

Information Theory of Blockchain Systems

Quan-Lin Li^a, Yaqian Ma^a, Jing-Yu Ma^{b*}, Yan-Xia Chang^a

^aSchool of Economics and Management,

Beijing University of Technology, Beijing 100124, China

^bBusiness School, Xuzhou University of Technology, Xuzhou 221018, China

September 12, 2023

Abstract

In this paper, we apply the information theory to provide an approximate expression of the steady-state probability distribution for blockchain systems. We achieve this goal by maximizing an entropy function subject to specific constraints. These constraints are based on some prior information, including the average numbers of transactions in the block and the transaction pool, respectively. Furthermore, we use some numerical experiments to analyze how the key factors in this approximate expression depend on the crucial parameters of the blockchain system. As a result, this approximate expression has important theoretical significance in promoting practical applications of blockchain technology. At the same time, not only do the method and results given in this paper provide a new line in the study of blockchain queueing systems, but they also provide the theoretical basis and technical support for how to apply the information theory to the investigation of blockchain queueing networks and stochastic models more broadly.

Keywords: Blockchain; Information theory; Maximum entropy principle; Steady-state probability distribution.

1 Introduction

Blockchain has become a prominent topic of discussion in recent years, revolutionizing various aspects of life through its significant impact on many practical application fields. For example, finance by Kowalski et al. [8]; the Internet of Things by Torky and Hassanein

[24]; healthcare by Sudeep et al. [23]; and others. The active participation of miners in the mining process is fundamental to ensuring the secure and stable operation of the blockchain system, as well as guaranteeing its sustainable development. However, the inner workings of blockchain mining are extremely obscure and challenging to examine. Conducting direct measurements on mining networks is highly complex due to the miners' privacy concerns, whereas blockchain data provides a method of direct measurement. Consequently, it is essential to develop statistical techniques using accessible blockchain data for investigating blockchain systems.

So far blockchain research has obtained many important advances, readers may refer to a book by Swan [22]; a key research framework shown by Daneshgar et al. [3], Lindman et al. [13] and Risius and Spohrer [19]; decision in blockchain mining by Ma and Li [16] and Chen et al. [2]; and others by Lu et al. [15] and Yang et al. [25].

Applying queueing theory and Markov processes to analyze blockchain systems is interesting but challenging, since each blockchain system not only is a complicated stochastic system but also has multiple key factors and a physical structure with different levels. Li et al. [10] provided a two-stage queueing model of the PoW blockchain system, clearly described and expressed the physical structure with multiple key factors, furthermore the matrix geometric solution was applied to give a complete solution such that the performance evaluation of the PoW blockchain system was established in a simple form. Seol et al. [20] proposed an $M(1, n)/M_n/1$ queueing model to analyze the blockchain system in Ethereum; Zhao et al. [26] established a non-exhaustive queueing model with a limited batch service and a possible zero-transaction service, derived the average number of transactions and the average confirmation time of a transaction; Mišić et al. [17] applied the Jackson network to analyze the blockchain network.

Compared with the queueing theory, the Markov process is mainly used to evaluate the throughput, confirmation time, security and privacy protection of the blockchain systems. Huang et al. [4] proposed the Markov process with an absorption state and conducted an analysis on the performance of the Raft consensus algorithm in private blockchains. Srivastava [21] calculated the transaction confirmation time in blockchain systems. Li et al. [11] discussed block access control mechanisms in wireless blockchain networks. Nguyen et al. [18] investigated the task offloading problem in mobile blockchain with privacy protection using Markov processes and deep reinforcement learning.

The traditional reluctance of miners to share insider information regarding their com-

petitive advantages, leading to great difficulties for these two approaches when dealing with more complex blockchain systems, such as those involving multiple mining pools. The purpose of this paper is to apply the maximum entropy principle to provide an approximate expression for blockchain systems. In information theory, entropy serves as a probabilistic measure to quantify the uncertainty of information associated with random variables. In recent years, the information entropy has been implemented in various practical domains of blockchain technology. For example, industrial Internet of Things by Khan and Byun [7]; renewable energy by Liu et al. [14]; fake news prevention by Chen et al. [1]; and medical data sharing by Liang et al. [12].

