IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 13, 2020, accepted March 26, 2020, date of publication April 15, 2020, date of current version May 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2986084

Nash Equilibrium and Social Optimization of Transactions in Blockchain System Based on Discrete-Time Queue

JIAXING QI, JING YU, AND SHUNFU JIN
School of Information Science and Engineering, Yanshan University, Qinhuangdao 066004, China
Corresponding author: Shunfu Jin (jsf@ysu.edu.cn)

This work was supported in part by the National Natural Science Foundation under Grant 61872311 and Grant 61973261, and in part by the Natural Science Foundation of Hebei Province, China, under Grant F2017203141.

ABSTRACT Blockchain technology has been used in many fields such as data management, cloud computing and Internet of Things with the features of decentralization, transparency and immutability. In order to study the performance of a blockchain system with a light-load traffic, we establish a discrete-time non-exhaustive vacation queue with batch service and gated service. In this model, we regard transaction initiation, mining processing and block verification as arrival, vacation and service period, respectively. By using an embedded Markov chain method and a regeneration cycle approach, we derive the average response time of transactions. Experiment results with analysis and simulation show that the average response time of transactions is impacted by the arrival rate of transactions. Finally, we study the Nash equilibrium behavior and the socially optimal behavior of transactions, and present a pricing policy for transactions to maximize the social profit.

INDEX TERMS Blockchain system, discrete-time vaction queue, regeneration cycle, response time, pricing policy.

I. INTRODUCTION

Since Satoshi Nakamoto proposed the concept of Bitcoin in 2008 [1], cryptocurrencies have developed rapidly. As the core supporting technology of Bitcoin, blockchain has gained widespread attention [2]. Blockchain is a public and decentralized data storage structure. With the characteristics of decentralization, transparency and immutability, blockchain has wide application scenarios and important research significance [3].

Blockchain technology has been applied in the fields of managing medical information [4]–[6], cloud computing [7]–[9], Internet of Things (IoT) [10]–[12], smart voting [13]–[15] and security services [16]–[18]. Considering the third-party's security of cross-domain image sharing, Patel, V. developed a distributed data store framework based on blockchain technology [4]. The main feature of this structure is that patients have easy access to their own medical information and control access to other institutions.

The associate editor coordinating the review of this manuscript and approving it for publication was Xujie Li.

In [7], Wilczyński, A. and Kołodziej, J. proposed a Blockchain Scheduler for the cloud computing. In this Blockchain Scheduler, a novel 'proof–of–schedule' consensus algorithm based on the 'proof-of-work' was designed. Together with Stackelberg games, the approval of generated schedules was improved. This Blockchain Scheduler not only optimized the resource scheduling scheme, but also improved the system security in the task allocation, data storage and transmission among the cloud nodes and clusters. Using blockchain technology, Sharma, P.K. et.al proposed a distributed secure SDN architecture (DistBlockNet) for IoT [10]. In this architecture all the IoT forwarding devices can easily and efficiently interact with each other without a central controller. With the operational flexibility, the DistBlockNet architecture can efficiently generate and deploy protections. Khoury, D. et.al proposed a decentralized trustless voting platform [13]. The blockchain environment of this voting platform is Ethereum Virtual Machine. On this voting platform, each voting event is a transparent, consistent and deterministic smart contract deployed by organizer. For the purpose of centrally sharing heterogeneous

logistics resources with different customers, Li, M. et.al proposed a blockchain-enabled workflow operating system (Bc-WfOS) [16]. The Bc-WfOS includes three key innovative technologies: the virtual resource gateway, the multi-dimensional workflow model and the blockchain-enabled agent-based workflow management method. The main function of blockchain technology in this operating system is to guarantee data reliability and truthfulness. All the application research above have brought great help to industries, but ignored performance analysis of the blockchain system.

Blockchain architectures face serious latency issues which may be proved more significant as they evolve [19]. In this situation, mathematical modeling of blockchain performance becomes very important.

To study the effect of micro payment on the confirmation time of small amount transactions, Kasahara, S. and Kawahara, J. investigated a priority queueing system with batch service [20]. In this queueing system, the confirmation process of transactions was regarded as a service. The average confirmation time of transactions was derived by using the supplementary variable method. In [21] and [22], Kawase, Y. and Kasahara, S. built a queueing model with batch service to study the influence of the block-size limit on the confirmation time of transactions. Considering that the mining work does not stop even though there are no transactions in the system, the server was assumed to be always busy. The average confirmation time of transactions was derived by the supplementary variable method [21] and by the matrix analytic method [22], respectively. In the research above, the mining period and the block verification period in the confirmation process of transactions were combined together as a service period. During the service period, at most b transactions, including the transactions arriving within the service period, were served in a batch. These mathematical models are inappropriate to capture the impact of the proof-of-work on the system performance.

In order to better capture the workflow of the blockchain system, Li, Q.L. et.al built a Markovian batch-service queueing system with two different service stages [23]. By using the method of the matrix-geometric solution, they derived the average number of transactions in the queue, the average number of transactions in a block and the average confirmation time of transactions. However, empty blocks in the blockchain system were not taken into account in this queueing system.

Considering empty blocks, Zhao, W. et.al established a non-exhaustive vacation queueing system with a limited batch service to model the blockchain system [24]. By analyzing the elapsed time for a mining cycle, they derived the average confirmation time of transactions and showed the influence of arrival rate on the average confirmation time of transactions. To maximize the overall revenue of the blockchain system, they proposed a pricing policy forcing the transactions to accept the socially optimal arrival rate. The limited batch service discipline is more suitable for investigating the blockchain system with heavy trading volume. However, if a blockchain system is at a light-load traffic, the vacation queueing model with gated service is the preferred one to study the system performance.

In this paper, considering a light-load blockchain system, we separate the confirmation process of transactions into two periods, and we build a non-exhaustive vacation queue with batch service and gated service. In particular, the batch service considered in this paper is different from that in [20]–[22]. In this paper, the block verification period is regarded as a service period. During the service period, all the transactions present at the beginning instant of the service period are served in a batch, and transactions arriving during a service period get service at the next service period. We evaluate the performance of the blockchain system and give a pricing policy charging for transactions to maximize the total benefit of all the transactions and the blockchain system.

The remainder of this paper is organized as follows. In Section II, we build a queueing model based on the confirmation process of transactions in a light-load blockchain system. In Section III, using the regeneration cycle approach, we analyze the queueing model and derive the average confirmation time of transactions. In Section IV, we carry out experiments with analysis and simulation to demonstrate how the parameters of the blockchain system affect the average confirmation time of transactions. In Section V, we propose a pricing policy to regulate the arrival rate of transactions to maximize the social profit. Finally, we give concluding remarks in Section VI.

II. MATHEMATICAL MODEL OF A BLOCKCHAIN SYSTEM

A. CONFIRMATION PROCESS OF TRANSACTIONS IN A BLOCKCHAIN SYSTEM

In this subsection, we will take Bitcoin as an example to discuss the confirmation process of transactions in a blockchain system.

In a blockchain system, there are three types of elements: transaction, block and chain. The payment nodes broadcast the transactions to the system, and each transaction has it's own digital signatures. The transactions are packaged into blocks, and then, blocks are linked together following a First Come First Served (FCFS) order to form a chain. The node that successfully packages a block will get fees from the transactions in this block and obtain reward from the blockchain system. So, many nodes participate in the confirmation process to compete this valuable income, and these nodes are called miners. As seen in Fig. 1, the confirmation process for a batch of transactions is divided into two periods: packaging period and verification period. No matter in which period, all the miners continually receive the new transactions and put them into memory pool.

The first period is packaging period, and the packaging period is also called mining period. During the mining period, each miner packages a certain amount of transactions in it's memory pool into a block. When the traffic load of the blockchain system is light, all the unconfirmed transactions

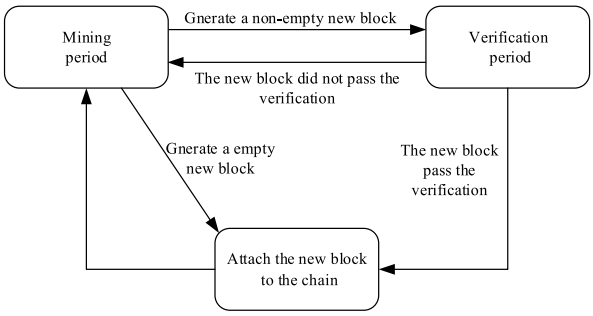

FIGURE 1. State-transition diagram for the blockchain sytem.

in memory will be packaged into one block. Miners work hard to find a random value to complete the proof-of-work issued by the blockchain system. The difficulty coefficient of the proof-of-work is expressed as a mining parameter, and the mining parameter is called as mining rate. As the mining rate increases, a mining period lasts shorter time. The first miner who completed the proof-of-work is called a successful miner, whereas the other miners are called unsuccessful miners. The successful miner broadcasts a new block to all the unsuccessful miners. After a newly generated block is successfully broadcasted, the blockchain system enters to a verification period from the mining period.

When the blockchain system is in the verification period, all the unsuccessful miners will consecutively receive a newly generated block. And then, all the unsuccessful miners verify the hash value, transactions and proof-of-work, etc. in the new block. If an unsuccessful miner doesn't accept the new block, the unsuccessful miner will abandon this block. Otherwise, the unsuccessful miner will attache the new block to it's own chain and remove all the transactions in this block from memory pool. If the number of unsuccessful miners accepting the new block reaches the blockchain system threshold, the successful miner also attaches the new block to it's own chain, and the confirmation process for transactions contained in the new block is completed. Conversely, if the number of unsuccessful miners not accepting the new block reaches the system threshold, the successful miner abandons the new block. No matter the new block is accepted or not, the blockchain system will return back to the mining period from the verification period.

B. QUEUEING MODEL

Based on the confirmation process of transactions in the blockchain system with a light-load traffic, we establish a discrete-time non-exhaustive vacation queueing model with gated and batch service.

We firstly introduce a gated service. Once a verification period ends, the blockchain system will enter a mining period, regardless of whether exist unconfirmed transactions in the blockchain system or not. If there are no unconfirmed transactions in the blockchain system at the end instant of a mining period, an empty block will be generated, and the blockchain system enters a new mining period directly. Here, we ignore the verification process of an empty block. Otherwise, the blockchain system packages all the unconfirmed transactions in the system into a new block and starts to verify the new block. Consequently, transactions arriving during a verification period can only be verified in the next verification period.

