Blockchain Systems, Technologies and Applications: A Methodology Perspective

Bin Cao, *Senior Member, IEEE*, Zixin Wang, Long Zhang, Daquan Feng, Mugen Peng, *Fellow, IEEE*, Lei Zhang, *Senior Member, IEEE*, and Zhu Han, *Fellow, IEEE*

***Abstract*—In the past decade, blockchain has shown a promising vision to build trust without any powerful third party in a secure, decentralized and scalable manner. However, due to the wide application and future development from cryptocurrency to the Internet of things, blockchain is an extremely complex system enabling integration with mathematics, computer science, communication and network engineering, etc. By revealing the intrinsic relationship between blockchain and communication, networking and computing from a methodological perspective, it provided a view to the challenge that engineers, experts and researchers hardly fully understand the blockchain process in a systematic view from top to bottom. In this article we first introduce how blockchain works, the research activities and challenges, and illustrate the roadmap involving the classic methodologies with typical blockchain use cases and topics. Second, in blockchain systems, how to adopt stochastic process, game theory, optimization theory, and machine learning to study the blockchain running processes and design the blockchain protocols/algorithms are discussed in details. Moreover, the advantages and limitations using these methods are also summarized as the guide of future work to be further considered. Finally, some remaining problems from technical, commercial and political views are discussed as the open issues. The main findings of this article will provide a survey from a methodological perspective to study theoretical model for blockchain fundamentals understanding, design network service for blockchain-based mechanisms and algorithms, as well as apply blockchain for the Internet of things, etc.**

***Index Terms*—Blockchain, stochastic process, game theory, optimization theory, machine learning, network**

This work was partially supported by National Key R&D Program of China under No. 2021YFB1714100 and No. 2020YFB1806700, Zhejiang Lab under No. 2021KF0AB03, National Natural Science Foundation of China under No. 61925101 and 61831002, and NSF CNS-2107216 and CNS-2128368. (*Corresponding author: Daquan Feng.*)

Bin Cao, Zixin Wang, and Mugen Peng are with State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China. Bin Cao is also with Zhejiang Lab, Hangzhou 311121, China. E-mail: caobin@bupt.edu.cn, wangzx@bupt.edu.cn, pmg@bupt.edu.cn.

Long Zhang is with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China. E-mail: zhanglong3211@yeah.net.

Daquan Feng is with the Shenzhen Key Laboratory of Digital Creative Technology, the Guangdong Province Engineering Laboratory for Digital Creative Technology, Guangdong Key Laboratory of Intelligent Information Processing, College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518060, China.

Lei Zhang is with the James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, U.K. E-mail: lei.zhang@glasgow.ac.uk.

Z. Han is with the Department of Electrical and Computer Engineering at the University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul, South Korea, 446-701. E-mail: hanzhu22@gmail.com.

I. Introduction

ORIGINALLY proposed as the backbone technology of Bitcoin [1], Ethereum [2], and many other digital currencies [3], blockchain has become a revolutionary decentralized data management framework that establishes consensuses and agreements in a trust-less and distributed environment [4]. In addition to the soaring in the finance sector, blockchain has been attracted much attention from many other major industrial sectors ranging from supply chain [5], transportation [6], entertainment [7], retail [8], healthcare [9], information management [10], financial services [11], etc. As such, Gartner forecasts that by 2030, blockchain will generate an annual business value of more than US $3 trillion, and envisions that 10% to 20% of global economic infrastructure will be running on blockchain-based systems [12].

Fundamentally, blockchain is a decentralized ledger management system for recording and validating transactions. It allows two parties to complete a transaction in a peer-to-peer (P2P) network [13]. Without involvement of an authority or the third party, all peer nodes work together to maintain public ledger with the aim of realizing trust, security, transparency and immutability. The recorded transaction in blockcahin can be any form of data that involves the ownership transfer or sharing of resource, where it can be tangible such as money, houses, land, or copyright, and digital documents.

Essentially, blockchain is built on a physical network that relies on the communication, computing and caching, which serves the basis of blockchain functions such as incentive mechanism or consensus. As such, blockchain systems can be depicted as a two-tier architecture: an infrastructure layer and a blockchain layer. The infrastructure layer is the underlying entity and responsible for maintaining P2P network, building connection through wired/wireless communication, computing and storing data. The top is the blockchain layer that can realize trust and security functions based on underlying information exchanging. More specifically, blockchain features several key components which are summarized as: transaction, block and chain of blocks. *Transaction* contains the information requested by the client and need to be recorded by public ledger; *block* securely records an amount of transactions or other useful information; using consensus mechanism, blocks are linked orderly to constitute a *chain of blocks*, which indicates logical relation among the blocks to construct blockchain. As a core function of the blockchain, the consensus mechanism works in the blockchain layer ensures a clear sequence of transactions and ensures the integrity and

consistency of the blockchain across geographically distributed nodes [14]. The state of a blockchain is updated when a valid transaction is recorded on chain, and smart contract can be used to automatically trigger transactions under certain conditions [15]. Therefore, due to its autonomy and efficiency, smart contract is being used for a wide range of purposes, from self-managed identities on public blockchains to allowing automated business collaboration on blockchains.

Driven by the continuous development of 5G technology, more and more services have been launched to improve network performance and user experience. Importantly, features such as data immutability and transparency are the key factors to ensure the successful launch of new services such as IoT data collection, driverless cars, and drones. Blockchain is regarded as a very promising technology to meet these new requirements with its decentralization, openness, tamper resistance, anonymity and traceability. Therefore, in order to thoroughly explore the potential of blockchain and make it better serve the requirements of modern networks, it is necessary to comprehensively and systematically understand blockchain from top to bottom. Methodology advocates going to the bottom of the problem, digging into the essence behind the phenomenon, and forming a theoretical system with a certain depth. It is possible to reveal the internal contradiction of a problem and determine its fundamental solution from a methodological perspective. In light of this, the methodology can be well used to reveal the principles of blockchain operation process and blockchain protocol/algorithm design in blockchain systems, providing theoretical support for solving specific problems. Therefore, this paper aims to provide a comprehensive survey to introduce how to exploit the mathematical methods, such as, stochastic process, game theory, optimization theory, and machine learning, to analyze and solve the specific problems in blockchain system.

A. Existing Surveys and Tutorials

Recognising the wide applications of blockchain technology, a novel survey or tutorial paper can help researchers in various fields build good foundations on the subject to guide actual developments. Recently, several works have reviewed the advanced development of blockchain from various views, which are summarized in I.

For security and privacy, Salman *et al.* in [13] present blockchain-based security services in authentication, confidentiality, privacy and access control, etc. Waheed *et al*. in [16] summarize the research efforts of using machine learning algorithms and blockchain technology to address security and privacy issues for the Internet of things (IoT). Conti *et al.* in [17] focus on the security and privacy threats of Bitcoin, and discusses the feasibility and limitations of potential solutions. Saad *et al*. in [18] focus on how attacks affect public blockchain and discuss the relationships between a sequence of possible attacks.

Besides, as the core of blockchain, consensus determines the performance and security of the blockchain in many ways, Ferdous *et al*. in [19] utilize comprehensive taxonomy of properties to analyze a wide range of consensus algorithms, and examines in detail the meaning of the different problems that are still prevalent in the consensus algorithm. Wang *et al*. in [20] review the state of the art consensus protocols and game theory in mining strategy management. Xiao *et al*. in [21] introduce the classic theory of fault tolerance and analyze blockchain consensus protocols using a five-component framework.

For the scalability of the blockchain, Xie *et al*. in [22] study the scalability of the blockchain system, analyze the scalability from the perspective of throughput, storage and network, and introduces the existing enabling technology of the scalable blockchain system. Yu *et al*. in [23] study the sharding problem in the blockchain includes providing a detailed comparison and a quantitative evaluation of the main sharding mechanisms, as well as an analysis of the characteristics and limitations of existing solutions. Gamage *et al*. in [24] discuss issues of the existing blockchains such as 51% attack, nothing-at-stake problem together with improvements for the scalability issues in current blockchains.

The integration of blockchain and 5G has become a mainstream trend, Nguyen *et al*. in [25] provide the latest survey on the integration of blockchain with 5G networks and other networks. It gives an extensive discussion about the potential of blockchain for enabling key technologies of 5G, and further explores and analyzes the opportunities that blockchain may give important 5G services. Yue *et al*. in [26] provide a concise review of the recent efforts on blockchain decentralization application in 5G and beyond. Moreover, by enabling the integration of blockchain and other advanced technologies, various works have explored potential applications and research challenges in IoT [27] [28], smart city [29], cloud computing [30], edge computing [31], and fog computing [32].

From the perspective of mathematical tools, Liu *et al*. in [33] provide overviews and discussions using game theory in detail to address a variety of problems on the subject of security, mining management and blockchain applications. In the context of artificial intelligence, Liu *et al*. in [34] discuss feasible solutions integrating blockchain and machine learning for communications and networking system.

B. Motivation

Existing surveys and tutorials mainly focus on blockchain architectures, protocols, the integration of blockchain and other network technologies, etc. However, the intrinsic relationship between blockchain and communication, networking and computing from the methodological perspective has not been well studied. As a frontier research of multi-technology integration, blockchain requires researchers with multidisciplinary knowledge backgrounds in communication, networking, and computing to understand the operating environment, basic principles, and the emerging applications in B5G/6G, IoT, and other fields.

Therefore, this motivates us to review the state of the art of blockchain to reveal the relations of blockchain system with communication, networking, and computing and how they interact with each other. Furthermore, to facilitate the deployment of blockchain-based applications, many researchers

pay attention to how to carry out mathematical methods to solve a specific blockchain problem. Still, very few surveys or tutorials explicitly discuss the use of blockchain from the perspective of methodologies.

We aim to reveal the intrinsic relationship between blockchain and communication, networking and computing through classical methodological approaches, including stochastic process, game theory, optimization theory, and machine learning. Stochastic process can help us model blockchain running processes to reveal the intrinsic nature of blockchain networks and inter-node communication since it can establish a system model in complex and uncertain environments. Besides, game theory describes the conflict and cooperation between resource competitors, and optimization theory seeks the optimal solution with constraints. As such, they are helpful in exploring the impact of blockchain node behavior on blockchain system performance and resource allocation. Additionally, machine learning is also a valuable tool for improving blockchain system performance, such as malicious node detection and attack identification. Meanwhile, blockchain enables machine learning models to protect against single point of failure. Therefore, the analysis and research on the fusion of blockchain and machine learning can support the design of blockchain-based network services.

Specifically, the main contributions of this survey can be summarized as follows:

- We provided a background of blockchain research and discussed the applications and limitations of blockchain in practical networks, including scalability, overhead and interoperability;
- We outlined the research activities of blockchain in terms of theoretical models, network service mechanisms and vertical applications, as well as discussed the remaining challenge of blockchain system;
- We analyzed the fundamental theory of blockchain and the design of blockchain-based network services, and the applications of blockchain from the perspective of methodologies involving stochastic process, game theory, optimization theory, and machine learning;
- We presented some case studies applying classical methodologies in blockchain and summarized the challenges involved, providing feasible guidance for practical deployment;
- We discussed the remaining problems and open issues based on the comprehensive survey, including cryptography, smart contract, blockchain architectures and protocols, and commercial and political views.

C. The Structure of the Paper

This paper aims to provide a comprehensive survey on the theoretical model, network service and management, and the application for blockchain systems from the methodology perspective. Section II first introduces the workflow, key technologies and applications of blockchain, then discusses the research activities and challenges, and finally shows the connections between classic methodologies. Section III-VI analyze the applications of these methodologies in blockchain. To be more specific, in each of Section III-VI, we provide a brief model and case study for each methodology, summarize the classical issues and related literature involved, and discuss lessons learned. Section VII discusses open issues of blockchain. Finally, Section VIII concludes this paper. For convenience of readers, the organization of this paper is illustrated in Fig.1.

II. Research Activity and Challenge

Recently, lots of work have been done on the application of blockchain and the improvement of network system performance, involving of the blockchain-based functions design and network optimization. The blockchain-based functions such as the consensus protocol, incentive mechanism and smart contract have significant impacts on the reliability, efficiency and scalability of the blockchain system [35]. However, the design of blockchain-based functions also faces challenges due to storage constraints, computing overhead and delay constraints. One of the most important issues is that how blockchain and network system interact with each other, especially in wireless scenario which is called as wireless blockchain networks (WBN) [36]. On the one hand, with the advent of 5G, the explosive information would be exchanged through wireless networks, and thus WBN is proposed to build a safe and trust wireless network. On the other hand, blockchain relies on frequent communication among consensus nodes to reach consensus. While the highly dynamic wireless network environment will bring performance and degradation to the communication within blockchain consensus nodes.

Therefore, the above-mentioned challenges greatly hinder the safe and efficient application of blockchain in practical systems and weaken the contribution of blockchain to better improve the practical systems performances. To cope with those challenges, it is first necessary to understand the fundamentals of blockchain, the operating process of practical communication systems, as well as the impact of the resources (e.g., communication, networking, computing resources, and etc.) and other uncertain factors on the performance of blockchain. Thus, an accurate and efficient theoretical model need to be established to analyze blockchain system performances and its influencing factors in essence. Then the design of network services for blockchain-based mechanisms and algorithms can be implemented, but which often require the help of classical methodologies. Finally, in order to facilitate the deployment of blockchain-based applications in IoT, Internet of Vehicles (IoV) and other scenarios, it is also necessary to explore how to use mathematical methods to define a specific blockchain problem, and examine various constraints and application requirements in the practical systems from the perspective of methodology. Therefore, methodology is the basis for studying the fundamentals, performances and applications of blockchain, and has been recognized.

However, most of the existing review research directions focus on the combination of blockchain and other advanced technologies, the integration of blockchain and novel networks, and the security and privacy issues of blockchain technology, etc., with the advantage of providing theoretical

TABLE I: Summary of existing surveys and tutorials

Aspect	Ref.	Main contributions
Security and privacy	[13]	• Presenting blockchain-based security services; • Comparing blockchain-based approaches to provid security services
	[16]	• Categorizing various security and privacy threats reported in the IoT domain; • Summarizing research efforts using machine learning and blockchain to address security and privacy issues in the IoT domain
	[17]	• Reviewing the existing vulnerabilities in Bitcoin and its major underlying technologies; • Discussing the feasibility and limitations of potential solutions in Bitcoin
	[18]	• Discussing attacks that effect public blockchain and the relationships between a sequence of possible attacks; • Outlining effective defense measures
Consensus protocols	[19]	• Analyzing a wide range of consensus algorithms; • Presenting a decision tree of algorithms to test the suitability of consensus algorithms
	[20]	• Reviewing consensus protocols from the perspective of distributed consensus system design and the perspective of incentive mechanism design; • Reviewing the strategy adoption from game-theoretic point of view
	[21]	• Introducing the classic theory of fault tolerance; • Identifying five-component framework to analyze consensus protocols
Scalability	[22]	• Analyzing the scalability from the perspective of throughput, storage and network; • Introducing the existing enabling technology of the scalable blockchain system
	[23]	• Studying the sharding problem in the blockchain; • Analyzing the characteristics and limitations of existing solutions
	[24]	• Reviewing blockchain with its applications, issues, and suggested improvements
Integration with 5G	[25]	• Discussing the potential of blockchain for enabling key 5G technologies; • Exploring the potential of blockchain enabling 5G services
	[27]	• Providing a classification of threat models; • Providing a taxonomy to compare the methods towards secure and privacy-preserving blockchain technologies
	[26]	• Defining nine fundamental modules of blockchains; • Presenting the capabilities of blockchain for decentralizing applications through reviewing DApps for 5G and beyond
	[28]	• Providing an evaluation framework for blockchain platforms to satisfy the requirements of IoT applications
	[29]	• Reviewing the application of blockchain technology in smart cities
	[30]	• Reviewing recent efforts in the technical fusion of blockchain and clouds in three dimensions: service, security, and performance; • summarizing the integration of blockchain and edge computing systems
	[31]	• Discussing the network control, storage and computation at the network edges; • Analyzing the realization of the network security, data integrity and computation verification by the integration of blockchain into the edge computing
	[32]	• Reviewing recent efforts in the integration of blockchain and fog computing
Methodology	[33]	• Reviewing the game models applied in addressing blockchain-related issues
	[34]	• Discussing feasible solutions integrating blockchain and machine learning for communications and networking system
Our work		• Analyzing the fundamental theory of blockchain, blockchain-based network services and applications from a methodological perspective; • Discussing classic methodologies used to tackle major issues for blockchain; • Revealing the intrinsic relationship between blockchain and communication, networking and computing

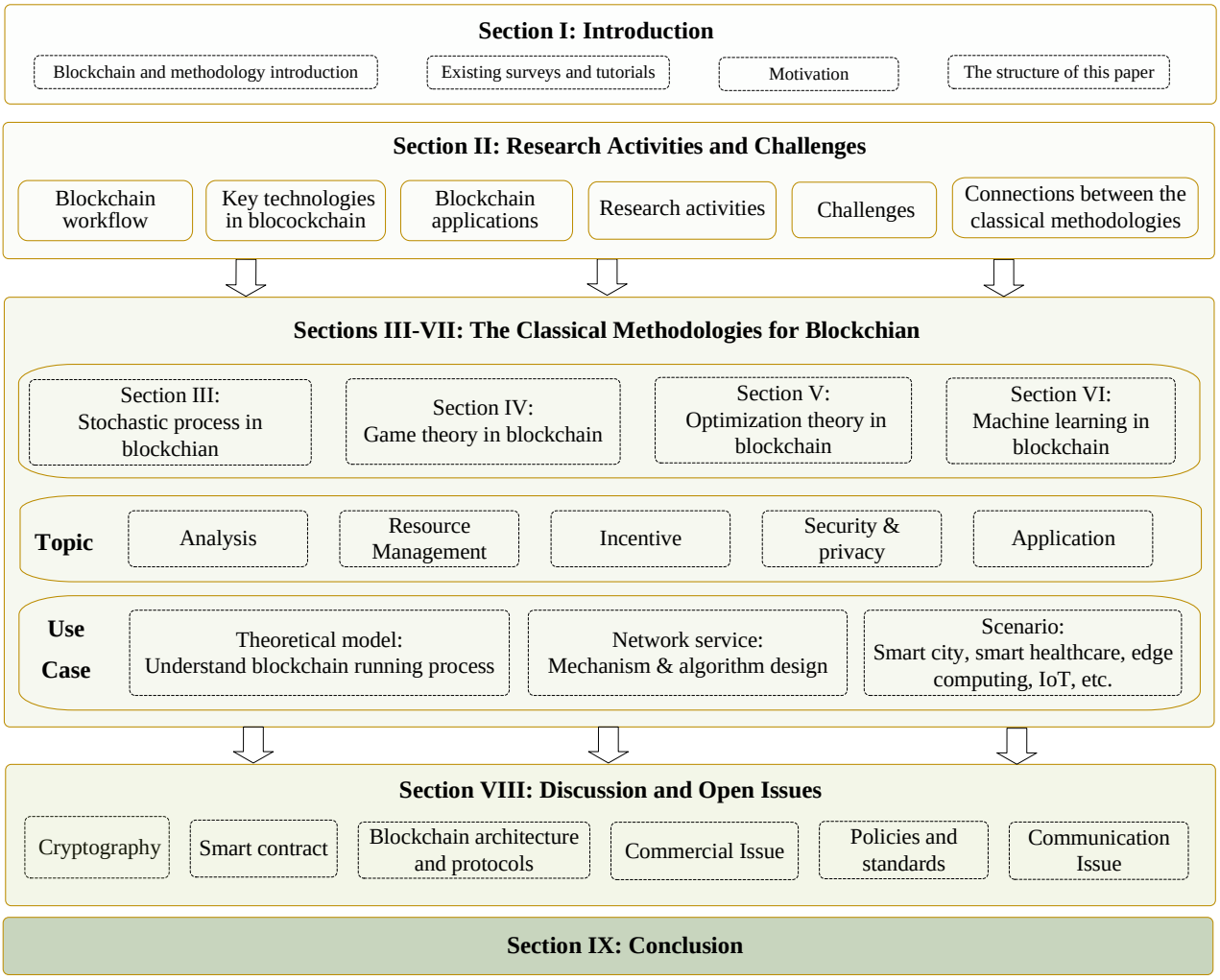


Fig. 1: Organization structure of this paper

support for blockchain applications. But, it may also have certain limitations, which are affected by complex and uncertain factors in the practical system, and thus fail to further support the optimization of blockchain function design and network performance improvement. Therefore, it is necessary to systematically and comprehensively study the blockchain systems, technologies and applications from the perspective of methodology, and objectively evaluate their advantages and limitations.

In this Section, we first introduce the blockchain workflow in Section II-A and the key technologies of blockchain in Section II-B. Next, we study the applications of blockchain in II-C and the research activity in Section II-D. Then, we discuss the remaining challenges of blockchain system in Section II-E and show the connections between the classical methodologies in Section II-F.

A. How Does Blockchain Work

Both the infrastructure and blockchain layers are interrelated and interact with each other. Although the detailed procedure might be different in practical scenarios, some basic steps may be the same, as shown in Fig. 2. With these steps, multiple blocks are linked to form a chronological chain. In particular, each block contains a hash value of the immediately preceding block, which makes the linked data immutable.

Through this workflow, the transaction is finally agreed by the majority of nodes and recorded in blockchain, where malicious nodes cannot subvert the consensus results. This decentralized architecture ensures robust and safe operations on the blockchain, with the advantages of resisting tamper and single point of failure. It can be seen from the Fig. 2 that each blockchain node in the blockchain system undertakes all or part of functions, such as communication between nodes, maintenance of P2P networks, and computation of consensus mechanisms. Thus, the underlying communication, networking and computating is crucial to establish an effective and secure blockchain system. This encourages us to study how communication, networking and computing affect blockchain systems. Fortunately, some classic methodologies can provide good ideas, such as stochastic process for block generation and nodes communication, machine learning for P2P network performance improving, and optimization theory for resource

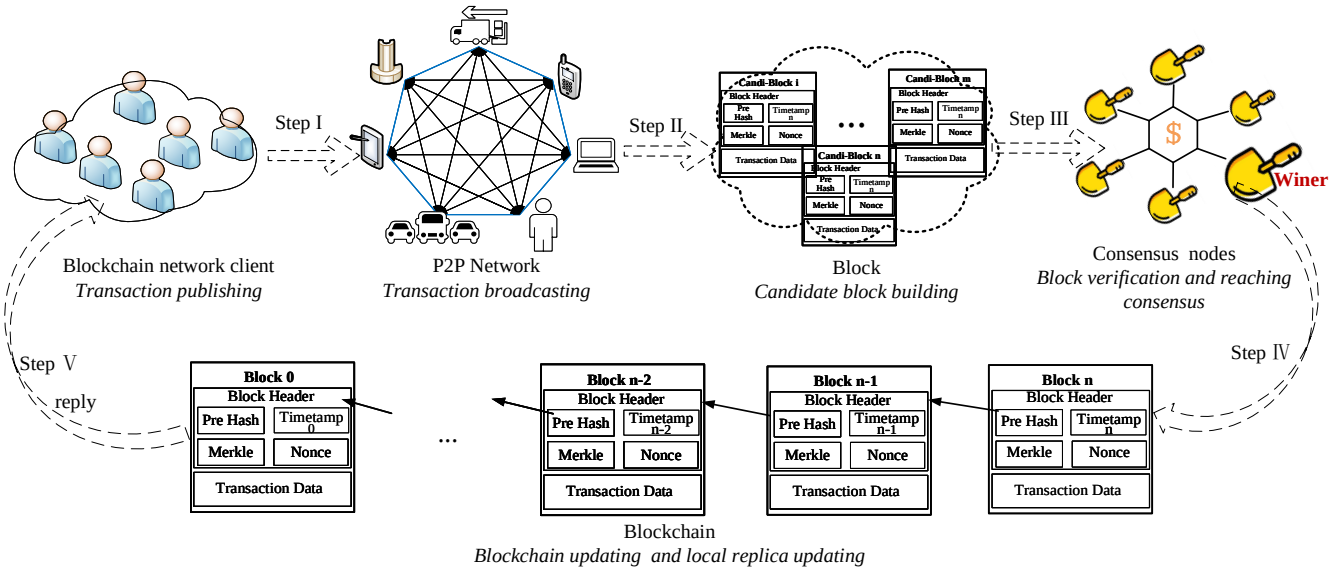


Fig. 2: An overview of blockchain workflow

allocation. Therefore, it is feasible and valuable to explore the interaction process of communication, networking and computing and their impact on the blockchain system from the perspective of methodology, and even can provide help for revealing the essential problems in the operation process of the blockchain system.

B. Key technologies in blockchain

Key technologies used in blockchain include cryptography, P2P network, consensus mechanism, smart contract, data storage and incentive mechanism.

1) Cryptography: In blockchain, cryptography is mainly used for data encryption and privacy protection, such as asymmetric encryption algorithm, hash algorithm, and zero-knowledge proof (ZKP) [37]. Asymmetric cryptography is often adopted for encryption and digital signature, which guarantees the security and reliability of data in blockchains. The hash algorithm, that any slight changes in the hash input will lead to a totally different hash output, can ensure the immutability of blockchains, which is often utilized for block performing and transaction information verification. By using ZKP, verifiers can verify provers without revealing any information about the provers, significantly improving blockchain privacy [38].

2) P2P network: P2P network enables direct data exchange between different nodes in blockchains [39]. As for P2P network structure, it can be divided into structureless network, structured network, and hybrid network. With the development of blockchain, the hybrid network that is characterized by decentralization and high communication efficiency is becoming the mainstream solution driven by the demands for efficient communication and network governance [40].

3) Consensus mechanism: As the essential component for blockchain systems to achieve state consistency, the consensus mechanism plays a crucial and irreplaceable role and mainly determines the security boundary and performance of

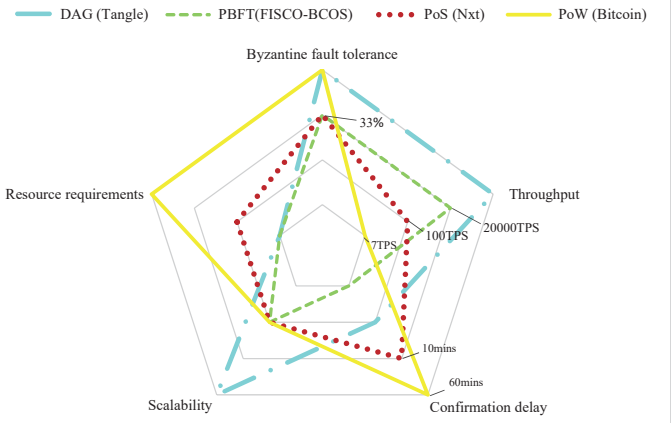


Fig. 3: Multi-dimensional graph for performance comparison of typical consensus mechanisms in blockchain

blockchain systems. Generally, the consensus mechanism is the rule that constrains each node in the decentralized network and ensures all participants agree on a unified transaction ledger without central authority [41]. There are various consensus mechanisms proposed for different projects, and most of them are originated from typical Proof-of-Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Direct Acyclic Graph (DAG). Fig. 3 provides a multi-dimensional performance comparison for several typical consensus mechanisms.

4) Smart contract: Smart contract is a computer program running on top of blockchain, designed to automatically facilitate direct negotiations or contract terms between users when certain conditions are met [42]. Besides, smart contract execution is not dependent on any third party, nor can any entity modify the rules defined in it, which reduces the risk of tampering. These features allow the smart contract to further extend the functionality of blockchain to meet the needs of

various applications.

5) Data storage: As a distributed database, blockchain requires efficient underlying storage that can accommodate large-scale storage requirements [43]. Currently, various storage technologies have been applied in blockchain, such as LevelDB, CouchDB, RocksDB, MySQL, and InterPlanetary File System.

6) Incentive mechanism: The incentive mechanism is the driving force to maintain the safety and sustainability of a blockchain system by encouraging participants through a monetary or non-monetary approach. The monetary-based incentive mechanism increases the cost of attacking or selfish behavior by means of economic balance, while the non-monetary-based incentive mechanism seeks to motivate participants to cooperate through credibility or reputation [44].

C. Blockchain Applications

This subsection highlights the significant applications of blockchain in communication systems and services, focusing on architecture improvement, system performance enhancement, and integration with other technologies.

1) Flexible and trusted network deployment: Various service deliveries can be achieved by blockchain. For example, access control [45], authentication [46], and service response [47] can be implemented on the decentralized ledgers among network participants without additional management infrastructure [25]. In addition, by leveraging the blochain features, such as decentralization, tamper-proof, and traceability, a large number of non-mutually trusted subnetworks can cooperate to build a large-scale trusted network, providing flexibility for dynamic and large-scale network deployments [48].

2) Spectrum sharing enhancement: Increasing mobile data traffic puts pressure on the management of communication system resources, especially the radio spectrum. Blockchain offers a promising solution for overcoming spectrum monopoly and low spectrum utilization to increase communication system throughput and reduce latency. Various researches have recently focused on secure and dynamic spectrum trading [49]–[51], spectrum sensing [52]–[54], and spectrum management [55]–[58] using blockchain.

3) Security and trust enhancement: Blockchain has been investigated and integrated with mobile edge computing (MEC), cloud computing, device-to-device communication, etc., to meet the requirements of IoV, IoT, and industrial networks in terms of secure communication, reliable information sharing, and trusted authentication. Besides, blockchain has the potential to enhance the security of serval emerging technologies, such as federated learning (FL) [59] and transfer learning (TL) [60]. Blockchain is also combined with space-air-ground integrated networks [61] and tactile networks [62], aiming to build a ubiquitous trust system to meet the requirements of 6G in terms of high security, reliability, and privacy.

Although blockchain applications have attracted extensive attention from both academia and industry, there are still many limitations to be further addressed before apply it in practical environments, including resource consumption, scalability, and interoperability.

1) Resource consumption: High resource consumption in communication, storage, and computing are significant burdens affecting the practical blockchain applications. Blockchain relies on frequent communication among nodes to reach consensus, which would lead to a high communication resource (e.g., spectrum) consumption, and thus causing strain on wireless networks especially when the network is large [35]. Besides, in traditional blockchain networks, each consensus node needs to store a copy of the entire ledger, which would significantly pressure lightweight devices for storage. Moreover, most lightweight devices cannot provide sufficient computing capability to perform some computationally complex consensus mechanisms.

2) Scalability: Poor scalability is a key barrier to the large-scale application of blockchain in practical environments. In communication networks, scalability is related to the two significant factors, i.e., communication resource and transmission power [35]. In particular, the growing number of nodes would lead to a rapid increase in the communication resource requirement, which results in low consensus efficiency and poor scalability. Besides, in wireless networks, the transmission power could affect the coverage and thus the blockchain scalability when the node density is fixed. Currently, many enabling technologies have been developed to improve the blockchain scalability. However, it is usually at the cost of other key performances. For instance, sharding is often used to avoid the duplicating communication in each full node, but the security of blockchain decreases as the number of shardings increases [63]. Therefore, it is inevitable to balance scalability and other performance, i.e., security, when leveraging blockchains in practical applications.

3) Interoperability: Interoperability is also an important requirement for blockchain applications in practical environments. Currently, various blockchain systems with different characteristics have been proposed for different scenarios. However, since there lacks of interoperability in underlying functions, these systems would act as island networks without interconnections. It would result in a barrier to secure and efficient data sharing and business collaboration among different blockchains.

D. Research Activities

In this subsection, we first classify the mainstream research activities into theoretical modeling for blockchain performance analysis, blockchain-based function design for network services, and blockchain-based solution for vertical applications. Moreover, the contributions and potential developments of these research activities are discussed.

1) Theoretical modeling for blockchain performance analysis: The establishment of accurate and effective theoretical models is significant for studying the system performance, such as the necessary conditions for achieving consistency, delay and cost of achieving consistency, and processing capacity of blockchain. Existing projects and studies on system performance focus on theoretically analyzing in stochastic variable analysis, consensus protocol design for specific applications, and decoupling of the traditional centralized network

architectures for security and scalability [64]–[66]. In addition, the innovation of different types of consensus algorithms that have unique characteristics and serve other purposes has great significance to the security and efficiency of blockchain systems, thus attracting many scholars' attention [19].

However, in practical blockchain systems, the factors affecting its performance are rich and complex. Therefore, to better perform blockchain performance analysis, resource constraints and uncertain aspects of communication, networking and computing also need to be considered. Thus, there is a need to further design a theoretical model that can capture the characteristics of complex dynamic scenarios for the optimal design of the blockchain system and the network service design based on blockchain, to provide the theoretical guidance and design ideas for technological innovation and breakthroughs.

2) Blockchain protocol for network services: Apart from the initial financial service, more researches related to blockchain services are concentrated on specific areas relevant to network services, such as public and social services [67], cloud services [68], and other Internet services. For distributed systems with blockchain participation, state consistency among nodes is the key to ensuring integrity and security. Therefore, many researchers intend to develop improved consensus mechanisms to meet different purposes and applications, such as Proof-of-Trust for high throughput and low resource consumption [69], Proof of Authority for Sybil attack resistance [70], and Multi-Layer PBFT for scalability [71]. Besides, incentive mechanism is also essential to regulate entity behaviors to improve blockchain-based network service performance. Different incentive mechanisms have currently been proposed, such as incentives to participate [72]–[74] and cooperate [75]–[77].

In addition to protocol design, a systematic analytical framework is required to describe the operational logic of blockchain protocols and network services to depict how specific network environments, resource requirements, and behavioral patterns affect network-wide consensus reaching, system performance and security.

3) Blockchain-based solution for vertical applications: Owning to the benefits of building trust, reducing cost and accelerating transactions, blockchain technology is expanding to other areas including IoV, industry 4.0, smart homes, and such [14], [78]–[80]. Various blockchain platforms have been built for different vertical applications. Bitcoin, ETH, and Hashgraph, for example, are blockchain platforms that are focused on providing high security and low transaction cost. These platforms are suitable for applications where data security is of the most importance, such as health data sharing, payments and credit reporting. Some platforms, such as Nxt, IOTA, Hyperledger Fabric and EOS, has its advantage in high scalability which can be implemented in IoT, supply chain traceability and logistics traceability. A more detailed analysis of existing typical platforms is in Table III.

Furthermore, relying on the underlying technology and blockchain platform, specific industry applications can be developed according to the actual application scenarios of various industries, so as to realize the innovation of business collaboration mode in the vertical industry.

E. Challenges

1) Systematic theoretical model: Notably, a solid theoretical foundation can provide theoretical guidance for rational applications and technological breakthroughs, which would further advance blockchain development. However, the performance analysis of the current studies is mainly conducted through experimental simulations or application implements without systematic theoretical arguments [85] [86]. Therefore, accurate and extensible theoretical models are required to guide the rapid popularity of blockchain applications.

2) Cost-effective protocol design: Integrating blockchain into practical systems, especially wireless networks, with limited computing, storage and communication capacity, is still a challenging issue. As the mainstream blockchain protocols, PoW is of high resource consumption, PoS faces posterior corruption and wealth centralization risk, and DAG's performance is greatly influenced by information load, while Byzantine fault tolerance is of high communication complexity. These characteristics prevent these protocols from applying to the practical system with diversified service requirements. Therefore, a dedicated and cost-effective blockchain protocol for practical systems is necessary to address the mismatch in communication, networking and computing.

3) Joint optimization: The performance and security of wireless network-based blockchain are not only affected by the designed blockchain protocol but also by the application scenarios. For example, in blockchain-enabled MEC systems [87], except for the delay/time to finality (DTF) for the blockchain system, energy consumption for the MEC system is also a key performance metric that needs to be considered. Then, to avoid sub-optimal performance, a joint optimization scheme is required to achieve optimal trade-off between the two metrics. Generally, when emerging blockchain with other technologies, joint optimization must be considered to eliminate unilateral bottlenecks and ultimately achieve overall system performance optimization from the perspective of multi-dimensional requirements.

F. Connections between the classical methodologies

In this subsection, we summarize the classical methodologies mentioned in this work, as shown in Table II. Also, we present the connections of these methodologies, shown in Fig. 4.

Stochastic process and machine learning: Generally, a stochastic process is used to build mathematical models for systems that vary in a random manner. Instead, machine learning is used to explore data patterns and structures for more accurate predictions and decisions. With advantages in modeling complex and dynamic environments, the stochastic process can reveal the essence of blockchain operations, optimize the performance of blockchain networks and guide the deployment of blockchain applications. Meanwhile, machine learning is dedicated to providing efficient and intelligent decisions for blockchain to support performance optimization.

TABLE II: Summary of classic methodologies

Methodologies	Essence	Advantages	Applications	Benefits of combining with blockchain
Stochastic process	Building mathematical models of systems and phenomena that appear to vary in a random manner	Modeling of complex and dynamic environments	Theoretical modeling for blockchain performance analysis	• Revealing the essence of blockchain operations; • Optimizing the performance of blockchain networks; • Guiding the deployment of blockchain-based applications in actual systems.
Machine learning	Analyzing data using systematic mathematical methods and drawing conclusions	Providing efficient and intelligent decision	• Blockchain-based function for network services; • Blockchain-based solution for vertical applications	• Optimizing the performance of blockchain networks; • Designing network services based on blockchain mechanisms and algorithms
Game theory	A set of mathematical tools for analyzing the interaction among rational decision-makers.	Describing the conflict and cooperation between participants	• Theoretical modeling; • Blockchain-based function for network services	• Optimizing the performance of blockchain networks; • Designing network services based on blockchain mechanisms and algorithms
Optimization theory	The choice of the best solution of an existing collection for a specific purpose	Finding the best optimal solution among existing solutions under constrains	• Theoretical modeling; • Blockchain-based function for network services	• Optimizing the performance of blockchain networks; • Designing network services based on blockchain mechanisms and algorithms

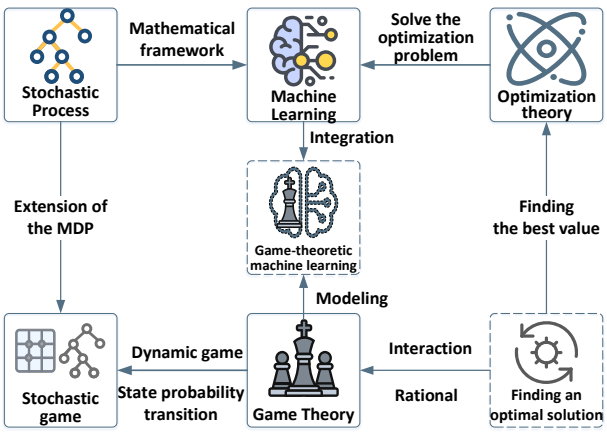


Fig. 4: Connections between the classical methodologies

Game theory and optimization theory: The main objective of game theory and optimization theory is to find the optimal solution under the given conditions. Game theory describes the conflict and cooperation among the participants to develop a rational decision for players in a dynamic environment. Therefore, game theory is commonly used to analyze the behavior of blockchain users to optimize the system performance accordingly. Optimization theory aims to solve an optimization problem that describes the mathematical relationships between different factors affecting network performance. Thus, optimization theory is usually applied to quantify the association among essential factors in blockchain networks based on the instantaneous state of each node and finds the optimal solution for performance improvement.

III. Stochastic Process in Blockchain

Stochastic Process [88] is a mathematical method to establish mathematical model and analyze its performance for complex and stochastic systems, by which a set of time-dependent

TABLE III: Major blockchain platforms

Platforms	Bitcoin [1]	Nxt [3]	ETH [2]	Hashgraph [81]	IOTA [82]	Hyperledger Fabric [83]	EOS [84]
Application layer	Bitcoin transaction	DAPP/Nxt transaction	DAPP/ETH transaction	Public network	IOTA transaction	Enterprise block application	Operating system
Programming language	JavaScript	Java	Solidity/ Serpent	-	JavaScript/ Java/C#/Go	Go/Java	C++
Data model	Transaction model	Account model	Account model	-	Account model	Account model	Account model
Block storage	LevelDB	-	LevelDB	-	-	FileSystem	-
Communication protocol	P2P	P2P	P2P	-	HTTP	P2P	P2P
Category	Public blockchain	Private blockchain	Public blockchain	Consortium blockchain/ Private blockchain	Public blockchain	Consortium blockchain	Consortium blockchain
Consensus algorithm	PoW	PoS	PoW	BFT	Tangle	BFT	DPoS
Architecture	Continuous single chain architecture	Continuous single chain architecture	Continuous single chain architecture	Based on DAG architecture	Based on DAG architecture	Continuous chain architecture	Continuous chain architecture
Solution	Computational power competition	Coin age	Computational power competition	Virtual voting, gossip protocols	Self-weight and cumulative weight	Gossip protocols, endorsement and ordering	Virtual voting
Characteristic	Low transaction fee, high security, low network resource consumption	Proof-of-Stake consensus, universal blockchain framework, decentralized asset exchange, proven stability	Low transaction fee, high security, low network resource consumption	Low consensus cost, high security, high transaction throughput, low confirmation latency	High scalability, low resource requirements, zero-fee transactions, secure data transfer, offline transactions, quantum immune	High scalability, permission control and modular architecture	Flexible, scalable, user-friendly
Open source address	https://bitcoincore.org/en/download/	https://bitbucket.org/Jelurida/nxt/src/master/	https://geth.ethereum.org/downloads/	https://github.com /hashgraph/hedera-improvement-proposal	https://github.com/iotaledger/iota.js	https://github.com/hyperledger/fabric	https://github.com/EOSIO/eos

random variables are used to describe the system state at a specific time. Typically, in wireless communication scenario, due to the fact that information is usually stochastic, leading to the complex environment in wireless communication. The Markov process is now most widely used stochastic process to modeling such communication environment. As for Markov process, if the current system state is determined, the future system state would be also known, no matter what the system state is in the past. Therefore, the Markov process can be used to predict the system state, user action and network performance. Meanwhile, stochastic geometry [89] is another mathematical tool widely used in the modeling and analysis of communications and networking [90]. In communication networks, the actual network nodes and spatial locations can be formulated as random point processes, such as Homogeneous Poisson Point Process (HPPP), which is to eliminate the randomness by traversal to analyze the system performance and provide design ideas theoretically.

A. Classical Issues

In this subsection, we introduce classical issues in blockchain networks that could be solved by the stochastic process, which can be categorized as follows.

1) Analysis of blockchain operation process: In practical blockchain systems, there are many random behaviors, such as block generation time, confirmation delay, chain growth rate and forking, which make it difficult to analyze the growth and evolution of blockchain networks. Due to the ability to model complex and uncertain scenarios, a stochastic process is used to formulate the operation process of blockchains effectively and accurately, such as Markov chain for consensus modeling [91], non-homogeneous Poisson process for difficulty-of-work re-adjustment [92], and MDP for stale block rate [70].

2) Security enhancement: In order to prevent or minimize the impact of attacks, exploring the security boundaries of blockchain networks is another important topic in the blockchain field. By modeling and analyzing malicious behavior modes, the stochastic process can reveal the impact of different attack schemes on system performance and clarify the cost of successful attacks.

3) Performance improvement: Stochastic process also improves blockchain performance in terms of network optimization, node deployment, etc. For example, the Poisson point process (PPP) can be applied to model the location distribution and transaction arrival rate to investigate the impact of key factors, such as communication throughput and transaction

throughput, on the large-scale deployment of blockchain in practical networks.

B. Model Briefs

In this subsection, we discuss how to use stochastic process in blockchain system on the typical issues of consensus, security and deployment. In order to formulate the consensus process in blockchain system as a stochastic process, it is necessary to define a metric (like the cumulative block in PoW, or the cumulative weight in DAG) to indicate the consensus state at the different time. Moreover, if it satisfies Markov properties, the consensus process can be formulated as a Markov chain model with one-step transition probability $P = P\{X_{n+1} = i_{n+1} | X_{n+1} = i_n\}$.

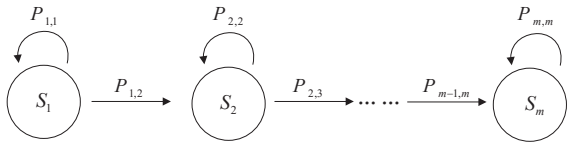


Fig. 5: The stochastic process in consensus process of the Blockchain.

As shown in Fig. 5, we use a Markov chain to model the consensus process. In this process, $S_i(i = 1, 2..., m)$ represents the state in the consensus process, and $P_{i,j}$ is the one-step transition probability in the Markov chain mode. Accordingly, we can learn the consensus process and gradually understand the inner-action. Furthermore, it is also useful to analyze the malicious forking attack for security.

As the most famous consensus process, the PoW-based mining task proposed by bitcoin is a competition among minors, where the winner has the right to generate a new block to obtain an amount of reward. For malicious purposes like double-spending in the blockchain, forking attack launched by the malicious node which generates blocks to build a parasite chain privately, it would succeed if the parasite chain is longer than the main chain built by the honest node due to Longest-Chain-Rule (LCR). Indeed, this attack can be treated as a competition between honest and malicious nodes. Particularly, without any malicious node, this competition is also the consensus process formulated previously. Therefore, the competition for block generation can be modeled as a Poisson process to study the relationship between honest and malicious nodes, which is shown in Fig. 6. The malicious nodes compete against the honest nodes to generate the block. The node which has the biggest probability will have the right to generate the block. Accordingly, the factors affecting the vulnerability of blockchain can be known, and the successful probability of malicious node can be determined. As a result, the theoretical insight can be provided to resist forking attack, optimize consensus mechanisms, and improve network security.

Like the classic base station deployment problem in heterogeneous networks, deployment of blockchain function node (or called as full node in some literatures) can be solved using a stochastic method/stochastic methods in the same manner. The blockchain system is decentralized which is composed

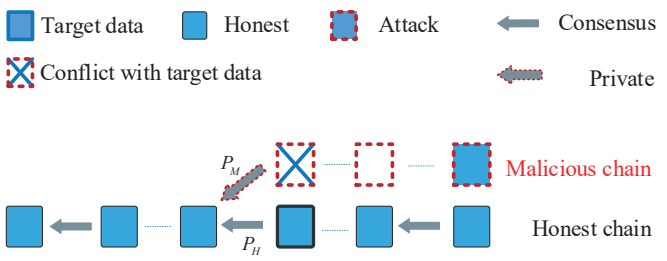


Fig. 6: The stochastic process in the block generation of the Blockchain.

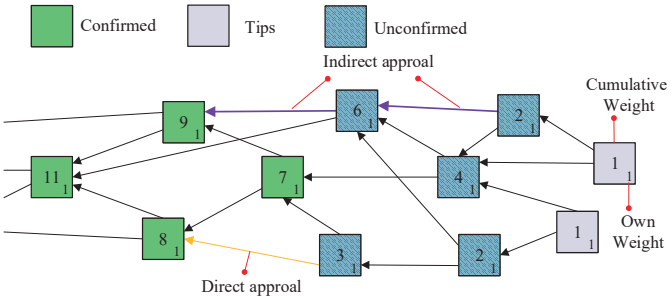


Fig. 7: An example of consensus process in Tangle [93].

of multiple distributed blockchain nodes, their geographical distribution can be modeled as a HPPP. In this way, we can construct an effective blockchain system architecture, and analyze the impact of blockchain node distribution on the communication throughput, SNR, security and other network metrics. Therefore, a valuable theoretical guidance is developed to optimize the blockchain node deployment in order to improve the system performance.

C. Case Study

In this subsection, we will use our previous work [93] as an example to introduce how to model the classic blockchain problem as a stochastic process. Tangle, one of the most typical DAG consensuses, has attracted extensive attention in DAG-based ledgers. Therefore, we adopt it as a typical example to introduce the DAG consensus process. Fig. 7 shows an example of the consensus process in Tangle.

DAG consensus allows any node to insert a new block into the ledger immediately, as long as they process the unapproved transactions called tips. For an observed transaction in a DAG-based ledger, its cumulative weight is its own weight plus the weight of the transactions that approve it, where the average own weight of each transaction is normalized into 1. Therefore, $W(t)$, the cumulative weight of an observed transaction at time t, will increase with the approval of new transactions over time, which is a stochastic process. Meanwhile, $L(t)$, the number of tips at time t, is also a stochastic process. Therefore, when the new transaction arrives slowly, resulting in a low network load, the future states of $L(t)$ and $W(t)$ are determined by their current states only and can be formulated as a discrete-time Markov chain.

When a new transaction x arrives, the change in system state can be expressed as

$$W(k+1) = \begin{cases} W(k) & a_x = 1, \\ W(k)+1 & a_x = 0, \end{cases} \tag{3.1}$$

$$L(k+1) = L(k) - 1, \tag{3.2}$$

where the $a_x = 1$ represents the situation that the observed transaction has been approved by an incoming new transaction, and $a_x = 0$ indicates the situation that the observed transaction has not been approved. Since the new transaction should select two unselected transactions randomly, and thus (3.2) indicates that the new transaction replaces two unselected transactions as a new one.

Therefore, the corresponding one-step transition probabilities and Markov chain can be shown in Fig. 8.

For example, if the network is from high to low with an unsteady state, the one-step transition probabilities can be expressed as:

$$\begin{cases} P\{i+1, j-1 \mid i, j\} = 2/j, \\ \quad i = 1, 2, \cdots, L_h - 1; j = 2, 3, \cdots, L_h, \\ P\{i, j-1 \mid i, j\} = 1 - 2/j, \\ \quad i = 1, 2, \cdots, L_h - 1; j = 2, 3, \cdots, L_h, \\ P\{i+1, 1 \mid i, j\} = 1, \quad i = 2, 3, \cdots, \infty; j = 1. \end{cases} \tag{3.3}$$

This model is for low network load cases, and we can also obtain the modeling for high network load cases in the same manner. According to this Markov chain model, it is possible to provide theoretical guidance for the blockchain implementation, which can help analyze the key performance indicators in terms of cumulative weight and confirmation delay under different network loads, and it is able to evaluate the security performance based on the understanding the impact of network loads.

D. Related Works

1) Existing surveys and tutorials: Dachian *et al*. in [94] provide a review on the estimation of cusp locations for stochastic process, where models involve Gaussian, ergodic diffusion processes, independent identically distributed observations, etc. For the application of stochastic process in various fields, Lei *et al*. in [95] focus on stochastic models in addressing the challenges of network embedding in data processing and modeling, as well as summarize the network embedding works in terms of the data side and the model side from a stochastic perspective. Karr *et al*. in [96] is concerned with the role of stochastic process in imaging and gives some examples about Markov random field imaging model and Poisson process model for laser radar. Shakarami *et al*. in [97] review the application of stochastic process in decision making, highlighting the advantages and limitations of Markov chain, Markov process and Hidden Markov model applied to offloading decision.

For blockchain, Kang *et al*. in [98] provide a comprehensive survey of stochastic models proposed to analyze essential issues in blockchain. Specifically, this survey starts with classifying the stochastic models for analyzing blockchains into network-oriented and application-oriented, where the network-oriented stochastic models are further divided into performance models and security models. Then, for each of these categories, the major contributions of related work are discussed.

2) Control of mining difficulty: Kraft *et al*. in [92] discuss the difficulty-of-work re-adjustment in the blockchain system. In order to achieve a relatively ideal average block generation rate over a period of time, the mining work is formulated as a non-homogeneous Poisson process and a new method of the difficulty-of-work re-adjustment is proposed. However, the randomness of the hash rate in the blockchain system has not been addressed yet. To this end, Fullmer *et al*. in [99] consider this situation and introduces a random model about block arrival time, in which the marginal distribution of block arrival time and its both expectation and variance are derived. Accordingly, we can know that the target difficulty value both is a function related to the arrival time of the previous block and affects the block arrival time in the next retargeting period.

3) Modeling and analysis: Using the stochastic reward network, Sukhwani *et al*. propose a new Hyperledger Fabric v1.0 + system model and study the performance indicators such as throughput, transaction delay, node utilization, and queue length in [100]. This proposed model can provide a quantitative framework to help system architects evaluate performance as a function of different system configurations and make design trade-offs decisions. Papadis *et al*. in [101] propose a stochastic network model to describe the joint dynamics of "frontier" processes, track the dynamic evolution of blockchain networks, capture important blockchain features, and study the impact of delay on security. Nayak *et al*. in [102] adopt Markov Decision Process (MDP) to study the selfish mining and further explore how a miner can amplify its gain by non-trivially composing mining attacks with network-level eclipse attacks. Li *et al*. in [103] apply Markov chain model to analyze the performance of the four proposed blockchain-based access schemes in terms of transaction throughput, block discard rate, etc. For private blockchain, Huang *et al*. in [91] use Markov chain model to analyze the performance of Raft and predict the network split time and probability to facilitate the optimization of RAFT parameters. Except for Markov chain model, Meng *et al*. in [104] propose a queueing network-based approach to research consistency properties of consortium blockchain protocols. Alia *et al*. in [105] explore the optimal strategies of service providers and miners to maximize their long-term benefits using fully- and partially observable Markov decision models. Ma *et al*. in [106] describe PBFT queues using a two-dimensional Markov process and perform a detailed analysis of the performance evaluation of PBFT consensus mechanisms by matrix-geometric solution. To understand important factors such as replica node latency and primary node latency in healthcare blockchain network, Zheng *et al*. in [107] simulate the time response of healthcare blockchain network based on PBFT using continuous-time Markov chain model, which provides a basis for the optimal design of blockchain network.

4) blockchain node deployment: Based on the RAFT consensus mechanism, Xu *et al*. in [108] study the security performance of wireless blockchain networks under malicious interference, and provides analysis guidance for the actual de-

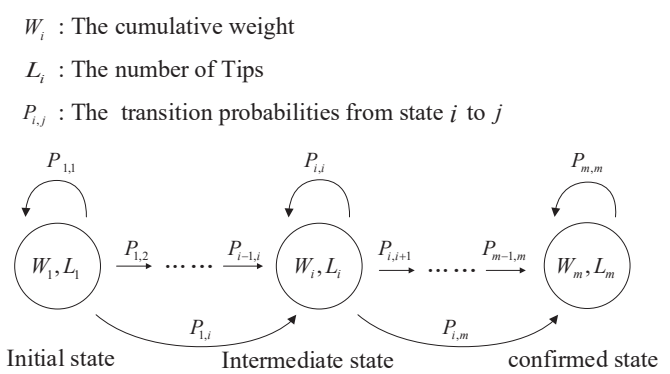


Fig. 8: The Markov chain for DAG-based consensus process.

ployment of wireless blockchain networks. Zhu *et al*. in [109] introduce the blockchain-based heterogeneous network in a air-to-ground IoT heterogeneous network. Moreover, stochastic geometry method is adopted to model the deployment of Ground Sensors, Air Sensors, and the place of eavesdroppers with interference attacks. Sun *et al*. in [110] model the location deployment and transaction arrival rate in IoT network as a PPP to study the relationship between communication throughput and transaction throughput, and propose an optimal communication node deployment algorithm, which achieves the maximum communication and transaction throughput with the minimum communication node density. Liu *et al*. in [111] formulate the location deployment of base stations and mobile users as a HPPP for MEC, and derive the theoretical expressions of relevant performance indicators in various modes using stochastic geometric methods.

E. Lessons Learned

Due to the randomness of blockchain system, stochastic methods is commonly used for formulation, which can accurately describe the distribution of blockchain nodes, the arrival of transactions, the behavior of blockchain users, etc. Through these mathematical modeling, researchers can track the dynamic evolution of the blockchain system, and further analyze of the consensus process, throughput, and security performance. Accordingly, the corresponding theoretical basis can be provided for performance improving, such as malicious attack preventing, and blockchain application accelerating.

Although stochastic process has been widely used in the literature, there are still issues that should be considered and improved in the future.

1) Most existing researches formulate the blockchain system as a certain stochastic process assuming a simple model such as the Poisson distribution. However, in the actual environment, the blockchain running process usually is more complicated, and how to abstract the common random variables accurately without lossing generality should be well studied. In other word, the mathematical formulation must accurately describe the blockchain system in practice, while considering the property, complexity and constraint in the view of theoretical approach.
2) Currently, some typical issues in a few specific scenarios have been widely investigated. In contrast, a generalized stochastic model is in need to describe the whole blockchain system. In the future, we should further consider how to use stochastic process to model an end-to-end blockchain system model, which can systematical study the actions of blockchain user and the system performance. In addition, understanding the interactions between various functions of hash operation, cache, consensus, communication network and smart contract is another direction for future research.

IV. Game Theory in Blockchain

Game theory [112] [113] is a mathematical theory to study the strategy selection in competitive behaviors. A basic game consists of four basic elements: player (decision maker), strategy (the player's action), reward (the game result obtained after the player chooses a strategy) and equilibrium (a balance). We can use the game theory to formulate the conflicts and cooperations between selfish and rational decision-makers. By analyzing both expected and actual behaviors of the players, we can study how each player generate and optimize individual strategy under different situation. In a game, if no player can obtain more profits by changing his own strategy alone, we call that the strategy set of all players at this time is at the state of Nash equilibrium [114]. Nash equilibrium guarantees that each player's strategy is optimal no matter how the strategy of other players changes. In recent years, game theory has become an important tool for communication and network research, in which most interactions can be analyzed as game behaviors to find the optimal competitive strategy.

A. Classical Issues

In this subsection, we summarize and classify classical issues in blockchain networks that could be solved by game theory.

1) Analysis of blockchain operation process: Game theory can be used to investigate the operation process of blockchain mechanisms and the behavior of blockchain users. Besides, game theory is also useful in describing the dynamic evolution of the mining pool selection process with multiple parameters, which can provide engineers with a valuable perspective on mining pool management.

2) Security enhancement: Game theory can be utilized to study security strategies that discourage the nodes from misbehaving or launching attacks by modeling the behavior patterns of the nodes in blockchain networks. Specifically, the evolutionary game is often applied to describe the dynamic evolution of pool selection strategies which are used against the miner dilemma problem and block withholding attack [115]–[117]. The non-cooperative game and Stackelberg game are applied to model the stakeholder interactions to avoid double-spending attacks [118], [119]. Besides, contract theory enables the exploration of the balance between security and economic incentives [120].

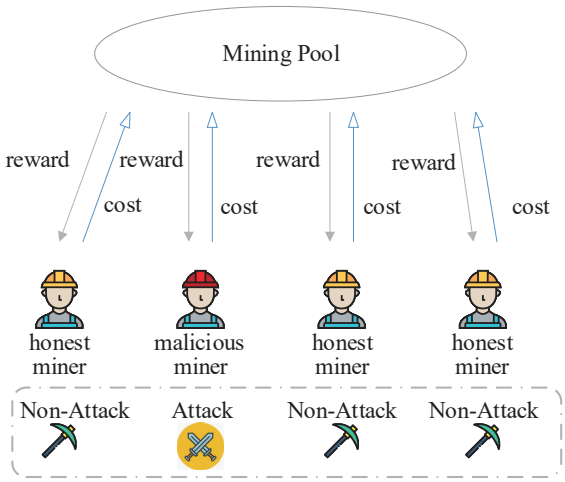


Fig. 9: A Non-cooperative game framework for the mining process

3) Resource allocation: Game theory can be applied to develop resource allocation strategies that motivate participants to share resources since each participant in the resource allocation process is rational and self-interested in attempting to maximize its own benefits. For example, the Stackelberg game enables the description of the interactions between resource sellers and buyers and maximizes the revenue for both parties in blockchain-based networks [121], while the non-cooperative game and stochastic game perform resource allocation by analyzing the behavior patterns of participants [122], [123].

B. Model Briefs

Considering the malicious characteristic, a miner launches an attack to increase his/her own winning probability while unfairly reducing the wining probability of others. In fact, any selfish and rational miner would like to maximize its own overall reward, which is determined by the environment feedbacks, cost and successful attacking probability simultaneously. Therefore, a miner must consider all possible re-actions of others to choose the strategy that is most beneficial to itself in this typical non-cooperative game. Therefore, the miner can be treated as the player, its strategy is whether to launch an attacking, and the reward function is the expected reward if the attacking succeeds minus the cost for attacking. In this manner, we can formulate this mining process as a game shown in Fig. 9, to study the impact of miners' strategies (to be honest or malicious) on the blockchain network. Based on the analysis and equilibrium solution, a game model can be employed and to provide a theoretical guidance to optimize the consensus process in order to improve the security (refrain from launching the attacking action).

During the mining process, a miner should allocate certain amount of computing resources to increase the wining probability to get the right that generates a new block with corresponding reward. Meanwhile, the more computing resources consumed, the higher cost would be generated. It means there is an effective trade-off between cost and benefit needs to be made. Accordingly, this problem can be also formulated as a game to study the interaction among miners and analyze the best strategy. For instance, game theory is often used to study equilibrium-based strategy, which guarantees the optimal reward of each miner while avoiding the meaningless mining competition caused by greedy resource allocation. Fig. 10 is a game theory model based on auction, the miners will bid for the computing resource, and the computing service providers will provide different computing resource. The more bid, the more resource. Therefore, the miner need to balance the cost and revenue.

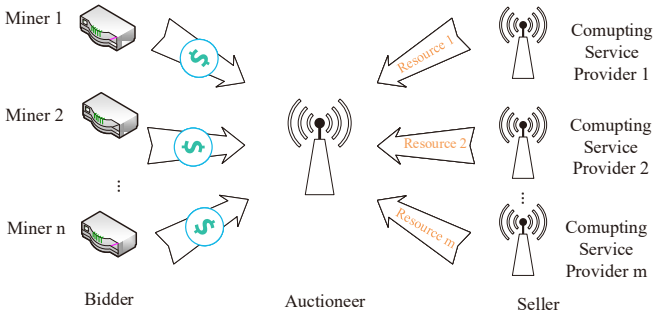


Fig. 10: A auction-based non-cooperative game model for computing resource allocation.

Using MEC in blockchain networks, the miner can offload its mining task to edge server, which can solve the limitation of computing resource of blockchain users to extend the blockchain application in wireless scenarios effectively. To encourage the miner to offload reasonably and motivate edge server to process effectively, the miner should pay an amount of payment to edge server for offloading. As shown in Fig. 11, the miners will offload some mining task to mobile edge. The more computing resource the miner buy, the greater the probability of successfully minings. Stackelberg game can be employed based on the concerning of resource allocation as mentioned above. If addressing the mining task assignment (the association between edge server and miner), auction model is a common approach.

C. Case Study

In this subsection, we will use our previous work [124] as an example to introduce how to motivate honest actions of participants in blockchain-based scenarios.

In the typical MEC enabled WBN, controlled by the MEC manager, edge servers are just treated as network resources providers, including computational resources and storage resources. However, the MEC server manager may become a central node that is independent of the blockchain system, thereby undermining the distributed nature of the blockchain system and further damaging its security. To this end, in this example, the underlying P2P network consists of edge servers, who are treated as blockchain miners, undertaking blockchain functionality operations and earning transaction fees, while IoT devices are treated as blockchain users offloading transactions to blockchain with specified transaction rate requirements. As shown in Fig. 12, the blockchain users submit

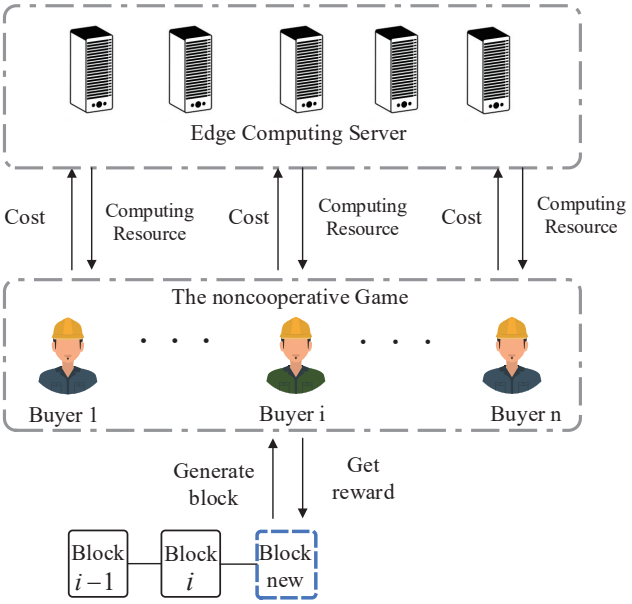


Fig. 11: A MEC-basd non-cooperative game for mining strategy

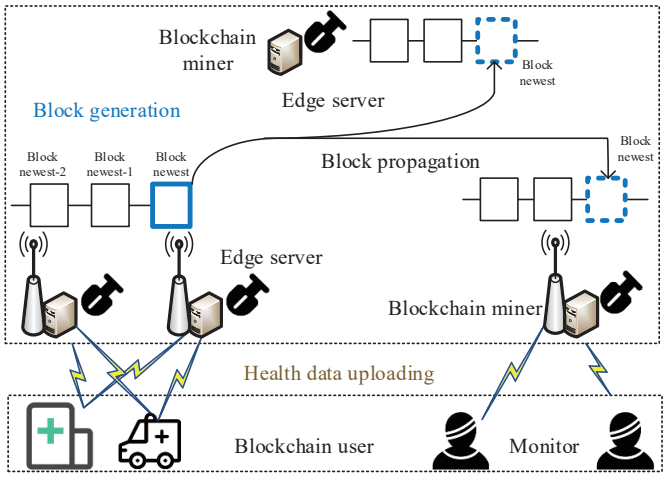


Fig. 12: The explaination of the case study in Game Theory [124]

transactions to blockchain miners, and then the blockchain miners execute the mining task and successfully generate a block. Finally, it will be added to the local ledger and broadcast to peers and this operations will also be performed by other blockchain miners once they have verified it as a valid block.

For blockchain users, the utility includes the satisfaction degree and incentive cost, i.e., the transaction fee. Thus, in order to maximize the utility by requiring considerable transaction rate γ_j, the optimization problem for f_j can be formulated as

$$\begin{aligned} \max_{\gamma_j} \quad & U_{f_j} = S_{f_j}(\gamma_j) - C_{f_j}(\gamma_j) \\ & s.t. \sum_{j=1}^{N} \gamma_j \leq \Gamma_{max}, \end{aligned} \tag{4.1}$$

where $S_{f_j}(\gamma_j)$ is the satisfaction degree, $C_{f_j}(\gamma_j)$ is the transaction fees and Γ_{max} is the maximum transaction rate blockchain system can afford.

For blockchain miners, the utility is defined as charged transaction fees minus computational resources consumption. Thus, to maximize their revenue, the optimization problem can be expressed as

$$\max_{\beta} \quad U_l = S_l\left(\sum_{j=1}^{N}\gamma_j, \beta\right) - C_l\left(\sum_{j=1}^{N}\gamma_j\right), \tag{4.2}$$

where N is the number of blockchain users, $S_l(\sum_{j=1}^{N}\gamma_j, \beta)$ is the earning by publishing $\sum_{j=1}^{N}\gamma_j$ transactions per hour and $C_l(\sum_{j=1}^{N}\gamma_j)$ is the corresponding cost of resources consumption.

With blockchain miners acting as the leader while blockchain users acting as followers, a single-leader-multiple-followers Stackelberg game can be used to model interaction between them. Based on the Karush-Kuhn-Tucker (KKT) conditions and backward induction method, a distributed algorithm can be designed to reach the optimal strategy (β^*, γ_j^*) in an iterative manner.

D. Related Work

1) Existing surveys and tutorials: Mkiramweni *et al.* in [125] provide a comprehensive review of game theory in unmanned aerial vehicle-based wireless networks. This work starts with an introduction to the basics of game theory and its relation to wireless networks. It then provides an overview of the contributions of game theory in addressing the challenges of UAVs, in terms of resource optimization, interference management, and network security. Pawlick *et al.* in [126] review the contributions of game theory in dealing with deception. Specifically, this work outlines the classical game-theoretic models used to study cybersecurity and privacy. The focus is placed on game-theoretic models applied in deception defense and shows how game-theoretic concepts capture the intrinsic differences in various deceptions. Hoang *et al.* in [127] present a detailed survey on the application of repeated games in different wireless networks. This work classifies the applications of repeated games in wireless networks based on network models. For each classification, it summarizes the contributions of repeated games in solving the major problems, including multiple access control and security for cellular and wireless local area network, energy consumption for Wireless Ad-hoc Networks, spectrum trading for cognitive radio networks.

In the domain of combining game theory and blockchain, Liu *et al.* in [33] give a comprehensive survey of game models applied to tackle important issues in blockchain. In particular, this work reviews and studies game models from three aspects: security, mining management, and blockchain applications. The security issue is further divided into selfish mining, most attacks and denial of service attacks. The mining management issue includes computational power allocation, reward distribution and pool selection. The blockchain application issue involves blockchain economy and energy trading.

2) Mining pool management: Game theory has been widely used for mining pool management. In [117], Liu *et al*. use an evolutionary game to describe the dynamic evolution of pool selection strategies for individual miners, analyze the evolution of the mining pool selection strategy considering the hash rate, and the broadcast delay of the block. In [128], Li *et al*. define the mining as a non-priority queuing problem that is determined entirely by transaction fee, and propose a transaction queuing game model to study the role of transaction fee in the consensus process. Based on this model, the authors analyze the relationship between the mining reward and the time cost, and prove the existence of Nash equilibrium. In order to improve the mining rate, the authors in [129] and [130] formulate the mining process in a PoW-based blockchain as iterative game, and apply the zero-determinant strategy to optimize the mining strategy in order to solve the miners' dilemma problem. Jiang *et al*. in [131] define and analyze the block size game to explore the relation between the miner's payoff and block sizes. Amirheckmat *et al*. in [132] first adopt a non-cooperative game to formulate the mining competition among the players in a blockchain network, and then the mean field game theory is applied to perform equilibrium analysis of mining games in blockchain networks. Chen *et al*. in [133] derive a mathematical model to describe the impact of computing power competition among mining pools on the temporary fork. Moreover, this work designs an evolutionary game framework based on temporary fork modeling to reveal the long-term trend of computing power distribution among competing pools.

3) Security strategy: Game theory is also potential to study the behaviors of blockchain users and the strategies for security concerns. Feng *et al*. in [134] introduce a risk management framework for blockchain service, and a Stackelberg game is adopted to describe the interactions among blockchain providers, network insurance companies and blockchain users. Based on this game model, the existence and uniqueness of equilibrium are discussed, and the three-party equilibrium-based strategy is analyzed to avoid the double-spending attacking. Kim *et al*. in [135] use the evolutionary game to study the dynamics of mining pool strategy, in which the pool can choose some participating miners to infiltrate into other pools to launch a block withholding attack. Based on the formulated model, the authors qualitatively analyzed the influence of malicious infiltrators on mining pool strategy and the feasibility of automatic migration among pools. Li *et al*. in [136] obtain the security conditions to achieve the design purpose of the Paxos mechanism (each node adheres to the cooperative strategy) by solving the perfect Nash equilibrium solution of each subgame in the game. Li *et al*. in [120] investigate the balance between security incentives and economic incentives in blockchain networks based on contract theory.

4) Resource management: In order to study the issues of resource management and pricing between cloud computing providers and miners, Yao *et al*. in [137] propose a multi-agent reinforcement learning algorithm to find the Nash equilibrium of the proposed model, and prove that the Nash equilibrium point of service demand in the system is related to the expected reward of each miner. Jiao *et al*. in [138] propose an auction-based model to study the interaction between miners and edge service providers, and analyze the allocation and pricing of edge computing resource in the blockchain network. Considering the reward of service providers, Luong *et al*. in [139] propose an optimal auction model using deep learning to solve service providers reward and resource management issues. Xu *et al*. in [140] study the security issues in blockchain edge networks using the game theory as well. In this work, a penalty scheme based on behavioral records is designed considering the conditions of Nash equilibriums.

Stackelberg game is a strategic game where both the leaders and the followers are typically rational and aim to maximize their own utilities. It is used to model the interaction between resource buyers and sellers. Xiong *et al.* formulate a two-stage Stackelberg game model for efficient edge resource management in mobile blockchain in [141], and a Stackelberg game formulation for price-based computing resource management in blockchain networks assisted by cloud/fog computing in [142]. Kang *et al.* in [143] use the Stackelberg game to jointly maximize the utility of blockchain users and the individual profit of miners, to incentivize miners to take part in mined block propagation to decrease consensus propagation delay. Besides, Qiu *et al*. in [144] adopt a consortium blockchain to the facilitate secure and reliable spectrum trading between mobile network operator (MNO) and UAV operators, where the Stackelberg game is used to solve the utility optimization problem for the MNOs and UAV operators. Guo *et al*. in [145] formulate the resource allocation problem in a collaborative mining network as a double auction game, and take Stackelberg game model to obtain the optimal price and resource allocation method.

E. Lessons Learned

As an analysis tool, game theory is widely used to study security, mining, and resource allocation problems in blockchain networks. A game model can be built by capturing the characteristic of the addressed problem in terms of the role of blockchain users, behavior of blockchain decision-maker and the performance of blockchain system. Thus, the game modling can help researchers understand the impact of different strategy and analyze the optimal strategy based on the equilibrium solution.

Meanwhile, some problems are still remaining to be addressed as follows.

1) To achieve the equilibrium solution, multi-round iterations in game theory are needed usually. However, the communication delay caused by the multi-round iterations, would generate a significant impact on the performance and the security of blockchain system. Therefore, it is necessary to consider communication resources consumption in the game process and develop a lightweight game theory mechanism.
2) Rationality and selfishness are the basic assumptions in game theory. However, these assumptions might be invalid especially for the malicious attacker, whose purpose is to launch an attacking to ruin the blockchain system regardless of the cost. Therefore, understanding

and studying this extremely malicious behavior is of great significance for improving security and privacy.

V. Optimization Theory in Blockchain

Optimization theory [146] [147] is a well-known computational tool to solve theoretical analysis and practical engineering issues. Generally, the goal of the optimization theory is to make the best decisions under some constraints. As a subfield of optimization theory, convex optimization [146] has been widely investigated and applied. Since lots of optimization problems can be transformed into a convex optimization, this section mainly focuses on the applications of convex optimization in blockchain. In addition, because optimization problems in the large-scale and complicated network environments are usually nonconvex, convex optimization can also be effectively applied by relaxing or/and approximating some nonconvex conditions.

A basic form of convex optimization can be regarded as a constrained optimization problem, which can be formulated as

$$\min_{x} f(x) \quad s.t. \begin{cases} g_i(x) \leq 0, i = 1, \cdots, m, \\ h_j(x) = 0, j = 1, \cdots, p, \end{cases} \tag{5.1}$$

where the objective function $f(x)$ and the inequality constrained function $g(x)$ are convex functions on R^n, and the equality constraint function $h_i(x) = a_i^T x - b_i$ must be affine.

A. Classical Issues

In this subsection, we summarize classical issues in blockchain networks that could be solved by optimization theory.

1) Security enhancement: The design of security strategies can be performed by solving optimization problems that are related to the corresponding security metrics. Various optimization methods are applied to solve different optimization problems, such as the alternating direction method of multipliers (ADMM) for optimization problems with linear constraints [148], [149], the adaptive moment estimation (Adam) for non-convex optimization problems with large data sets and high dimensional space [150], and the adaptive gradient algorithm (AdaGra) for sparse gradient problems [151]. Besides, Optimization theory with dynamic reward and punishment mechanisms can also be utilized to avoid malicious node aggregation.

2) Resource allocation: Resource allocation strategies can be improved by using optimization theory to quantify the relationship among essential factors in blockchain networks. Specifically, an optimization problem that describes the relationship between the optimization objectives and constraints can be formulated by abstracting the factors that affect resource allocation. Then, the optimal allocation strategy can be obtained by solving the optimization problem with the corresponding methods.

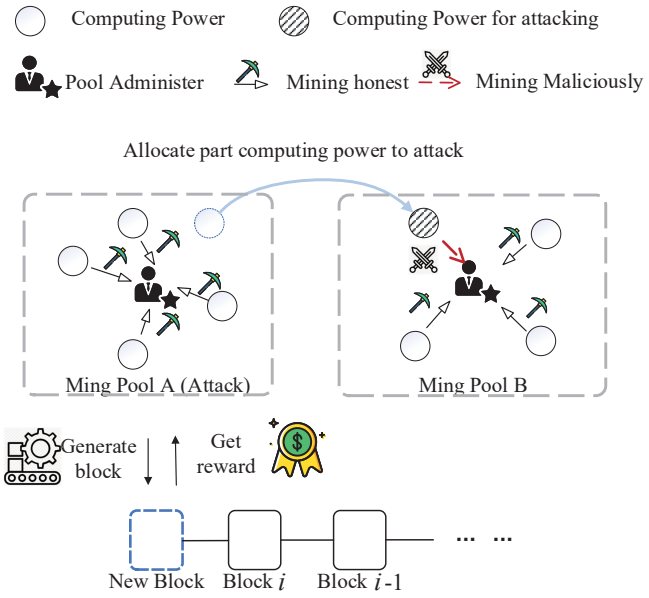


Fig. 13: The explaination of BWH attack.

B. Model Briefs

As well known, the mining reward for miners is an important factor to encourage the contribution of computing resource. Optimization theory provides solutions for mining management by maximizing the reward and promoting the accomplish of the consensus process. In order to increase the successful mining probability, miners usually choose to join the mining pool. Generally, as long as any miner in the pool succeeds in mining, the mining reward will be distributed to each miner in the pool. Different mining pools may adopt different reward mechanisms. Therefore, the miner should consider how to choose the optimal pool selection strategy to maximize its reward, and this problem can be transformed into a mathematical optimization problem. For this optimization problem, the mining reward obtained by miners under different reward mechanisms can be formulated as the objective function, the variable is the miner's pool selection strategy, and the constraints are determined by the actual situation. Through this mining pool selection optimization problem, we can study the impact of different reward mechanisms on the blockchain network in term of the objective function, and determine the optimal selection under the constraints.

When miners join the mining pool and cooperate with others, the competition among miners becomes the competition among the mining pools. In order to win for mining reward, some mining pools may choose to take the Block Withholding (BWH) attacking on other mining pools. As shown in Fig. 13, the pool A will allocate a part of computing power α to another pool B for attacking. The greater computing power consumed by the attacker, the greater the malicious impact on other pools would be happened. The malicious impacts would decline the computing power for consensus and is costly to the attacker itself. As a result, the attacker should choose the optimal computing power for attacking, which can be considered as an

optimization problem. In this case, the objective function is to maximize the mining reward as well as successful attacking probability with the computing power for attacking as the variable. Through the optimization analysis, we can know the optimal attacking strategy, which is the baseline to analyze and design the consensus process for security based on the understanding the malicious action of the attacker.

As discussed before, mining task offloading from the miners to the edge servers can be also formulated as an optimization problem with resource allocation. In this case, the miner should choose an appropriate offloading strategy to determine whether to offload, or to which edge server to offload, and how many resources (computing, communication and cache) the edge server allocates to the offloading task. Using this optimal offloading formulation, we can analyze the impact of the offloading on the performance and security of the blockchain network, and the optimal solution is to provide a theoretical guidance for the blockchain development and application.

C. Case Study

In this subsection, we use the previous work [152] as an example to introduce how to perform optimization in blockchain. In this work, to improve the security and privacy of D2D (device to device) communication, the authors introduce a new distributed and secure data sharing framework called D2D blockchain. The simplified procedure for transaction relaying and block verification is shown in Fig. 14. In this framework, the authors deploy a series of Access Point (APs) to incentivize the transaction relay and block verification using DPoS-Based Lightweight Block Verification Scheme. Therefore, an important problem for AP is that how to improve the efficiency of transaction relaying and DPoS based block verification, while the payment (cost) is small.

In this work, a two-stage contract theory based on joint optimization scheme is proposed, where the AP serves as an employer who designs all kinds of contracts, pays rewards for employees, relays devices, and verifiers serve as employees. Relay devices should consider their battery energy, resource of occupied bandwidth, etc., and verifiers should consider their CPU cycles, energy consumption, etc. In order to maximize the expected utility of AP while satisfying the individual rationality and the incentive compatible constraints for transaction relaying and block verification, the objective function in the optimization problem is formulated as

$$\begin{aligned} \max_{\substack{R_{TR,s},V_{TR,s}\\ R_{BV,q},V_{BV,q}}} \quad & U_{AP} = V_R - R_R + V_V - R_V \\ s.t. \quad & \{a,b,c,d,e\}, \end{aligned} \tag{5.2}$$

where the limiting conditions $\{a,b,c,d,e\}$ are respectively expressed as

(a) For each relay device, the reward paid from AP should be not less than its cost due to the rationality.
(b) Similarly, for each verifier, the reward paid from AP should be not less than its cost due to the rationality.
(c) AP needs to design the contract for the relay device or verifier flexibly according to their corresponding types.

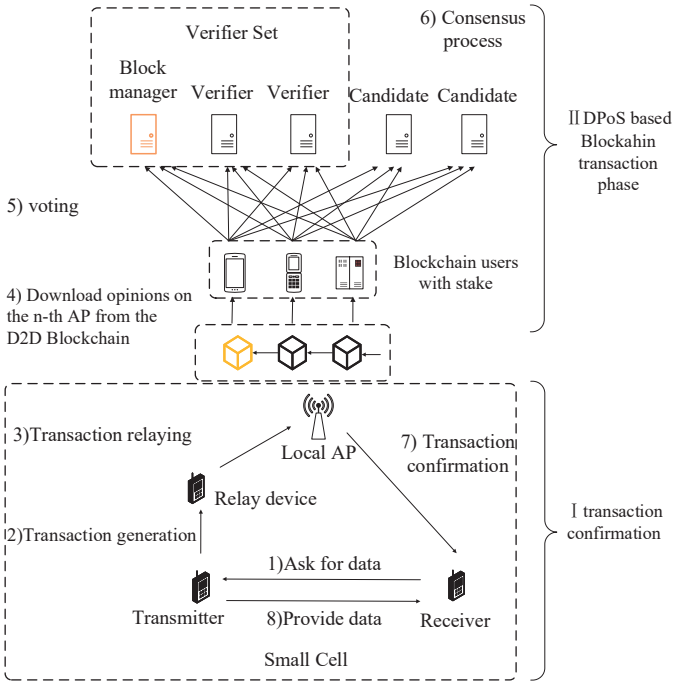


Fig. 14: The simplified procedure for transaction relaying and block verification [152]

(d) Similarly, AP needs design the contract for the verifier flexibly according to their corresponding types.
(e) For AP, the reward paid to relay devices and verifiers must be reasonable following a limitation.

Here $R_{TR,s}$ and $R_{BV,q}$ are relay fee to type-s relay device and transaction fee to type-q verifier, respectively. $V_{TR,s}$ and $V_{BV,q}$ present the required value of transaction relaying and block verification, respectively. V_R is the whole value of transaction relaying created by all the relay devices, and R_R is the whole payment from AP to relay devices. Similarly, V_V is the whole value of block verification created by all the verifiers, and R_V is the whole payment from AP to verifiers.

However, to solve the optimization problem in a practical system, the constraint conditions often are set to non-convex, and thus (5.2) cannot be solved directly. By reducing some constraints, this optimization problem can be transferred into a convex problem. Finally, the optimal solution is the best strategy for transaction relaying and block verification, which can maximize the utility of AP while incentivizing the relay devices and block verifiers to accomplish their tasks optimally.

D. Related Works

1) Existing surveys and tutorials: Sun *et al*. in [153] summarize the optimization problems and classical optimization methods. This work first details the underlying theory of optimization methods while introducing the research progress of optimization algorithms in recent years. Then, application of optimization methods are discussed, and some approaches to improve their performance are presented. Integrating ensemble strategies into population-based optimization algorithms (POAs) can ease computationally intensive offline tuning for

a given optimization problem. Therefore, Wu *et al*. in [154] review the application of ensemble strategies to POAs, as well as discuss other similar schemes. Molzahn *et al*. in [155] first summarize distributed algorithms for offline solution of the optimal power flow (OPF) problem, and then outline the applications of offline distributed optimization and control algorithms in power systems. In addition, this work presents an overview of the progress of online optimization and control algorithms, such as real-time solving OPF and optimal frequency control. Yang *et al*. in [156] bring a survey of distributed optimization algorithms. This work starts with outlining discrete-time and continuous-time distributed optimization algorithms for undirected graphs. Then potential options for extending these algorithms in different directions are discussed. In addition, the application of distributed optimization to the optimal coordination of distributed energy sources is emphasized. Those efforts can also provide a reference for applying optimization theory in blockchain with distributed properties.

2) Security: As one of the most important issue in blockchain, the security topic has been widely formulated as an optimization problem. Onireti *et al*. in [157] propose a practical modeling framework for PBFT, and the viable area for the wireless PBFT network is defined to ensure the minimum number of replication nodes required for protocol security and activity. Considering the secured communication and data sharing between vehicles, Kang *et al*. in [158] propose a two-stage security enhancement solution to solve collusion attacks in IoV. In the first stage, the system selects active miners and standby miners (candidates) based on reputation voting. Hence, the active miners selected get the chance to generate block. In the second stage, standby miners will verify the block generated by active miners. Therefore, the internal collusion among active miners is avoided. However, how to incentivize the standby miners to participate is an important problem, which is solved using contract theory. Saad *et al*. in [159] model the malicious behavior as a Lyapunov optimization problem. Then they study how attacker uses the impact of memory pool overflow on blockchain users to launch an DDoS attacking. To prevent DDoS attacks, the authors propose two effective countermeasures: fee-based and age-based design. The core of the fee-based design is to conduct transaction relay with minimum relay fee to reject spam transactions. Similarly, the core of the age-based design is to compare transaction mining fee and minimum mining fee. While spam transactions are rejected, the DDoS attacks are also resolved. Sharding mechanism is an effective way to enhance the scalability of blockchain, but also its security remains a debatable issue. Cai *et al*. in [160] design a multi-objective optimization algorithm based on a dynamic reward and punishment mechanism to hinder malicious node aggregation, thus improving blockchain sharding security. Although permissioned blockchains are conducive to the rapid implementation of the consensus mechanism, pre-selected miners are susceptible to arbitrary manipulation by attackers and might become compromised miners. Therefore, Kang *et al*. in [161] present a universal credit-based secure miner selection scheme to prevent compromised and misbehaved miners from participating in the consensus process.

3) Resource allocation: Considering the high-resource consumption, MEC is a nature design for the blockchain-enabled wireless networks. Wu *et al*. in [162] convert the computing resource allocation problem in multi-access MEC-based blockchain into a mathematical form of joint optimization problem. To maximize the total revenue of the mobile terminals while ensuring the fairness of the mobile terminals, they consider two different scenarios, namely a single-edge-server scenario and a multi-edge-servers scenario. For the two scenarios, the authors propose two layered algorithms to solve the non-convex optimization problem above. Fu *et al*. in [163] study the issue of joint resource allocation in blockchain-based IoT systems. To maximize the system energy-efficiency, the authors use stochastic programming to solve the joint optimization problem above. Wang *et al*. in [164] design a blockchain-based framework for mobile device cloud (MDC), which enable the decentralization and prevented dishonesty by incorporating a plasma-based blockchain into the MDC. Different smart contracts are designed for distributed management of worker registration, task allocation, rewards and penalties. Xiong *et al*. in [165] adopt ADMM algorithm to search the optimal solution for the benefit of miners and cloud/edge providers. In terms of sharding cache system optimization, Lorenzo *et al*. in [166] focus on two important metrics, load balancing and caching performance, in a sharding system. This work first studies the factors that cause load imbalance in a sharding system and then analyzes how sharding affects cache hit performance. Based on those research results, the sliced system's load balancing and cache performance are investigated to reveal the operational characteristics of the sliced cache system.

4) Optimal algorithm and strategy design: The optimization problem can be also used to describe various purposes in blockchain system. Zhang *et al*. in [167] study the routing issue in a blockchain-based payment channel network. The authors analyze the payment routing problem using the convex optimization method. While considering the constraints of timeliness and feasibility, the authors propose a distributed optimization scheme to achieve the lowest total transaction costs from the sender to the receiver. Applying the consortium blockchain technology to electric taxi charging scenarios with multiple operators, Zhang *et al*. in [168] propose a new Byzantine fault tolerance algorithm to address the problem of trust among operators of charging stations. In addition, this work designs a system model based on multi-objective optimization to maximize operating efficiency and customer satisfaction while minimizing the time and distance costs of electric taxis. Jin *et al*. in [169] propose EdgeChain, a blockchain-based architecture to make mobile edge application placement decisions for multiple service providers. Blockchain is used to store all placement transactions, which can be traceable by every mobile edge service providers and application vendors who consume resources at the mobile edge.

E. Lessons Learned

For blockchain system, the mathematical optimization tool is typically introduced to find the best pool selection strategy

for miners to determine the best task offloading strategy, and to allocate resource for consensus process. Although existing researches show that the optimization theory can achieve the better system performance and security, some problems should be further studied in the future.

1) The optimization problem and corresponding solution are usually for a specific situation in static or semi-static state. However, the practical blockchain system is dynamic and stochastic with some important parameters and constraints that are uncertain and might be changed over time and space. Therefore, these uncertainties should be further considered in optimization formulation.
2) Due to the complexity of blockchain system, the solution to the formulated optimization problem might be challenging. For example, the original problem should be transformed into a standard convex problem, decomposed into multi-subproblem, or design an iterative approach to achieve a sub-optimal solution instead of the optimal one. Therefore, in such scenarios, how to balance the accurate description of dynamic states and performance (like quality, convergence speed and overhead) of obtained results should be further considered. In another word, some basic assumptions and simplifications with some typical mathematical properties are necessary especially for problem formulation and analysis, but they cannot describe the actual blockchain system accurately.

VI. Machine Learning in Blockchain

Machine learning [170] [171] is a method of designing and analyzing algorithm to "learn" automatically, which allows computers to analyze from a large amount of data, find out the hidden laws for prediction or classification based on characteristics of data. Machine learning usually involves the algorithms of supervised learning [172], unsupervised learning and reinforcement learning [173], and the models of Surport Vector Machine (SVM) [174], Random Forest (RF) [175] and Deep Learning (DL) [176] [177]. Those models and algorithms mentioned above are widely used in the analysis, prediction, and optimization of communications and networking. Supervised learning is to train labeled data and analyze the training data to solve classification and regression problems. In contrast, unsupervised learning trains data with no labels to achieve clustering or dimensionality reduction by finding similarities or internal relationships in the data. Different from supervised/unsupervised learning, reinforcement learning is mainly used to solve decision-making problems in a trial-and-error process based on the interaction and feedback between the agent and environment. SVM discriminates two classes by fitting an optimal linear separating hyperplane to the training samples of two classes in a multi-dimensional feature space [178]. Random forest is a more accurate and stable model obtained by building multiple decision trees and fusing them together, with the advantage of high accuracy and efficient operation [179], which is suitable for the case of non-differentiable model with discrete features and limited values. Deep learning allows computational models that are composed of multiple processing layers to learn representations of data with multiple levels of abstraction [180]. It involves AtuoEncode, Variational Auto-Encoder and Generative Adversarial Network based on unsupervised learning, Deep Neural Networks, Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN) based on supervised learning [181]. It is based on basic features and uses multi-layer activation functions to learn high-dimensional nonlinear features, including CNN networks suitable for image domains, RNN networks suitable for time series and WiDE & Deep networks suitable for recommendation domains, etc [182].

A. Classical Issues

The combination of blockchain and machine learning is a promising approach to achieving decentralized, secure, intelligent, and efficient network operation and management. Machine learning is a powerful tool for blockchain to handle huge amounts of data and various types of transactions. Here, we classify the contributions of machine learning to blockchain in the following categories.

1) Security enhancement: Machine learning can provide blockchain with intelligent means of detecting anomalies. In particular, machine learning can be applied to identify attack types and malicious nodes by monitoring and classifying the motives of participants, thus effectively preventing attacks [183]–[186].

2) Performance improvement: Machine learning empowers the blockchain efficiency and stability more brilliantly for resource allocation, block size setting, and transaction scheduling through efficient and fast Besides, a viable approach can be provided by machine learning for adaptive consensus mechanism selection in specific application environment due to its speedy computation and prediction.

B. Model Briefs

In recent years, machine learning has been widely used in pattern recognition [187], data mining [188], etc., due to its capabilities in data management, analysis, and decision-making. In blockchain, machine learning can provide an efficient and intelligent approach to discover the malicious action and recognize the attacks to guarantee the data reliability, system security and user privacy.

Malicious attackers can launch double spend attacking [189], denial of service attacking, and eclipse attacking on the blockchain network, which will cause the deteriorated security risk. In recent years, machine learning is introduced in blockchain to solve security problems. By using unsupervised/supervised learning algorithms such as the K-means algorithm and supervised SVM, we can monitor the transaction in consensus process and the behavior of blockchain users [190]. Accordingly, as shown in Fig. 15, we can learn the characteristic of both honest and malicious actions, identify suspicious transaction, and malicious attacker or illegal activity in the network, which can reduce the possibility of successful attacks. Nowadays, the resource consumption is an barrier for blockchain applications, especially in the case which is

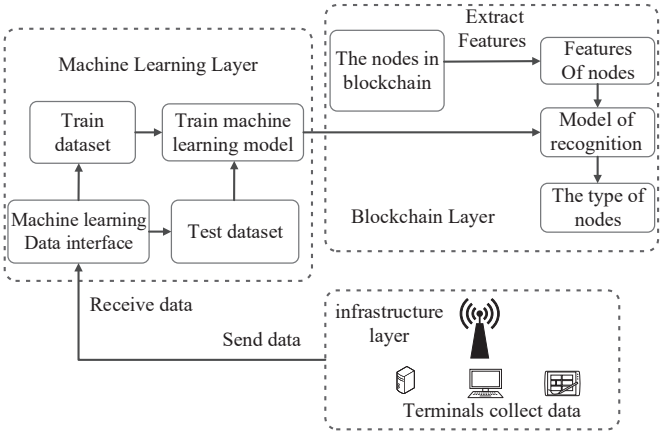


Fig. 15: Using machine learning to recognize the type of blockchain nodes.

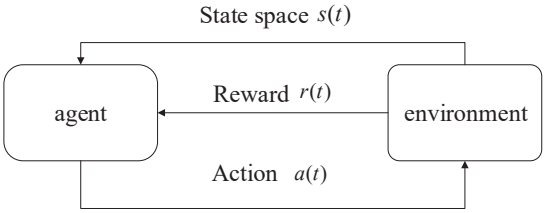


Fig. 16: The explaination of the interaction and feedback between agent and environment in a machine learning manner.

resource-limited such as the IoT device in the wireless network [14]. Therefore, it is necessary to consider the energy-saving in mechanism design and resource allocation. To develop an optimal strategy, we can define the state space $s(t)$, the action space $a(t)$, and the reward function $r(t)$ to represent the agent, environment, and the feedback between them in a machine learning manner [191]. The interaction among $s(t)$, $a(t)$ and $r(t)$ is shown in Fig. 16. In a real environmental transformation, the probability of going to the next state $s(t+1)$, is related to both the current state $s(t)$ and the previous state $s(t-1)$, occasionally related to even earlier state $s(t-2)$, so that the environmental transformation model may be too complex to model. Therefore, the way to simplify the environmental transformation model of reinforcement learning is to assume the markov property of state transformation: the probability of transformation to the next state $s(t+1)$ is only related to the current state $s(t)$, and has nothing to do with the previous state [192]. Accordingly, to maximize the long-term reward, the optimal strategy determination considering the interaction and feedback over time can be treated as a Markov decision process, and it is able to be achieved using reinforcement learning or deep reinforcement learning algorithms.

In addition, blockchain is a potential solution to the problems in machine learning. Most typically, the decentralized feature of blockchain can be used to solve the problem of single point of failure caused by aggregating machine learning models using centralized servers.

C. Case Study

In this section, the previous work [193] is used as an example to illustrate the benefits of the combination of blockchain and machine learning.

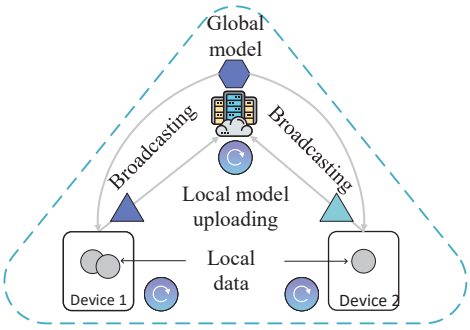
FL as a promising training paradigm, was proposed by Google to tackle the privacy and security problems of centralized machine learning and to alleviate the communication load of the core network [194], [195]. As shown in Fig. 17 (a), many devices collaborate in solving a machine learning problem by updating the local model with their own local data, under the coordination of the centralized FL server. However, the traditional FL, which relies on a centralized FL server for model aggregation is vulnerable to experience service paralysis even when a single point of failure happens. All local models updated from devices will be distorted by the inaccurate global model aggregated at the FL server. In addition, for some devices with massive amounts of data, if there is no credible incentive mechanism, they are usually unwilling to participate in training, which brings great challenge to the rapid convergence of the FL model.

To address the problems mentioned above, H. Kim proposed a blockchained FL (BlockFL) architecture, which is shown in Fig. 17 (b). With the distributed and non-tamperable characteristics of the blockchain, the use of a blockchain network instead of the centralized FL server can effectively overcome the issue of single point failure. The model parameters uploaded by the devices are taken as the transactions, and will be recorded in the candidate block after being verified by the associated miner. After all miners reached a consensus, devices can obtain the latest global model by aggregating the local model updates contained in the newly generated block downloaded from the associated miner. Generally, the global model is aggregated anywhere as long as the latest block can be obtained. In addition, the data reward for devices will be issued by the associated miner according to the size of the device data sample; the mining reward for miners will be issued by the blockchain network according to the total volume of data used by the connected devices. With the reasonable incentives, the blockchain-based FL can be positively driven for efficient training.

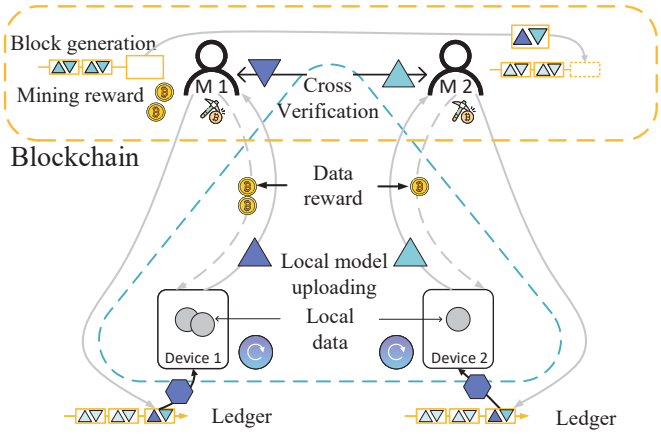
Due to the decentralized architecture of BlockFL, the malfunction of each miner only distorts the global model of its own devices instead of paralyzing the entire system. Moreover, such distortion can be recovered by interaction with other regular miners or federating with other devices associated with regular miners. Besides, by optimizing the block generation rate, the time for BlockFL to complete the model training can be reduced and the performance of the system can be improved.

D. Related Works

1) Existing surveys and tutorials: Baltruaitis *et al*. in [196] review research advances in multimodal machine learning in terms of the core technical challenges of multimodal machine learning. Olowononi *et al*. in [197] investigate the



(a) Traditional FL



(b) BlockFL

Fig. 17: (a) The structure of traditional FL; (b) The structure of the proposed BlockFL [193]

applications of resilient machine learning in resilient cyber-physical systems. This article focuses on the vital role of machine learning in enhancing the security and resilience of information-physical systems, especially adversarial machine learning. In addition, common machine-learning methods, as well as their application scenarios, are presented. Luong *et al*. outline deep reinforcement learning in communications and networking in [198]. This article begins by providing a concise tutorial on deep reinforcement learning. In contrast, Bout *et al*. in [199] do not focus on the contribution of machine learning in enhancing system security schemes, but on machine learning-based intelligent attack schemes, especially in the IoT scenario. Attacks constructed based on different machine learning methods are reviewed. Based on this, future research directions are presented in terms of jamming, adversarial machine learning attacks, side channels, and false data injection.

For the integration of blockchain and machine learning, Wu *et al*. in [200] give an overview of the application of blockchain and machine learning in the industrial IoT regarding consensus mechanisms, storage, and communication. Importantly, this work provides a more in-depth insight into blockchain security and privacy risks from a machine learning perspective. Dibaei *et al*. in [201] present a survey to explore how the combination of blockchain and machine learning can improve the performance of vehicular networks. It investigates the contribution of using blockchain technology to enhance the security of vehicular networks, such as secure data storage, transmission, and secure access mechanism design. In addition, this work discusses machine learning methods for vehicular networks in terms of the application, topology and technical dimensions. Nguyen *et al*. in [202] review the fundamentals of federated learning and blockchain, as well as discuss the potential of blockchain-based federated learning in MEC networks, such as edge data sharing, edge content caching and edge crowdsensing. Especially this survey identifies the crucial issues in the integrated design of FL and blockchain, including resource allocation, security and privacy protection, communication cost, etc.

2) Security: Due to the capability of learning, analyzing and classifying, machine learning is used to monitor behaviors and to detect the malicious attack for the blockchain security. Dey *et al*. in [190] combine machine learning and game theory to solve the majority-attack problem. In this work, the activities of attackers and participants in the network are monitored to judge and classify both participants' motivation and the service value in transactions, and then detect network anomalies. Therefore, the probability of majority-attack will be reduced. Tang *et al*. in [203] introduce a deep learning-based algorithm to identify and classify malicious nodes by classifying behavior patterns in the network. The proposed algorithm can reduce the probability of the blockchain network being attacked by malicious nodes. In order to detect anomalies (such as DDoS, double-spend and denial-of-service attacks) in electronic transactions of Bitcoin, Sayadi *et al*. in [204] propose an anomaly detection model based on machine learning. Experimental results show that the proposed model can accurately identify the types of attacks, and can provide the theoretical guidance to improve the security of the electronic trading system based on Bitcoin. Thai *et al*. in [205] focus particularly on the anomaly detection to the Bitcoin transaction network, with the goal of detecting suspicious users and transactions. Shin *et al*. in [206] propose a clustering method for bitcoin block and transaction data analysis, which defines the data that can be collected from the Bitcoin network, and the statistics of the blocks that can be extracted from the collected data. In addition, this work performs a clustering experiment by applying Principal Component Analysis (PCA) to the extracted data, and also testes how to apply PCA to the clustering data. Khan *et al*. in [207] propose a blockchain-based deep extreme learning machine to implement intrusion identification and prediction. This lightweight algorithm is efficient and adapts to the power and processing limitations of smart home devices. Liu *et al*. in [208] propose a collaborative intrusion detection mechanism based on distributed FL and blockchain. In this work, distributed FL is employed to reduce the single point of failure probability and enhance user data privacy, while blockchain guarantees the security of the training model.

3) Performance improvement: Machine learning is widely used for performance improvement of the blockchain systems. To meet the great demand of the blockchain, the solution need

to be found for the scalability problem. Nowadays, sharding method is found to resolve the scalability problem of the blockchain. Bugday *et al*. in [209] propose a method which uses adaptive machine learning model and Verifiable Random Functions together to assign nodes to achieve shards. As sharding method solves the scalability problem, the performance of the blockchain is improved. In order to optimize the system performance of the blockchain-based IoV, Liu *et al*. in [210] use deep reinforcement learning to select the consensus algorithm and the block generated nodes, as well as adjust the block size and the interval between block generations. The solution proposed can be applied to the dynamic IoV scenario, and it can maximie the system throughput without affecting the system's decentralization, latency and security. Hao *et al*. in [211] establish a trust-enhanced blockchain P2P topology (BlockP2P-EP) that considers the transmission rate and transmission reliability to improve the performance of the blockchain network in achieving fast and reliable broadcasting. BlockP2P-EP first uses K-means to cluster neighboring peer nodes. Then on top of the trust-enhanced blockchain topology, BlockP2P-EP executes the parallel spanning tree broadcasting algorithm to achieve fast data broadcasting among nodes in terms of intra- and inter-clusters.

In addition, machine learning has been applied with blockchain together to improve communications and networking, as discussed and analyzed in several forward-looking works. Hu *et al*. in [212] propose a novel architecture for dynamic resource sharing to improve resource utilization, where blockchain is for system security in a decentralized manner, and deep reinforcement learning is for improving the performance of pattern recognition and decision-making. Kang *et al*. in [213] integrate federated edge learning with blockchain to guarantee security and privacy. Especially, federated edge learning is adopted to collaboratively train globally shared models without revealing participants' private raw data. At the same time, blockchain is employed to store the training records and manage reputation data to avoid involving unreliable edge devices in training. Li *et al*. in [214] propose a multi-agent deep reinforcement learning method to improve the long-term performance of computation offloading in PoW-based blockchain.

4) Application in vertical industries: Since data transmission is affected by dynamics and uncertainties in blockchain-enabled IoT systems, Xiong *et al.* in [215] present a learning-assisted resource allocation method to support intelligent data transmission. In this work, deep reinforcement learning algorithm is used to directly sample the current and historical transaction data and output to determine deep-Q network weights and optimal actions without checking the whole extensive sets of system states and actions. In order to implement blockchain technology into IoT fields and achieve the condition-based management on the blockchain, Id *et al.* in [216] applies blockchain and machine learning into the task of anomaly detections in the IoT. To ensure the performance of data aggregation, data storage, and data processing in IoT services, Luong *et al.* in [217] use blockchain to support IoT services which is based on cognitive radio network. To help IoT devices to choose an optimal transaction transmission under intricate conditions, the authors get an optimal transaction transmission policy for secondary users by adopting a double deep-Q network algorithm that can allow the secondary users to learn the optimal policy above. Yao *et al*. in [137] introduce blockchain and cloud computing into IoT to offload computational task from the IIoT network itself. In order to simultaneously meet the requirements of IIoT for security and privacy, Qu *et al*. in [218] leverage federated learning with privacy protection to break data island and enhance system security through the decentralized property of blockchain. He *et al*. in [219] adopt blockchain to ensure IoT data security and reliability and use asynchronous advantage actor critic to solve the problem of multi-user edge resource allocation with different QoS requirements. To address the fact that heterogeneity and lack of trust among IoT nodes hinder the efficiency and security of machine learning results, Qiu *et al*. in [220] employ lightweight IoT nodes to train parts of the learning layer, then sharing the learning results using blockchain.

5) Application in smart grid: To protect the smart grid from suffering cyber attacks, Ferrag *et al*. in [221] propose a deep learning and blockchain-based energy framework, consisting of two schemes: a blockchain based scheme and a deep learning-based scheme. The blockchain-based scheme is used to facilitate the exchange of excess energy among neighboring nodes. The deep learning-based scheme is used to detect attacks and fraudulent transactions to enhance the system reliability and security. Jamil *et al*. in [222] propose a blockchain-based smart energy trading platform designed to facilitate peer-to-peer transactions between producers and consumers. Machine learning is used to implement an energy prediction analytic module for predicting short-term energy consumption to minimize the cost of electricity to consumers. Lalle *et al*. in [223] employ blockchain and machine learning to guarantee the data privacy of smart water grid users. First, k-means++ is used to partition users into clusters, and then a private blockchain is adopted to store user data of each cluster.

6) Application in VANETs: For the problem that the data collected by different entities in the vehicle social network usually contains very different attributes, Shen *et al*. in [174] propose a privacy-preserving SVM classifier training scheme over vertically-partitioned datasets possessed by multiple data providers. In addition, consortium blockchain and threshold homomorphic cryptosystem are used to establish a secure SVM classifier training platform without a trusted third-party. To improve the security and reduce the attack in the vehicular ad hoc networks (VANETs), Dai *et al*. in [224] propose an indirect reciprocity security framework. This framework tries to encourage the On Board Units (OBUs) to help each others to reduce attacks, and apply the blockchain technique to protect the reputation from being tampered. Liao *et al*. in [225] develop a secure and intelligent task collaboration framework. In this work, an intelligent task offloading algorithm based on online learning is designed to minimize the average task offloading delay and blockchain is used to achieve safe task offloading.

E. Lessons Learned

A number of works have shown that using machine learning in both data management and analysis can effectively monitor and classify the behavior of blockchain users, as well as recognize malicious behavior, suspicious user and illegal activity in the system, and therefore both reduce the possibility of attacks and optimize the performance of system. Comparing with the traditional method of optimization or game theory, machine learning can adjust its strategy according to the changing of environment based on the long-term reward maximizing. However, there are still two existing problems that should be further investigated.

1) Machine learning is valuable to understand the process and behavior in blockchain to optimize system performance and security (such as the transaction processing speed and malicious attack recognition). However, how to use the ability of machine learning in management, analysis and prediction to provide an intelligent guideline for decision-making and mechanism design is still an open issue.
2) Blockchain has great potential in improving the security and credibility of machine learning due to its decentralized characteristics, especially distributed machine learning such as FL. However, it is difficult to handle the large-scale machine learning tasks due to the huge resource consumption, limited throughput and high communication complexity. Therefore, it is necessary to further study how to break through the limitations in blockchain mentioned-above, in order to achieve the balance between the advantages and defects for blockchain in machine learning.

VII. Discussion and Open Issues

For brevity, references supporting the above discussion are summarized and classified in Table IV. Furthermore, some remaining problems in terms of cryptography, smart contracts, blockchain architectures and protocols, commercial and political views are still needed to be discussed as open issues and future work.

A. Cryptography

Cryptography is the basic theory of blockchain and has been widely used to guarantee the security of transactions and the privacy of user information. As for the privacy issue caused by data stored in the blockchain, some schemes can be adopted involving of public key encryption scheme with keyword searchable, anonymous digital certificate publishing scheme, and ZKP. Homomorphic encryption technology enables data processing security in the blockchain, in the meantime, we can apply cryptography for access control and authentication in the blockchain systems, such as shown in Fig. 18.

Moreover, several surveys and tutorials have reviewed the background, application, development and challenges of cryptography [227], [228]. Especially, Q. Feng *et al.* in [229] present a concise tutorial on blockchain privacy threats, cryptographic defense mechanisms and typical approaches for

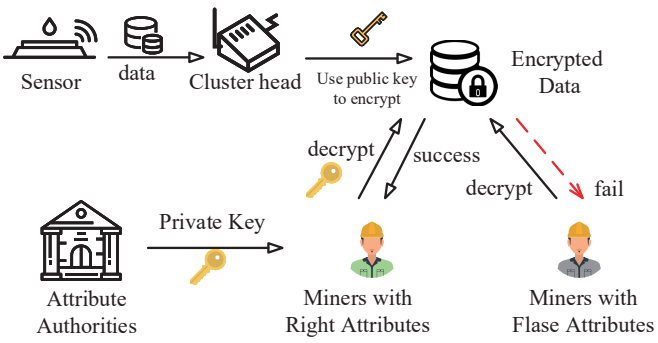


Fig. 18: Cryptography theory for access control and authentication in blockchain systems

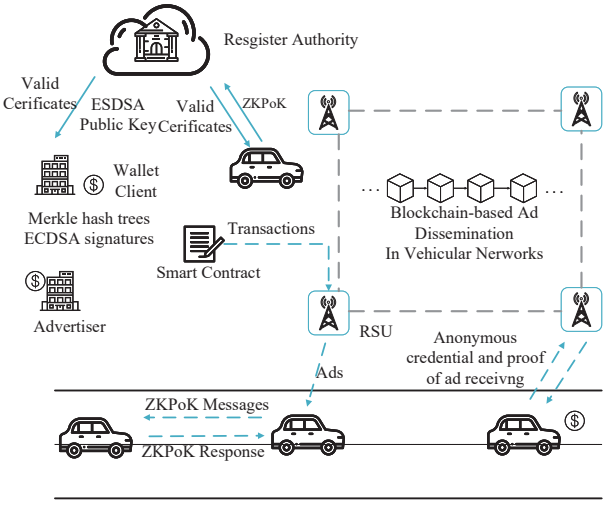


Fig. 19: The blockchain-based AD Dissemination framework [230]

privacy-preserving in blockchain. A previous work [230] introduced the application of cryptography in blockchain, it solves the vehicle privacy problem of the blockchain-based vehicular networks, by using Zero-knowledge proof of knowledge (ZKPoK) to propose a new blockchain-based ad dissemination framework which is shown in Fig. 19.

We further divide most of the existing efforts into 5 categories, including security schemes about hash-based signatures [231], [232] and fork in blockchain [233] , privacy, which includes user privacy and data privacy [234]–[237], ZKP protocols [238]–[241], verification methods [242]–[244] and solutions to nonsupervisability [245], [246].

These efforts proposed some key methods which focus on security and privacy protection in an external manner, and are to design a powerful wall around the blockchain system to deny the attacks from malicious users. However, the system would be vulnerable if any bugs found by the attacker to break. Therefore, how to empower the security and privacy ability of blockchain system in a systematic manner providing inherent safety is still an open issue. Moreover, the mechanism and

TABLE IV: Reference classification on methodology perspective

Method \ Research category		Theoretical model	Network service	Application
Stochastic	Markov process	selfish mining [102], modeling and performance analysis [103] [91] [104] [106]	-	performance and security analysis in IoT [93], in healthcare [107]
	Poisson process	mining difficulty control [92] [99]	-	node deployment in IoT [110], node deployment in MEC [111]
	Stochastic geometry	-	-	node deployment in IoT [109]
	Others	modeling and performance analysis [100] [101]	optimal strategy design [105]	-
Game theory	Stackelberg game	- [141] [142]	incentive mechanismin [124] [143], security strategy in network [134], resource management in MEC [137] [141] [142]	spectrum trading [144]
	Evolutionary game	mining pool management [117] [133], mining pool security strategy [135]	-	-
	Iterative game	mining pool management [129] [130]	-	-
	Auction	-	resource management in MEC [138] [139]	-
	Others	mining pool management [128] performance analysis [131] mining competition analysis [132] security condition acquisition [136] [226]	security in edge networks [140] resource allocation [145]	-
Optimization theory	Convex optimization	-	security in D2D communication [152]	-
	Geometric programming	-	resource allocation in IoT [163]	-
	Stochastic programming	-	optimal algorithm and strategy design in mobile edge network [169]	-
	Lyapunov Optimization	DDoS attack avoidance [159]	resource allocation in mobile device cloud [164]	-
	Others	analytical framework modeling for PBFT [157] sharding security [160] performance analysis [166] [165]	security [158] [161], resource allocation in MEC [162], optimal algorithm and strategy design in payment channel network [167]	optimal algorithm and strategy design in electric taxi charging scenarios [168]
Machine Learning	Supervised learning	majority-attack avoidance [190]	-	-
	Unsupervised learning	performance optimization [211]	security in Bitcoin [204] [205] [206]	energy trading [222] data privacy [223]
	Federated learning	-	privacy and security in centralized machine learning [193] intrusion identification [208] privacy protection [218] [213]	-
	Deep learning	identify malicious nodes [203]	-	application in IoT [217], application in smart grid [221]
	Reinforcement learning	-	resource management in IoT [137]	-
	Deep reinforcement learning	performance optimization [214]	security enhancement [224] [215] resource sharing [212]	performance optimization in IoV [210]
	Others	-	sharding management [209], collaborative anomaly detection in IoT [216]	SVM traning platform for VSNs [174] data security in IoT [219] [220] task collaboration [225]

protocol should be designed to optimize the performance as well as security simultaneously.

B. Smart Contract

Nowadays, there are many blockchain platforms supporting the deployment of smart contracts such as EOS, Fabric, Zcash, etc. The comparison of blochchain system which supports smart contract system is showing in Table V.

For widely application and development of blockchain, smart contract is the most important function to help users/consumers operating the whole system from top to down easily. However, smart contract is not powerful and effective currently, there are some obvious drawbacks should be investigated and improved in the future work shown as follows.

- **Blockchain limitation:** Since the majority of smart contracts are triggered by the corresponding transaction, the TPS capability of blockchain is the most fundamental factor affecting the corresponding performance. Accordingly, some solution in terms of hierarchical architecture, shard scheme and high-capacity consensus mechanism need more research. In addition, smart contracts need frequent adjustments and rapid updates due to various reasons in automated and decentralized applications, such as inevitable code bugs, application changes, or security requirements. However, there is currently lack of general upgrade and renewal solutions for smart contracts.
- **Execution engine limitation:** As the smart contracts become more functional, the need of speeding up execution becomes more urgent. However, execution engine largely affects the execution efficiency of smart contracts. Therefore, developing new execution engine to improve the efficiency of smart contract need further research.

TABLE V: Blockchain system comparison [247]

Blockchian System	Application Type	Running Environment	Programming Language	Turing completeness	Data storage type	Note
Ethereum	General application	EVM	Solidity, Serpent, Mutan	Yes	Account-based	Best community support; Developer friendly
Hyperledger	General application	Docker	Golang, Java	Yes	Account-based	Contracts need to be invoked after permission but support to upgrade
EOS	General application	WASM	C++	Yes	Account-based	
Bitcoin	Cryptocurrency	Embedded operation	Golang, C++	Not	Transaction-based	
Zcash	Cryptocurrency	Embedded operation	C++	Not	Transaction-based	
Quorum	General application	EVM	Golang	Yes	Account-based	
Parity	General application	EVM	Solidity, Serpent, Mutan	Yes	Account-based	
Litecoin	Cryptocurrency	Embedded operation	Golang, C++	Unknown	Transaction-based	
Corda	Digital Asset	JVM	Kotlin, Java	Yes	Transaction-based	
Sawtooth	General application	Embedded operation	Python	Yes	Unknown	
Kadena	General application	Embedded operation	Pact	Not	Form-Based	

C. Blockchain Architectures and Protocols

From the resource consumption perspective, many blockchain protocols, which consumes less power than PoW, have been proposed, such as PoS and IOTA. However, they struggle to be widely used in wireless networks because of their scalability. As to another type of blockchain protocols which vote instead of calculating, such as PBFT and Hashgraph, they are still not widely applicable to wireless networks due to their communication complexity. From the communication perspective, caused by blockchain's transaction release, consensus interaction, ledger updating and so on, additional communication overhead is bound to be incurred along with the improvement of data security brought by blockchain. There have to be a tradeoff between the communication performance and the security performance of the blockchain network. In conclusion, essential questions to be technologically addressed include: 1) how to design a blockchain protocol with high scalability and appropriate power consumption, communication complexity while ensuring its security? 2) how to compromise between blockchain's performance and network's performance?

D. Commercial Issues

In addition to technical matters, the development of killer applications [248] and business models is also an important issue that must be broken through to achieve large-scale application of blockchain. For private or consortium blockchains, only the untamperability of the data on chain can be guaranteed. While the authenticity of the data off chain requires the cooperation of other technologies form the Internet of Things. In terms of public chain, it is more about the transformation of the whole system, which is suitable for the system without effective incentive system or reliable allocation mechanism. Therefore, the first areas to be implemented will be those that have formed a consensus but lack incentives and cannot be implemented on a large scale.

E. Policies and Standards

The large-scale commercialization of blockchain relies on the support of regulations, standards, and other related policy issues. With the vigorous development of blockchain, governments and organizations have increased their strategic layout for the blockchain industry and focused on encouraging technology and policy regulations. From 2019 to 2020, there are 24 countries around the world have issued special policies or laws for the development and regulation of the blockchain industry [249]. Although governments and organizations are actively carrying out policy research on blockchain at this stage, the unification of policies, regulations, and standards is still needed to be further promoted. Moreover, policymakers need to explore the application path of blockchain pragmatically in combination with reality, and jointly to solve the problems and challenges in the process of empowering the real economy.

F. Communication Issues

Blockchain is built in a P2P network, which means that a large amount of communication cost will be added in terms of network traffic and system processing capacity. Because current applications are highly dynamic and data sources frequently change, nodes may have to send a large number of update transactions, which will further increase the communication overhead. On the other hand, blockchain deployment in wireless is foreseeable in the near future [35]. In this case, blockchain services rely on wireless communication networks to reach consensus. During the consensus process, blockchain nodes are connected through wireless channels. However, due to factors such as wireless channel fading and

unauthorized malicious interference, the wireless connection among blockchain nodes may be attacked, and the uplink or downlink transmission may fail, thereby reducing the probability of successful transactions. Therefore, in the wireless blockchain system, a framework is needed to measure the communication overhead and communication quality in the communication process.

VIII. Conclusion

Blockchain is an emerging technology that is considered as one of the key enablers of 5G networks due to its unique features of decentralization, scalability, security and the corresponding characteristics. In this article, we presented a comprehensive survey focusing on the current most advanced achievements in exploring the intrinsic nature of blockchain from a methodological perspective. This article aims to systematically and and comprehensively analyze the blockchain in terms of the operation process, algorithm design and application methods, especially the wireless blockchain in model building, node deployment, protocol design, etc. This is of great significance for exploring the essence of blockchain and further exploiting the potential of blockchain thoroughly. Based on the state of art literatures, we outlined the theoretical model research for blockchain fundamentals understanding, the network service design for blockchain-based mechanisms and algorithms, as well as the application of blockchain for IoT and etc. We first introduced the working principles, research activities, and challenges of blockchain, as well as illustrated the roadmap involving the classic methodology with typical blockchain use cases and topics. Subsequently, we discussed the contribution of the methodology to the performance of blockchain systems, focusing on the role of stochastic process, game theory, optimization theory, and machine learning in both the study of blockchain operation process and the design of blockchain protocol/algorithm. Finally, we pointed out several blockchain issues from technical, commercial, and political perspectives. Although the blockchain is still in its infancy, it is clear that blockchain will significantly improve the landscape and experience of future network services and applications. We believe our timely study would shed valuable light on the research of the blockchain topics as well as motivate the interested researchers and practitioners to put more research efforts into this promising area.

References

[1] S. Nakamoto. (2009) Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] V. Buterin. Ethereum whitepaper. [Online]. Available: https://ethereum.org/en/whitepaper/

[3] N. community, "Nxt: a peer-to-peer digital socioeconomic system," *White paper*, Feb. 2016.

[4] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *IEEE Security and Privacy Workshops*, San Jose, CA, May. 2015, pp. 180–184.

[5] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired RFID-based information architecture for food supply chain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5803–5813, Mar. 2019.

[6] Y. Yuan and F. Wang, "Towards blockchain-based intelligent transportation systems," in *IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*. Rio de Janeiro, Brazil: IEEE, Nov. 2016, pp. 2663–2668.

[7] D. Bhowmik and T. Feng, "The multimedia blockchain: A distributed and tamper-proof media transaction framework," in *22nd International Conference on Digital Signal Processing (DSP)*. London, UK: IEEE, Aug. 2017, pp. 1–5.

[8] D. Liu, A. Alahmadi, J. Ni, X. Lin, and X. Shen, "Anonymous Reputation System for IIoT-Enabled Retail Marketing Atop PoS Blockchain," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3527–3537, Jun. 2019.

[9] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, "BeepTrace: Blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3915–3929, Sept. 2021.

[10] N. Al-Zaben, M. M. Hassan Onik, J. Yang, N. Lee, and C. Kim, "General data protection regulation complied blockchain architecture for personally identifiable information management," in *2018 International Conference on Computing, Electronics Communications Engineering (iCCECE)*, Southend, UK, Aug. 2018, pp. 77–82.

[11] R. S. Sangwan, M. Kassab, and C. Capitolo, "Architectural considerations for blockchain based systems for financial transactions," *Procedia Computer Science*, vol. 168, pp. 265 – 271, Jan. 2020.

[12] B. Granetto, R. Kandaswamy, J. Lovelock, and M. Reynolds, "Forecast: Blockchain business value, worldwide, 2017-2030," *Gartner*, 2017.

[13] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858–880, Aug. 2019.

[14] H. Xu, P. Valente Klaine, O. Onireti, B. Cao, M. Imran, and L. Zhang, "Blockchain-enabled Resource Management and Sharing for 6G Communications," *Digital Communications and Networks*, vol. 6, no. 3, pp. 261–269, Aug. 2020.

[15] Y. Hu, M. Liyanage, A. Mansoor, K. Thilakarathna, G. Jourjon, and A. Seneviratne, "Blockchain-based smart contracts - applications and challenges," *arXiv preprint arXiv:1810.04699*, 2018.

[16] N. Waheed, X. He, M. Usman, and M. Usman, "Security & Privacy in IoT Using Machine Learning & Blockchain: Threats & Countermeasures," *arXiv preprint arXiv:2002.03488*, 2020.

[17] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, Fourthquarter 2018.

[18] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the Attack Surface of Blockchain: A Comprehensive Survey," *IEEE Internet of Things Journal*, vol. 22, no. 3, pp. 1977–2008, Mar. 2020.

[19] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: A survey," *arXiv preprint arXiv:2001.07091*, 2020.

[20] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. Kim, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, pp. 22 328–22 370, Jan. 2019.

[21] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, Secondquarter 2020.

[22] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Network*, vol. 33, no. 5, pp. 166–173, Sep. 2019.

[23] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang, and R. P. Liu, "Survey: Sharding in blockchains," *IEEE Access*, vol. 8, pp. 14 155–14 181, Jan. 2020.

[24] H. T. M. Gamage, H. Weerasinghe, and N. G. J. Dias, "A survey on blockchain technology concepts, applications, and issues," *SN Computer Science*, vol. 1, no. 2, pp. 1–15, Mar. 2020.

[25] D. C. Nguyen, P. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *Journal of Network and Computer Applications*, p. 102693, May. 2020.

[26] K. Yue, Y. Zhang, Y. Chen, Y. Li, L. Zhao, C. Rong, and L. Chen, "A survey of decentralizing applications via blockchain: The 5G and beyond perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2191–2217, Fourthquarter 2021.

[27] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[28] M. Chowdhury, M. Ferdous, K. Biswas, N. Chowdhury, and V. Muthukkumarasamy, "A survey on blockchain-based platforms for iot use-cases," *The Knowledge Engineering Review*, vol. 35, May. 2020.

[29] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830, Thirdquarter 2019.

[30] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain meets cloud computing: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2009–2030, Thirdquarter 2020.

[31] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, Secondquarter 2019.

[32] H. Baniata and A. Kertesz, "A survey on blockchain-fog integration approaches," *IEEE Access*, vol. 8, pp. 102 657–102 668, Jun. 2020.

[33] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y. Liang, and D. Kim, "A survey on blockchain: A game theoretical perspective," *IEEE Access*, vol. 7, pp. 47 615–47 643, Apr. 2019.

[34] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1392–1431, Secondquarter 2020.

[35] L. Zhang, H. Xu, O. Onireti, M. A. Imran, and B. Cao, "How much communication resource is needed to run a wireless blockchain network?" *IEEE Network*, vol. 36, no. 1, pp. 128–135, Jan. 2022.

[36] Y. Li, B. Cao, L. Liang, D. Mao, and L. Zhang, "Block access control in wireless blockchain network: Design, modeling and analysis," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9258–9272, Sept. 2021.

[37] S. Zhai, Y. Yang, J. Li, C. Qiu, and J. Zhao, "Research on the application of cryptography on the blockchain," *Journal of Physics: Conference Series*, vol. 1168, no. 3, pp. 32–77, Feb. 2019.

[38] A. A. Rasheed, R. N. Mahapatra, C. Varol, and N. Karpoor, "Exploiting zero knowledge proof and blockchain towards the enforcement of anonymity, data integrity and privacy (ADIP) on IoT," *IEEE Transactions on Emerging Topics in Computing*, pp. 1–1, Jul. 2021.

[39] W. Hao, J. Zeng, X. Dai, J. Xiao, Q.-S. Hua, H. Chen, K.-C. Li, and H. Jin, "Towards a trust-enhanced blockchain P2P topology for enabling fast and reliable broadcast," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 904–917, Jun. 2020.

[40] W. Hyun, "Hybrid peer-to-peer network based layered blockchain architecture for enhancement of synchronization performance," in *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju Island, Korea, Oct. 2021, pp. 1461–1463.

[41] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, Secondquarter 2020.

[42] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, "When Internet of things meets blockchain: Challenges in distributed consensus," *IEEE Network*, vol. 33, no. 6, pp. 133–139, Jul. 2019.

[43] R. Kumar and R. Tripathi, "Large-scale data storage scheme in blockchain ledger using ipfs and nosql," in *Large-Scale Data Streaming, Processing, and Blockchain Security*. IGI Global, 2021, pp. 91–116.

[44] R. Han, Z. Yan, X. Liang, and L. T. Yang, "How can incentive mechanisms and blockchain benefit with each other? A survey," *ACM Computing Surveys (CSUR)*, Jun. 2022.

[45] X. Ling, J. Wang, T. Bouchoucha, B. C. Levy, and Z. Ding, "Blockchain radio access network (b-ran): Towards decentralized secure radio access paradigm," *IEEE Access*, vol. 7, pp. 9714–9723, Jan. 2019.

[46] H. Xu, L. Zhang, Y. Sun *et al.*, "BE-RAN: Blockchain-enabled open RAN with decentralized identity management and privacy-preserving communication," *arXiv preprint arXiv:2101.10856*, 2021.

[47] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, "Guardian: Blockchain-based secure demand response management in smart grid system," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 613–624, Jul. 2020.

[48] X. Ling, J. Wang, Y. Le, Z. Ding, and X. Gao, "Blockchain radio access network beyond 5G," *IEEE Wireless Communications*, vol. 27, no. 6, pp. 160–168, Dec. 2020.

[49] S. Ding, G. Shen, K. X. Pan, S. K. Bose, Q. Zhang, and B. Mukherjee, "Blockchain-assisted spectrum trading between elastic virtual optical networks," *IEEE Network*, vol. 34, no. 6, pp. 205–211, Dec. 2020.

[50] G. O. Boateng, G. Sun, D. A. Mensah, D. M. Doe, R. Ou, and G. Liu, "Consortium blockchain-based spectrum trading for network slicing in 5G RAN: A multi-agent deep reinforcement learning approach," *IEEE Transactions on Mobile Computing*, pp. 1–15, Jul. 2022.

[51] L. Xue, W. Yang, W. Chen, and L. Huang, "STBC: A novel blockchain-based spectrum trading solution," *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 1, pp. 13–30, Mar. 2022.

[52] R. Zhu, H. Liu, L. Liu, X. Liu, W. Hu, and B. Yuan, "A blockchain-based two-stage secure spectrum intelligent sensing and sharing auction mechanism," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2773–2783, Apr. 2022.

[53] G. Rathee, F. Ahmad, F. Kurugollu, M. A. Azad, R. Iqbal, and M. Imran, "CRT-BIoV: A cognitive radio technique for blockchain-enabled Internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4005–4015, Jul. 2021.

[54] S. Zheng, Y. Jiang, X. Ge, Y. Xiao, Y. Huang, and Y. Liu, "Cooperative spectrum sensing and fusion based on tangle networks," *IEEE Transactions on Network Science and Engineering*, pp. 1–1, May 2022.

[55] H. Zhang, S. Leng, Y. Wei, and J. He, "A blockchain enhanced coexistence of heterogeneous networks on unlicensed spectrum," *IEEE Transactions on Vehicular Technology*, pp. 1–1, Apr. 2022.

[56] S. Hu, Y. Pei, and Y.-C. Liang, "Sensing-mining-access tradeoff in blockchain-enabled dynamic spectrum access," *IEEE Wireless Communications Letters*, vol. 10, no. 4, pp. 820–824, Apr. 2021.

[57] M. Jiang, Y. Li, Q. Zhang, G. Zhang, and J. Qin, "Decentralized blockchain-based dynamic spectrum acquisition for wireless downlink communications," *IEEE Transactions on Signal Processing*, vol. 69, pp. 986–997, Jan. 2021.

[58] P. Fernando, K. Dadallage, T. Gamage, C. Seneviratne, A. Madanayake, and M. Liyanage, "Proof-of-sense: A novel consensus mechanism for spectrum misuse detection," *IEEE Transactions on Industrial Informatics*, pp. 1–1, Apr. 2022.

[59] C. Zhang, Y. Xu, H. Elahi, D. Zhang, Y. Tan, J. Chen, and Y. Zhang, "A blockchain-based model migration approach for secure and sustainable federated learning in iot systems," *IEEE Internet of Things Journal*, pp. 1–1, May 2022.

[60] P. K. Deb, S. Misra, T. Sarkar, and A. Mukherjee, "Magnum: A distributed framework for enabling transfer learning in B5G-enabled industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 7133–7140, Oct. 2021.

[61] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, "Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 160–209, Firstquarter 2022.

[62] K. Shahzad, A. O. Aseeri, and M. A. Shah, "A blockchain-based authentication solution for 6G communication security in tactile networks," *Electronics*, vol. 11, no. 9, p. 1374, Apr. 2022.

[63] J. Wang and H. Wang, "Monoxide: Scale out blockchains with asynchronous consensus zones," in *16th USENIX Symposium on Networked Systems Design and Implementation*. Boston, MA: USENIX Association, Feb. 2019, pp. 95–112.

[64] Z. Zhang, M. Zargham, and V. Preciado, "On modeling blockchain-enabled economic networks as stochastic dynamical systems," *Applied Network Science*, vol. 5, no. 1, pp. 1–24, Dec. 2020.

[65] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, Aug. 2020.

[66] A. Gopalan, A. Sankararaman, A. