check the consensus bounds for network delay parameters and adversarial computing percentages. Huang et al. [89] set up a Markov process with an absorbing state to analyze performance measures of the Raft consensus algorithm for a private blockchain.

Markov decision processes

Note that the selfish miner may adopt different mining policies to release some blocks under the longest-chain rule, which is used to control the block-forking structure. Thus, it is interesting to find an optimal mining policy in the blockchain system. To do this, Sapirshtein et al. [90], Sompolinsky and Zohar [91] and Gervais et al. [92] applied the Markov decision processes to find the optimal selfish-mining strategy, in which four actions: adopt, override, match and wait, are introduced in order to control the state transitions of the Markov decision process.

Random walks

Goffard [93] proposed a random walk method to study the double-spending attack problem in the blockchain system and focused on how to evaluate the probability of the double-spending attack ever being successful. Jang and Lee [94] discussed profitability of the double-spending attack in the blockchain system through using the random walk of two independent Poisson counting processes.

Fluid limit

Frolkova and Mandjes [95] considered a bitcoin-inspired infinite-server model with a random fluid limit. King [96] developed the fluid limit of a random graph model to discuss the shared ledger and the distributed ledger technologies in the blockchain systems.

Contributions

The main contributions of this paper are twofold. The first contribution is to develop a more general framework of block-structured Markov processes in the study of blockchain systems. We design a two-stage, Service-In-Random-Order and batch service queueing system, whose original aim is to generalize the blockchain queue studied in Li et al. [75] both "from exponential to phase-type" service times and "from Poisson to MAP" transaction arrivals. Note that the transaction MAP arrivals and two stages of PH service times make our new blockchain queueing model more suitable to various practical conditions of blockchain systems. Using the matrix-geometric solution, we obtain a sufficient stable condition of the more general blockchain system and provide simple expressions for two key performance measures: the average stationary number of transactions in the queueing waiting room, and the average stationary number of transactions in the block.

The second contribution of this paper is to provide an effective method for computing the average transaction–confirmation time of any transaction in a more general blockchain system. In general, it is always very difficult and challenging to analyze the transaction–confirmation time in the blockchain system with MAP inputs and PH service times, because the service discipline of the blockchain system is new from two key points: (1) the "block service" is a class of batch service and (2) some transactions are chosen into a block by means of the Service-In-Random-Order. In addition, the MAP inputs and PH service times also make analysis of the blockchain queue more complicated. To study the transaction–confirmation time, we set up a Markov process with an absorbing state (see Fig. 4) according to the blockchain system (see Figs. 1 and 2). Based on this, we show that the transaction–confirmation time of any transaction is the first passage time of the Markov process with an absorbing state, hence we can discuss the transaction–confirmation time (or the first passage time) by means of both the PH distributions of infinite sizes and the RG factorizations. Based on this, we propose an effective algorithm for computing the average transaction–confirmation time of any transaction. We hope that our approach given in this paper can be applicable to deal with the transaction–confirmation times in more general blockchain systems.

The structure of this paper is organized as follows. "Model description" section describes a two-stage, Service-In-Random-Order and batch service queueing system,

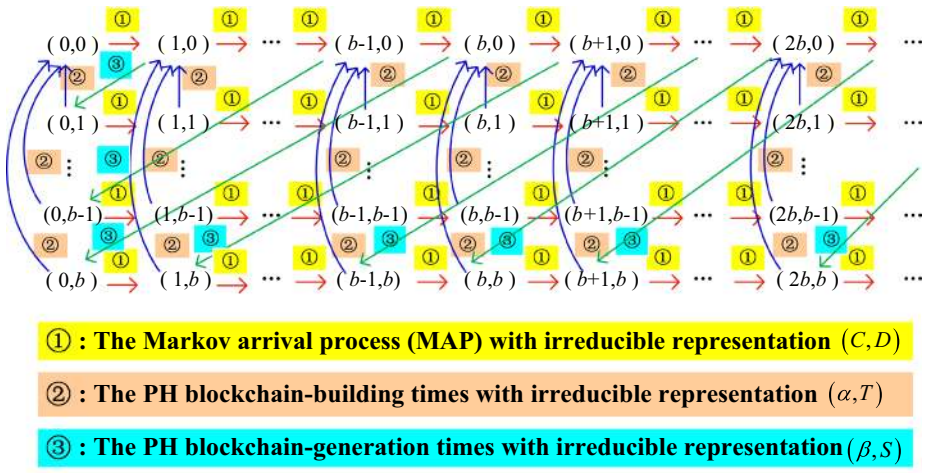

Fig. 2 State transition relations of the Markov process

where the transactions arrive at the blockchain system according to a Markovian arrival process (MAP), the block-generation and blockchain-building times are all of phase type (PH). "A Markov process of GI/M/1 type" section establishes a continuous-time Markov process of GI/M/1 type, derives a sufficient stable condition of the blockchain system, and expresses the stationary probability vector of the blockchain system by means of the matrix-geometric solution. "The stationary transaction numbers" section provides simple expressions for the average stationary number of transactions in the queueing waiting room, the average stationary number of transactions in the block, and uses some numerical examples to verify computability of our theoretical results. To compute the average transaction–confirmation time of any transaction, "The transaction–confirmation time" section develops a computational technique of the first passage times by means of both the PH distributions of infinite sizes and the *RG* factorizations. Finally, some concluding remarks are given in last section.

Model description

In this section, from a more general point of view of blockchain, we design an interesting and practical blockchain queueing system, where the transactions arrive at the blockchain system according to a Markovian arrival process (MAP), while the block-generation and blockchain-building times are all of phase type (PH).

From a more practical background of blockchain, it is necessary to extend and generalize the blockchain queueing model, given in Li et al. [75], to a more general case not only with non-Poisson transaction inputs but also with non-exponential block-generation and blockchain-building times. At the same time, we further abstract the block-generation and blockchain-building processes as a two-stage, Service-In-Random-Order and batch service queueing system by means of the MAP and the PH distribution. Such a blockchain queueing system is depicted in Fig. 1.

From Fig. 1, now we provide some model descriptions as follows:

Arrival process

Transactions arrive at the blockchain system according to a Markovian arrival process (MAP) with matrix representation (C, D) of order m_0, where the matrix $C + D$ is the infinitesimal generator of an irreducible Markov process; C indicates the state transition rates that only the random environment changes without any transaction arrival, D denotes the arrival rates of transactions under the random environment C; $(C + D)e = 0$, and e is a column vector of suitable size in which each element is one. Obviously, the Markov process $C + D$ with finite states is irreducible and positive recurrent. Let ω be the stationary probability vector of the Markov process $C + D$, it is clear that $\omega(C + D) = 0$ and $\omega e = 1$. Also, the stationary arrival rate of the MAP is given by $\lambda = \omega De$.

In addition, we assume that each arriving transaction must first enter a queueing waiting room of infinite size. See the lower left part corner of Fig. 1.

A block-generation process

Each arriving transaction first needs to enter a waiting room. Then, it may be chosen into a block of the maximal size b. This is regarded as the first stage of service, called a *block-generation* process. Note that the arriving transactions will be continually chosen into the block until the block-generation process is over under which a nonce is appended to the block by a mining winner. See the lower middle part of Fig. 1 for more details.

The block-generation time begins the initial epoch of a mining process until a nonce of the block is found (i.e., the cryptographic mathematical puzzle is solved for sending a nonce to the block), then the mining process is terminated immediately. We assume that all the block-generation times are i.i.d., and are of phase type with an irreducible representation (β, S) of order m_2, where $\beta e = 1$, the expected blockchain-building time is given by $1/\mu_2 = -\beta S^{-1} e$.

The block-generation discipline

A block can consist of some transactions but at most b transactions. Once the mining process begins, the transactions in the queueing waiting room are chosen into a block, but they are not completely based on the First Come First Service (FCFS) from the order of transaction arrivals. For example, several transactions in the back of this queue are possible to be chosen into the block. When the block is formed, it will not receive any new arriving transaction again. See the lower middle part of Fig. 1.

A blockchain-building process

Once the mining process is over, the block with a group of transactions will be pegged to a blockchain. This is regarded as the second stage of service due to the network latency, called a *blockchain-building* process, see the lower right corner of Fig. 1. In addition, the upper part of Fig. 1 also outlines the blockchain and the internal structure of every block.

In the blockchain system, we assume that the blockchain-building times are i.i.d, and have a common PH distribution with an irreducible representation (α, T) of order m_1, where $\alpha e = 1$, and the expected block-generation time is given by $1/\mu_1 = -\alpha T^{-1} e$.

The maximum block size

To avoid the spam attacks, the maximum size of each block is limited. We assume that there are at most b transactions in each block. If there are more than b transactions in the queueing waiting room, then the b transactions are chosen into a full block so that those redundant transactions are still left in the queueing waiting room, and they find a new choice to set up another possible block. In addition, the block size b maximizes the batch service ability in the blockchain system.

Independence

We assume that all the random variables defined above are independent of each other.

Remark 1 This paper is the first one to consider a blockchain system with non-Poisson transaction arrivals (MAPs) and with non-exponential block-generation and blockchain-building times (PH distributions), and it also provides a detailed analysis for the blockchain queueing model by means of the block-structured Markov processes and the *RG* factorizations. However, so far analysis of the blockchain queues with renewal arrival process or with general service time distributions has still been an interesting open problem in queueing research of blockchain systems.

Remark 2 In the blockchain system, there are some key factors including the maximum block size, mining reward, transaction fee, mining strategy, security of blockchain and so on. Based on this, we may develop reward queueing models, decision queueing models, and game queueing models in the study of blockchain systems. Therefore, analysis for the key factors will be not only theoretically necessary but also practically important in development of blockchain technologies.

