Article | Received 29 November 2022; Accepted 14 January 2023; Published 2 February 2023
https://doi.org/10.55092/blockchain20230005

Performance evaluation, optimization and dynamic decision in blockchain systems: a recent overview

Quan-Lin Li[1], Yan-Xia Chang[1,*] and Qing Wang[2]

[1]School of Economics and Management, Beijing University of Technology, Beijing, China
[2]Monash Business School, Monash University, Melbourne, Australia

* Correspondence author; E-mail: changyanxia@emails.bjut.edu.cn.

Abstract: With rapid development of blockchain technology as well as integration of various application areas, performance evaluation, performance optimization, and dynamic decision in blockchain systems are playing an increasingly important role in developing new blockchain technology. This paper provides a recent systematic overview of this class of research, and especially, developing mathematical modeling and basic theory of blockchain systems. Important examples include (a) performance evaluation: Markov processes, queuing theory, Markov reward processes, random walks, fluid and diffusion approximations, and martingale theory; (b) performance optimization: Linear programming, nonlinear programming, integer programming, and multi-objective programming; (c) optimal control and dynamic decision: Markov decision processes, and stochastic optimal control; and (d) artificial intelligence: Machine learning, deep reinforcement learning, and federated learning. So far, a little research has focused on these research lines. We believe that the basic theory with mathematical methods, algorithms and simulations of blockchain systems discussed in this paper will strongly support future development and continuous innovation of blockchain technology.

Keywords: blockchain; performance evaluation; performance optimization; optimal control; dynamic decision

1. Introduction

Since Bitcoin was proposed by Nakamoto [1] in 2008, blockchain technology has received tremendous attention from both practitioners and academics. So far, blockchain has made remarkable progress by means of many interesting and creative combinations of multiple key computer technologies, such as distributed systems, consensus mechanism, network and information security, privacy protection, encryption technology, peer-to-peer networks, edge computing, Internet of Things, and artificial intelligence. At the same time, some effective scalable frameworks and security designs of blockchain have been further developed, for example, off-chain, side-chain, cross-chain, shard, fault tolerant, and attack detection. However, compared with rapid development of blockchain technology, mathematical modeling and analysis of blockchain systems is relatively backward, thus it is clear that developing blockchain technology extremely needs such important basic theory and necessary mathematical methods, some part of which have been falling with much research of blockchain technologies.

In this paper, we review mathematical modeling and analysis methods in some aspects (but no completeness) of blockchain technology, including some important progress that can further drive developing new potential blockchain technologies. To this end, our overview in this paper is listed as follows: **(1)** Mining processes and management; **(2)** consensus mechanism; **(3)** performance evaluation; **(4)** performance optimization; **(5)** optimal control and dynamic decision; **(6)** machine learning; **(7)** blockchain economy and market; and **(8)** blockchain ecology. Note that the eight survey points aim to setting up stochastic models and associated mathematical methods to theoretically improve blockchain's performance, scalability, security, privacy protection, work efficiency, economic benefit and so on. In what follows, we use Figures 1 to 6 to describe and analyze the eight survey points **(1)** to **(8)** simply. In this paper, we will not like to explain more for the six figures. However, we believe that each of them will motivate readers to be able to understand or find more interesting research topics of blockchain. Perhaps this is the value of our simple and vague introduction.

(1) Mining processes and management

For mathematical modeling and analysis on this research direction, we need to discuss the key system factors or parameters that largely influence performance, scalability, security, and privacy protection of blockchain systems. For example, the miners, the mining pools, the difficulty of solving the cryptographic puzzle, the transaction fee, the blockchain reward, the competitive behavior, the tree with forked structure, the work efficiency, the economic benefit; the attack strategies, the security, the vulnerability, the fault tolerance, and privacy protection. See Figure 1 for more details.

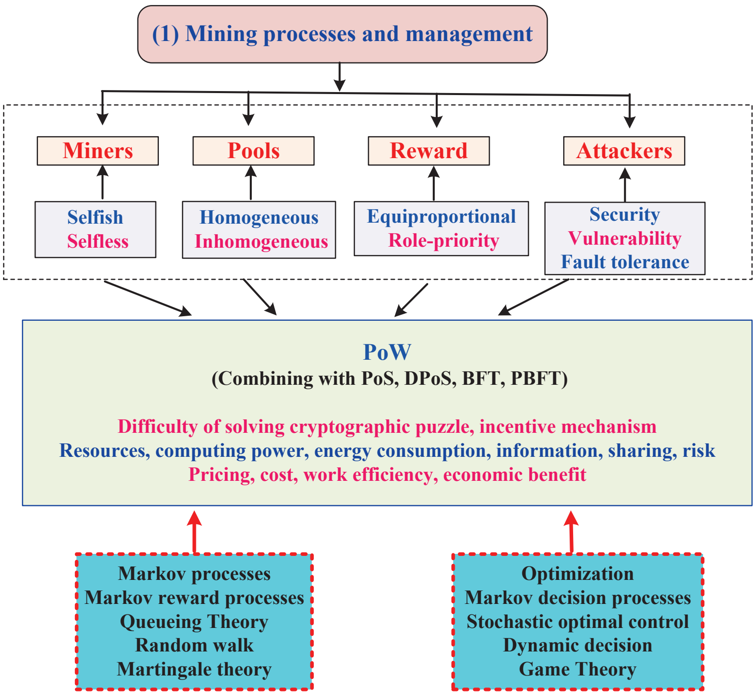

Figure 1. The mining processes and management

(2) Consensus mechanism

For mathematical modeling and analysis on this research direction, we need to discuss the random consensus-accomplished times for different consensus protocols (or algorithms), such as PoW, PoS, DPoS, BFT, PBFT, Raft, and DAG. Furthermore, we need to analyze the blockchain systems under different consensus protocols and to study the throughput, security, privacy protection, and scalability of blockchain systems. Our main concerns include a set of basic factors, such as consensus types, efficiency, convergence, consistency, network delay, and energy consumption. See Figure 2 for more details.

(3) Performance evaluation

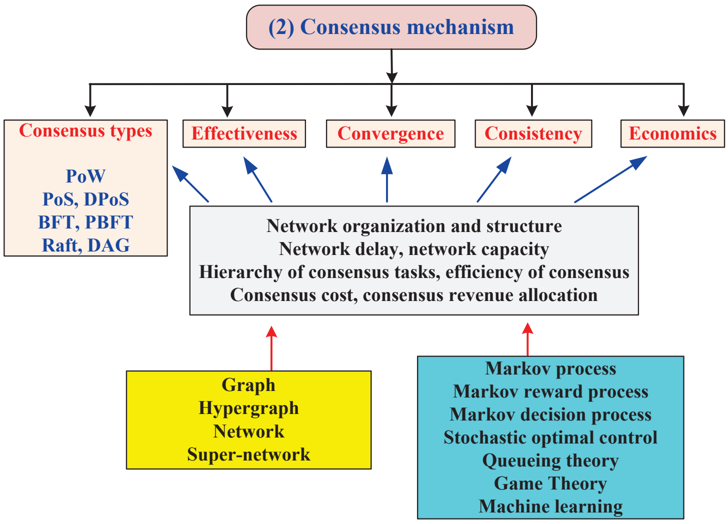

Figure 2. The consensus mechanism

In this class of mathematical modeling and analysis, we need to set up performance models of blockchain systems when considering different consensus mechanisms or protocols or algorithms (PoW, PoS, DPoS, PBFT, DAG and so on), different blockchain types (Bitcoin, Ethereum, side-chain, cross-chain, off-chain and so on), and innovation and new network architectures of blockchain systems. See Figure 3 for more details.

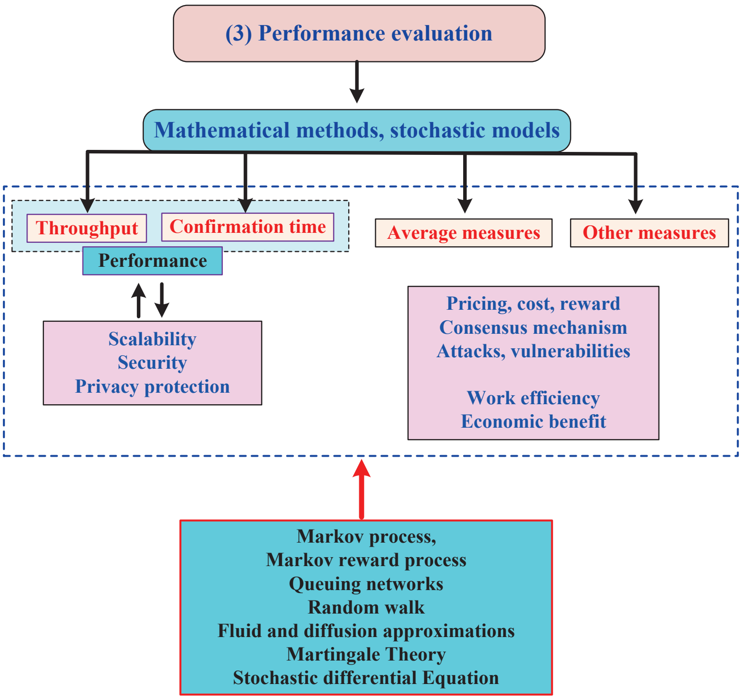

Figure 3. Performance modeling and analysis of blockchain systems

(4) to (6) Performance optimization, dynamic decision, and machine learning

In this class of mathematical modeling and analysis **(4)**, we need to optimize the performance measures of a blockchain system by means of linear programming, nonlinear programming, integer programming, multi-objective programming and so on.

In this class of mathematical modeling and analysis **(5)**, we need to realize optimal control and dynamic decision of a blockchain system by using the Markov decision processes, sensitivity-based optimization, and stochastic optimal control. See Figure 4 for more details.

For machine learning **(6)**, we need to develop machine learning, deep reinforcement learning, and federated learning. See Figure 4 for more details.

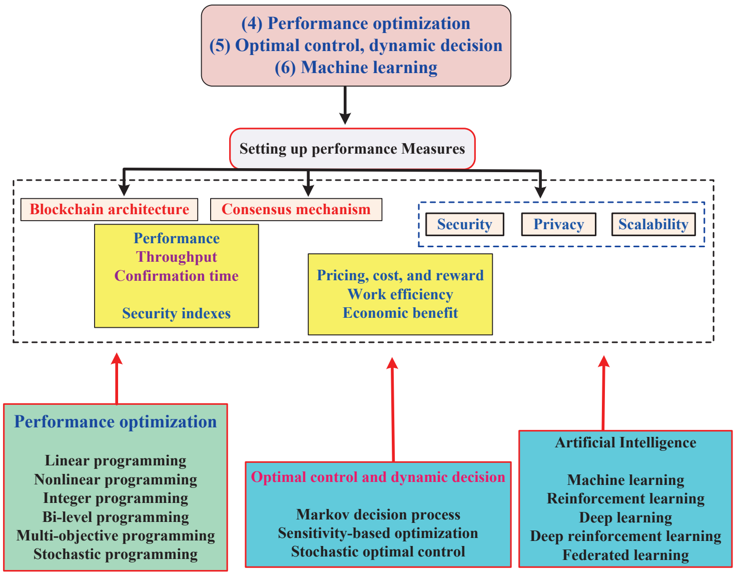

Figure 4. Performance optimization, dynamic decision, and machine learning

(7) Blockchain economy and market, and (8) blockchain ecology

For the blockchain economy and market **(7)** as well as the blockchain ecology **(8)**, readers may refer to Figures 5 and 6 for a simple introduction, respectively.

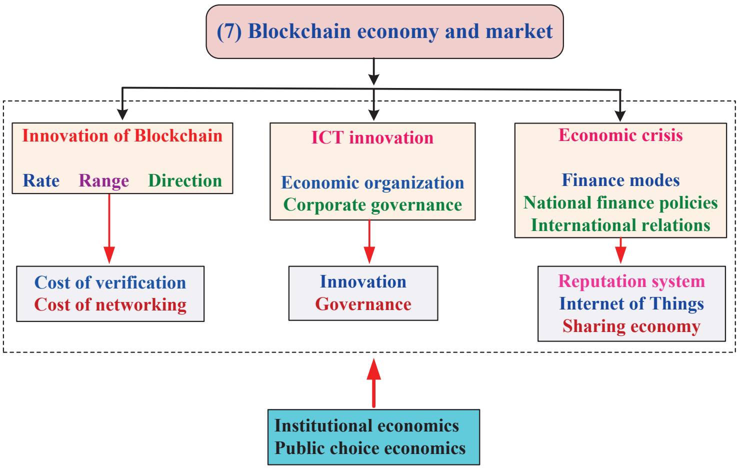

Figure 5. The blockchain economy and market

With fast development of blockchain, new blockchain technology continue to emerge. Thus, performance evaluation, performance optimization, optimal control and dynamic decision of blockchain systems become progressively. In particular, performance modeling and mathematical methods have been increasingly lacking and insufficient up to now, and especially, for dealing with the newly developing blockchain technology. Blockchain is a hierarchical comprehensive database, and it operates under a consensus mechanism of distribute systems in a peer-to-peer network. In addition, blockchain is an interesting and creative combination of multiple computer technologies, such as encryption techniques, consensus mechanism, security, privacy protection, and scalability; and wireless, mobility, cloud computing, edge computing, Internet of Things, and quantum. Based on this, blockchain is always a complicated stochastic system under a

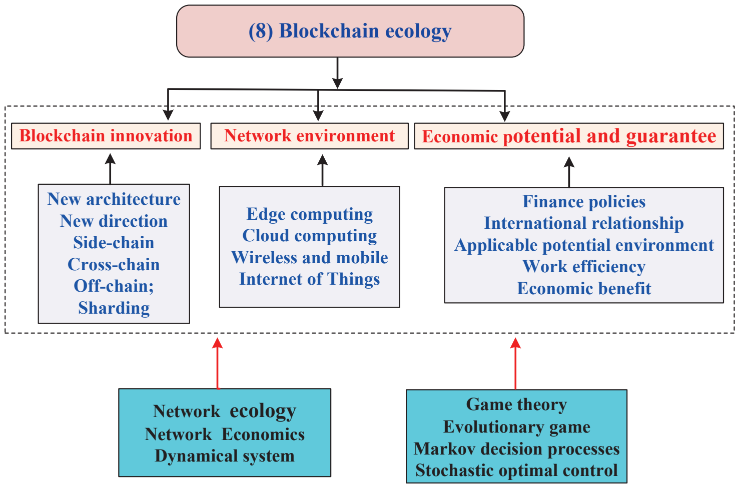

Figure 6. The blockchain ecology

strongly practical environment. In this situation, performance evaluation, performance optimization, optimal control and dynamic decision of blockchain systems always become interesting and challenging in their theoretical study.

So far, a few survey papers have discussed blockchain technology with a simple introduction to performance analysis of blockchain systems. See Table 1 for more details. From Table 1, it is easy to see that those survey papers focused on several key perspectives: Performance, scalability, security, and privacy protection.

To open the scope of our survey research on performance evaluation, performance

Table 1. Survey papers for performance evaluation of blockchain systems

Year	Surveys or reviews	Research scope
2018	Kim *et al* [2]	Scalability solutions
2019	Rouhani and Deters [3]	Security, performance, and applications of smart contracts
2019	Wang *et al* [4]	Performance benchmarking tools; optimization methods
2019	Zheng *et al* [5]	Challenges and progresses in blockchain from a performance and security perspective
2020	Smetanin *et al* [6]	Effective simulation and modeling approaches
2020	Singh *et al* [7]	Side-chains for improving scalability, privacy protection, security of blockchain
2020	Zhou *et al* [8]	Scalability of blockchain
2020	Yu *et al* [9]	Sharding for blockchain scalability
2020	Fan *et al* [10]	Stochastic models for blockchain systems: Game theory, perfor-mance optimization, machine learning, *etc.*
2021	Cao *et al* [11]	Mathematical models for blockchain such as stochastic process, game theory, optimization, and machine learning
2021	Huang *et al* [12]	Performance models, and analysis tools of blockchain systems or networks
2022	Wang and Wu [13]	Operations research problems from the aspects of security and stability, efficiency and performance, and resource allocation

optimization, optimal control and dynamic decision of blockchain systems, this paper chooses a collection of research materials from major scientific journals, international conferences, and preprint sites including IEEE Xplore, ACM digital library, Elsevier, SpringerLink, MPDI, arXiv, HAL, and so on. Based on these research materials, we provide a detailed review and analysis from the literature with respect to research on performance evaluation, performance optimization, optimal control and dynamic decision of multiple blockchain systems, including the consensus mechanism or protocols or algorithms (PoW, PoS, DPoS, PBFT, DAG and so on), the blockchain types (Bitcoin, Ethereum, side-chain, cross-chain, off-chain, and so on), and the new network architecture of blockchain. At the same time, we provide how to set up stochastic models and to develop effective methods, algorithms or simulations for dealing with the performance evaluation, performance optimization, optimal control and dynamic decision. Note that such a study of blockchain technology is interesting and challenging in not only the basic theory but also many practical applications.

Based on the above analysis, we summarize the main contributions of this paper as follows:

(1) We provide a basic overview for the available mathematical methods (in particular, stochastic analysis), which greatly support performance modeling and computation in performance evaluation, performance optimization, optimal control and dynamic decision.

(2) We provide a clear outline and structure for performance evaluation and performance optimization of blockchain systems. Important mathematical methods and techniques include **(a)** performance evaluation: Queueing theory, Markov processes, Markov reward process, random walk, fluid and diffusion approximations, martingale theory; and **(b)** performance optimization: Linear programming, nonlinear programming, integer programming, and multi-objective programming.

(3) We summarize optimal control and dynamic decision of blockchain systems by means of, for example, **(c)** Markov decision process, sensitivity-based optimization, and stochastic optimal control; and **(d)** machine learning, deep reinforcement learning, and federated learning. These issues are interesting and challenging with greater potential in future study of blockchain technology.

The remainder of this paper is organized as follows. Section 2 reviews the recent literature on the performance evaluation of blockchain systems by means of the queueing theory, the Markov processes, and the Markov reward processes. Furthermore, Section 3 provides some further methods for performance evaluation of blockchain systems by using, for example, the random walks, the fluid approximation, the diffusion approximation, and the martingale theory. Section 4 reviews performance optimization of blockchain systems by means of the linear programming, the nonlinear programming, the integer programming, and the multi-objective programming. Section 5 focuses on the overview of applications of the Markov decision processes and sensitivity-based optimization to find the optimal dynamic strategy of blockchain systems. Section 6 summarizes applications of machine learning (e.g., deep reinforcement learning and federated learning) to performance optimization, optimal control and dynamic decision of blockchain systems. Section 7 highlights some concluding remarks.

2. Performance evaluation

In this section, we summarize performance evaluation models of blockchain systems by means of queueing theory, the Markov processes and Markov reward processes. Note that some other mathematical methods for performance evaluation are left for the next section.

2.1. Queueing theory

Queueing theory is a key mathematical tool to set up performance measures and performance evaluation of blockchain systems. Applying queueing theory to performance analysis of 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. Specifically, the key factors include **(1)** transactions arrivals, **(2)** transaction fees, **(3)** block size, **(4)** network delay, **(5)** block generated process (e.g., mining process or voting process), **(6)** the pegging process of a block (or a sub-chains), **(7)** mining competition among multiple mining pools (e.g., a tree structure), **(8)** mining reward, and **(9)** computing power distribution. The physical structure is influenced by **(1)** consensus mechanism (e.g., PoW, PoS, DPoS, PBFT, and DAG), and **(2)** organization relation (e.g., side-chain, cross-chain, and off-chain). The research objectives of blockchain systems are designed as, for example, **(a)** performance: Throughput, confirmation time; **(b)** security; **(c)** privacy protection; and **(d)** scalability. Based on these specific examples, we can see that it is useful and necessary to apply queueing theory to set up performance models and to analyze performance measures in the study of blockchain systems.

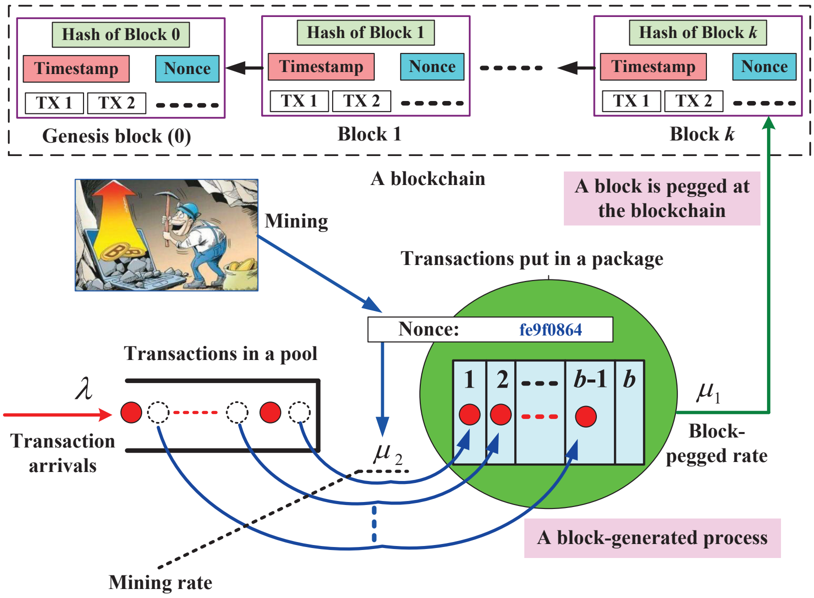

Figure 7. A simple physical structure of the PoW blockchain system

Understanding a blockchain system and its physical structure is not always simple. Li *et al* [14] may be the first one to provide a simple diagram of the physical structure of the PoW blockchain system with a miner (or a mining pool). See Figure 7 for more details.

For the other blockchain systems (e.g., PoS, DPoS, BFT, PBFT, and Raft), Chang *et al* [15] provided a queueing platform to evaluate their performance measures once the voting processes are determined by using the Markov modeling technology. Based on this, the first step is to study the voting processes, and the second step is to set up a queueing platform through the voting processes are regarded as the service processes. See Figure 8 for more details. In this queueing platform, it first needs to determine the two random variables: The block-generated time and the orphan-block-generated time, which can respectively be related to the arrival and service times in a queueing model $\mathrm{M} \oplus \mathrm{M}^{\mathrm{b}}/\mathrm{M}^{\mathrm{b}}/1$ or $\mathrm{M} \oplus \mathrm{PH}^{\mathrm{b}}/\mathrm{PH}^{\mathrm{b}}/1$.