We also consider a batch service. Note that only if all the transactions in a new block are verified, the new block can be linked to the blockchain. In the blockchain system with a light-load traffic, all the unconfirmed transactions in memory will be packaged into one block without constraints of the block size, and the transactions in one block are called as a batch of transactions. We assume that when the verification period starts, the blockchain system starts to verify all the transactions in a batch. The verifications of the transactions in a batch are completed simultaneously at the end instant of a verification period. Obviously, this type of bath service is more appropriate to investigate the performance of the blockchain system with a light-load traffic.

We regard the verification period as a service period. Let S_p be the time length of a service period. S_p is supposed to be a general, independent and identically distributed discrete-time random variable. The probability mass function (p.m.f.) b_k, the probability generating function (p.g.f.) $S_p(z)$ and the average value $E\left[S_p\right]$ of S_p are given by

$$b_k = P\left\{S_p = k\right\}, \quad S_p(z) = \sum_{k=1}^{\infty} z^k b_k,$$

$$E\left[S_p\right] = \sum_{k=1}^{\infty} k b_k = \frac{1}{\mu}, \quad 0 < \mu < 1,$$

where μ is the service parameter.

We regard the mining period as a vacation period. Let V be the time length of a vacation period. V is supposed to be a general, independent and identically distributed discrete-time random variable. The p.m.f. v_k, the p.g.f. $V(z)$ and the average value $E[V]$ of V are given by

$$v_k = P\{V = k\}, \quad V(z) = \sum_{k=1}^{\infty} z^k v_k,$$

$$E[V] = \sum_{k=1}^{\infty} k v_k = \frac{1}{\theta}, \quad 0 < \theta < 1,$$

where θ is the mining rate.

A service cycle, or simply a cycle, is defined as the time period between the beginnings of two service periods. Let C be the time length of a vacation period and Q_b be the number of transactions in the system at the beginning instant of a service period. Following the service discipline under consideration, the time length of a service cycle depends on whether there are new transaction arrivals or not within a service period.

According to whether there are new transaction arrivals or not within a service period, we discuss the queueing situation following four cases as shown in Fig. 2.

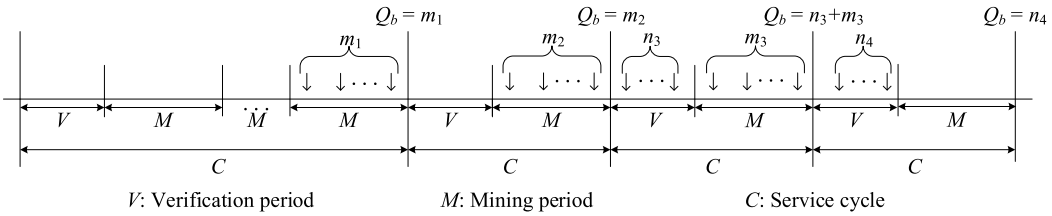

FIGURE 2. Workflow of the queueing model.

- If no transaction arrives during the verification period of a service cycle and no transaction arrives during the first mining period of the service cycle, the service cycle is continued until the end of a mining period with transaction arrivals. If the number of transactions arriving within this mining period is m_1, the number of transactions in the system at the beginning instant of next verification period is $Q_b = m_1$.
- If no transaction arrives during the verification period of a service cycle, but at least one transaction arrives during the first mining period of the service cycle, the service cycle ends in the first mining period. If the number of transactions arriving within this mining period is m_2, the number of transactions in the system at the beginning instant of next verification period is $Q_b = m_2$.
- If there are transaction arrivals during both the verification period of a service cycle and the first mining period of the service cycle, the service cycle ends in the first mining period. If the number of transactions arriving within the verification period is n_3 and the number of transactions arriving within the mining period is m_3, the number of transactions in the system at the beginning instant of next verification period is $Q_b = n_3 + m_3$.
- If there are transaction arrivals during the verification period of a service cycle, but no transaction arrivals during the first mining period of the service cycle, the service cycle ends in the first mining period. If the number of transactions arriving within this verification period is n_4, the number of transactions in the system at the beginning instant of next verification period is $Q_b = n_4$.

III. MODEL ANALYSIS

We assume that transactions arrive just before the end instant of the nth slot, $n = 1, 2, \ldots$, and verification process starts or ends just after the end instant of the nth slot, $n = 2, 3, \ldots$. This class of system is also called "late arrival" system with delay access [25]. We assume that the system buffer is infinite, and the arrival interval T of transactions follows a geometric distribution with parameter p ($p > 0$).