The degree of randomness in a random variable can be measured by applying maximum entropy when its information is most uncertain. For example, a large amount of information can only be partially obtained and utilized. For random variables, Jaynes [5,6] initially proposed the maximum entropy principle, which offers an approximate computational approach for unknown probability distributions. Such an approach provides a uniquely correct self-consistent method of inference for estimating probability distributions based on the available information.

The main contributions of this paper are twofold. The first one is to apply the maximum entropy principle to study blockchain queueing systems for the first time. Different from previous works for applying queueing theory or Markov processes, we just need to take statistical techniques by simple observation on miners. The second contribution of this paper is to provide the approximate expression of the steady-state probability distribution for blockchain systems. So far, numerous categories of blockchain systems have yet to be thoroughly analyzed using queueing theory or Markov processes due to difficulties in the expression of the steady-state probability distributions. Therefore, the results of this paper give new insights into applying the maximum entropy principle to more complex blockchain systems. For example, the PoW blockchain system with multiple mining pools, the PBFT blockchain system of dynamic nodes, the DAG-based blockchain systems, the Ethereum, and the large-scale blockchain systems with either cross-chain, side-chain, or off-chain.

The rest of this paper is organized as follows. Section 2 introduces the blockchain queueing model briefly. In Section 3, we apply the maximum entropy principle to give the approximate expression of the steady-state probability distribution for the blockchain system. We also conduct numerical experiments to analyze how the key factors of the

approximate expression depend on some crucial parameters in Section 4. Finally, the whole work is concluded in the last section.

2 Model Distribution

In this section, we describe a blockchain system as two stages of asynchronous processes: block-generation and blockchain-building, which is depicted in Fig. 1. To ensure clarity, we review the blockchain queuing model and adopt the notations of Li et al. [10] briefly .

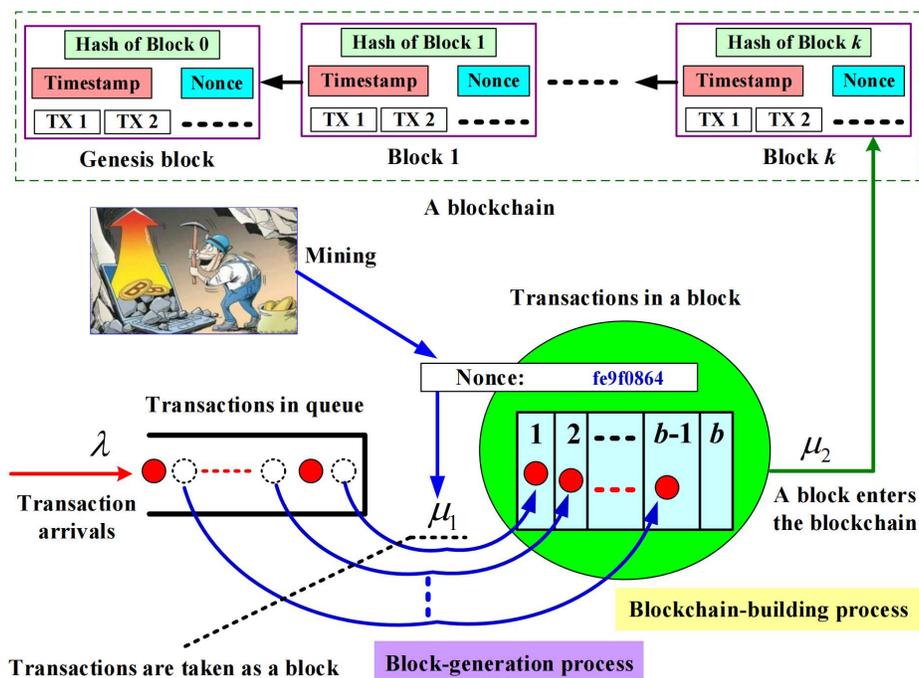


Figure 1: A blockchain queuing system.

Arrival processes: Transactions arrive at the blockchain system according to a Poisson process with arrival rate λ . Each transaction must first enter and queue up in a transaction pool with infinite size.