Kawase and Kasahara [16] may be the first to apply queueing theory to study the PoW blockchain system with a miner, and a further paper by Kasahara and Kawahara [17] considered a single-server queue with batch service and priority mechanism to analyze the transaction-confirmation time. Because the block-generation time (note that it also includes block-pegged time) is a general probability distribution, the system of differential-difference equations given in the two papers by using the supplementary variable method will be unsolvable. For this reason, Li *et al* [14] provided a Markov

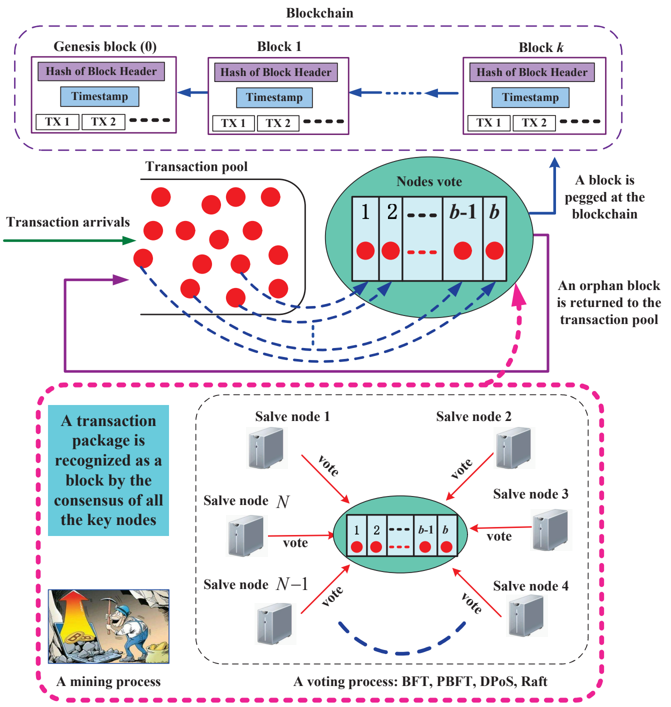

Figure 8. A queueing platform of different blockchain systems

queue with two stages (the block-generated time and the block-pegged time) to analyze the PoW blockchain system with a miner. Li *et al* [14] may be the first paper that can clearly describe and express the physical structure with multiple key factors of the PoW blockchain system, as seen in Figure 7. For the two-stage queue of the PoW blockchain system, the matrix geometric solution was applied to give a complete solution of this system such that the performance evaluation of the PoW blockchain system was established in a simple form and was further analyzed by means of a more detailed numerical analysis. In later studies, Li *et al* [18] relaxed the model assumptions of Li *et al* [14] to a more general case that the transaction arrivals are a Markovian arrival process (MAP), and the block-generated time and the block-pegged time are all of phase type (PH). Obviously, computing the mean transaction-confirmation time becomes very difficult and complicated due to the complicated blockchain structure, as suggested by Li *et al* [18].

Kawase and Kasahara [16] and Li *et al* [14] have inspired numerous later strain of literature to apply the queueing theory to performance evaluation of blockchain systems. Now, we list some literature as follows:

Geissler *et al* [19] neglected the information propagation delays and assumed the immediate distribution of transactions and blocks to all the peers in the network. They developed a discrete-time queueing model that allows performance evaluation of a blockchain system, such as the transaction waiting time distribution. Zhao *et al* [20] regarded the mining process as a vacation, and the block-verification process as a service. Specially, they established a non-exhaustive queueing model with a limited batch service and a possible zero-transaction service and derived the average number of transactions and the average confirmation time of a transaction in the blockchain system. Krieger *et al* [21] proposed a Markovian non-purging (n, k) fork-join queueing model to analyze the delay time of the synchronization process among the miners, where a vote-based consensus procedure is used. Ahmad *et al* [22] presented an end-to-end blockchain system for dealing with the audit trail applications, and analyzed the time, space, consensus, search complexity, and security of this blockchain system by using the queueing theory.

Mišić *et al* [23] applied the Jackson network model to the entire network, in which each individual node operates as a priority M/G/1 queue, and developed an analytical model for analyzing the Bitcoin's blockchain network. He *et al* [24] introduced a queueing model with priority to incorporate the operational feature of blockchain, the interplay between miners and users, and the security issue associated with the decentralized nature of the blockchain system. Fang and Liu [25] proposed a dynamic mining resources allocation algorithm (DMRA) to reduce the mining cost in the PoW blockchain networks through using the logical queueing-based analytical model.

Frolkova and Mandjes [26] proposed a G/M/∞-like Bitcoin queueing model to consider the propagation delay between two individual users. Fralix [27] provided a further discussion for the infinite-server queue introduced in Frolkova and Mandjes [26].

Seol *et al* [28] proposed an embedded Markov chain to analyze a blockchain system with a specific interest in Ethereum. Gopalan *et al* [29] analyzed the stability and scalability of the DAG-based blockchain system by using queueing networks. Meng *et al* [30] proposed a queueing model for studying the three stages of the consortium blockchain consensus, analyze the consistency properties of consortium blockchain protocols, and provided performance evaluation for the main stages of the blockchain consensus. Sun *et al* [31] provided a queueing system with three service stages, which express the three-stage consensus process of the RC-chain and the building of a new block. By using the queueing model, they obtained three key performance measures: The average number of transactions in system, the average transaction confirmation time, and the average transaction throughput. Altarawneh *et al* [32] set up a queueing model to compute the average waiting time for the victim client transactions, and evaluated the security and reliability of the blockchain system.

Ricci *et al* [33] proposed a framework encompassing machine learning and a queueing model M/G/1 to identify which transactions will be confirmed, and characterized the confirmation time of confirmed transactions.

Sukhwani *et al* [34] presented a performance method of Hyperledger Fabric v1.0+ by using a stochastic Petri net modeling (stochastic reward nets) to compute the throughput, utilization, mean queue length at each peer, and the critical processing stages within a peer.

Li *et al* [35] discussed a queueing game with a non-preemptive priority of a blockchain system and considered both the miners' mining rewards and the users' time costs. For ease of reading, we summarize the queueing models of blockchain systems in Table 2.

By means of the queueing theory, some papers have conducted research on the simulation and empirical study of blockchain systems. Important examples include among which Memon *et al* [36] and Spirkina *et al* [37] proposed a queueing theory-based simulation model to understand the performance measures of the blockchain system. Wilhelmi *et al* [38] proposed a batch-service queue model for evaluating the network delay in a blockchain system. Furthermore, they provided some simulations to assess the performance of the synchronous and asynchronous mechanisms.

In the queueing models of blockchain systems, Bowden *et al* [39] is a key work because the generation time is related to the service time. They showed that the generation time of a new block has some key statistical properties, for example, the generation time is non-exponential, and it can also be affected by many physical factors.

So far, many classes of blockchain systems have still been lacking research on performance evaluation by using the queueing theory. 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. Therefore, the queueing models of blockchain systems are always interesting and challenging in the future study of blockchain technology.

Table 2. The queueing models of blockchain systems

Paper	Year	Queue type	Research scope
[34]	2018	Petri Nets model	Throughput; utilization; mean queue length at each peer; critical processing stages within a peer
[35]	2018	A queueing game	The miners' mining rewards; the users' time cost
[19]	2019	$GI/G^X/1$	Queue size; waiting time of transactions
[20]	2019	$M/G^X \oplus G/1$	The average number of transactions; the average confirmation time of transactions
[21]	2019	Fork-join queue	The delay performance of the synchronization process among the miners
[22]	2019	M/D/c	The time, space, consensus, and search complexity; security
[23]	2019	Jackson network model; M/G/1	Probability distributions of block and transaction distribution time; node response time; forking probabilities; network partition sizes; duration of ledger's inconsistency period.
[33]	2019	M/G/1	Identify which transactions will be confirmed; the confirmation time of confirmed transactions
[26]	2019	$GI/M/\infty$	Propagation delay between two individual users
[27]	2020	Infinite-server queue	A further study of the infinite-server queue studied in [26]; related infinite-server queues have similar dynamics
[28]	2020	$M^X/M^X/1$	The average number of slots; the average waiting time per slot; throughput
[24]	2020	$M/M^X/1$ with priority	Users' equilibrium behavior; total fee rate; confirmation latency; system equilibria
[29]	2020	Monotone separable queuing models	Stability and scalability of the DAG network
[25]	2020	Logical queueing-based analytical model	Mining resources allocation; mining cost; stability
[30]	2021	$M/H_2/1$; M/M/1; M/Er/1	The consistency and security of consortium blockchain protocols
[32]	2021	M/M/1; $M/M/\infty$	The average waiting time for the victim client transactions; security; reliability
[31]	2021	Three-phase service queuing process	The average number of transactions; the average transaction confirmation time; the average transaction throughput.
[38]	2021	A novel batch-service queue model	The learning completion delay of blockchain-enabled federated learning; performance of synchronous and asynchronous mechanisms
[15]	2022	$M \oplus M^b/M^b/1$	Throughput of the dynamic PBFT blockchain system; the stationary rate (or probability) that a block is pegged on the blockchain; the stationary rate (or probability) that an orphan block is returned to the transaction pool

2.2. Markov processes and Markov reward processes

In performance evaluation of blockchain systems, Markov processes and Markov reward processes are two effective mathematical methods. See Li [40] for a set of Markov models and computational methods by using the RG-factorizations. Note that Markov processes are used to evaluate throughput, confirmation time, and security and privacy protection of blockchain systems; while the Markov reward processes are applied to analyzing work efficiency, economic benefits, and cost control of blockchain systems.

For the vulnerability and forked structure of the PoW blockchain systems with two mining pools (honest and dishonest), Eyal and Sirer [41] proposed a selfish mining strategy for the competitive mining process between the two mining pools, and set up a simple Markov process with a special reward structure to discuss the competitive behavior between the two mining pools. By means of an intuitive reward analysis, they indicated that the selfish miner can win a higher mining reward through violating the honest agreement in the blockchain system. However, Li *et al* [42] showed that the Markov process with rewards given in Eyal and Sirer [41] is not correct from the ordinary theory of Markov processes.

For a PoW blockchain system with two mining pools (honest and dishonest), Li *et al* [42] showed the competitive behavior between the two mining pools by means of Figure 9.