Let A_s be the number of transactions arriving within a service period. The p.m.f. a_{sj} and the p.g.f. $A_s(z)$ of A_s are given as

$$\begin{aligned} a_{sj} &= P\{A_s = j\} \\ &= \sum_{k=j}^{\infty} P\left\{S_p = k\right\} \binom{k}{j} p^j \overline{p}^{k-j}, \quad j = 0, 1, 2, \ldots \end{aligned} \tag{1}$$

$$\begin{aligned} A_s(z) &= \sum_{j=0}^{\infty} z^j a_{sj} \\ &= \sum_{k=1}^{\infty} P\left\{S_p = k\right\} (\overline{p} + pz)^k \\ &= S_p(\lambda(z)), \end{aligned} \tag{2}$$

where $\lambda(z) = \overline{p} + pz$.

Similarly, the p.g.f. $A_v(z)$ for the number of transactions arriving within a vacation period can be written as

$$A_v(z) = V(\lambda(z)). \tag{3}$$

Based on (1), we get the probability a_{s0} that no transaction arrives within a service period as

$$\begin{aligned} a_{s0} &= \sum_{k=0}^{\infty} P\left\{S_p = k\right\} \binom{k}{0} \overline{p}^k \\ &= S_p(\overline{p}). \end{aligned} \tag{4}$$

Similarly, the probability a_{v0} that no transaction arrives within a vacation period can be written as

$$a_{v0} = V(\overline{p}). \tag{5}$$

Based on (4) and (5), we get the probability that there are transactions arrive within a service period or a vacation period is $1 - S_p(\overline{p})$ and $1 - V(\overline{p})$, respectively. Note that in a queueing system with a gated service, only those customers present at the server's return from a vacation are candidates for service during the server visit, subsequent arrivals are deferred until the next server visit. For the blockchain system considered in this paper, the transactions present in the system at the beginning instant of a service period are those arrived within the previous service cycle. The p.g.f. $Q_b(z)$ for the number Q_b of transactions in the system at the beginning instant of a service period is then obtained as follows:

$$Q_b(z) = \left(1 - S_p(\overline{p})\right) \frac{S_p(\lambda(z)) - S_p(\overline{p})}{1 - S_p(\overline{p})} V(\lambda(z))$$

$$+S_p(\overline{p})\frac{V(\lambda(z))-V(\overline{p})}{1-V(\overline{p})}$$
$$=S_p(\lambda(z))V(\lambda(z))$$
$$+\frac{S_p(\overline{p})V(\overline{p})}{1-V(\overline{p})}(V(\lambda(z))-1). \quad (6)$$

Differentiating (6) with respect to z at $z=1$, the average value $E[Q_b]$ of Q_b is given as follows:

$$E[Q_b]=pE[S_p]+\left(1+\frac{S_p(\overline{p})+V(\overline{p})}{1-V(\overline{p})}\right)pE[V]. \quad (7)$$

Let Φ be the number of transactions verified during a service period. Following the gated service discipline, Φ equals to the number of transactions in the system at the beginning instant of this service period. So we have

$$\Phi=Q_b. \quad (8)$$

In a batch service queueing model, the verifications of all the transactions should be completed simultaneously. In order to clarify the model analysis, we assume that transactions are verified one by one during infinitesimal interval just before the end instant of a verification period. Using the imbedded Markov chain method, we identify the instant just after the end of every verification period as the Markov chain points.

Let L_n^+ be the number of transactions in the system immediately after the nth transaction gets verified. We have

$$L_n^+=Q_b-n+A_s,\quad n=1,2,\ldots,Q_b. \quad (9)$$

$\{L_n^+, n=1,2,\ldots\}$ constitutes a discrete-time Markov chain.

Let L^+ denote the steady-state distribution for the Markov chain $\{L_n^+, n=1,2,\ldots\}$. Using regeneration cycle approach [26], the p.g.f. $L^+(z)$ of L^+ can be expressed as follows:

$$L^+(z)=\frac{1}{E[\Phi]}E\left[\sum_{n=1}^{\Phi}z^{L_n^+}\right]. \quad (10)$$

Substituting (7) and (9) into (10) yields

$$L^+(z)=\frac{S_p(\lambda(z))}{(z-1)}\times\Big(\frac{\left(S_p(\lambda(z))V(\lambda(z))-1\right)(1-V(\overline{p}))}{p\left((1-V(\overline{p}))\left(E\left[S_p\right]+E[V]\right)+S_p(\overline{p})V(\overline{p})E[V]\right)}+\frac{S_p(\overline{p})V(\overline{p})(V(\lambda(z))-1)}{p\left((1-V(\overline{p}))\left(E\left[S_p\right]+E[V]\right)+S_p(\overline{p})V(\overline{p})E[V]\right)}\Big). \quad (11)$$

Differentiating (11) with respect to z at $z=1$, the average value $E\left[L^+\right]$ of L^+ is given as follows:

$$E\left[L^+\right]=pE\left[S_p\right]+\frac{p(1-V(\overline{p}))}{2(1-V(\overline{p}))\left(E\left[S_p\right]+E[V]\right)+2S_p(\overline{p})V(\overline{p})E[V]}\times\frac{\left(E\left[S_p\left(S_p-1\right)\right]+E[V(V-1)]+2E\left[S_p\right]E[V]\right)}{2(1-V(\overline{p}))\left(E\left[S_p\right]+E[V]\right)+2S_p(\overline{p})V(\overline{p})E[V]}. \quad (12)$$

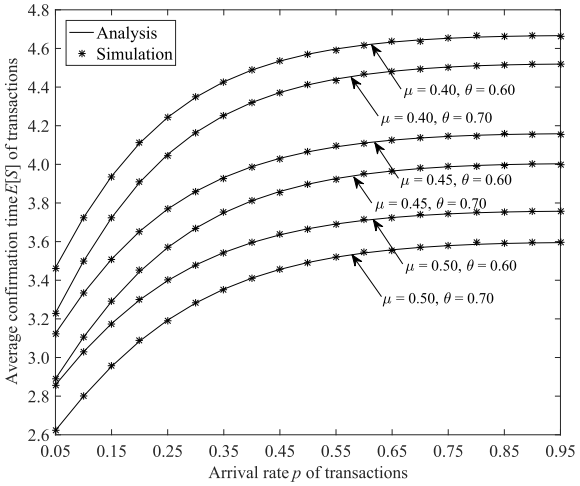

FIGURE 3. Change trend for the average confirmation time $E[S]$ of transactions.

Applying Little's Law, we get the average response time $E[S]$ of transactions as follows:

$$E[S]=\frac{E\left[L^+\right]}{p}=E\left[S_p\right]+\frac{(1-V(\overline{p}))}{2(1-V(\overline{p}))\left(E\left[S_p\right]+E[V]\right)+2S_p(\overline{p})V(\overline{p})E[V]}\times\frac{\left(E\left[S_p\left(S_p-1\right)\right]+E[V(V-1)]+2E\left[S_p\right]E[V]\right)}{2(1-V(\overline{p}))\left(E\left[S_p\right]+E[V]\right)+2S_p(\overline{p})V(\overline{p})E[V]}. \quad (13)$$

IV. NUMERICAL EXPERIMENTS

In order to study the impacts for the arrival rate p of transactions, mining rate θ and service parameter μ on the confirmation time of transactions in the blockchain system, we carry out numerical experiments and simulation experiments, respectively.

The hardware environment of the experiments is as follows: Intel(R) Core(TM) i7-4790 CPU @ 3.60 GHz, 8.00 GB RAM. The software environment of the experiments with analysis is Matlab. The software environment of the simulation system encrypted by the Java programming language is MyEclipse.

To make the experiments feasible, we assume that both the mining period and the verification period follow a geometric distribution. We set the mining rate as $\theta=0.6, 0.7$, the service parameter as $\mu=0.4, 0.45, 0.5$. As seen in Fig. 3, when the arrival rate p of transactions ranges from 0.05 to 0.95, the results of numerical experiments and simulation experiments are in perfect agreement.

Fig. 3 illustrates the change trend for the average confirmation time $E[S]$ of transactions along with the arrival rate p of transactions, for different combination service parameter μ and mining rate θ.

From Fig. 3, we find that as the arrival rate p of transactions increases, the average confirmation time $E[S]$ shows an increasing tendency. Based on the gated service discipline, as the arrival rate of transactions increases, more transactions are likely to arrive at the blockchain system during the verification period. Transactions arriving during the verification period will last longer before getting verification, so the average confirmation time of transactions will be greater.

We also find that for a fixed arrival rate p of transactions the larger the mining rate θ or the service parameter μ is, the smaller the average confirmation time $E[S]$ of transactions is. The larger the mining rate is, the shorter the mining period is, on the other hand, the higher the service parameter is, the shorter the verification period is. Both the increase in the mining rate and the increase in the service parameter will reduce the time length of the service cycle, and then the average confirmation time of transactions will be shorter.

Experimental results mentioned above show that the arrival rate of transactions, the mining rate and the service parameter directly impact the average confirmation time of transactions. From the perspective of an individual transaction, lower arrival rate of transactions is more advantageous. However, from the perspective of the whole blockchain system, higher arrival rate of transactions is more valuable. So, we need to study how to balance the interests of an individual transaction and the whole blockchain system.

V. PERFORMANCE OPTIMIZATION AND PRICING POLICY

In this section, considering the interests of the individual transaction and the whole blockchain system, we present a reasonable pricing policy based on the Nash equilibrium behavior and the socially optimal behavior of transactions.

A. NASH EQUILIBRIUM BEHAVIOR AND SOCIALLY OPTIMAL BEHAVIOR

In the blockchain system, when a transaction is confirmed, the payment node will get trading benefit. However a transaction need pay time cost for being confirmed. When the arrival rate of transactions is lower, the average confirmation time of transactions is smaller, and the tradings will be profitable for most transactions. On the contrary, when the arrival rate of transactions is higher, the average confirmation time of transactions is longer, and some transactions will take risk of being at a loss. How to regulate the number of transactions arriving at the blockchain system is important.

Regarding payment nodes as players, we discuss a non-cooperative game between payment nodes who want to get trading benefit by broadcasting transactions. For this, we give some hypothesis as follows:

(1) Before a transaction is broadcasted, the node generating the transaction has no information on the system state.
(2) The reward of a confirmed transaction is R.
(3) The time cost of a transaction staying in the blockchain system is C per slot.

Based on the hypothesis mentioned above, we use the average confirmation time $E[S]$ of transactions given in Sect. III to obtain the average net benefit $U_{ind}(p)$ of a transaction as follows:

$$U_{ind}(p) = R - CE[S]. \tag{14}$$

We set the lowest arrival rate of transactions as p_{min} and the highest arrival rate of transactions as p_{max}. In the Nash equilibrium strategy, all the players will play best response to each other, so we discuss the Nash equilibrium behavior of transactions within the closed interval $[p_{min}, p_{max}]$ as follows:

(1) If $U_{ind}(p_{min}) \leq 0$, the average net benefit $U_{ind}(p)$ of a transaction is negative. Obviously, not broadcasting transactions to the system is a domain strategy for a payment node.
(2) If $U_{ind}(p_{max}) \geq 0$, the average net benefit $U_{ind}(p)$ of a transaction is positive. Therefore, broadcasting transactions to the system is a domain strategy for a payment node.
(3) For the case of $U_{ind}(p_{min}) > 0$ and $U_{ind}(p_{max}) < 0$, if $p = p_{max}$, a payment node can't get a positive net benefit by broadcasting. Hence, broadcasting transaction to system cannot be an equilibrium strategy. When $p = p_{min}$, a payment node can get a positive net benefit by broadcasting transactions to the system, more than not broadcasting. Hence, not broadcasting transactions to system cannot be an equilibrium strategy too. But there exists a unique arrival rate p_e of transactions subject to $U_{ind}(p_e) = 0$. We call that the arrival rate p_e of transactions with zero net benefit the Nash equilibrium arrival rate of transactions.

Referencing to [27], the social profit is defined as the total benefit of all the transactions and the blockchain system. If no admission fees are imposed, the social profit is the sum of the individual benefits of all transactions. The social profit $U_{soc}(p)$ per slot is given as follows:

$$U_{soc}(p) = p(R - CE[S]), \tag{15}$$

where p is the arrival rate of transactions. p is in fact the average number of transactions arriving at the blockchain system per slot. We call the arrival rate of transactions with the highest social profit the socially optimal arrival rate p^* of transactions.

In this paper, the time length of mining period and the time length of verification period are assumed to follow general distributions. As a result, the uniqueness of the Nash equilibrium arrival rate p_e of transactions is difficult to be proved strictly. For this, we carry out analysis experiments based on (14) and (15) to continue investigate the Nash equilibrium behavior and socially optimal behavior of transactions.

Using the parameters set in Sect. IV and taking $R = 35$ and $C = 10$ as an example, we demonstrate the change trend for the average net benefit $U_{ind}(p)$ of a transaction in Fig. 4.

From Fig. 4, we find that for a fixed arrival rate p of transactions, the larger the mining rate θ or the service parameter

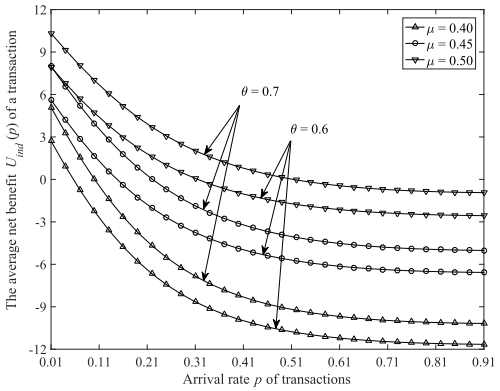

FIGURE 4. Change trend for the average net benefit $U_{ind}(p)$ of a transaction.

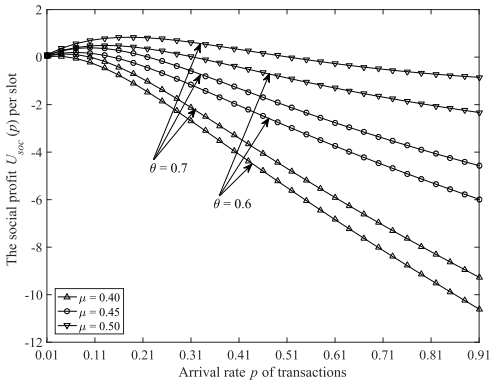

FIGURE 5. Change trend for the social profit $U_{soc}(p)$ per slot.

TABLE 1. Experimental results for the nash equilibrium arrival rate of transactions.

Service parameter μ	Mining rate θ	Nash equilibrium arrival rate p_e of transactions
0.40	0.60	0.056 3
0.40	0.70	0.100 4
0.45	0.60	0.147 1
0.45	0.70	0.220 9
0.50	0.60	0.314 9
0.50	0.70	0.513 4

TABLE 2. Experimental results for the socially optimal arrival rate of transactions.

Service parameter μ	Mining rate θ	Socially optimal arrival rate p^* of transactions
0.40	0.60	0.027 7
0.40	0.70	0.048 4
0.45	0.60	0.068 9
0.45	0.70	0.099 0
0.50	0.60	0.131 1
0.50	0.70	0.180 4

μ is, the bigger the average net benefit $U_{ind}(p)$ is. When the arrival rate p is fixed, the larger the mining rate is, the smaller the average confirmation time of transactions will be. For this case, the transactions will pay the smaller time cost, and the average net benefit will be improved. Similarly, when the arrival rate p is fixed, the larger the service parameter is, the bigger the average net benefit will be.

From the numerical experiment results in Sect. IV, we note that as the arrival rate p of transactions increases, the average confirmation time $E[S]$ of transactions will be longer. Therefore, the function for the average net benefit of a transaction has decreasing property. As seen in Fig. 4, when the arrival rate increases, all curves of the average net benefit of a transaction will decline and across the line $U_{ind}(p) = 0$. When $p \leqslant p_e$, the average net benefit of a transaction is non-negative. When $p > p_e$, the average net benefit of a transaction is negative. We also note that the Nash equilibrium arrival rate p_e of transactions is unique from Fig. 4.

The Nash equilibrium arrival rates p_e of transactions for different combination of service parameter μ and mining rate θ are summarized in Table 1.

Using the same parameters as in Fig. 4. We demonstrate the change trend for the social profit $U_{soc}(p)$ per slot in Fig. 5.

From Fig. 5, we find that for a fixed arrival rate p of transactions, the larger the mining rate θ or the service parameter μ is, the bigger the social profit $U_{soc}(p)$ will be. When the arrival rate of transactions is fixed, the larger the mining rate θ or the service parameter μ is, the bigger the average net benefit will be. For this case, the social profit will be higher. We also find that all curves of the social profit present an upper convex behavior.

The socially optimal arrival rate p^* of transactions for different combination of service parameter μ and mining rate θ are summarized in Table 2.

Comparing Tables 1 and 2, we observe that the Nash equilibrium arrival rate of transactions is always bigger than the socially optimal arrival rate of transactions for all the combination of service parameter and mining rate. That is to say, with Nash equilibrium strategy, more transactions will be broadcasted to the blockchain system. This will obviously reduce the social profit.

B. PRICING POLICY

In order to oblige the Nash equilibrium arrival rate of transactions to subject to the socially optimal arrival rate of transactions, we present a pricing policy by charging an admission fee for each transaction. The admission fee should be deducted from the individual benefit of transactions. So, the average net benefit $U'_{ind}(p)$ of a transaction with the admission fee is modified as follows:

$$U'_{ind}(p) = R - CE[S] - f, \tag{16}$$

where f is the admission fee.

In the pricing policy, the admission fees of transactions are charged by the blockchain system. That is to say, the admission fees are transferred from transactions to the blockchain system. Therefore, the pricing policy not have impact on the social profit.

TABLE 3. Numerical results of the admission fee.

Service parameter μ	Mining rate θ	Socially optimal arrival rate p^* of transactions	Admission fee f
0.40	0.60	0.027 7	1.641 1
0.40	0.70	0.048 4	2.789 9
0.45	0.60	0.068 9	2.924 0
0.45	0.70	0.099 0	3.988 7
0.50	0.60	0.131 1	3.766 1
0.50	0.70	0.180 4	4.638 1

Substituting the socially optimal arrival rate p^* of transactions given in Table 2 into (16) and setting $U'_{ind}(p^*) = 0$, we calculate the admission fee f. The numerical results of the admission fees f for different combination of service parameter μ and mining rate θ are summarized in Table 3.

From Table 3, we find that the greater the service parameter μ or the mining rate θ is, the higher the admission fee f is. As described in Sect. IV, the increase either in the mining rate or the service parameter leads to shorter average confirmation time of transactions, and makes blockchain tradings more attractive for transactions. If the service parameter or the mining rate is greater, we need set a higher admission fee to regulate the arrival rate of transactions. Otherwise, a lower admission fee is reasonable.

VI. CONCLUSION

In this paper, we investigated Nash equilibrium and social optimization of transactions in blockchain system with a light-load traffic. By dividing the confirmation process of transactions into mining period and verification period, we established a discrete-time non-exhaustive vacation queue with batch service and gated service. Choosing the instant just after the end of every verification period as the Markov chain point, we constructed a Markov chain. Using the regeneration cycle approach and Little's Law, we derived the average confirmation time of transactions. Numerical experiments not only verify the accuracy of model analysis, but also demonstrate the impact of arrival rate of transactions on the confirmation time of transactions. By calculating the individual benefit and social profit, we investigated the Nash equilibrium and socially optimal arrival rate of transactions. From the social point of view, we regulated the arrival rate of transactions by charging an appropriate admission fee to each transaction and maximized the social profit.

REFERENCES

[1] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Honolulu, HI, USA, Jun. 2017, pp. 557–564.

[3] A. Firdaus, M. F. A. Razak, A. Feizollah, I. A. T. Hashem, M. Hazim, and N. B. Anuar, "The rise of 'blockchain': Bibliometric analysis of blockchain study," *Scientometrics*, vol. 120, no. 3, pp. 1289–1331, 2019, doi: 10.1007/s11192-019-03170-4.

[4] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Informat. J.*, vol. 25, no. 4, pp. 1398–1411, Dec. 2019, doi: 10.1177/1460458218769699.

[5] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K.-R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Jan. 2018, doi: 10.1109/MCC.2018.011791712.

[6] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "MediBchain: A blockchain based privacy preserving platform for healthcare data," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage,* Guangzhou, China, 2017, pp. 534–543.

[7] A. Wilczyński and J. Kołodziej, "Modelling and simulation of security-aware task scheduling in cloud computing based on Blockchain technology," *Simul. Model. Pract. Theory*, vol. 99, Feb. 2020, Art. no. 102038, doi: 10.1016/j.simpat.2019.102038.

[8] Y. Zhang, R. Deng, X. Liu, and D. Zheng, "Outsourcing service fair payment based on blockchain and its applications in cloud computing," *IEEE Trans. Services Comput.*, early access, Aug. 7, 2018, doi: 10.1109/TSC.2018.2864191.

[9] M. Taghavi, J. Bentahar, H. Otrok, and K. Bakhtiyari, "Cloudchain: A blockchain-based coopetition differential game model for cloud computing," in *Proc. Int. Conf. Service-Oriented Comput.*, Hangzhou, China, 2018, pp. 146–161.

[10] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, 2017, doi: 10.1109/MCOM.2017.1700041.

[11] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[12] L. Wu, X. Du, W. Wang, and B. Lin, "An Out-of-band authentication scheme for Internet of Things using blockchain technology," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Maui, HI, USA, Mar. 2018, pp. 769–773.

[13] D. Khoury, E. F. Kfoury, A. Kassem, and H. Harb, "Decentralized voting platform based on ethereum blockchain," in *Proc. IEEE Int. Multidisciplinary Conf. Eng. Technol. (IMCET)*, Beirut, Lebanon, Nov. 2018, pp. 1–6.

[14] H. Yi, "Securing e-voting based on blockchain in P2P network," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 1–9, Dec. 2019, doi: 10.1186/s13638-019-1473-6.

[15] S. Agbesi and G. Asante, "Electronic voting recording system based on blockchain technology," in *Proc. 12th CMI Conf. Cybersecurity Privacy (CMI)*, Copenhagen, Denmark, Nov. 2019, pp. 1–8.

[16] M. Li, L. Shen, and G. Q. Huang, "Blockchain-enabled workflow operating system for logistics resources sharing in E-commerce logistics real estate service," *Comput. Ind. Eng.*, vol. 135, pp. 950–969, Sep. 2019, doi: 10.1016/j.cie.2019.07.003.

[17] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, May 2018, doi: 10.1109/MNET.2018.1700344.

[18] A. Dorri, F. Luo, S. S. Kanhere, R. Jurdak, and Z. Y. Dong, "SPB: A secure private blockchain-based solution for distributed energy trading," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 120–126, Jul. 2019, doi: 10.1109/MCOM.2019.1800577.

[19] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Informat.*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[20] S. Kasahara and J. Kawahara, "Effect of bitcoin fee on transaction-confirmation process," *J. Ind. Manage. Optim.*, vol. 15, no. 1, pp. 365–386, 2019, doi: 10.3934/jimo.2018047.

[21] Y. Kawase and S. Kasahara, "Transaction-confirmation time for bitcoin: A queueing analytical approach to blockchain mechanism," in *Proc. Int. Conf. Queueing Theory Netw. Appl.*, Qinhuangdao, China, 2017, pp. 75–88.

[22] Y. Kawase and S. Kasahara, "A batch-service queueing system with general input and its application to analysis of mining process for bitcoin blockchain," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Halifax, NS, Canada, Jul. 2018, pp. 1440–1447.

[23] Q. L. Li, J. Y. Ma, and Y. X. Chang, "'Blockchain queue theory," in *Proc. Int. Conf. Comput. Social Netw.*, Shanghai, China, 2018, pp. 25–40.

[24] W. Zhao, S. Jin, and W. Yue, "Analysis of the average confirmation time of transactions in a blockchain system," in *Proc. Int. Conf. Queueing Theory Netw. Appl.*, Ghent, Belgium, 2019, pp. 379–388.

[25] J. Hunter, "Mathematical techniques of applied probability," in *Discrete Time Models: Techniques and Applications*, vol. 2. New York, NY, USA: Academic, 1983.
[26] H. Takagi, *Queueing Analysis Vacation and Priority Systems*, vol. 1. Amsterdam, The Netherlands: Elsevier, 1991.
[27] R. Hassin and M. Haviv, *To Queue or Not to Queue: Equilibrium Behavior in Queueing Systems*. Boston, MA, USA: Springer, 2003.

JIAXING QI received the B.Eng. degree from the Liren College, Yanshan University, Qinhuangdao, Hebei, China. He is currently pursuing the master's degree with the School of Information Science and Engineering, Yanshan University. His research interest is in performance analysis of blockchain systems.

JING YU received the B.Eng. degree in computer and application and the M.Eng. and Dr.Eng. degrees in computer science and technology from Yanshan University, Qinhuangdao, China. She is currently an Associate Professor with the School of Information Science and Engineering, Yanshan University. Her research interests include spatial database, data security, and performance evaluation for system and networks.

SHUNFU JIN received the B.Eng. degree in computer and application from the North East Heavy Machinery College, Qiqihaer, China, and the M.Eng. degree in computer science and the Dr.Eng. degree in circuit and system from Yanshan University, Qinhuangdao, China. She is currently a Professor with the School of Information Science and Engineering, Yanshan University. Her research interests include stochastic modeling for telecommunication, performance evaluation for computer system and networks, and application for queueing systems.