Block-generation processes: Each arrival transaction first queues up in the transaction pool and then waits to be mined into a block successfully. We assume that the block-generation times are i.i.d. and exponential with service rate μ_1 . The transactions are chosen into the block, but they are not completely based on the First Come First Service (FCFS) from the order of transaction arrivals.

Block capacity: To avoid the spam attacks, we assume that the maximum size of each block is limited to b transactions. If there are more than b transactions in the transaction pool, then the b transactions are selected to form a full block while the rest of transactions are still waiting in the transaction pool and may be used to construct another block.

Blockchain-building processes: The block with a group of transactions will be pegged to a blockchain. We assume that the blockchain-building times are i.i.d. and exponential with the service rate μ_2 .

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

Let $I(t)$ and $J(t)$ be the numbers of transactions in the block and in the transaction pool at time t , respectively. Then, $(I(t), J(t))$ may be regarded as a state of the blockchain system at time t . The state space of this blockchain system is

$$\Omega = \{(i, j), 0 \leq i \leq b, 0 \leq j \leq \infty\}.$$

The following lemma provides a necessary and sufficient condition under which the blockchain system is stable. Here, we only restate it without proof, while readers may refer to Chapter 3 of Li [9] and Li et al. [10] for more details.

Lemma 1 *The blockchain system is stable if and only if*

$$\frac{b\mu_1\mu_2}{\mu_1 + \mu_2} > \lambda. \tag{1}$$

In what follows we assume that the stable condition (1) is satisfied, then this blockchain system is stable. The limit

$$\lim_{t \rightarrow +\infty} p\{I(t) = i, J(t) = j\}$$

exists and is unique. Let

$$p(i, j) = \lim_{t \rightarrow +\infty} p\{I(t) = i, J(t) = j\}.$$

Then, $p(i, j), (i, j) \in \Omega$ is the steady-state probability distribution of the blockchain system.

By using the matrix-geometric solution, we can write the steady-state probability distribution under the stable condition (1), see Li et al. [10]. In the next section, we will introduce the maximum entropy principle to provide the approximate expression of the steady-state probability distribution for the blockchain system.

3 Maximum Entropy in Blockchain Systems

In this section, we provide an entropy function and some prior information, and use Lagrange method of undetermined multipliers to give the approximate expression of the steady-state probability distribution.

3.1 Entropy Function

Based on the steady-state probability distribution $p(i, j)$, we introduce the entropy function

$$H(p) = - \sum_{(i,j) \in \Omega} p(i, j) \ln p(i, j)$$

or

$$H(p) = - \sum_{j=0}^{\infty} \sum_{i=0}^b p(i, j) \ln p(i, j). \quad (2)$$

The maximum entropy principle states that of all distributions satisfying the constraints supplied by the given information, the minimally prejudiced distribution $p(i, j), (i, j) \in \Omega$ is the one that maximizes the entropy function of the blockchain queueing system.

3.2 Prior information

To approximate the steady-state probability distribution $p(i, j), (i, j) \in \Omega$ using the maximum entropy principle by maximizing (2), we need to provide some prior information as follows:

(i) The normalisation:

$$\sum_{(i,j) \in \Omega} p(i, j) = 1. \quad (3)$$

(ii) The average number of transactions in the block:

$$\sum_{i=0}^b i \sum_{j=0}^{\infty} p(i, j) = I. \quad (4)$$

(iii) The average number of transactions in the transaction pool:

$$\sum_{j=0}^{\infty} j \sum_{i=0}^b p(i, j) = J. \quad (5)$$

Remark 1 Note that the statistics of prior information selected always may be known numerically via system measurements during finite observation periods or can be determined symbolically via known analytic formulae based on operational or stochastic assumptions. For example, blockchain data has the advantage of providing direct measurements, as the fields of a block are filled by the miner of that block.

3.3 The maximum entropy principle

The steady-state probability distribution $p(i, j)$ is considered as an independent variable. We maximize the entropy function (2) subject to constraints (3)-(5), the optimization model of the maximum entropy principle can be written as

$$\begin{aligned} \max H(p) &= - \sum_{j=0}^{\infty} \sum_{i=0}^b p(i, j) \ln p(i, j), \\ \text{s.t.} \quad &\begin{cases} \sum_{j=0}^{\infty} \sum_{i=0}^b p(i, j) = 1, \\ \sum_{i=0}^b i \sum_{j=0}^{\infty} p(i, j) = I, \\ \sum_{j=0}^{\infty} j \sum_{i=0}^b p(i, j) = J. \end{cases} \end{aligned}$$

The following theorem provides the approximate expression of the steady-state probability distribution for the blockchain system by the maximum entropy principle.

Theorem 1 For the steady-state probability distribution $p(i, j)$ of blockchain systems, there exists a tuple of positive numbers x , y and z that satisfy

$$\tilde{p}(i, j) = xy^i z^j.$$

Proof: By introducing β_0 , β_1 and β_2 to equations (3)-(5), we write Lagrangian function as

$$\begin{aligned} L(p, \beta_0, \beta_1, \beta_2) &= - \sum_{j=0}^{\infty} \sum_{i=0}^b p(i, j) \ln p(i, j) + \beta_0 \left(1 - \sum_{j=0}^{\infty} \sum_{i=0}^b p(i, j) \right) \\ &\quad + \beta_1 \left(I - \sum_{i=0}^b i \sum_{j=0}^{\infty} p(i, j) \right) + \beta_2 \left(J - \sum_{j=0}^{\infty} j \sum_{i=0}^b p(i, j) \right), \quad (6) \end{aligned}$$

where β_0 , β_1 and β_2 are the Lagrange multipliers corresponding to constraints (3)-(5), respectively.

To find the maximum entropy solution $p(i, j)$, maximizing (2) subject to constraints (3)-(5) is equivalent to maximizing (6).

The Lagrangian function $L(p, \beta_0, \beta_1, \beta_2)$ is a multivariate function with respect to variables $p(i, j)$, β_0 , β_1 and β_2 . To obtain the maximum entropy solutions, we take the partial derivatives of $L(p, \beta_0, \beta_1, \beta_2)$ with respect to $p(i, j)$ and then set the results equal to zero, i.e., $\partial L / \partial p(i, j) = 0$.

If (i, j) is determined, then

$$\frac{\partial}{\partial p(i, j)} \left[- \sum_{j=0}^{\infty} \sum_{i=0}^b p(i, j) \ln p(i, j) \right] = - \ln p(i, j) - 1.$$

It is clear that for all (\bar{i}, \bar{j}) , $\bar{i} \neq i$ and $\bar{j} \neq j$,

$$\frac{\partial}{\partial p(i, j)} p(\bar{i}, \bar{j}) \ln p(\bar{i}, \bar{j}) = 0.$$

Thus, we obtain

$$\frac{\partial L}{\partial p(i, j)} = [- \ln p(i, j) - 1] - \beta_0 - \beta_1 i - \beta_2 j = 0,$$

which indicates

$$\ln p(i, j) = -1 - \beta_0 - \beta_1 i - \beta_2 j. \quad (7)$$

It follows from (7) that

$$p(i, j) = \exp[-(1 + \beta_0)] \exp(-\beta_1 i) \exp(-\beta_2 j). \quad (8)$$

Let

$$x = \exp[-(1 + \beta_0)], y = \exp(-\beta_1) \text{ and } z = \exp(-\beta_2).$$

Then, we rewrite (8) as

$$p(i, j) = x y^i z^j. \quad (9)$$

Substituting (9) into (3) and utilizing algebraic knowledge, we have

$$x = \frac{(1 - y)(1 - z)}{1 - y^{b+1}}. \quad (10)$$

Similarly, substituting (9) into (4) and (5), respectively, we have

$$y^{b+1} - \sum_{n=1}^b \frac{1}{b - I} y^n + \frac{I}{b - I} = 0 \quad (11)$$

and

$$z = \frac{J}{1+J}. \quad (12)$$

Therefore, if the average number of transactions in the block and the transaction pool can be provided, respectively, the positive numbers x , y and z exist to give the approximate expression for $\tilde{p}(i, j)$. This completes the proof.

Remark 2 *The theoretical expressions of the mean values I and J given by Li et al. [10] are restricted to Poisson arrival processes and exponential service times, meaning that these expressions are only theoretically applicable in this particular case. Nevertheless, the maximum entropy principle is not dependent on this assumption of the Poisson arrival processes and the exponential service times. It can be applied to non-Poisson arrival processes and non-exponential service times, as long as I and J can be provided, the non-linear equations can be solved to derive the approximate expression of the steady-state probability distribution for the blockchain queueing system. Therefore, the approximate expression derived in Section 3.3 has broad applicability.*

4 Numerical experiments

In this section, we provide some numerical examples to verify computability of our theoretical results and analyze how the key factors y and z of the approximate expression depend on some crucial parameters of the blockchain queueing system.

Taking the situation of the Poisson arrival processes and the exponential service times in Li et al. [10] as an example, since the theoretical expressions of the mean values I and J are composed of the crucial parameters λ , μ_1 , μ_2 and b , we can observe the relation between the key factors and crucial parameters. Note that x is represented by y and z according to equations (10)-(12), we just need to focus on how y and z depend on these crucial parameters through numerical examples.

In the Examples 1 and 2, we take some common parameters: The maximum block size $b = 80$, the block-generation service rate $\mu_1 = 6, 7.5, 10$, blockchain-building service rate $\mu_2 = 2$ and the arrival rate $\lambda \in (1, 3.5)$.

Example 1 We analyze how y depends on λ and μ_1 . From Fig. 2, it is seen that y decreases as λ increases, while it also decreases as μ_1 increases.

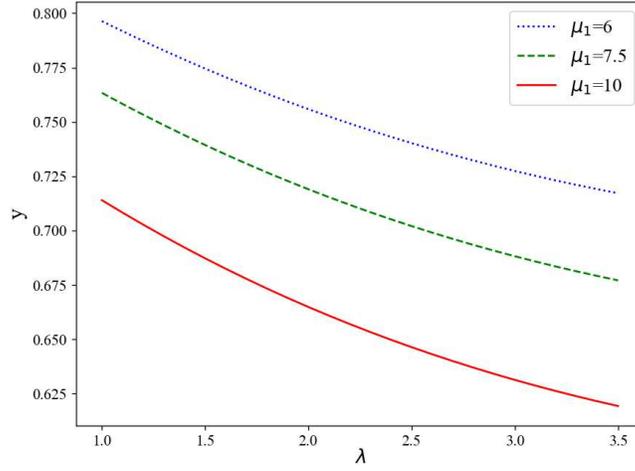


Figure 2: y vs. λ for three different values of μ_1 .

Example 2 We analyze how z depends on λ and μ_1 . From Fig. 3, it is seen that z increases as λ increases, while it increases as μ_1 decreases.

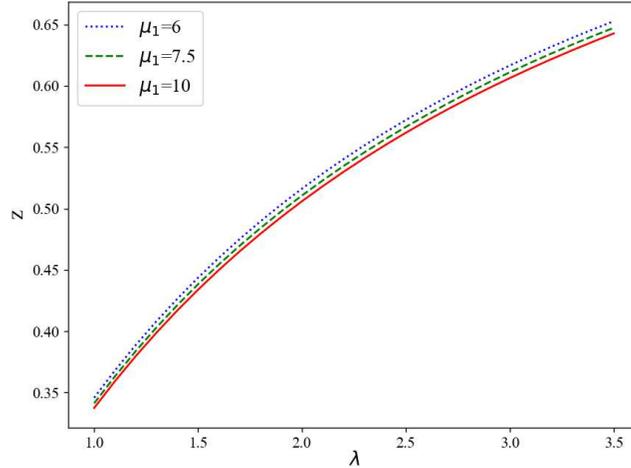


Figure 3: z vs. λ for three different values of μ_1 .

Example 3 We specifically observe how y and z depend on the maximal block size b , respectively. We take some common parameters: The arrival rate $\lambda = 1.5$, the blockchain-building service rate $\mu_2 = 2$, the maximum block size $b = 40, 80, 160$ and the block-generation service rate $\mu_1 \in (1, 2.5)$. From Fig. 4 and Fig. 5, it is seen that y and z decrease as μ_1 increases, while they increase as b increases.

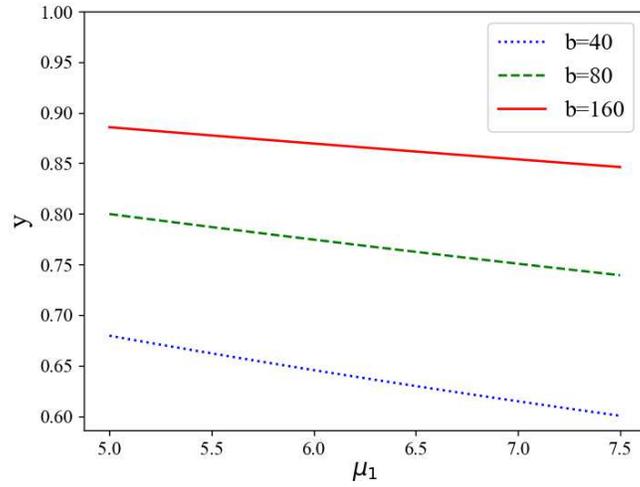


Figure 4: y vs. μ_1 for three different values of b .

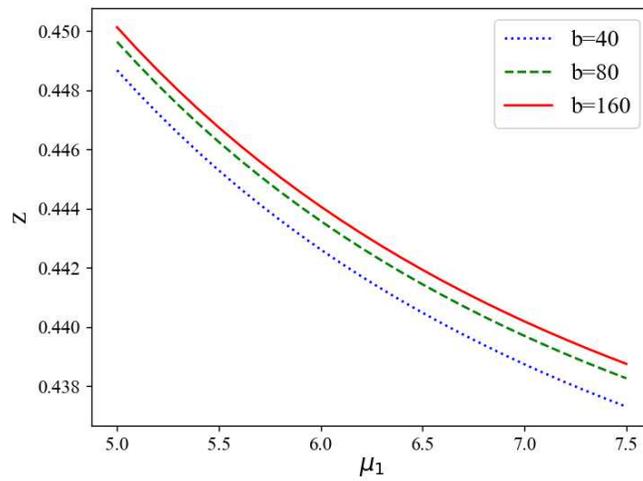


Figure 5: z vs. μ_1 for three different values of b .

5 Concluding Remarks

In this paper, we apply the maximum entropy principle of the information theory to study the blockchain queueing system, and provide an approximate expression of its steady-state probability distribution. By obtaining this approximation, we have partially resolved a challenging issue in the blockchain technology, i.e., how to directly express the steady-state probability distributions of some large-scale and complex blockchain queueing systems. On the other hand, we use numerical examples to verify the computability of our theoretical results and analyze how the key factors of the approximate expression depend on some crucial parameters. Along these lines, we will continue our future research in the following directions:

- Investigating blockchain queueing systems with multiple mining pools, different consensus mechanisms and so on.
- Extending the information theory to blockchain queueing networks or stochastic models.
- Applying the information theory to provide a more accurate approximate expression with more prior information such as the second moment and the third moment.

References

- [1] Chen, C.C., Du, Y., Peter, R., et al.: An implementation of fake news prevention by blockchain and entropy-based incentive mechanism. *Soc. Netw. Anal. Min.* **12**(1), 114 (2022)
- [2] Chen, J., Cheng, Y., Xu, Z., et al.: Decision on block size in blockchain systems by evolutionary equilibrium analysis. *Theor. Comput. Sci.* **942**, 93–106 (2023)
- [3] Daneshgar, F., Ameri Sianaki, O., Guruwacharya, P.: Blockchain: A research framework for data security and privacy. In: the International Conference on Advanced Information Networking and Applications, Matsue, pp. 966–974. Springer (2019)
- [4] Huang, D., Ma, X., Zhang, S.: Performance analysis of the Raft consensus algorithm for private blockchains. *IEEE Trans. Syst. Man. Cybern. Syst.* **50**(1), 172–181 (2019)
- [5] Jaynes, E.T.: Information theory and statistical mechanics. *Phys. Rev.* **106**(4), 620–630 (1957)

- [6] Jaynes, E.T.: Information theory and statistical mechanics II. *Phys. Rev.* **108**(2), 171–190 (1957)
- [7] Khan, P.W., Byun, Y.: A blockchain-based secure image encryption scheme for the industrial Internet of Things. *Entropy.* **22**(2), 175 (2020)
- [8] Kowalski, M., Lee, Z.W., Chan, T.K.: Blockchain technology and trust relationships in trade finance. *Technol. Forecast. Soc.* **166**, 120641 (2021)
- [9] Li, Q.L.: *Constructive Computation in Stochastic Models with Applications: The RG-Factorizations.* Springer, Heidelberg (2010)
- [10] Li, Q.L., Ma, J.Y., Chang, Y.X.: Blockchain queue theory. In: *The 7th International Conference on Computational Social Networks, Shanghai*, pp. 25–40. Springer (2018)
- [11] Li, Y., Cao, B., Liang, L., et al.: Block access control in wireless blockchain network: Design, modeling and analysis. *IEEE Trans. Veh. Technol.* **70**(9), 9258–9272 (2021)
- [12] Liang, X., Chen, W., Li, J., et al.: Incentive mechanism of medical data sharing based on information entropy in blockchain environment. *Journal of Physics: Conference Series.* **1302**(2), 022056 (2019)
- [13] Lindman, J., Tuunainen, V.K., Rossi, M.: Opportunities and risks of blockchain technologies – a research agenda. In: *Proceedings of the 50th Hawaii International Conference on System Sciences, Hawaii*, pp. 1533–1542 (2017)
- [14] Liu, Z., Huang, B., Hu, X., et al.: Blockchain-based renewable energy trading using information entropy theory. *IEEE T. Netw. Sci. Eng.* 1–12 (2023)
- [15] Lu, Y., Huang, X., Zhang, K., et al.: Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. *IEEE Trans. Veh. Technol.* **69**(4), 4298–4311 (2020)
- [16] Ma, J.Y., Li, Q.L.: Optimal dynamic mining policy of blockchain selfish mining through sensitivity-based optimization. *J. Comb. Optim.* **44**(5), 3663–3700 (2022)
- [17] Mišić, J., Mišić, V.B., Chang, X.: Performance of bitcoin network with synchronizing nodes and a mix of regular and compact blocks. *IEEE T. Netw. Sci. Eng.* **7**(4), 3135–3147 (2020)

- [18] Nguyen, D.C., Pathirana, P.N., Ding, M., et al.: Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning. *IEEE Trans. Netw. Service Manag.* **17**(4), 2536–2549 (2020)
- [19] Risius, M., Spohrer, K.: A blockchain research framework. *Bus. Inform. Syst. Eng.* **59**(6), 385–409 (2017)
- [20] Seol, J., Kancharla, A., Ke, Z., et al.: A variable bulk arrival and static bulk service queueing model for blockchain. In: *The 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, Taipei, pp. 63–72. Association for Computing Machinery (2020)
- [21] Srivastava, R.: Mathematical assessment of blocks acceptance in blockchain using Markov model. *Int. J. Blockchains Cryptocurrencies*, **1**(1), 42–53 (2019)
- [22] Swan, M.: *Blockchain: Blueprint for a new economy*. O’Reilly Media, Inc. (2015)
- [23] Sudeep, T., Karan, P., Richard, E.: Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **50**, 102407 (2020)
- [24] Torkey, M., Hassanein, A.E. Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. *Comput. Electron. Agr.* **178**, 105476 (2020)
- [25] Yang, L., Li, M., Si, P., et al.: Energy-efficient resource allocation for blockchain-enabled industrial Internet of Things with deep reinforcement learning. *IEEE Internet Things J.* **8**(4), 2318–2329 (2020)
- [26] Zhao, W., Jin, S., Yue, W.: Analysis of the average confirmation time of transactions in a blockchain system. In: *International Conference on Queueing Theory and Network Applications*, Belgium, pp. 379–388. Springer (2019)