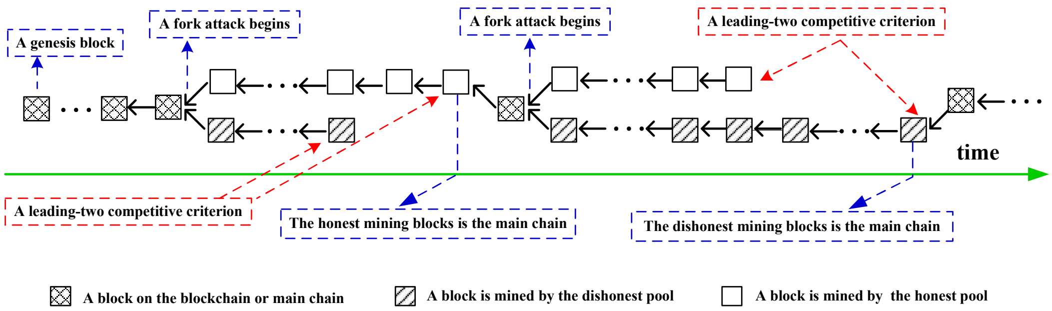

Figure 9. The competitive behavior between the two mining pools

When the two block branches forked at a common tree root, let $I(t)$ and $J(t)$ be the numbers of blocks mined by the honest and dishonest mining pools at time t, respectively. It is seen from Li *et al* [42] that $\{(I(t), J(t)) : t \geq 0\}$ is a continuous-time Markov process whose infinitesimal generator is given by

$$Q = \begin{pmatrix} Q_{\tilde{\mathbf{0}},\tilde{\mathbf{0}}} & Q_{\tilde{\mathbf{0}},0} & Q_{\tilde{\mathbf{0}},1} & & & & \\ Q_{0,\tilde{\mathbf{0}}} & Q_{0,0} & Q_{0,1} & & & & \\ Q_{1,\tilde{\mathbf{0}}} & & Q_{1,1} & Q_{1,2} & & & \\ B & & & A & C & & \\ B & & & & A & C & \\ \vdots & & & & & \ddots & \ddots \end{pmatrix}.$$

For the PoW blockchain system with two mining pools (honest and dishonest), Gőbel *et al* [43] set up a two-dimensional Markov process with network propagation delay and provided performance evaluation of the PoW blockchain system. Javier and Fralix [44] further discussed the two-dimensional Markov process given by Gőbel *et al* [43] and developed a new computational method. Li *et al* [42] set up a new two-dimensional pyramidal Markov (reward) process of the blockchain system, which leads to a novel theoretical framework for performance evaluation of a PoW blockchain system with adding new random factors by means of a new class of matrix geometric solutions.

Using the Markov process approach of Eyal and Sirer [41], Nayak *et al* [45] introduced a new type of mining strategy: The stubborn mining strategy and also established its two extended forms: The equal-fork stubborn mining strategy and the path stubborn mining strategy. Further important examples include Wang *et al* [46] and Liu *et al* [47]. In addition, inspired by the Markov process approach of Eyal and Sirer [41], the selfish mining strategy was extended to the Ethereum system. Readers can see Grunspan and Pérez-Marco [48] and Niu and Feng [49] for more details. Also, the impact of the selfish mining behavior of multiple mining pools on the blockchain system has also been paid widespread attention, e.g., see Bai *et al* [50], Bai *et al* [51], Chang [52], Liu *et al* [53], Marmolejo-Cossío *et al* [54] and Xia *et al* [55].

From the ordinary theory of Markov processes, we summarize some works that use the Markov processes or Markov reward processes to study other interesting issues of blockchain systems as follows.

Song *et al* [56] provided a Markov process theory for network growth processes of DAG-based blockchain systems. Li *et al* [57] established a Markov process to analyze performance and security of the IoT ledgers with a directed acyclic graph.

Chang *et al* [15] applied a large-scale Markov process to study the dynamic-PBFT blockchain system. Ma *et al* [58] established a two-dimensional Markov process to provide performance evaluation of PBFT blockchain systems.

Carlsten [59] applied the Markov process to study the impact of transaction fees on the selfish mining strategy of the blockchain. Shi *et al* [60] developed a new consensus protocol (Proof-of-Age, PoA) and employed a continuous time Markov chain to show that the consensus protocol can disincentivize the pooled mining. Kiffer *et al* [61] set up a Markov-chain to analyze the consistency properties of blockchain protocols. Huang *et al* [62] established a Markov process with an absorbing state to give performance analysis of the raft consensus algorithm in private blockchains. Srivastava [63] computed the transaction confirmation time of blockchain by using a Markov model. Li *et al* [64] established the Markov process to study the block access control mechanism in the wireless blockchain network. Piriou and Dumas [65] constructed a Markov process to analyze the blockchain system and developed a simulation model of blockchain technology.

Nguyen *et al* [66] applied the Markov process and deep reinforcement learning to study the task offloading problem in the mobile blockchain with privacy protection.

Jofré *et al* [67] established a Markov process to study the convergence rate of blockchain mining games.

It is worthwhile to note that these studies outline a critical role of Markov processes and Markov reward processes in performance evaluation of blockchain systems. This will be a potential and interesting area for future study.

3. Further methods for performance evaluation

In this section, we summarize further methods for performance evaluation of blockchain systems, including the random walk, the fluid approximation, the diffusion approximation, and the martingale theory.

3.1. The random walk

The random walk is a key mathematical method in analyzing many stochastic models, such as queueing systems, inventory models and information and communication technology (ICT) systems. See Spitzer [68], Prabhu [69], and Xia *et al* [70] for more details.

Recent, a few papers have studied blockchain systems by using the random walk, and especially, analyzing the double-spending attacks of blockchain.

Goffard [71] refined a random walk model underlying the double-spending problem and provided a fraud risk assessment of the blockchain system.

In contrast with Goffard's model [71], Jang and Lee [72] proposed another random walk model to study the probability distribution of catch-up time spent in the fraudulent chain to catch up with the honest chain, which takes into account the block confirmation. They discussed the profitability of the double-spending attacks that manipulate a priori mined transaction in a blockchain system.

Brown *et al* [73] studied the duration and probability of success of a double-spend attack in terms of the random walk.

Grunspan and Pérez-Marco [74] determined the minimal number of confirmations requested by the recipient such that the double spend strategy is non-profitable by means of the random walk.

3.2. The fluid and diffusion approximations

The fluid and diffusion approximations are two key mathematical methods in analyzing many stochastic models with some general random variables, such as queueing systems, inventory models, supply chains, and communication networks. The fluid and diffusion approximations describe a deterministic process that aims to approximately analyze the evolution of stochastic processes, that is, they can analyze the evolution of generalized stochastic processes by using the idea of weak limits. Recently, fluid and diffusion approximations have been widely used in analysis of large-scale complex networks with the tendency of scale expansion, complex structure, and dynamic behavior. See Chen and Yao [75], Whitt [76], Dai *et al* [77], Büke and Chen [78], Chen and Shanthikumar [79] for more details.

So far, fluid and diffusion approximations have been applied to the analysis of blockchain systems. Important examples include among which Frolkova and Mandjes [26] developed a Bitcoin-inspired infinite-server model by means of a random fluid limit. King [80] proposed a fluid approximation of the random graph model and discussed the related technologies of shared ledgers and distributed ledgers in blockchain systems. Ferraro *et al* [81] studied the stability of unverified transaction systems in the DAG-based distributed ledgers by means of the fluid approximation. Koops [82] applied the diffusion approximation to predict the confirmation time of Bitcoin transactions.

There are a few blockchain works that analyze the evolution of generalized stochastic processes by using the idea of weak limits. For example, Corcino *et al* [83] discussed the mean square displacement of fluctuations of Bitcoin unit prices over time on a daily basis by applying the method of Brownian motion and Gaussian white noise analysis. Chevallier *et al* [84] used the Lévy jump diffusion Markov switching model to study the price fluctuation characteristics of Bitcoin.

For the fluid and diffusion approximations of blockchain systems, it is interesting and challenging to study the PoW blockchain systems with multiple mining pools. See Li *et al* [85] for a general tree representation of complicated mining competition among multiple mining pools. Note that the fluid and diffusion approximations can also provide performance evaluation of blockchain systems, thus there exists a great potential and innovation in the future research of many blockchain systems (e.g., PoS, DPoS, PBFT, and DAG).

3.3. The martingale theory

The martingale theory not only enriches the contents of probability theory but also provides a powerful method for studying stochastic processes and stochastic models, and it has been widely applied in economics, networks, decision, and control. Grunspan and Pérez-Marco applied the martingale theory to study the profits of miners under different attacks of blockchain systems since 2018. Using the martingale theory, the research on common attacks in blockchain systems is summarized in Table 3.

Table 3. Research on attacks of blockchain by using martingale theory

Year	Attack type	Research scope	Method or theory
2018	Selfish mining [86]	Expected duration of attack cycles; the profitability model by using repetition games; improvement of Bitcoin protocol; the miner's attraction to the selfish mining pools	Martingale theory; Doob stopping time theorem
2018	Stubborn mining [87]	The profitabilities of stubborn mining strategies	Martingale theory; Catalan numbers and Catalan distributions
2018	Trailing mining [88]	The revenue ratio of the trail stubborn mining strategy in the Bitcoin network; the profitability of other block-withholding strategies	Martingale theory; classical analysis of hiker problems
2020	SM; LSM; EFSM and so on [89]	The profitabilities of various mining strategies	Martingale theory; Markov chains; Dyck words
2020	SM, intermittent SM and smart mining [90]	The closed forms for the profit lag; the revenue ratio for the strategies "selfish mining" and "intermittent selfish mining"	Martingale theory; foundational set-up from previous companion article
2021	Nakamoto double spend [74]	The exact profitability for Nakamoto double spend strategy; the minimal number of confirmations to be requested by the recipient such that this double spend strategy is non-profitable	Martingale theory; glambler ruin; random walk

4. Performance optimization

In this section, we provide an overview for performance optimization of blockchain systems by using different optimal methods.

Performance optimization is to optimize performance measures of blockchain systems by means of mathematical programming (e.g., linear programming, nonlinear programming, integer programming, and multi-objective programming). Also, it composes four elements: Optimization problem, optimization variables, objective functions, and restrictive conditions. The optimization process needs to accomplish such a task: When the restrictive conditions are satisfied, the optimization variables are adjusted to make that these objective functions go to either the maximum or the minimum.

Performance optimization is necessary and important in the study of blockchain systems, including design, organization, control, and management of blockchain systems. Such a study will strongly support the overall development of theoretical research and practical applications of blockchain technology.

So far, performance optimization of blockchain systems has been studied in at least three aspects as follows:

(1) From consensus mechanism and network architecture of blockchain systems, it is interesting to optimize performance (e.g., throughput and confirmation time), work efficiency, economic benefit; improve scalability, security, privacy protection and degree of decentralization; and balancing operations costs and efficiency, and allocation of profits. Important examples include Lundbaek and D'Iddio [91], Liang [92], Nguyen *et al* [93], Wang *et al* [94], Saad *et al* [95], Reddy and Sharma [96], Leonardos *et al* [97], Liu *et al* [98], Varma and Maguluri [99], and Li *et al* [100].

(2) From some key factors (e.g., operations costs, pricing, computing power, transaction fee, network delay) of PoW blockchain systems, it is necessary to consider the optimal strategies of dishonest miners, for example, how to pack a transaction package from a transaction pool? How to incentive honest miners to jump into the dishonest mining pool? How to incentive the dishonest miners to keep mining in a round of competition? How to maximize miners' economic benefit or work efficiency? Important examples include Kang *et al* [101], Aggarwal *et al* [102], Ramezan *et al* [103], and Liu *et al* [98].

(3) For users or enterprises with pricing, cost, transaction fee, and platform selection, how to maximize user (or enterprise) utility? Important examples include Kang *et al* [101], Riehl and Ward [104], Zhou *et al* [105], Varma and Maguluri [99], and Liu *et al* [98].