A Markov process of GI/M/1 type

In this section, to analyze the blockchain queueing system, we first establish a continuous-time Markov process of GI/M/1 type. Then, we derive a system stable condition and express the stationary probability vector of this Markov process by means of the matrix-geometric solution.

Let $N_1(t), N_2(t), I(t), J_1(t)$ and $J_2(t)$ be the number of transactions in the queueing waiting room, the number of transactions in the block, the phase of the MAP, the phase of a blockchain-building PH time, and the phase of a block-generation PH time at time t, respectively. We write $\mathbf{X} = \{(N_1(t), N_2(t), I(t), J_1(t), J_2(t)), t \geq 0\}$. Then, it is easy to see that $\mathbf{X}$ is a continuous-time Markov process with block structure whose state space is given by

$$\begin{aligned}\mathbf{\Omega} = &\{(0,0;i), 1 \leq i \leq m_0\} \\ &\cup \left\{\left(0,l;i,j\right), 1 \leq l \leq b, 1 \leq i \leq m_0, 1 \leq j \leq m_1\right\} \\ &\cup \left\{(k,0;i,r), k \geq 1, 1 \leq i \leq m_0, 1 \leq r \leq m_2\right\} \\ &\cup \left\{\left(k,l;i,j\right), k \geq 1, 1 \leq l \leq b, 1 \leq i \leq m_0, 1 \leq j \leq m_1\right\}.\end{aligned}$$

From Fig. 1, it is easy to set up the state transition relations of the Markov process $\mathbf{X}$, see Fig. 2 for more details. It is a key in understanding of Fig. 2 that there is a different transition between State $(k,0)$ for the block generation and State (k,l) for the blockchain building with $1 \le l \le b$ because the block-generation and blockchain-building processes cannot simultaneously exist at a time, and specifically, a block must first be generated, then it can enter the blockchain-building process.

Using Fig. 2, the infinitesimal generator of the Markov process $\mathbf{X}$ is given by

$$\mathbf{Q} = \begin{pmatrix} B_1 & B_0 & & & & & & \\ B_2 & A_1 & A_0 & & & & & \\ B_3 & & A_1 & A_0 & & & & \\ \vdots & & & \ddots & \ddots & & & \\ B_{b+1} & & & & A_1 & A_0 & & \\ & A_{b+1} & & & & A_1 & A_0 & \\ & & A_{b+1} & & & & A_1 & A_0 \\ & & & \ddots & & & \ddots & \ddots \end{pmatrix}, \tag{1}$$

where $\otimes$ and $\oplus$ are the Kronecker product and the Kronecker sum of two matrices, respectively,

$$A_0 = \begin{pmatrix} D \otimes I & & & \\ & D \otimes I & & \\ & & \ddots & \\ & & & D \otimes I \end{pmatrix}, \quad A_1 = \begin{pmatrix} C \oplus S & & & \\ I \otimes \left(T^0 \beta\right) & C \oplus T & & \\ \vdots & & \ddots & \\ I \otimes \left(T^0 \beta\right) & & & C \oplus T \end{pmatrix},$$

$$A_{b+1} = \begin{pmatrix} 0 & \cdots & 0 & I \otimes \left(S^0 \alpha\right) \\ & & & \end{pmatrix},$$

and

$$B_0 = \begin{pmatrix} D \otimes \beta & & & \\ & D \otimes I & & \\ & & \ddots & \\ & & & D \otimes I \end{pmatrix}, \; B_1 = \begin{pmatrix} C & & & \\ I \otimes T^0 & C \oplus T & & \\ \vdots & & \ddots & \\ I \otimes T^0 & & & C \oplus T \end{pmatrix},$$

$$B_2 = \begin{pmatrix} 0 & I \otimes \left(S^0 \alpha\right) & 0 & \cdots & 0 \\ & & & & \end{pmatrix}, \ldots, B_{b+1} = \begin{pmatrix} 0 & \ldots & 0 & I \otimes \left(S^0 \alpha\right) \\ & & & \end{pmatrix}.$$

Clearly, the continuous-time Markov process $\mathbf{X}$ is of GI/M/1 type.

Now, we use the mean drift method to discuss the system stable condition of the continuous-time Markov process $\mathbf{X}$ of GI/M/1 type. Note that the mean drift method for checking system stability is given a detailed introduction in Chapter 3 of Li [97].

From Chapter 1 of Neuts [98] or Chapter 3 of Li [97], for the Markov process of GI/M/1 type, we write

$$\begin{aligned}\mathbf{A} &= A_0 + A_1 + A_{b+1} \\ &= \begin{pmatrix} D\otimes I + C\oplus S & & & I\otimes\left(S^0\alpha\right) \\ I\otimes\left(T^0\beta\right) & D\otimes I + C\oplus T & & \\ \vdots & & \ddots & \\ I\otimes\left(T^0\beta\right) & & D\otimes I + C\oplus T & \\ I\otimes\left(T^0\beta\right) & & & D\otimes I + C\oplus T \end{pmatrix}.\end{aligned} \tag{2}$$

Clearly, the matrix $\mathbf{A}$ is the infinitesimal generator of an irreducible, aperiodic and positive recurrent Markov process with two levels (i.e., levels 0 and b), together with $b-1$ instantaneous levels (i.e., levels $1,2,\ldots,b-1$) which will vanish as the time t goes to infinity. On the other hand, such a special Markov process $\mathbf{A}$ will not influence applications of the matrix-geometric solution because it is only related to the mean drift method for establishing system stable conditions.

The following theorem discusses the invariant measure θ of the Markov process $\mathbf{A}$, that is, the vector θ satisfies the system of linear equations $\theta\mathbf{A}=0$ and $\theta e = 1$.

Theorem 1 *There exists the unique invariant measure* $\theta = (\theta_0, 0, \ldots, 0, \theta_b)$ *of the Markov process* $\mathbf{A}$, *where* (θ_0, θ_b) *is the stationary probability vector of the irreducible positive-recurrent Markov process whose infinitesimal generator*

$$\mathfrak{R} = \begin{pmatrix} D\otimes I + C\oplus S & I\otimes\left(S^0\alpha\right) \\ I\otimes\left(T^0\beta\right) & D\otimes I + C\oplus T \end{pmatrix}.$$

Proof It follows from $\theta\mathbf{A}=0$ that

$$\theta_1(D\otimes I + C\oplus S) + \sum_{k=1}^{b-1}\theta_k\left[I\otimes\left(T^0\beta\right)\right] + \theta_b\left[I\otimes\left(T^0\beta\right)\right] = 0, \tag{3}$$

$$\theta_k[D\otimes I + C\oplus T] = 0, \quad 1\le k\le b-1, \tag{4}$$

$$\theta_1\left[I\otimes\left(S^0\alpha\right)\right] + \theta_b(D\otimes I + C\oplus T) = 0. \tag{5}$$

For Eq. (4), note that

$$\begin{aligned} D\otimes I + C\oplus T &= D\otimes I + C\otimes I + I\otimes T \\ &= (C+D)\otimes I + I\otimes T \\ &= (C+D)\oplus T, \end{aligned}$$

where $C+D$ is the infinitesimal generator of an irreducible and a positive-recurrent Markov process; thus, its eigenvalue of the maximal real part is zero so that all the other eigenvalues have a negative real part; while T, coming from the PH distribution with

irreducible representation (α, T), is invertible with the real part of each eigenvalue be negative due to the fact that $Te \lneqq 0$, and the matrix T has the properties that all diagonal elements are negative, and all off-diagonal elements are nonnegative. Note that each eigenvalue of the matrix $(C + D) \oplus T$ is the sum of an eigenvalue of the matrix $C + D$ and an eigenvalue of the matrix T; thus, each eigenvalue of the matrix $(C + D) \oplus T$ has a negative real part (i.e., it is non-zero). This shows that the matrix $(C + D) \oplus T$ is invertible by means of $\det((C + D) \oplus T) \neq 0$, which is the product of all the eigenvalues of $(C + D) \oplus T$. Hence, from Equation $\theta_k[D \otimes I + C \oplus T] = 0$ for $1 \leq k \leq b - 1$, we obtain

$$\theta_1 = \theta_2 = \cdots = \theta_{b-1} = 0.$$

This gives

$$\theta = (\theta_0, 0, \ldots, 0, \theta_b).$$

It follows from (3) and (5) that

$$\begin{cases} \theta_0(D \otimes I + C \oplus S) + \theta_b\left[I \otimes \left(T^0\beta\right)\right] = 0, \\ \theta_0\left[I \otimes \left(S^0\alpha\right)\right] + \theta_b(D \otimes I + C \oplus T) = 0. \end{cases}$$

Thus, we have

$$(\theta_0, \theta_b)\begin{pmatrix} D \otimes I + C \oplus S & I \otimes \left(S^0\alpha\right) \\ I \otimes \left(T^0\beta\right) & D \otimes I + C \oplus T \end{pmatrix} = (0, 0).$$

Let

$$\mathfrak{R} = \begin{pmatrix} D \otimes I + C \oplus S & I \otimes \left(S^0\alpha\right) \\ I \otimes \left(T^0\beta\right) & D \otimes I + C \oplus T \end{pmatrix}.$$

Then, the matrix $\mathfrak{R}$ is the infinitesimal generator of an irreducible positive-recurrent Markov process. Thus, the Markov process $\mathfrak{R}$ exists the stationary probability vector (θ_0, θ_b), that is, there exists the unique solution to the system of linear equations: $(\theta_0, \theta_b)\mathfrak{R} = 0$ and $\theta_0 e + \theta_b e = 1$. This completes the proof. □

The following theorem provides a necessary and sufficient conditions under which the Markov process **Q** is positive recurrence.

Theorem 2 *The Markov process* **Q** *of GI/M/1 type is positive recurrent if and only if*

$$(\theta_0 + \theta_b)(D \otimes I)e < b\theta_0\left[I \otimes \left(S^0\alpha\right)\right]e. \tag{6}$$

Proof Using the mean drift method given in Chapter 3 of Li [17] (e.g., Theorem 3.19 and the continuous-time case in Page 172), it is easy to see that the Markov process **Q** of GI/M/1 type is positive recurrent if and only if

$$\theta A_0 e < b\theta A_{b+1} e. \tag{7}$$

Note that

$$\begin{aligned} \theta A_0 e &= \theta_0 (D \otimes I)e + \theta_b (D \otimes I)e \\ &= (\theta_0 + \theta_b)(D \otimes I)e \end{aligned} \tag{8}$$

and

$$b\theta A_{b+1} e = b\theta_0 \left[I \otimes \left(S^0 \alpha \right) \right] e, \tag{9}$$

thus, we obtain

$$(\theta_0 + \theta_b)(D \otimes I)e < b\theta_0 \left[I \otimes \left(S^0 \alpha \right) \right] e.$$

This completes the proof. □

It is necessary to consider a special case in which the transaction inputs are Poisson with arrival rate λ, and the blockchain-building and block-generation times are exponential with service rates μ_1 and μ_2, respectively. Note that this special case was studied in Li et al. [75], here we only restate the stable condition as the following corollary.

Corollary 3 *The Markov process* $\mathbf{Q}$ *of GI/M/1 type is positive recurrent if and only if*

$$\frac{b\mu_1\mu_2}{\mu_1 + \mu_2} > \lambda. \tag{10}$$

By observing (10), it is easy to see that $1/(b\mu_1) + 1/(b\mu_2) < 1/\lambda$, that is, the complicated service speed of transactions is faster than the transaction arrival speed, under which the Markov process $\mathbf{Q}$ of GI/M/1 type is positive recurrent. However, it is not easy to understand Condition (6) which is largely influenced by the matrix computation with respect to the MAP and the PH distribution.

If the Markov process $\mathbf{Q}$ of GI/M/1 type is positive recurrent, we write its stationary probability vector as

$$\pi = (\pi_0, \pi_1, \pi_2, \ldots),$$

where for $k = 0$

$$\begin{aligned} \pi_0 &= \left(\pi_{0,0}, \pi_{0,1}, \ldots, \pi_{0,b}\right), \\ \pi_{0,0} &= \left(\pi_{0,0}^{(i)} : 1 \le i \le m_0\right), \end{aligned}$$

and for $1 \le l \le b$

$$\pi_{0,l} = \left(\pi_{0,l}^{(i,j)} : 1 \le i \le m_0, 1 \le j \le m_1\right);$$

for $k \geq 1$

$$\begin{aligned}\pi_k &= \left(\pi_{k,0}, \pi_{k,1}, \ldots, \pi_{k,b}\right),\\ \pi_{k,0} &= \left(\pi_{k,0}^{(i,r)} : 1 \leq i \leq m_0, 1 \leq r \leq m_2\right),\end{aligned}$$

and for $1 \leq l \leq b$

$$\pi_{k,l} = \left(\pi_{k,l}^{(i,j)} : 1 \leq i \leq m_0, 1 \leq j \leq m_1\right).$$

Note that in the above expressions, the vector $\mathbf{a} = \left(a^{(i,j)} : 1 \leq i \leq I, 1 \leq j \leq J\right)$ is based on the lexicographical order of the elements, that is,

$$\mathbf{a} = \left(a^{(1,1)}, a^{(1,2)}, \ldots, a^{(1,J)}; a^{(2,1)}, a^{(2,2)}, \ldots, a^{(2,J)}; \ldots; a^{(I,1)}, a^{(I,2)}, \ldots, a^{(I,J)}\right).$$

If $(\theta_0 + \theta_b)(D \otimes I)e < b\theta_0\left[I \otimes \left(S^0\alpha\right)\right]e$, then the Markov process $\mathbf{Q}$ of GI/M/1 type is irreducible and positive recurrent. Thus, the Markov process $\mathbf{Q}$ exists a unique stationary probability vector, which is also matrix-geometric. Thus, to express the matrix-geometric stationary probability vector, we need to first obtain the rate matrix R, which is the minimal nonnegative solution to the following nonlinear matrix equation

$$R^{b+1}A_{b+1} + RA_1 + A_0 = 0. \tag{11}$$

In general, it is very complicated to solve this nonlinear matrix equation (11) due to the term $R^{b+1}A_{b+1}$ of size $b+1$. In fact, for the blockchain queueing system, here we cannot provide an explicit expression for the rate matrix R yet. In this case, we can use some iterative algorithms, given in Neuts [98], to give its numerical solution. For example, an effective iterative algorithm given in Neuts [98] is described as

$$\begin{aligned}R_0 &= 0,\\ R_{N+1} &= \left(R_N^{b+1}A_{b+1} + A_0\right)(-A_1)^{-1}.\end{aligned}$$

Note that this algorithm is fast convergent, that is, after a finite number of iterative steps, we can numerically obtain a solution of higher precision which is used to approximate the rate matrix R.

The following theorem directly comes from Theorem 1.2.1 of Chapter 1 in Neuts [98]. Here, we restate it without a proof.

Theorem 4 *If the Markov process* $\mathbf{Q}$ *of GI/M/1 type is positive recurrent, then the stationary probability vector* $\pi = (\pi_0, \pi_1, \pi_2, \ldots)$ *is given by*

$$\pi_k = \pi_1 R^{k-1}, \quad k \geq 2. \tag{12}$$

where the vector (π_0, π_1) *is the stationary probability vector of the censoring Markov process* $\mathbf{Q}^{(1,2)}$ *of levels 0 and 1 which is irreducible and positive recurrent. Thus, it is the unique solution to the following system of linear equations:*

$$\begin{cases} (\pi_0, \pi_1)\mathbf{Q}^{(1,2)} = (\pi_0, \pi_1), \\ \pi_0 e + \pi_1 (I - R)^{-1} e = 1, \end{cases} \tag{13}$$

where

$$\mathbf{Q}^{(1,2)} = \begin{pmatrix} B_1 & B_0 \\ \sum_{k=2}^{b+1} R^{k-2} B_k & A_1 + R^b A_{b+1} \end{pmatrix}.$$

Proof Here, we only derive the boundary condition (13). It follows from $\pi \mathbf{Q} = 0$ that

$$\begin{cases} \pi_0 B_1 + \pi_1 B_2 + \cdots + \pi_b B_{b+1} = 0, \\ \pi_0 B_0 + \pi_1 A_1 + \pi_{b+1} A_{b+1} = 0. \end{cases}$$

Using the matrix-geometric solution $\pi_k = \pi_1 R^{k-1}$ for $k \geq 2$, we have

$$\begin{cases} \pi_0 B_1 + \pi_1 \left(B_2 + R B_3 + \cdots + R^{b-1} B_{b+1} \right) = 0, \\ \pi_0 B_0 + \pi_1 \left(A_1 + R^b A_{b+1} \right) = 0. \end{cases}$$

This gives the desired result and completes the proof. □

The stationary transaction numbers

In this section, we discuss two key performance measures: the average stationary numbers of transactions both in the queueing waiting room and in the block and give their simple expressions by means of the vectors π_0 and π_1, and the rate matrix R. Finally, we use numerical examples to verify computability of our theoretical results and show how the performance measures depend on the main parameters of this system.

If $(\theta_0 + \theta_b)(D \otimes I)e < b\theta_0 \left[I \otimes \left(S^0 \alpha \right) \right] e$, then the blockchain system is stable. In this case, we write that w.p.1,

$$N_1 = lim_{t \to +\infty} N_1(t), \quad N_2 = lim_{t \to +\infty} N_2(t),$$

where $N_1(t)$ and $N_2(t)$ are the random numbers of transactions in the queueing waiting room and of transactions in the block at time $t \geq 0$, respectively.

a. The average stationary number of transactions in the queueing waiting room

It follows from (12) and (13) that

$$\begin{aligned} E[N_1] &= \sum_{k=1}^{\infty} k \sum_{i=1}^{m_0} \sum_{r=1}^{m_2} \pi_{k,0}^{(i,r)} + \sum_{k=1}^{\infty} k \sum_{l=1}^{b} \sum_{i=1}^{m_0} \sum_{j=1}^{m_1} \pi_{k,l}^{(i,j)} \\ &= \sum_{k=1}^{\infty} k \sum_{l=0}^{b} \pi_{k,l}\, e \\ &= \sum_{k=1}^{\infty} k\, \pi_k\, e = \pi_1 R (I - R)^{-2} e. \end{aligned}$$

Note that the above three vectors e have different sizes, for example, the size of the first one is $m_0 \times m_2$ for $l = 0$ and $m_0 \times m_1$ for $1 \leq l \leq b$, while the sizes of the second and third are $m_0 \times (m_2 + bm_1)$. For simplicity of description, here we use only a vector e whose size can easily be inferred by the context.

b. The average stationary number of transactions in the block

Let $\mathbf{h} = (0, e, 2e, \ldots, be)^T$. Then

$$\begin{aligned} E[N_2] &= \sum_{l=0}^{b} l \sum_{k=0}^{\infty} \sum_{i=1}^{m_0} \sum_{j=1}^{m_1} \pi_{k,l}^{(i,j)} \\ &= \sum_{l=0}^{b} l \sum_{k=0}^{\infty} \pi_{k,l}\, e \\ &= \sum_{k=0}^{\infty} \pi_k\, \mathbf{h} \\ &= \left[\pi_{\mathbf{0}} + \pi_1 (I - R)^{-1}\right] \mathbf{h}. \end{aligned}$$

In the remainder of this section, we provide some numerical examples to verify computability of our theoretical results, and to analyze how the two performance measures $E[N_1]$ and $E[N_2]$ depend on some crucial parameters of the blockchain queueing system.

In the two numerical examples, we take some common parameters: The block-building service rate $\mu_1 \in [0.05, 1.5]$, the block-generation service rate $\mu_2 = 2$, the arrival rate $\lambda = 0.3$, the maximum block size $b = 40, 320, 1000$, respectively.

From Fig. 3, it is seen that $E[N_1]$ and $E[N_2]$ decrease, as μ_1 increases. At the same time, $E[N_1]$ decreases as b increases, but $E[N_2]$ increases as b increases.

The transaction–confirmation time

In this section, we provide a matrix-analytic method based on the *RG* factorizations for computing the average transaction–confirmation time of any transaction, which is always an interesting but difficult topic because of the batch service for a block of transactions, and of the Service-In-Random-Order for choosing some transactions from the queueing waiting room into a block.

In the blockchain system, the transaction–confirmation time is the time interval from the time epoch that a transaction arrives at the queueing waiting room to the time point that the block including the transaction is first confirmed and then it is built in the blockchain. Obviously, the transaction–confirmation time is the sojourn time of the transaction in the blockchain system, and it is the sum of the block-generation and blockchain-building times with respect to the transaction taken in the block. Let $\mathfrak{I}$ denote the transaction–confirmation time of any transaction when the blockchain system is stable.

To study the transaction–confirmation time $\mathfrak{I}$, we need to introduce the stationary life time Γ_s of the PH blockchain-building time Γ with an irreducible representation (α, T).

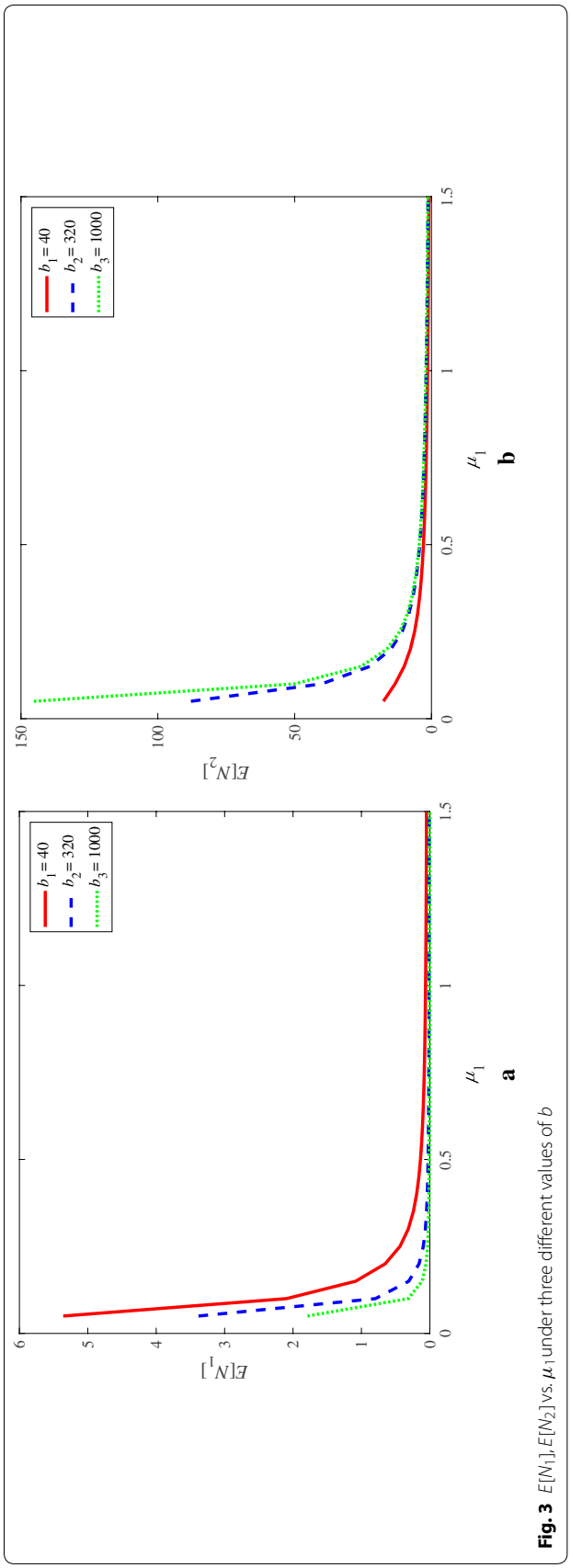

Fig. 3 $E[N_1], E[N_2]$ vs. μ_1 under three different values of b

Let ϖ be the stationary probability vector of the Markov process $T + T^0\alpha$. Then, the stationary life time Γ_s is also a PH distribution with an irreducible representation (ϖ, T), e.g., see Property 1.5 in Chapter 1 of Li [97]. Clearly, $E[\Gamma_s] = -\varpi T^{-1}e$.

Now, we introduce a Markov process $\{Y(t) : t \geq 0\}$ with an absorbing state, whose state transition relation is given in Fig. 4 according to Figs. 1 and 2. At the same time, we define the first passage time as

$$\xi = \inf\{t : Y(t) = \text{the absorbing state}, t \geq 0\}.$$

For $k \geq 0, 1 \leq i \leq m_0$ and $1 \leq r \leq m_2$, if $Y(0) = (k, 0; i, r)$, then we write the first passage time as $\xi_{|(k,0;i,r)}$.

Remark 3 It is necessary to explain the absorbing rates in the below part of Fig. 4.

1. If $Y(0) = (k, l)$ for $1 \leq k \leq b$ and $0 \leq l \leq b$, then the k transactions can be chosen into a block once the previous block is pegged to the blockchain, a tagged transaction of the k transactions is chosen into the block with probability 1.

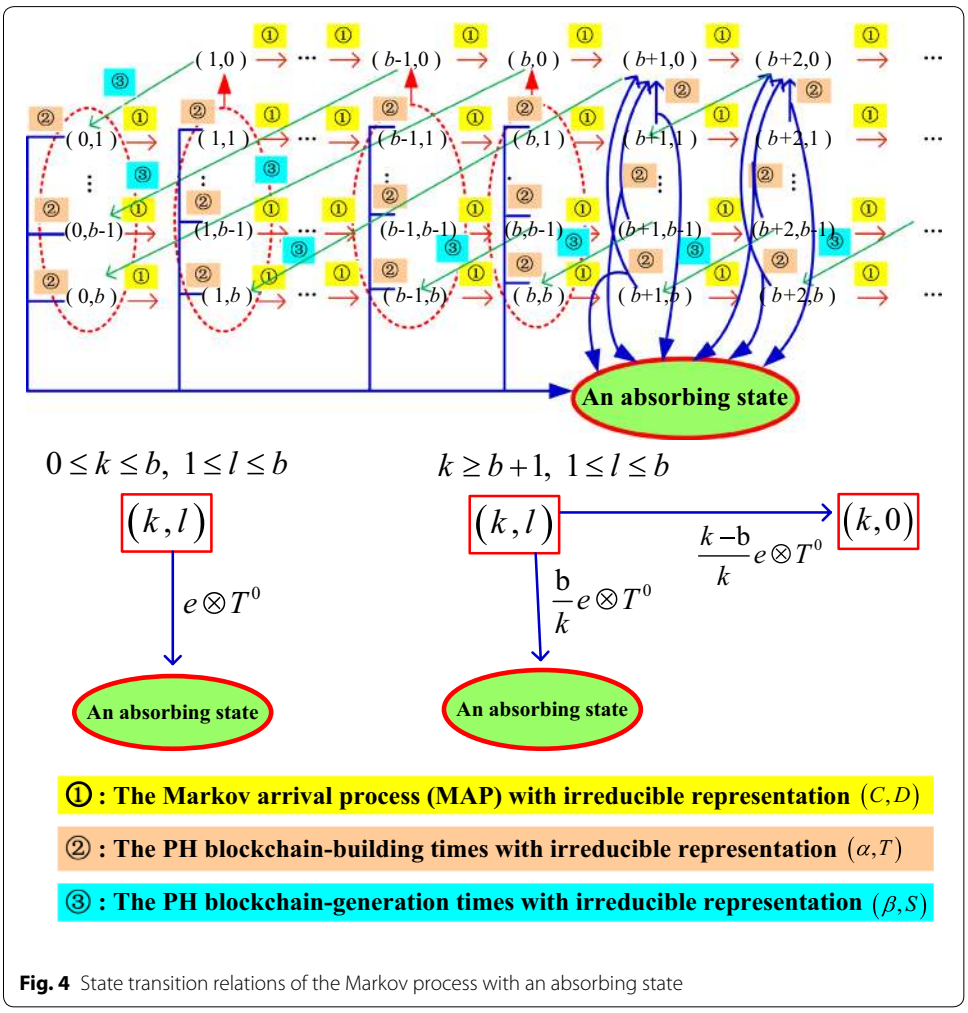

Fig. 4 State transition relations of the Markov process with an absorbing state

2. If $Y(0) = (k, l)$ for $k \geq b + 1$ and $0 \leq l \leq b$, then any b transactions of the k transactions can randomly be chosen into a block once the previous block is pegged to the blockchain; thus, a tagged transaction of the k transactions is chosen into the block of the maximal size b with probability b/k.

When a transaction arrives at the queueing waiting room, it can observe the states of the blockchain system having two different cases:

Case one: state $(k, 0; i, r)$ for $k \geq 1$; $1 \leq i \leq m_0$ and $1 \leq r \leq m_2$. In this case, with the initial probability $\pi_{k,0}^{(i,r)}$, the transaction–confirmation time $\mathfrak{I}$ is the first passage time $\xi_{|(k,0;i,r)}$ of the Markov process with an absorbing state, whose state transition relation is given in Fig. 4.

Case two: state $(k, l; i, r)$ for $k \geq 1, 1 \leq l \leq b$; $1 \leq i \leq m_0$ and $1 \leq j \leq m_1$. In this case, with the initial probability $\pi_{k,l}^{(i,j)}$, the transaction–confirmation time $\mathfrak{I}$ is decomposed into the sum of the random variable Γ_s and the first passage time $\xi_{|(k,0;i,r)}$ given in Case one. It is easy to see from Fig. 4 that there exists a stochastic decomposition: $\mathfrak{I} = \Gamma_s + \xi_{|(k,0;i,r)}$.

From the above analysis, it is easy to see that computation of the first passage time $\xi_{|(k,0;i,r)}$ is a key in analyzing the transaction–confirmation time.

Based on the state transition relation given in Fig. 4, now we write the infinitesimal generator of the Markov process $\{Y(t) : t \geq 0\}$ as

$$\mathbf{H} = \begin{pmatrix} \widetilde{B}_1 & \widetilde{B}_0 & & & & & & & \\ \widetilde{B}_2 & \widetilde{A}_1 & A_0 & & & & & & \\ \widetilde{B}_3 & & \widetilde{A}_1 & A_0 & & & & & \\ \vdots & & & \ddots & \ddots & & & & \\ \widetilde{B}_{b+1} & & & & \widetilde{A}_1 & A_0 & & & \\ & A_{b+1} & & & & \widetilde{A}_1^{(b+1)} & A_0 & & \\ & & A_{b+1} & & & & \widetilde{A}_1^{(b+2)} & A_0 & \\ & & & \ddots & & & & \ddots & \ddots \end{pmatrix}, \tag{14}$$

where

$$A_0 = \begin{pmatrix} D \otimes I & & & \\ & D \otimes I & & \\ & & \ddots & \\ & & & D \otimes I \end{pmatrix}, A_{b+1} = \begin{pmatrix} 0 & \cdots & 0 & I \otimes (S^0 \alpha) \\ & & & \end{pmatrix},$$

$$\widetilde{A}_1 = \begin{pmatrix} C \oplus S & & & \\ & C \oplus T & & \\ & & \ddots & \\ & & & C \oplus T \end{pmatrix},$$

for $k \geq b + 1$

$$\widetilde{A}_1^{(k)} = \begin{pmatrix} C \oplus S & & & \\ I \otimes \left(\frac{k-b}{k} T^0 \beta\right) & C \oplus T & & \\ \vdots & & \ddots & \\ I \otimes \left(\frac{k-b}{k} T^0 \beta\right) & & & C \oplus T \end{pmatrix};$$

$$\widetilde{B}_0 = \begin{pmatrix} 0 & D \otimes I & & & \\ & D \otimes I & & & \\ & & \ddots & & \\ & & & D \otimes I \end{pmatrix}, \widetilde{B}_1 = \begin{pmatrix} C \otimes I & & & \\ & C \oplus T & & \\ & & \ddots & \\ & & & C \oplus T \end{pmatrix},$$

$$\widetilde{B}_2 = \begin{pmatrix} I \otimes \left(S^0 \alpha\right) & 0 & 0 & \cdots & 0 \\ & & & & \end{pmatrix}, \ldots, \widetilde{B}_{b+1} = \begin{pmatrix} 0 & \cdots & 0 & I \otimes \left(S^0 \alpha\right) \\ & & & \end{pmatrix}.$$

If the blockchain system is stable, then the probability that a transaction observes State $(0, 0; i)$ only after arrived at the instant is $\pi_{1,0}^{(i,r)}$; for $1 \le l \le b$, the probability that a transaction observes State $\left(0, l; i, j\right)$ only after arrived at the instant is $\pi_{1,l}^{(i,j)}$; for $k \ge 2$, the probability that a transaction observes State $(k-1, 0; i, r)$ only after arrived at the instant is $\pi_{k,0}^{(i,r)}$; for $k \ge 2, 1 \le l \le b$, the probability that a transaction observes State $\left(k-1, l; i, j\right)$ only after arrived at the instant is $\pi_{k,l}^{(i,j)}$. Obviously, for $0 \le l \le b$, States $(0, 0; i)$ and $\left(0, l; i, j\right)$ will not be encountered by the transaction only after arrived at the instant and, thus, the stationary probabilities $\pi_{0,0}^{(i)}$ and $\pi_{0,l}^{(i,j)}$ should be omitted by means of the observation of any arriving transaction. Based on this, we introduce a new initial probability vector for the observation of any transaction only after arrived at the instant as follows:

$$\gamma = (\gamma_1, \gamma_2, \gamma_3, \ldots),$$

where for $k \ge 1$

$$\gamma_k = \left(\gamma_{k,0}, \gamma_{k,1}, \ldots, \gamma_{k,b}\right),$$
$$\gamma_{k,0} = \left(\frac{1}{1 - \pi_0 e} \pi_{k,0}^{(i,r)} : 1 \le i \le m_0, 1 \le r \le m_2\right)$$

and for $1 \le l \le b$

$$\gamma_{k,l} = \left(\frac{1}{1 - \pi_0 e} \pi_{k,l}^{(i,j)} : 1 \le i \le m_0, 1 \le j \le m_1\right).$$

To emphasize on the event that the transaction observes State $(k-1, 0; i, r)$ only after arrived at the instant, we introduce a new initial probability vector

$$\varphi = (\varphi_1, \varphi_2, \varphi_3, \ldots),$$

where for $k \ge 1$

$$\varphi_k = \left(\gamma_{k,0}, 0, 0, \ldots, 0\right).$$

In addition, we take

$$\psi = \gamma - \varphi.$$

Theorem 5 *If the blockchain system is stable, then the first passage time $\xi_{|(k,0;i,r)}$ is a PH distribution of infinite size with an irreducible representation $(\eta(k,0;i,r),\mathbf{H})$, where $\mathbf{H}$ is given in (14), and*

$$\eta(k,0;i,r) = \left(0,0,\ldots,0,\frac{1}{1-\pi_0 e}\pi_{k,0}^{(i,r)},0,0,\ldots,0\right).$$

Also, we have

$$\begin{aligned}\mathbf{H}^0 &= -\mathbf{H}e \\ &= \left(e\otimes T^0, e\otimes T^0,\ldots,e\otimes T^0;\frac{b}{b+1}e\otimes T^0,\frac{b}{b+2}e\otimes T^0,\ldots\right).\end{aligned}$$

Proof If the blockchain system is stable, then $\xi_{|(k,0;i,r)}$ is the first passage time of the Markov process $\mathbf{H}$ (or $\{Y(t):t\geq 0\}$) with an absorbing state and under the initial state $Y(0)=(k,0;i,r)$. Note that the original Markov process $\mathbf{Q}$ given in (1) is irreducible and positive recurrent and, thus, $\xi_{|(k,0;i,r)}$ is a PH distribution of infinite size with an irreducible representation $(\eta(k,0;i,r),\mathbf{H})$. At the same time, a simple computation gives

$$\mathbf{H}^0 = \left(e\otimes T^0, e\otimes T^0,\ldots,e\otimes T^0;\frac{b}{b+1}e\otimes T^0,\frac{b}{b+2}e\otimes T^0,\ldots\right).$$

This completes the proof. □

Based on Theorem 5, now we extend the first passage time $\xi_{|(k,0;i,r)}$ to $\xi_{|(\mathbf{0},\varphi)}$, which is the first passage time of the Markov process $\mathbf{H}$ with an initial probability vector $(\mathbf{0},\varphi)$. The following corollary shows that $\xi_{|(\mathbf{0},\varphi)}$ is PH distribution of infinite size, while its proof is easy and is omitted here.

Corollary 6 *If the blockchain system is stable, then the first passage time $\xi_{|(\mathbf{0},\varphi)}$ is a PH distribution of infinite size with an irreducible representation $((\mathbf{0},\varphi),\mathbf{H})$, and*

$$\begin{aligned}E\left[\xi_{|(\mathbf{0},\varphi)}\right] &= -(\mathbf{0},\varphi)\mathbf{H}^{-1}e, \\ Var\left[\xi_{|(\mathbf{0},\varphi)}\right] &= (\mathbf{0},\varphi)\mathbf{H}^{-2}e - \left[(\mathbf{0},\varphi)\mathbf{H}^{-1}e\right]^2.\end{aligned}$$

The following theorem provides a simple expression for the average transaction–confirmation time $E[\mathfrak{I}]$ by means of Corollary 6.

Theorem 7 *If the blockchain queueing system is stable, then the average transaction–confirmation time $E[\mathfrak{I}]$ is given by*

$$E[\mathfrak{I}] = E\left[\xi_{|(\mathbf{0},\varphi)}\right] + (1-\varphi e)E[\Gamma_s],$$

where Γ_s *is the stationary life time of the PH blockchain-building time with an irreducible representation* (α, T). *Further, we have*

$$E[\mathfrak{I}] = -(\mathbf{0},\varphi)\mathbf{H}^{-1}e - (1-\varphi e)\varpi T^{-1}e,$$

where ϖ *is the stationary probability vector of the Markov process* $T + T^0\alpha$.

Proof We first introduce two basic events

$$\begin{aligned}\Theta = \big\{&\text{The transaction observes States } (0,0;i) \text{ and } (k,0;i,r)\\ &\text{for } 1 \le i \le m_0, k \ge 1, 1 \le r \le m_2\\ &\text{only after arrived at the instant}\big\}\end{aligned}$$

and

$$\begin{aligned}\Theta^c = \big\{&\text{The transaction observes States } (k,l;i,j)\\ &\text{for } k \ge 1, 1 \le l \le b, 1 \le i \le m_0, 1 \le j \le m_1\\ &\text{only after arrived at the instant}\big\}.\end{aligned}$$

It is easy to see that $\Theta \cup \Theta^c = \Omega$. Thus, the two events are complementary according to the fact that the transaction can observe all the states of the Markov process $\mathbf{Q}$ only after arrived at the instant. If the blockchain system is stable, then it is easy to compute the probabilities of the two events as follows:

$$P\{\Theta\} = (\mathbf{0},\varphi)e = \varphi e$$

and

$$P\left\{\Theta^c\right\} = 1 - P\{\Theta\} = 1 - \varphi e.$$

Using the law of total probability, we obtain

$$\begin{aligned}E[\mathfrak{I}] &= P\{\Theta\}E[\mathfrak{I} \mid \Theta] + P\left\{\Theta^c\right\}E\left[\mathfrak{I} \mid \Theta^c\right]\\ &= \varphi e\, E\left[\xi_{|(\mathbf{0},\varphi)}\right] + (1-\varphi e)E\left[\Gamma_s + \xi_{|(\mathbf{0},\varphi)}\right]\\ &= E\left[\xi_{|(\mathbf{0},\varphi)}\right] + (1-\varphi e)E[\Gamma_s]\\ &= -(\mathbf{0},\varphi)\mathbf{H}^{-1}e - (1-\varphi e)\varpi T^{-1}e.\end{aligned}$$

The proof is completed. □

As shown in Theorem 7, it is a key in the study of PH distributions of infinite sizes whether or not we can compute the inverse matrix $\mathbf{H}^{-1}$ of infinite size. To this end, we

need to use the *RG* factorizations, given in Li [97], to provide such a computable path. In what follows, we provide only a simple interpretation on such a computation, while some detailed discussions will be left in our another paper in the future.

In fact, it is often very difficult and challenging to compute the inverse of a matrix of infinite size only except for the triangular matrices. Fortunately, using the *RG* factorizations, the infinitesimal generator $\mathbf{H}$ can be decomposed into a product of three matrices: two block-triangular matrices and a block-diagonal matrix. Therefore, the *RG* factorizations play a key role in generalizing the PH distributions from finite dimensions to infinite dimensions.

Using Subsection 2.2.3 in Chapter 2 of Li [97] (see Pages 88 to 89), now we provide the UL-type *RG* factorization of the infinitesimal generator $\mathbf{H}$. It will be seen that the *RG* factorization of $\mathbf{H}$ has a beautiful block structure, which is well related to the special block characteristics of $\mathbf{H}$ corresponding to the blockchain system. To this end, we need to define and compute the *R*-, *U*- and *G*-measures as follows.

The *R*-measure

Let R_k for $k \geq 0$ be the minimal nonnegative solution to the system of nonlinear matrix equations:

$$\begin{aligned}
R_0 &= \widetilde{B}_0 + R_0\widetilde{A}_1 + R_0R_1\cdots R_{b-1}R_bA_{b+1},\\
R_1 &= A_0 + R_1\widetilde{A}_1 + R_1R_2\cdots R_bR_{b+1}A_{b+1},\\
R_2 &= A_0 + R_2\widetilde{A}_1 + R_2R_3\cdots R_{b+1}R_{b+2}A_{b+1},\\
&\vdots\\
R_{b-1} &= A_0 + R_{b-1}\widetilde{A}_1 + R_{b-1}R_b\cdots R_{2b-2}R_{2b-1}A_{b+1},
\end{aligned}$$

and

$$\begin{aligned}
R_b &= A_0 + R_b\widetilde{A}_1^{(b+1)} + R_bR_{b+1}\cdots R_{2b-1}R_{2b}A_{b+1},\\
R_{b+1} &= A_0 + R_{b+1}\widetilde{A}_1^{(b+2)} + R_{b+1}R_{b+2}\cdots R_{2b}R_{2b+1}A_{b+1},\\
R_{b+2} &= A_0 + R_{b+2}\widetilde{A}_1^{(b+3)} + R_{b+2}R_{b+3}\cdots R_{2b+1}R_{2b+2}A_{b+1},\\
&\vdots
\end{aligned}$$

The *U*-measure

Based on the *R*-measure R_k for $k \geq 0$, we have

$$\begin{aligned}
U_0 &= \widetilde{B}_1 + R_0\widetilde{B}_2 + R_0R_1\widetilde{B}_3 + \cdots + R_0R_1\cdots R_{b-2}R_{b-1}\widetilde{B}_{b+1},\\
U_1 &= \widetilde{A}_1 + R_1R_2\cdots R_{b-1}R_bA_{b+1},\\
U_2 &= \widetilde{A}_1 + R_2R_3\cdots R_bR_{b+1}A_{b+1},\\
&\vdots\\
U_b &= \widetilde{A}_1 + R_bR_{b+1}\cdots R_{2b-2}R_{2b-1}A_{b+1},
\end{aligned}$$

and

$$\begin{aligned}
U_{b+1} &= \widetilde{A}_1^{(b+1)} + R_{b+1}R_{b+2}\cdots R_{2b-1}R_{2b}A_{b+1},\\
U_{b+2} &= \widetilde{A}_1^{(b+2)} + R_{b+2}R_{b+3}\cdots R_{2b}R_{2b+1}A_{b+1},\\
U_{b+3} &= \widetilde{A}_1^{(b+3)} + R_{b+3}R_{b+4}\cdots R_{2b+1}R_{2b+2}A_{b+1},\\
&\vdots
\end{aligned}$$

The *G*-measure

Based on the R-measure R_k for $k \geq 0$ and the U-measure U_k for $k \geq 0$, we have

$$\begin{aligned}
G_{1,0} &= (-U_1)^{-1}\left(\widetilde{B}_2 + R_1\widetilde{B}_3 + R_1R_2\widetilde{B}_4 + \cdots + R_1R_2\cdots R_{b-2}R_{b-1}\widetilde{B}_{b+1}\right),\\
G_{2,0} &= (-U_2)^{-1}\left(\widetilde{B}_3 + R_2\widetilde{B}_4 + R_2R_3\widetilde{B}_5 + \cdots + R_2R_3\cdots R_{b-2}R_{b-1}\widetilde{B}_{b+1}\right),\\
&\vdots\\
G_{b-1,0} &= \left(-U_{b-1}\right)^{-1}\left(\widetilde{B}_b + R_{b-1}\widetilde{B}_{b+1}\right),\\
G_{b,0} &= (-U_b)^{-1}\widetilde{B}_{b+1},
\end{aligned}$$

$$\begin{aligned}
G_{2,1} &= (-U_2)^{-1}R_2R_3\cdots R_{b-1}R_bA_{b+1},\\
G_{3,1} &= (-U_3)^{-1}R_3R_4\cdots R_{b-1}R_bA_{b+1},\\
&\vdots\\
G_{b,1} &= (-U_b)^{-1}R_bA_{b+1},\\
G_{b+1,1} &= \left(-U_{b+1}\right)^{-1}A_{b+1},
\end{aligned}$$

and for $k \geq 3$

$$\begin{aligned}
G_{k,k-1} &= (-U_k)^{-1}R_kR_{k+1}\cdots R_{k+b-3}R_{k+b-2}A_{b+1},\\
G_{k+1,k-1} &= \left(-U_{k+1}\right)^{-1}R_{k+1}R_{k+2}\cdots R_{k+b-3}R_{k+b-2}A_{b+1},\\
&\vdots\\
G_{k+b-2,k-1} &= \left(-U_{k+b-2}\right)^{-1}R_{k+b-2}A_{b+1},\\
G_{k+b-1,k-1} &= \left(-U_{k+b-1}\right)^{-1}A_{b+1}.
\end{aligned}$$

Based on the R-, U- and G-measures, we provide the UL-type RG factorization of the infinitesimal generator $\mathbf{H}$ as follows:

$$\mathbf{H} = (I - \mathbf{R}_U)\mathbf{U}(I - \mathbf{G}_L),$$

where

$$\mathbf{R}_U = \begin{pmatrix} 0 & R_0 & & & & \\ & 0 & R_1 & & & \\ & & 0 & R_2 & & \\ & & & 0 & R_3 & \\ & & & & \ddots & \ddots \end{pmatrix},$$

$$\mathbf{U} = \mathrm{diag}(U_0, U_1, U_2, U_3, \ldots)$$

and

$$\mathbf{G}_L = \begin{pmatrix} 0 & & & & & & & & \\ G_{1,0} & 0 & & & & & & & \\ G_{2,0} & G_{2,1} & 0 & & & & & & \\ \vdots & \vdots & \vdots & \ddots & & & & & \\ G_{b-1,0} & G_{b-1,1} & G_{b-1,b-2} & \cdots & 0 & & & & \\ G_{b,0} & G_{b,1} & G_{b,b-2} & \cdots & G_{b,k} & 0 & & & \\ & G_{b+1,1} & G_{b+1,b-2} & \cdots & G_{b+1,k} & G_{b+1,k+1} & 0 & & \\ & & G_{b+2,b-2} & \cdots & G_{b+2,k} & G_{b+2,k+1} & G_{b+2,k+2} & 0 & \\ & & & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \end{pmatrix}.$$

Based on the UL-type *RG* factorization $\mathbf{H} = (I - \mathbf{R}_U)\mathbf{U}(I - \mathbf{G}_L)$, we obtain

$$\mathbf{H}^{-1} = (I - \mathbf{G}_L)^{-1}\mathbf{U}^{-1}(I - \mathbf{R}_U)^{-1},$$

where the inverse matrices $(I - \mathbf{G}_L)^{-1}$, $\mathbf{U}^{-1}$ and $(I - \mathbf{R}_U)^{-1}$ are given some expressions in Appendix A.3 of Li [97]: inverses of matrices of infinite size (see Pages 654 to 658). Once the inverse of matrix $\mathbf{H}$ of infinite size is given, the PH distribution of infinite size can be constructed under a computable and feasible framework. In fact, this is very important in the study of stochastic models. Also see Li et al. [99] and Takine [100] for more details.

Remark 4 In general, it is always very difficult and challenging to discuss the transaction–confirmation time of any transaction in a blockchain system due to two key points: The block service is a class of batch service, and some transactions are chosen into a block by means of the Service-In-Random-Order. For a more general blockchain system, this paper sets up a Markov process with an absorbing state, and shows that the transaction–confirmation time is the first passage time of the Markov process with an absorbing state. Therefore, this paper can discuss the transaction–confirmation time by means of the PH distribution of infinite size (corresponding to the first passage time) and provides an effective algorithm for computing the average transaction–confirmation time using the *RG* factorizations of block-structured Markov processes of infinite levels. We believe that the *RG* factorizations of block-structured Markov processes will play a key role in the queueing study of blockchain systems.

Concluding remarks

In this paper, we develop a more general framework of block-structured Markov processes in the queueing study of blockchain systems. To do this, we design a two-stage, Service-In-Random-Order and batch service queueing system with MAP transaction arrivals and two-stages of PH service times and discuss some key performance measures such as the average stationary number of transactions in the queueing waiting room, the average stationary number of transactions in the block, and the average transaction–confirmation time of any transaction. Note that the study of performance measures is a key to improve blockchain technologies sufficiently. On the other hand, an original aim of this paper is to generalize the two-stage batch-service queueing model studied in Li et al. [75] both "from exponential to phase-type" service times and "from Poisson to MAP" transaction arrivals. Note that the MAP transaction arrivals and the two stages of PH service times make our queueing model more suitable to various practical conditions of blockchain systems with key factors, for example, the mining processes, the reward incentive, the consensus mechanism, the block generation, the blockchain building and so forth.

Using the matrix-geometric solution, we first obtain a sufficient stable condition of the blockchain system. Then, we provide simple expressions for two key performance measures: the average stationary number of transactions in the queueing waiting room, and the average stationary number of transactions in the block. Finally, to deal with the transaction–confirmation time, we develop a computational technique of the first passage times by means of both the PH distributions of infinite sizes and the *RG* factorizations. In addition, we use numerical examples to verify computability of our theoretical results. Along these lines, we will continue our future research on several interesting directions as follows:

- Developing effective algorithms for computing the average transaction–confirmation times in terms of the *RG* factorizations.
- Analyzing multiple classes of transactions in the blockchain systems, in which the transactions are processed in the block-generation and blockchain-building processes according to a priority service discipline.
- When the arrivals of transactions are a renewal process, and/or the block-generation times and/or the blockchain-building times follow general probability distributions, an interesting future research is to focus on fluid and diffusion approximations of blockchain systems.
- Setting up reward function with respect to cost structures, transaction fees, mining reward, consensus mechanism, security and so forth. It is very interesting in our future study to develop stochastic optimization, Markov decision processes and stochastic game models in the study of blockchain systems.

Acknowledgements

The authors are grateful to the editor and two anonymous referees for their constructive comments and suggestions, which sufficiently help the authors to improve the presentation of this manuscript. Q.L. Li was supported by the National Natural Science Foundation of China under grant No. 71671158, and the Natural Science Foundation of Hebei Province in China under Grant No. G2017203277.

Authors' contributions
QL provided the main theoretical analysis and contributed ideas on content and worked on the writing. JY and YX completed the TEX file under the present version. YX ran the numerical experiments. JY, FQ and HB checked some mathematical derivations. All authors read and approved the final manuscript.

Availability of data and materials
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Author details
[1] School of Economics and Management, Beijing University of Technology, Beijing 100124, China. [2] School of Economics and Management, Yanshan University, Qinhuangdao 066004, China. [3] School of Science, Yanshan University, Qinhuangdao 066004, China.

Received: 23 April 2019 Accepted: 17 June 2019
Published online: 02 July 2019

References

1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system, working paper; 2008. p. 1–9.
2. Wattenhofer R. The science of the blockchain. California: CreateSpace Independent Publishing Platform; 2016.
3. Prusty N. Building blockchain projects. Birmingham: Packt Publishing Ltd; 2017.
4. Drescher D. Blockchain basics: a non-technical introduction in 25 steps. Berkely: Apress; 2017.
5. Bashir I. Mastering blockchain: distributed ledger technology, decentralization, and smart contracts explained. Birmingham: Packt Publishing Ltd; 2018.
6. Parker JF. Blockchain technology simplified: the complete guide to blockchain management, mining, trading and investing cryptocurrency. California: CreateSpace Independent Publishing Platform; 2018.
7. Zheng Z, Xie S, Dai H-N, Chen X, Wang H. Blockchain challenges and opportunities: a survey. Int J Web Grid Serv. 2018;14(4):352–75.
8. Constantinides P, Henfridsson O, Parker GG. Introduction-platforms and infrastructures in the digital age. Inf Syst Res. 2018;29(2):381–400.
9. Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where is current research on blockchain technology?—A systematic review. PLoS ONE. 2016;11(10):0163477.
10. Plansky J, O'Donnell T, Richards K. A strategist's guide to blockchain. PwC report; 2016. p. 1–12.
11. Lindman J, Tuunainen VK, Rossi M. Opportunities and risks of blockchain technologies—a research agenda. In: Proceedings of the 50th Hawaii international conference on system sciences; 2017. p. 1533–42.
12. Risius M, Spohrer K. A blockchain research framework. Bus Inf Syst Eng. 2017;59(6):385–409.
13. Parker T. Smart contracts: the ultimate guide to blockchain smart contracts—learn how to use smart contracts for cryptocurrency exchange!. California: CreateSpace Independent Publishing Platform; 2016.
14. Bartoletti M, Pompianu L. An empirical analysis of smart contracts: platforms, applications, and design patterns. In: International conference on financial cryptography and data security. Springer: New York; 2017. p. 494–509.
15. Alharby M, van Moorsel A. Blockchain-based smart contracts: a systematic mapping study. arXiv preprint arXiv :1710.06372. 2017.
16. Magazzeni D, McBurney P, Nash W. Validation and verification of smart contracts: a research agenda. Computer. 2017;50(9):50–7.
17. Diedrich H. Ethereum: blockchains, digital assets, smart contracts, decentralized autonomous organizations. Sydney: Wildfire Publishing; 2016.
18. Dannen C. Introducing ethereum and solidity: foundations of cryptocurrency and blockchain programming for beginners. Berkely: Apress; 2017.
19. Atzei N, Bartoletti M, Cimoli T. A survey of attacks on ethereum smart contracts (sok). In: International conference on principles of security and trust. Springer: New York; 2017. p. 164–86.
20. Antonopoulos AM, Wood G. Mastering ethereum: building smart contracts and DApps. California: O'Reilly Media; 2018.
21. Wang W, Hoang DT, Xiong Z, Niyato D, Wang P, Hu P, Wen Y. A survey on consensus mechanisms and mining management in blockchain networks. arXiv preprint arXiv:1805.02707. 2018.
22. Debus J. Consensus methods in blockchain systems. Frankfurt School of Finance & Management, Blockchain Center, technical report; 2017. p. 1–58.
23. Pass R, Seeman L, Shelat A. Analysis of the blockchain protocol in asynchronous networks. In: Annual international conference on the theory and applications of cryptographic techniques. Springer: New York; 2017. p. 643–73.
24. Pass R, Shi E. Hybrid consensus: efficient consensus in the permissionless model. In: 31st international symposium on distributed computing (DISC 2017). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik; 2017. p. 1–16.
25. Cachin C, Vukolić M. Blockchain consensus protocols in the wild. arXiv preprint arXiv:1707.01873. 2017.
26. Karame G, Audroulaki E. Bitcoin and blockchain security. Massachusetts: Artech House; 2016.
27. Lin I-C, Liao T-C. A survey of blockchain security issues and challenges. Int J Netw Secur. 2017;19(5):653–9.
28. Joshi AP, Han M, Wang Y. A survey on security and privacy issues of blockchain technology. Math Found Comput. 2018;1(2):121–47.
29. Swan M. Blockchain: blueprint for a new economy. California: O'Reilly Media; 2015.

30. Catalini C, Gans J. Some simple economics of the blockchain. Cambridge: National Bureau of Economic Research; 2016. p. 1–29.
31. Davidson S, De Filippi P, Potts J. Economics of blockchain. In: Public choice conference; 2016. p. 1–23.
32. Bheemaiah K. The blockchain alternative: rethinking macroeconomic policy and economic theory. Berkely: Apress; 2017.
33. Beck R, Müller-Bloch C, King JL. Governance in the blockchain economy: a framework and research agenda. J Assoc Inf Syst. 2018;19(10):1020–34.
34. Biais B, Casamatta C, Bisire C, Bouvard M. The blockchain folk theorem. Rev Financ Stud. 2019;32(5):1662–715.
35. Kiayias A, Koutsoupias E, Kyropoulou M, Tselekounis Y. Blockchain mining games. In: Proceedings of the 2016 ACM conference on economics and computation. ACM: New York; 2016. p. 365–82.
36. Abadi J, Brunnermeier M. Blockchain economics. New York: National Bureau of Economic Research; 2018. p. 1–82.
37. Foroglou G, Tsilidou A-L. Further applications of the blockchain. In: 12th student conference on managerial science and technology; 2015. p. 1–9.
38. Bahga A, Madisetti V. Blockchain applications: a hands-on approach. Blacksburg: VPT; 2017.
39. Xu X, Weber I, Staples M. Architecture for blockchain applications. Basel: Springer; 2019.
40. Tsai W-T, Blower R, Zhu Y, Yu L. A system view of financial blockchains. In: 2016 IEEE symposium on service-oriented system engineering (SOSE). IEEE: New York; 2016. p. 450–457.
41. Nguyen QK. Blockchain-a financial technology for future sustainable development. In: 2016 3rd international conference on green technology and sustainable development (GTSD). IEEE: New York; 2016. p. 51–4.
42. Tapscott A, Tapscott D. How blockchain is changing finance. Harv Bus Rev. 2017;1(9):2–5.
43. Treleaven P, Brown RG, Yang D. Blockchain technology in finance. Computer. 2017;50(9):14–7.
44. Casey M, Crane J, Gensler G, Johnson S, Narula N. The impact of blockchain technology on finance: a catalyst for change. Geneva: International Center for Monetary and Banking Studies (ICMB); 2018.
45. Mougayar W, Buterin V. The business blockchain: promise, practice, and application of the next internet technology. Hoboken: Wiley; 2016.
46. Morabito V. Business innovation through blockchain. Milan: Springer; 2017.
47. Fleming S. Blockchain technology and DevOps: introduction and its impact on business ecosystem. EU: Stephen Fleming via PublishDrive; 2017.
48. Beck R, Avital M, Rossi M, Thatcher JB. Blockchain technology in business and information systems research. Bus Inf Syst Eng. 2017;59(6):381–4.
49. Nowiński W, Kozma M. How can blockchain technology disrupt the existing business models? Entrep Bus Econ Rev. 2017;5(3):173–88.
50. Mendling J, Weber I, Aalst WVD, Brocke JV, Cabanillas C, Daniel F, Debois S, Ciccio CD, Dumas M, Dustdar S, et al. Blockchains for business process management-challenges and opportunities. ACM Trans Manag Inf Syst. 2018;9(1):4.
51. Hofmann E, Strewe UM, Bosia N. Supply chain finance and blockchain technology: the case of reverse securitisation. Heidelberg: Springer; 2017.
52. Korpela K, Hallikas J, Dahlberg T. Digital supply chain transformation toward blockchain integration. In: Proceedings of the 50th Hawaii international conference on system sciences; 2017.
53. Kim HM, Laskowski M. Toward an ontology-driven blockchain design for supply-chain provenance. Intell Syst Account Financ Manag. 2018;25(1):18–27.
54. Saberi S, Kouhizadeh M, Sarkis J, Shen L. Blockchain technology and its relationships to sustainable supply chain management. Int J Prod Res. 2018;57(7):2117–35.
55. Petersen M, Hackius N, von See B. Mapping the sea of opportunities: blockchain in supply chain and logistics. IT Inf Technol. 2018;60(5–6):263–71.
56. Sternberg H, Baruffaldi G. Chains in chains–logic and challenges of blockchains in supply chains. In: Proceedings of the 51st annual Hawaii international conference on system sciences; 2018. p. 3936–43.
57. Dujak D, Sajter D. Blockchain applications in supply chain. In: SMART supply network. Springer: New York; 2019. p. 21–46.
58. Conoscenti M, Vetro A, Martin JD. Blockchain for the internet of things: a systematic literature review. In: 2016 IEEE/ACS 13th international conference of computer systems and applications (AICCSA). IEEE: New Yrok; 2016. p. 1–6.
59. Bahga A, Madisetti VK. Blockchain platform for industrial internet of things. J Softw Eng Appl. 2016;9(10):533–46.
60. Dorri A, Kanhere SS, Jurdak R. Blockchain in internet of things: challenges and solutions. arXiv preprint arXiv :1608.05187. 2016.
61. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. IEEE Access. 2016;4:2292–303.
62. Zhang Y, Wen J. The IoT electric business model: using blockchain technology for the internet of things. Peer-to-Peer Netw Appl. 2017;10(4):983–94.
63. Huckle S, Bhattacharya R, White M, Beloff N. Internet of things, blockchain and shared economy applications. Procedia Comput Sci. 2016;98:461–6.
64. Hawlitschek F, Notheisen B, Teubner T. The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy. Electron Commer Res Appl. 2018;29:50–63.
65. De Filippi P. What blockchain means for the sharing economy. Harvard business review digital articles, 2017. pp 2-5. http://search.ebscohost.com.ezproxy.is.ed.ac.uk/login.aspx?direct=true&db=bth&AN=122087609&site=ehost-live
66. Pazaitis A, De Filippi P, Kostakis V. Blockchain and value systems in the sharing economy: the illustrative case of backfeed. Technol Forecast Soc Change. 2017;125:105–15.
67. Mettler M. Blockchain technology in healthcare: The revolution starts here. In: 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom). IEEE: New York; 2016. p. 1–3.
68. Rabah K. Challenges & opportunities for blockchain powered healthcare systems: a review. Mara Res J Med Health Sci. 2017;1(1):45–52 (ISSN 2523-5680).

69. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst. 2018;42(7):130.
70. Wang S, Wang J, Wang X, Qiu T, Yuan Y, Ouyang L, Guo Y, Wang F-Y. Blockchain-powered parallel healthcare systems based on the ACP approach. IEEE Trans Comput Soc Syst. 2018;99:1–9.
71. Oh S-C, Kim M-S, Park Y, Roh G-T, Lee C-W. Implementation of blockchain-based energy trading system. Asia Pac J Innov Entrep. 2017;11(3):322–34.
72. Aitzhan NZ, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans Dependable Secur Comput. 2018;15(5):840–52.
73. Noor S, Yang W, Guo M, van Dam KH, Wang X. Energy demand side management within micro-grid networks enhanced by blockchain. Appl Energy. 2018;228:1385–98.
74. Wu J, Tran N. Application of blockchain technology in sustainable energy systems: an overview. Sustainability. 2018;10(9):3067.
75. Li Q-L, Ma J-Y, Chang Y-X. Blockchain queue theory. In: International conference on computational social networks. Springer: New York; 2018. p. 25–40.
76. Kasahara S, Kawahara J. Effect of bitcoin fee on transaction–confirmation process. arXiv preprint arXiv:1604.00103. 2016.
77. Kawase Y, Kasahara S. transaction–confirmation time for bitcoin: a queueing analytical approach to blockchain mechanism. In: International conference on queueing theory and network applications. Springer: New York; 2017. p. 75–88.
78. Ricci S, Ferreira E, Menasche DS, Ziviani A, Souza JE, Vieira AB. Learning blockchain delays: a queueing theory approach. ACM SIGMETRICS Perform Eval Rev. 2019;46(3):122–5.
79. Memon RA, Li JP, Ahmed J. Simulation model for blockchain systems using queuing theory. Electronics. 2019;8(2):234.
80. Bowden R, Keeler HP, Krzesinski AE, Taylor PG. Block arrivals in the bitcoin blockchain. arXiv preprint arXiv :1801.07447. 2018.
81. Papadis N, Borst S, Walid A, Grissa M, Tassiulas L. Stochastic models and wide-area network measurements for blockchain design and analysis. In: IEEE INFOCOM 2018-IEEE conference on computer communications. IEEE: New York; 2018. p. 2546–54.
82. Jourdan M, Blandin S, Wynter L, Deshpande P. A probabilistic model of the bitcoin blockchain. arXiv preprint arXiv :1812.05451. 2018.
83. Bolch G, Greiner S, de Meer H, Trivedi KS. Queueing networks and Markov chains: modeling and performance evaluation with computer science applications. New York: Wiley; 2006.
84. Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. Commun ACM. 2018;61(7):95–102.
85. Nayak K, Kumar S, Miller A, Shi E. Stubborn mining: generalizing selfish mining and combining with an eclipse attack. In: 2016 IEEE European symposium on security and privacy (EuroS&P). IEEE: New York; 2016. p. 305–20.
86. Carlsten M. The impact of transaction fees on bitcoin mining strategies. Ph.D. thesis, Princeton University; 2016.
87. Göbel J, Keeler HP, Krzesinski AE, Taylor PG. Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay. Perform Eval. 2016;104:23–41.
88. Kiffer L, Rajaraman R, et al. A better method to analyze blockchain consistency. In: Proceedings of the 2018 ACM SIGSAC conference on computer and communications security. ACM: New York; 2018. p. 729–44.
89. Huang D, Ma X, Zhang S. Performance analysis of the raft consensus algorithm for private blockchains. IEEE Trans Syst Man Cybern Syst. 2019;. https://doi.org/10.1109/TSMC.2019.2895471.
90. Sapirshtein A, Sompolinsky Y, Zohar A. Optimal selfish mining strategies in bitcoin. In: International conference on financial cryptography and data security. Springer: New York; 2016. p. 515–32.
91. Sompolinsky Y, Zohar A. Bitcoin's security model revisited. arXiv preprint arXiv:1605.09193. 2016.
92. Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S. On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. ACM: New York; 2016. p. 3–16.
93. Goffard P-O. Fraud risk assessment within blockchain transactions. Working paper or preprint 2019. https://hal.archives-ouvertes.fr/hal-01716687.
94. Jang J. Lee H-N. Profitable double-spending attacks. arXiv preprint arXiv:1903.01711. 2019.
95. Frolkova M, Mandjes M. A bitcoin-inspired infinite-server model with a random fluid limit. Stoch Models. 2019;. https://doi.org/10.1080/15326349.2018.1559739.
96. King C. The fluid limit of a random graph model for a shared ledger. arXiv preprint arXiv:1902.05050. 2019.
97. Li Q-L. Constructive Computation in stochastic models with applications: the RG-factorizations. Berlin: Springer; 2010.
98. Neuts MF. Matrix-geometric solutions in stochastic models: an algorithmic approach. Maryland: Johns Hopkins University; 1981.
99. Li Q-L, Lian Z, Liu L. An *RG*-factorization approach for a BMAP/M/1 generalized processor-sharing queue. Stoch Models. 2005;21(2–3):507–30.
100. Takine T. Analysis and computation of the stationary distribution in a special class of Markov chains of level-dependent M/G/1-type and its application to BMAP/M/∞ and BMAP/M/c+M queues. Queueing Syst. 2016;84(1/2):49–77.

Publisher's Note