Based on the above analysis, we summarize performance optimization of blockchain systems in Table 4. It is seen from Table 4 that most of the research on performance optimization of blockchain systems focuses on discussing the following issues:

(i) Does there exist a better network architecture or consensus mechanism such that the blockchain system is more efficient, secure, and scalable?

(ii) Is there a better application scenario that makes blockchain more consistent and less waste of resources?

(iii) Is there a more effective economic incentive mechanism that makes blockchain more profitable, and lower cost of operations, verification and communication?

(iv) Is there a better trading platform and a more favorable market environment that make users in blockchain more usable and more credible among the users?

In a word, performance optimization of blockchain systems is an interesting, hot and frontier research topic, and also there exists a large capacity for research innovation through discussing broad blockchain systems (e.g., consensus mechanism and network architectures), for example, cross-chain, side-chain, off-chain, and interoperability of information and assets among different chains; data synchronization, data security; pricing, cost, economic benefit, and work efficiency; scalability, security, and privacy protection.

5. Markov decision processes

In this section, we apply the Markov decision processes (MDPs) to the study of blockchain systems and provide some algorithms for computing the optimal dynamic policy of such a Markov decision process. For the Markov decision processes, readers may refer to Puterman [106] and Li *et al* [107] for more details.

The Markov decision processes can be widely applied to deal with the selfish mining attacks in the PoW blockchain systems because the selfish mining process needs to choose a series of mining policies to be able to maximize the reward or to minimize the cost of the dishonest miners (or mining pools).

When a PoW blockchain system has two different miners or mining pools (honest and dishonest) to compete for a more mining reward, in which the dishonest miner may adopt different mining policies based on the longest chain rule. The dishonest miner can control the fork structure of block tree through releasing some parts of blocks to obtain his maximum benefit. Accordingly, an interesting topic focuses on how the dishonest miner finds an optimal mining policy (i.e., how many mined blocks are released in a round of competition). Important examples include among which Sapirshtein *et al* [108], Sompolinsky and Zohar [109] and Gervais *et al* [110] introduced four different policies: Adopt, cover, match, and wait for selfish miners, and they determined the optimal selfish mining policy.

Zur *et al* [111] studied the optimal selfish mining policy of the PoW blockchain system by using the Markov decision process and proposed a new method to solve the Markov decision process with an average reward criterion.

Bai *et al* [51] applied the Markov process to study the PoW blockchain system with

Table 4. Performance optimization of blockchain systems

Proposed for	Optimization scope	Optimization factors	Methods
Governed blockchains [91]	Solving the MINLP optimization problems for computing optimal Proof of Work configuration parameters that trade off potentially conflicting aspects such as availability, resiliency, security, and cost	Expected availability; resiliency; security; cost	Mixed integer nonlinear programming
A new system [92]	Re-innovating all the core elements of the blockchain technology to achieve the best balance among scalability, security and decentralization	Transaction confirmation time; information propagation latency	Min-max optimization
A new sharding paradigm [93]	Proposing OptChain that can minimize transactions and maintain a temporal balance among shards to improve the confirmation time and throughput	Confirmation time; transaction throughput; cross-shard transactions minimization; temporal balancing	Nonlinear programming
A new dynamic routing solution [94]	Proposing a new dynamic routing solution Flash to strike a better tradeoff between path optimality and probing overhead	Payment size; transaction fees; probing overhead; transaction throughput	Linear programming
A new form of attacks [95]	Studying a new form of attacks that can be carried out on the memory pools and proposing countermeasures that optimize the mempool size and help in countering the effects of DDoS attacks	Attack cost; relay fee; mining fee; memorypool size	Nonlinear programming
PoW blockchain and blockDAG [96]	Proposing two models to scale the transaction throughput	Block creation rate; transaction throughput; main chain block growth rate; propagation delay; risk	Nonlinear programming
PoS protocols [97]	Leveraging weighted majority voting rules that optimize collective decision making to improve the efficiency and robustness of the consensus mechanism	Validators' voting behavior; blockchain rewards; collective decision; collective welfare	Mixed integer nonlinear programming
Protocol designer, users, and miners [98]	Proposing a Fee and Waiting Tax (FWT) mechanism to improve the incentives for the miners' participation and blockchain security, and to mitigate blockchain insufficient fee issue	Storage costs of miners; users' transaction fee; fee choices and waiting tax for users; transaction waiting time	Multi-objective programming
Lightning and Spider network [99]	Setting up a two-sided queue model and propose a throughput optimal algorithm that stabilizes the system under any load within the capacity region	Transaction throughput; arrival rate; capacity region; payment requests	Linear programming
A new protocol [100]	Proposing EntrapNet protocol and optimize EntrapNet to deal with the fundamental tradeoff between security and efficiency	Security; efficiency	Nonlinear programming
Users, miners, and verifiers [101]	Considering the tradeoff between the network delay of block propagation process and offered transaction fee from the blockchain user to jointly maximize utility of the blockchain user and individual profit of the miners	Network delay of block propagation process; offered transaction fee from the blockchain user	Nonlinear programming
Miners [102]	Demonstrating BTC's robust stability, and find that the implemented design of emergency difficulty adjustment resulted in maximal miners' profits	Coinbase reward; competition cost reward; transaction fees; competition cost fees; mining cost; waiting cost; switching incentive; miners' profits	Mixed integer nonlinear programming
Miners [103]	How should miners pick up transactions from a transaction pool to minimize the average waiting time per transaction	Average waiting time per transaction	Mixed integer nonlinear programming
A new pricing mechanism [104]	Presenting a pricing mechanism that aligns incentives of agents who exchange resources on a decentralized ledger to greatly increase transaction throughput with minimal loss of security	Transaction pricing; expected transaction efficiency; block assembly; transaction throughput; security	Integer linear programming
Enterprises and users [105]	Choosing the most effective platform from many blockchains to control costs and share data	Technical, market and popularity indicators; improved global DEA-Malmquist measure	Nonlinear programming

multiple miners and used the Markov decision process with observable information to find the optimal selfish mining policy for a special case with two different miners.

Li *et al* [112] discussed the PoW blockchain system by using the hidden Markov decision process and proposed an improved selfish mining policy.

Ma and Li [113] analyzed the optimal selfish mining policy of the PoW blockchain system with two mining pools through using the sensitivity-based optimization theory.

In addition, the Markov decision processes are also applied to deal with other blockchain control issues as follows:

Niu *et al* [114] provided an incentive analysis for the Bitcoin-NG protocol by using the Markov decision process, and showed that the Bitcoin-NG protocol can maintain the incentive-compatible mining attacks.

Wüst [115] used the Markov decision process to study the data security in the blockchain system.

Chicarino *et al* [116] discussed the selfish mining inspection and tracking attacks in the PoW blockchain network by means of the Markov decision processes.

6. Machine learning

In this section, we summarize the applications of machine learning (e.g., deep reinforcement learning and federated learning) to performance optimization and dynamic decision of blockchain systems.

Recent, machine learning (e.g., deep reinforcement learning and federated learning) has been applied to study performance optimization and dynamic decision of blockchain systems. Since the Markov decision process of a blockchain system is always more complicated, it is difficult and challenging to find the optimal policy of the Markov decision process, while the machine learning can provide an approximate solution for such an optimal policy. Therefore, it is interesting to develop approximate methods or algorithms to find the optimal policy by using, such as artificial intelligence, machine learning, deep reinforcement learning, and federated learning.

The survey papers: Liu *et al* [117] provided a survey for the recent literature that the blockchain technology is analyzed by means of machine learning and discussed several interesting directions on this research line. Ekramifard *et al* [118] provided a systematic overview for applying artificial intelligence to the study of blockchain systems, including the Markov decision process and machine learning. Chen *et al* [119] applied machine learning to performance optimization and dynamic decision of blockchain systems and proposed several interesting topics for future research. Shafay *et al* [120] reviewed the recent literature on applications of deep reinforcement learning to develop the blockchain technology.

In what follows, we summarize the recent research on applications of machine learning to the study of blockchain systems from several different aspects: The mining policy, the mobile-edge computing, and the Internet of Things or Industrial Internet of Things.

The mining policy: Considering the optimal policy of selfish mining attacks in Bitcoin as well as the Nash equilibrium in block withholding attacks, Hou *et al* [121] proposed a SquirRL framework to apply deep reinforcement learning to analyze the impact of attacks on the incentive mechanism of PoW blockchain. Bar-Zur [122] used reinforcement learning to find the optimal policy for the miners of different sizes through solving a Markov decision process problem with an average reward criterion. Wang *et al* [123] applied reinforcement learning (machine learning) to find the optimal mining policy in the Bitcoin-like blockchain and designed a new multi-dimensional reinforcement learning algorithm to solve the mining MDP problem with a non-linear objective function (rather than a linear objective function in the standard MDP problems).

When the growth of PoW blockchain is modeled as a Markov decision process, a learning agent needs to make the optimal decisions over all the states of Markov environment in every moment. To track the generation of new blocks and their verification process (*i.e.*, solving the mathematical puzzles), You [124] set up the PoW consensus protocol (*i.e.*, solving mathematical puzzles) through dealing with a reinforcement learning problem. In this case, the verification and generation of new blocks are designed as a deep reinforcement learning iterative process.

Mobile-edge computing: Nguyen *et al* [93] applied the Markov processes and deep reinforcement learning to study the task offloading problem of mobile blockchain under privacy protection. Qiu *et al* [125] formulated the online offloading problem as a Markov decision process and proposed a new model-free deep reinforcement learning-based online computation offloading approach for the blockchain-empowered mobile edge computing, in which both the mining tasks and the data processing tasks are considered. Feng *et al* [126] developed a cooperative computation offloading and resource allocation framework for the blockchain-enabled mobile-edge computing systems and designed a multi-objective function to maximize the computation rate of mobile-edge computing systems and the transaction throughput of the blockchain systems by means of the Markov decision processes.

Asheralieva and Niyato [127] developed a hierarchical learning framework by means of the Markov decision processes with the service provider and the miners and studied resource management of edge computing to support the public blockchain networks. By applying the Markov decision process, Asheralieva and Niyato [128] presented a novel game-theoretic, Bayesian reinforcement learning and deep learning framework to represent the interactions among the miners for the public and consortium blockchains with mobile edge computing. Yuan *et al* [129] applied the Markov decision processes and deep reinforcement learning to study the sharding technology for the blockchain-based mobile edge computing.

Internet of Things: Waheed *et al* [130] provided a summary of the security and privacy protection of blockchain technology in the Internet of Things by using machine learning algorithms. Gao *et al* [131] studied the task scheduling of the mobile blockchain supporting applications of the Internet of Things by means of deep reinforcement learning and Markov decision processes.

Industrial Internet of Things: Qiu *et al* [132] and Luo *et al* [133] studied the blockchain-based software-defined Industrial Internet of Things by means of a dueling deep Q-learning approach and the Markov decision processes. Yang *et al* [134] studied the energy-efficient resource allocation for the blockchain-enabled Industrial Internet of Things by deep reinforcement learning and Markov decision processes. Wu *et al* [135] provided a review for the deep reinforcement learning applied to the blockchain systems in the Industrial Internet of Things.

Federated learning: Blockchain establishes a secure and reliable mechanism between untrusted parties, and federated learning, as a new machine learning technology in recent years, realizes artificial intelligence that protects privacy. At present, the integration of blockchain technology and federated learning has formed a new learning paradigm, which has attracted researchers and applicators to conduct some interesting research. Readers may refer to, for example, Ma *et al* [136], Qu *et al* [137], Wang and Hu [138], Awan *et al* [139], Javed *et al* [140], Ali *et al* [141], Martinez *et al* [142], Nguyen *et al* [143], Qu *et al* [144], Pokhrel and Choi [145], Lu *et al* [146, 147, 148], Zhao *et al* [149], and Rehman *et al* [150].

7. Concluding remarks

Since Nakamoto [1] proposed Bitcoin in 2008, research on blockchain has attracted tremendous attention from both theoretical research and engineering applications. With fast development of blockchain technology, blockchain has developed many imaginative applicable modes through a series of innovative combinations among distributed data storage, point-to-point transmission, consensus mechanisms, encryption techniques, network and data security, privacy protection, and other computer technologies. Also, their subversive and imaginative features can further inspire endless technological innovations of blockchain. Among them, the most representative technologies, such as timestamp-based chain block structure, DAG-based network data structure, distributed consensus mechanism, consensus mechanism-based economic incentives, and flexible and programmable smart contracts, have increased extremely rich colors to various practical applications. Important examples include digital economy [151], Fintech [152], cloud services [153], reputation systems [154], social security [155], e-commerce supply chain [156], artificial intelligence [157], sharing economy [158], and supply chain management [159].

Performance evaluation, performance optimization, and dynamic decision are one of the most basic theoretical research of blockchain systems, and they play a key role in design, control, stability, improvement, and applications of blockchain systems. So far, some blockchain pitfalls (e.g., low performance and scalability, weak security and privacy protection, and inconvenient interoperability among blockchain subsystems) have severely limited a wide range of applications of blockchain technology. To resolve these blockchain pitfalls, a few technologies or methods have been proposed and developed, e.g., see off-chain [160], side-chain and cross-chain [161], sharding [162], and DAG [163]. However, it is a key to deal with whether these novel technologies and methods can effectively improve these pitfalls of the blockchain systems, while such an interesting issue is to need to be sufficiently studied by means of some strictly mathematical analysis. On the other hand, it is an interesting topic to set up some useful mathematic relations among performance, scalability, security, privacy protection and so forth. Some intuitively understanding examples include among which increased security will result in low throughput; increased scalability will result in high throughput; increased security will result in strong privacy protection. Note that the mathematic relationships can be set up by means of research on performance evaluation, performance optimization, and dynamic decision of blockchain systems.

It is easy to understand that practical applications will lead to the innovation boundary of blockchain technology. That is, blockchain applications are a main driving force of blockchain technology development. When a new application of blockchain technology is launched, the interface between technology and application is not always friendly, the performance and stability are not always high, and there are also deficiencies in security and privacy protection. Note that all the necessary improvements or increasing maturity need some plentiful research on performance evaluation, performance optimization, and dynamic decision of blockchain systems. In addition, for the current blockchain technology, we need to actively create a social atmosphere and ecological environment for both theoretical research and practical applications of blockchain. Also, this can powerfully promote deep integration between the blockchain technology and the key information technologies (such as artificial intelligence, big data, and the Internet of Things).

For a large-scale blockchain system or a new blockchain technology, it is key to find the bottleneck through analyzing vulnerability and fault tolerance of network architecture by means of some new mathematical theory and methods developed in research on performance evaluation, performance optimization, and dynamic decision of blockchain systems. Thus, this motivates us in this paper to provide a recent systematic overview of performance evaluation, performance optimization, and dynamic decision of blockchain systems, which involves mathematical modeling and basic theory of blockchain systems. Important examples include **(a)** performance evaluation: Markov processes, queuing theory, Markov reward processes, random walks, fluid and diffusion approximations, and martingale theory; **(b)** performance optimization: Linear programming, nonlinear programming, integer programming, and multi-objective programming; **(c)** optimal control and dynamic decision: Markov decision processes, and stochastic optimal control; and **(d)** machine learning: Deep reinforcement learning and federated learning. We believe that the new basic theory with mathematical methods, algorithms, and simulations discussed in this paper will strongly support future development and continuous innovation of blockchain technology.

Based on the above analysis, we believe that there are still many interesting research directions to be explored, such as smart contract, DAG-based blockchain, cross-chain, side-chain, off-chain and other network architectures; and some basic or new consensus protocols. Our future research includes:

– Developing effective methods to compute and improve performance, stability, and scalability of blockchain systems.

– Setting up a mathematical theoretical framework for security and privacy protection of blockchain systems.

– Providing effective methods to optimize and dynamically control performance, security and privacy protection of large-scale blockchain systems.

– Developing machine learning for performance optimization and dynamic decision of blockchain systems.

–Developing a healthy ecological environment and reasonable operations management in the blockchain community by means of research on performance evaluation, performance optimization, and dynamic decision of blockchain systems.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under grant No. 71932002.

References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008, pp. 1-9. Available: http://bitcoin.org/bitcoin.pdf (accessed on 17 January 2023).

[2] Kim S, Kwon Y, Cho S. A survey of scalability solutions on blockchain. *2018 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, Korea (South), 2018, pp. 1204-1207.

[3] Rouhani S, Deters R. Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access* 2019, (7):50759-50779.

[4] Wang R, Ye K, Xu CZ. Performance benchmarking and optimization for blockchain systems: A survey. *International Conference on Blockchain*, Cham: Springer, 2019, pp. 171-185.

[5] Zheng X, Zhu Y, Si X. A survey on challenges and progresses in blockchain technologies: A performance and security perspective. *Appl Sci* 2019, 9(22):4731.

[6] Smetanin S, Ometov A, Komarov M, Masek P, Koucheryavy Y. Blockchain evaluation approaches: State-of-the-art and future perspective. *Sensors* 2020, 20(12):3358.

[7] Singh A, Click K, Parizi RM, Zhang Q, Dehghantanha A, *et al.* Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *J Netw Comput* 2020, 149:102471.
[8] Zhou Q, Huang H, Zheng Z, Bian J. Solutions to scalability of blockchain: A survey. *IEEE Access* 2020, 8:16440-16455.
[9] Yu G, Wang X, Yu K, Ni W, Zhang J, *et al.* Survey: sharding in blockchains. *IEEE Access* 2020, 8:14155-14181.
[10] Fan C, Ghaemi S, Khazaei H, Musilek P. Performance evaluation of blockchain systems: A systematic survey. *IEEE Access* 2020, 8:126927-126950.
[11] Cao B, Wang Z, Zhang L, Feng D, Peng M, *et al.* Blockchain systems, technologies and applications: A methodology perspective. *arXiv* 2021, arXiv:2105.03572.
[12] Huang H, Kong W, Zhou S, Zheng Z, Guo S. A survey of state-of-the-art on blockchains: Theories, modelings, and tools. *ACM Comput Surv* 2021, 54(2):1-42.
[13] Wang X, Wu LY. Operations research in the Blockchain technology. *Journal of the Operations Research Society of China* 2022, 10:401-422.
[14] Li QL, Ma JY, Chang YX. Blockchain queue theory. *International Conference on Computational Social Networks*, Cham: Springer, 2018, pp. 25-40.
[15] Chang YX, Li QL, Wang Q, Song XS. Dynamic practical byzantine fault tolerance and its blockchain system: A large-Scale markov modeling. *arXiv* 2022, arXiv:2210.14003.
[16] Kawase Y, Kasahara S. Transaction-confirmation time for bitcoin: A queueing analytical approach to blockchain mechanism. *International Conference on Queueing Theory and Network Applications*, Cham: Springer, 2017, pp. 75-88.
[17] Kasahara S, Kawahara J. Effect of Bitcoin fee on transaction-confirmation process. *J Ind Manag Optim* 2019, 15(1):365.
[18] Li QL, Ma JY, Chang YX, Ma FQ, Yu H. Markov processes in blockchain systems. *Comput* 2019, 6(1):1-28.
[19] Geissler S, Prantl T, Lange S, Wamser F, Hossfeld T. Discrete-time analysis of the blockchain distributed ledger technology. *2019 31st International Teletraffic Congress (ITC 31)*, Budapest, Hungary, 2019, pp. 130-137.
[20] Zhao W, Jin S, Yue W. Analysis of the average confirmation time of transactions in a blockchain system. *International Conference on Queueing Theory and Network Applications*, Cham: Springer, 2019, pp. 379-388.
[21] Krieger UR, Ziegler MH, Cech HL. Performance modeling of the consensus mechanism in a permissioned blockchain. *International Conference on Computer Networks*, Cham: Springer, 2019, pp. 3-17.
[22] Ahmad A, Saad M, Njilla L, Kamhoua C, Bassiouni M, *et al.* Blocktrail: A scalable multichain solution for blockchain-based audit trails. *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019, pp. 1-6.
[23] Mišić J, Mišić VB, Chang X, Motlagh SG, Ali MZ. Modeling of bitcoin's blockchain delivery network. *IEEE Trans Netw Sci Eng* 2019, 7(3):1368-1381.
[24] He J, Zhang G, Zhang J, Zhang R. An economic model of blockchain: The interplay between transaction fees and security. *Available at SSRN 3616869*, 2020, pp. 1-41.
[25] Fang M, Liu J. Toward low-cost and stable blockchain networks. *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland, 2020, pp. 1-6.
[26] Frolkova M, Mandjes M. A Bitcoin-inspired infinite-server model with a random fluid limit. *Stoch* 2019, 35(1):1-32.
[27] Fralix B. On classes of Bitcoin-inspired infinite-server queueing systems. *Queueing Syst* 2020, 95(1):29-52.
[28] Seol J, Kancharla A, Ke Z, Kim H, Park N. A variable bulk arrival and static bulk service queueing model for blockchain. In *Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, Taipei,

Taiwan, October 6, 2020, pp. 63-72.
[29] Gopalan A, Sankararaman A, Walid A, Vishwanath S. Stability and scalability of blockchain systems. In *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, online, June 2020, 4(2), pp. 1-35.
[30] Meng T, Zhao Y, Wolter K, Xu CZ. On consortium blockchain consistency: A queueing network model approach. *IEEE Trans Parallel Distrib Syst* 2021, 32(6): 1369-1382.
[31] Sun L, Yang Q, Chen X, Chen Z. RC-chain: Reputation-based crowdsourcing blockchain for vehicular networks. *J Netw Comput* 2021, 176:102956.
[32] Altarawneh A, Sun F, Brooks RR, Hambolu O, Yu L, *et al.* Availability analysis of a permissioned blockchain with a lightweight consensus protocol. *Comput Secur* 2021, 102:102098.
[33] Ricci S, Ferreira E, Menasche DS, Ziviani A, Souza JE, *et al.* Learning blockchain delays: A queueing theory approach. *ACM SIGMETRICS Performance Evaluation Review* 2019, 46(3):122-125.
[34] Sukhwani H, Wang N, Trivedi KS, Rindos A. Performance modeling of hyperledger fabric (permissioned blockchain network). *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, Cambridge MA, USA, 2018, pp. 1-8.
[35] Li J, Yuan Y, Wang S, Wang F. Transaction queuing game in bitcoin blockchain. *2018 IEEE Intelligent Vehicles Symposium*, Changshu, China, 2018, pp. 114-119.
[36] Memon RA, Li JP, Ahmed J. Simulation model for blockchain systems using queuing theory. *Electronics* 2019, 8(2):234.
[37] Spirkina AV, Aptrieva EA, Elagin VS, Shvidkiy AA, Savelieva AA. Approaches to modeling blockchain systems. *2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Brno, Czech Republic, 2020, pp. 242-247.
[38] Wilhelmi F, Giupponi L, Dini P. Blockchain-enabled server-less federated learning. *arXiv* 2021, arXiv:2112.07938.
[39] Bowden R, Keeler HP, Krzesinski AE, Taylor PG. Modeling and analysis of block arrival times in the Bitcoin blockchain. *Stoch* 2020, 36(4):602-637.
[40] Li QL. Constructive Computation in Stochastic Models with Applications: The RG-factorizations. Springer, 2010.
[41] Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. *Commun* 2018, 61(7):95-102.
[42] Li QL, Chang YX, Wu X, Zhang G. A new theoretical framework of pyramid markov processes for blockchain selfish mining. *J Syst Sci Syst Eng* 2021, 30(6):667-711.
[43] Gőbel J, Keeler HP, Krzesinski AE, Taylor PG. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Perform Evaluation* 2016, 104:23-41.
[44] Javier K, Fralix B. A further study of some Markovian Bitcoin models from Gőbel *et al. Stoch* 2020, 36(2):223-250.
[45] Nayak K, Kumar S, Miller A, Shi E. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. *2016 IEEE European Symposium on Security and Privacy*, Saarbruecken, Germany, 2016, pp. 305-320.
[46] Wang Z, Liu J, Wu Q, Zhang Y, Zhou Z. An analytic evaluation for the impact of uncle blocks by selfish and stubborn mining in an imperfect ethereum network. *Comput Secur* 2019, 87(101581): 1-10.
[47] Liu Y, Hei Y, Xu T, Liu J. An evaluation of uncle block mechanism effect on ethereum selfish and stubborn mining combined with an eclipse attack. *IEEE Access* 2020, 8:17489-17499.
[48] Grunspan C, Pérez-Marco R. Selfish mining in ethereum. *Mathematical Research for Blockchain Economy*, Cham: Springer, 2020, pp. 65-90.

[49] Niu J, Feng C. Selfish mining in ethereum. *2019 IEEE 39th International Conference on Distributed Computing Systems*, Dallas TX, USA, 2019, pp. 1306-1316.
[50] Bai Q, Zhou X, Wang X, Xu Y, Wang X, *et al.* A deep dive into blockchain selfish mining. *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019, pp. 1-6.
[51] Bai Q, Xu Y, Liu N, Wang X. Blockchain Mining with Multiple Selfish Miners. *arXiv* 2021, arXiv:2112.10454.
[52] Chang D. Revenue generation strategy through selfish mining focusing multiple pools of honest miners. Bachelor of Technology, Computer Science and Applied Mathematics, Indraprastha Institute of Information Technology, New Delhi, India, 2019.
[53] Liu H, Ruan N, Du R, Jia W. On the strategy and behavior of Bitcoin mining with N-attackers. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, Incheon, Republic of Korea, 4 June, 2018, pp. 357-368.
[54] Marmolejo-Cossío FJ, Brigham E, Sela B, Katz J. Competing (semi-) selfish miners in Bitcoin. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, Zurich Switzerland, October 21-23, 2019, pp. 89-109.
[55] Xia Q, Dou W, Xi T, Zeng J, Zhang F, *et al.* The impact analysis of multiple miners and propagation delay on selfish mining. *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, Madrid, Spain, 2021, pp. 694-703.
[56] Song XS, Li QL, Chang YX, Zhang C. A markov process theory for network growth processes of DAG-based blockchain systems. *arXiv* 2022, arXiv:2209.01458.
[57] Li Y, Cao B, Peng M, Zhang L, Zhang L, *et al.* Direct acyclic graph-based ledger for Internet of Things: Performance and security analysis. *IEEE ACM T Netw* 2020, 28(4):1643-1656.
[58] Ma FQ, Li QL, Liu YH, Chang YX. Stochastic performance modeling for practical Byzantine fault tolerance consensus in blockchain. *Peer Peer Netw Appl* 2021, 15(6):2516-2528.
[59] Carlsten M. The impact of transaction fees on bitcoin mining strategies. Master's Thesis, Department of Computer Science, Princeton University, 2016.
[60] Shi L, Wang T, Li J, Zhang S. Pooling is not favorable: Decentralize mining power of PoW blockchain using age-of-work. *arXiv* 2021, arXiv:2104.01918.
[61] Kiffer L, Rajaraman R, Shelat A. A better method to analyze blockchain consistency. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Toronto Canada, October 15-19, 2018, pp. 729-744.
[62] Huang D, Ma X, Zhang S. Performance analysis of the raft consensus algorithm for private blockchains. *IEEE Trans Syst Man Cybern Syst* 2019, 50(1):172-181.
[63] Srivastava R. Mathematical assessment of blocks acceptance in blockchain using Markov model. *Int J Blockchains Cryptocurrencies* 2019, 1(1): 42-53.
[64] Li Y, Cao B, Liang L, Mao D, Zhang L. Block access control in wireless blockchain network: Design, modeling and analysis. *IEEE Trans Veh Technol* 2021, 70(9):9258-9272.
[65] Piriou PY, Dumas JF. Simulation of stochastic blockchain models. *2018 14th European Dependable Computing Conference*, Iasi, Romania, 2018, pp. 150-157.
[66] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning. *IEEE Trans Netw Service Manag* 2020, 17(4):2536-2549.
[67] Jofré A, Pardo A, Salas D, Verdugo V, Verschae J. The convergence rates of blockchain mining games: A Markovian approach. *arXiv* 2021, arXiv:2107.08077.
[68] Spitzer F. Principles of Random Walk. Springer, 2001.
[69] Prabhu NU. Stochastic Storage Processes: Queues, Insurance Risk, and Dams, and Data Communication. Springer, 1998.
[70] Xia F, Liu J, Nie H, Fu Y, Wan L, *et al.* Random walks: A review of algorithms and

applications. *IEEE Transactions on Emerging Topics in Computational Intelligence* 2020, 4(2):95-107.
[71] Goffard PO. Fraud risk assessment within blockchain transactions. *Adv Appl Probab* 2019, 51(2):443-467.
[72] Jang J, Lee HN. Profitable double-spending attacks. *Appl Sci* 2020, 10(23):8477.
[73] Brown M, Peköz E, Ross S. Blockchain double-spend attack duration. *Probab Eng Inf Sci* 2021, 35(4):858-866.
[74] Grunspan C, Pérez-Marco R. On profitability of nakamoto double spend. *Probab Eng Inf Sci* 2021, 36(3):732-746.
[75] Chen H, Yao DD. Fundamentals of Queueing Networks: Performance, Asymptotics, and Optimization. Springer, 2001.
[76] Whitt W. Stochastic-process Limits: An Introduction to Stochastic-process Limits and Their Application to Queues. Springer, 2002.
[77] Dai JG, He S. Many-server queues with customer abandonment: A survey of diffusion and fluid approximations. *J Syst Sci Syst Eng* 2012, 21(1):1-36.
[78] Büke B, Chen H. Fluid and diffusion approximations of probabilistic matching systems. *Queueing Syst* 2017, 86(1):1-33.
[79] Chen H, Shanthikumar JG. Fluid limits and diffusion approximations for networks of multi-server queues in heavy traffic. *Discrete Event Dyn S* 1994, 4(3):269-291.
[80] King C. The fluid limit of a random graph model for a shared ledger. *Adv Appl Probab* 2021, 53(1):81-106.
[81] Ferraro P, King C, Shorten R. On the stability of unverified transactions in a DAG-based distributed ledger. *IEEE Trans Automat Contr* 2019, 65(9):3772-3783.
[82] Koops D. Predicting the confirmation time of bitcoin transactions. *arXiv* 2018, arXiv:1809.10596.
[83] Corcino R, Casas KP, Elnar AR. Bitcoin: A Non-markovian stochastic process. *J Eng Sci Technol* 2018, 6:287-298.
[84] Chevallier J, Goutte S, Guesmi K, Saadi S. On the Bitcoin price dynamics: An augmented Markov-switching model with Lévy jumps. *HAL Id: halshs-02120636* 2019, 1-17.
[85] Li QL, Chang YX, Zhang C. Tree representation, growth rate of Blockchain and reward allocation in Ethereum with multiple mining pools. *IEEE Trans Netw Service Manag*, online publication, 2022, pp. 1-19.
[86] Grunspan C, Pérez-Marco R. On profitability of selfish mining. *arXiv* 2018, arXiv:1805.08281.
[87] Grunspan C, Pérez-Marco R. On profitability of stubborn mining. *arXiv* 2018, arXiv:1808.01041.
[88] Grunspan C, Pérez-Marco R. On profitability of trailing mining. *arXiv* 2018, arXiv:1811.09322.
[89] Grunspan C, Pérez-Marco R. The mathematics of Bitcoin. *J Eur Math Soc* 2020, 115:31-37.
[90] Grunspan C, Pérez-Marco R. Profit lag and alternate network mining. *arXiv* 2020, arXiv:2010.02671.
[91] Lundbaek LN, D'Iddio AC, Huth M. Optimizing governed blockchains for financial process authentications. *arXiv* 2016, arXiv:1612.00407.
[92] Liang K. Fission: A provably fast, scalable, and secure permissionless blockchain. *arXiv* 2018, arXiv:1812.05032.
[93] Nguyen LN, Nguyen TD, Dinh TN, Thai MT. Optchain: optimal transactions placement for scalable blockchain sharding. *2019 IEEE 39th International Conference on Distributed Computing Systems*, Dallas TX, USA, 2019, pp. 525-535.
[94] Wang P, Xu H, Jin X, Wang T. Flash: efficient dynamic routing for offchain networks. In *Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies*, Orlando FL, USA, December 9-12, 2019, pp. 370-381.
[95] Saad M, Njilla L, Kamhoua C, Kim J, Nyang D, *et al.* Mempool optimization for

defending against DDoS attacks in PoW-based blockchain systems. *2019 IEEE international conference on blockchain and cryptocurrency*, Seoul, Korea (South), 2019, pp. 285-292.
[96] Reddy BS, Sharma GVV. Scalable consensus protocols for poW based blockchain and blockDAG. *arXiv* 2020, arXiv:2010.05447.
[97] Leonardos S, Reijsbergen D, Piliouras G. Weighted voting on the blockchain: Improving consensus in proof of stake protocols. *Int J Netw Manag* 2020, 30(5):e2093.
[98] Liu Y, Fang Z, Cheung MH, Cai W, Huang J. An incentive mechanism for sustainable blockchain storage. *arXiv* 2021, arXiv:2103.05866.
[99] Varma SM, Maguluri ST. Throughput optimal routing in blockchain-based payment systems. *IEEE Trans Control Netw Syst* 2021, 8(4):1859-1868.
[100] Li C, Zhang L, Fang S. EntrapNet: A blockchain-based verification protocol for trustless computing. *IEEE Internet Things J* 2021, 9(11):8024-8035.
[101] Kang J, Xiong Z, Niyato D, Wang P, Ye D, *et al.* Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks. *IEEE Wireless Commun Lett* 2018, 8(1):157-160.
[102] Aggarwal V, Tan Y. A structural analysis of bitcoin cash's emergency difficulty adjustment algorithm. *Available at SSRN 3383739*, 2019, pp. 1-36.
[103] Ramezan G, Leung C, Miao C. Optimal transaction queue waiting in blockchain mining. *arXiv* 2020, arXiv:2011.10886.
[104] Riehl JR, Ward J. Transaction pricing for maximizing throughput in a sharded blockchain ledger. *2020 Crypto Valley Conference on Blockchain Technology*, Rotkreuz, Switzerland, 2020, pp. 36-42.
[105] Zhou Z, Li R, Cao Y, Zheng L, Xiao H. Dynamic performance evaluation of blockchain technologies. *IEEE Access* 2020, 8:217762-217772.
[106] Puterman ML. Markov Decision Processes: Discrete Stochastic Dynamic Programming. John Wiley & Sons, 2014.
[107] Li QL, Ma JY, Fan RN, Xia L. An overview for Markov decision processes in queues and networks. *International Conference of Celebrating Professor Jinhua Cao's 80th Birthday*, Springer, Singapore, 2019, pp. 44-71.
[108] Sapirshtein A, Sompolinsky Y, Zohar A. Optimal selfish mining strategies in bitcoin. *International Conference on Financial Cryptography and Data Security*, Cham: Springer, 2016, pp. 515-532.
[109] Sompolinsky Y, Zohar A. Bitcoin's security model revisited. *arXiv* 2016, arXiv:1605.09193.
[110] Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, *et al.* On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, Vienna Austria, October 24-28, 2016, pp. 3-16.
[111] Zur RB, Eyal I, Tamar A. Efficient MDP analysis for selfish-mining in blockchains. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, New York NY, USA, October 21-23, 2020, pp. 113-131.
[112] Li T, Wang Z, Yang G, Cui Y, Chen Y, *et al.* Semi-selfish mining based on hidden Markov decision process. *Int J Intell* 2021, 36(7):3596-3612.
[113] Ma JY, Li QL. Sensitivity-based optimization for blockchain selfish mining. *J Comb Optim*, online publication, 2021, pp. 1-38.
[114] Niu J, Wang Z, Gai F, Feng C. Incentive analysis of Bitcoin-NG, revisited. *ACM SIGMETRICS Performance Evaluation Review* 2021, 48(3):59-60.
[115] Wüst K. Security of blockchain technologies. Master's Thesis, ETH Zürich, 2016.
[116] Chicarino V, Albuquerque C, Jesus E, Rocha A. On the detection of selfish mining and stalker attacks in blockchain networks. *Ann Telecommun* 2020, 75(3):143-152.
[117] Liu Y, Yu FR, Li X, Ji H, Leung VC. Blockchain and machine learning for communications and networking systems. *IEEE Commun Surv Tutor* 2020, 22(2):1392-1431.
[118] Ekramifard A, Amintoosi H, Seno AH, Dehghantanha A, Parizi RM. A systematic

literature review of integration of blockchain and artificial intelligence. *Blockchain Cybersecurity, Trust and Privacy* 2020, 147-160.
[119] Chen F, Wan H, Cai H, Cheng G. Machine learning in/for blockchain: Future and challenges. *Can J Stat* 2021, 49(4):1364-1382.
[120] Shafay M, Ahmad RW, Salah K, Yaqoob I, Jayaraman R, *et al.* Blockchain for deep learning: review and open challenges. *Cluster Comput*, 2022, pp. 1-25. Available: https://doi.org/10.1007/s10586-022-03582-7 (accessed on 17 January 2023).
[121] Hou C, Zhou M, Ji Y, Daian P, Tramer F, *et al.* SquirRL: Automating attack analysis on blockchain incentive mechanisms with deep reinforcement learning. *arXiv* 2019, arXiv:1912.01798.
[122] Bar-Zur R. Finding Optimal Strategies in Blockchain Protocols with Reinforcement Learning. Master's Thesis, Israel Institute of Technology, Haifa, 2020.
[123] Wang T, Liew SC, Zhang S. When blockchain meets AI: Optimal mining strategy achieved by machine learning. *Int J Intell* 2021, 36(5):2183-2207.
[124] You J. Blockchain framework for artificial intelligence computation. *arXiv* 2022, arXiv:2202.11264.
[125] Qiu X, Liu L, Chen W, Hong Z, Zheng Z. Online deep reinforcement learning for computation offloading in blockchain-empowered mobile edge computing. *IEEE Trans Veh Technol* 2019, 68(8):8050-8062.
[126] Feng J, Yu FR, Pei Q, Chu X, Du J, *et al.* Cooperative computation offloading and resource allocation for blockchain-enabled mobile-edge computing: A deep reinforcement learning approach. *IEEE Internet Things J* 2019, 7(7):6214-6228.
[127] Asheralieva A, Niyato D. Learning-based mobile edge computing resource management to support public blockchain networks. *IEEE Trans Mob Comput* 2019, 20(3):1092-1109.
[128] Asheralieva A, Niyato D. Bayesian reinforcement learning and bayesian deep learning for blockchains with mobile edge computing. *IEEE Trans Cogn* 2020, 7(1):319-335.
[129] Yuan S, Li J, Liang J, Zhu Y, Yu X, *et al.* Sharding for blockchain based mobile edge computing system: A deep reinforcement learning approach. *2021 IEEE Global Communications Conference (GLOBECOM)*, Madrid, Spain, 2021, pp. 1-6.
[130] Waheed N, He X, Ikram M, Usman M, Hashmi SS, *et al.* Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. *ACM Comput Surv* 2020, 53(6):1-37.
[131] Gao Y, Wu W, Nan H, Sun Y, Si P. Deep reinforcement learning based task scheduling in mobile blockchain for iot applications. *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland, 2020, pp. 1-7.
[132] Qiu C, Yu FR, Yao H, Jiang C, Xu F, *et al.* Blockchain-based software-defined industrial Internet of Things: A dueling deep Q-learning approach. *IEEE Internet Things J* 2018, 6(3):4627-4639.
[133] Luo J, Chen Q, Yu FR, Tang L. Blockchain-enabled software-defined industrial internet of things with deep reinforcement learning. *IEEE Internet Things J* 2020, 7(6):5466-5480.
[134] Yang L, Li M, Si P, Yang R, Sun E, *et al.* Energy-efficient resource allocation for blockchain-enabled industrial Internet of Things with deep reinforcement learning. *IEEE Internet Things J* 2020, 8(4):2318-2329.
[135] Wu Y, Wang Z, Ma Y, Leung VC. Deep reinforcement learning for blockchain in industrial IoT: A survey. *Comput Netw* 2021, 191:108004.
[136] Ma C, Li J, Shi L, Ding M, Wang T, *et al.* When federated learning meets blockchain: A new distributed learning paradigm. *IEEE Comput Intell Mag* 2022, 17(3):26-33.
[137] Qu Y, Uddin MP, Gan C, Xiang Y, Gao L, *et al.* Blockchain-enabled federated learning: A survey. *ACM Comput Surv* 2022, 55(4):1-35.
[138] Wang Z, Hu Q. Blockchain-based federated learning: A comprehensive survey.

arXiv 2021, arXiv:2110.02182.
[139] Awan S, Li F, Luo B, Liu M. Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, London United Kingdom, November 11-15, 2019, pp. 2561-2563.
[140] Javed AR, Hassan MA, Shahzad F, Ahmed W, Singh S, *et al*. Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey. *Sensors* 2022, 22(12):4394.
[141] Ali M, Karimipour H, Tariq M. Integration of blockchain and federated learning for Internet of Things: Recent advances and future challenges. *Comput Secur* 2021, 108:102355.
[142] Martinez I, Francis S, Hafid AS. Record and reward federated learning contributions with blockchain. *2019 International conference on cyber-enabled distributed computing and knowledge discovery (CyberC)*, Guilin, China, 2019, pp. 50-57.
[143] Nguyen DC, Ding M, Pham QV, Pathirana PN, Le LB, *et al*. Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet Things J* 2021, 8(16):12806-12825.
[144] Qu Y, Gao L, Luan TH, Xiang Y, Yu S, *et al*. Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet Things J* 2020, 7(6):5171-5183.
[145] Pokhrel SR, Choi J. Federated learning with blockchain for autonomous vehicles: Analysis and design challenges. *IEEE Trans Commun* 2020, 68(8):4734-4746.
[146] Lu Y, Huang X, Dai Y, Maharjan S, Zhang Y. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Trans Industr Inform* 2019, 16(6):4177-4186.
[147] Lu Y, Huang X, Zhang K, Maharjan S, Zhang Y. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. *IEEE Trans Veh Technol* 2020, 69(4):4298-4311.
[148] Lu Y, Huang X, Zhang K, Maharjan S, Zhang Y. Blockchain and federated learning for 5G beyond. *IEEE Netw* 2020, 35(1):219-225.
[149] Zhao Y, Zhao J, Jiang L, Tan R, Niyato D, *et al*. Privacy-preserving blockchain-based federated learning for IoT devices. *IEEE Internet Things J* 2020, 8(3): 1817-1829.
[150] ur Rehman MH, Salah K, Damiani E, Svetinovic D. Towards blockchain-based reputation-aware federated learning. *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops*, Toronto ON, Canada, 2020, pp. 183-188.
[151] Catalini C. How blockchain technology will impact the digital economy. *Blockchains Smart Contracts Internet Things* 2017, 4:2292-2303.
[152] Mori T. Financial technology: Blockchain and securities settlement. *Journal of Securities Operations & Custody* 2016, 8(3):208-227.
[153] Gupta A, Siddiqui ST, Alam S, Shuaib M. Cloud computing security using blockchain. *J Emerg Technol Innov Res* 2019, 6(6):791-794.
[154] Dennis R, Owen G. Rep on the block: A next generation reputation system based on the blockchain. *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, UK, 2015, pp. 131-138.
[155] Tang S, Wang Z, Dong J, Ma Y. Blockchain-enabled social security services using smart contracts. *IEEE Access* 2022, 10:73857-73870.
[156] Liu Z, Li Z. A blockchain-based framework of cross-border e-commerce supply chain. *Int J Inf Manag* 2020, 52:102059.
[157] Hussain AA, Al-Turjman F. Artificial intelligence and blockchain: A review. *Trans Emerg Telecommun* 2021, 32(9):e4268.
[158] 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.

[159] Saberi S, Kouhizadeh M, Sarkis J, Shen L. Blockchain technology and its relationships to sustainable supply chain management. *Int J Prod Res* 2019, 57(7):2117-2135.
[160] Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments. 2016, pp. 1-59. Available: https://www.bitcoinlightning.com/wp-content/uploads/2018/03/lightning-network-paper.pdf (accessed on 17 January 2023).
[161] Back A, Corallo M, Dashjr L, Friedenbach M, Maxwell G, *et al.* Enabling blockchain innovations with pegged sidechains. 2014, 72:201-224. Available: http://www. opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains (accessed on 14 January 2023).
[162] Luu L, Narayanan V, Zheng C, Baweja K, Gilbert S, *et al.* A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, Vienna Austria, October 24-28, 2016, pp. 17-30.
[163] Popov S. The Tangle. *IOTA Foundation Technical Report*. 2016, pp. 131-156.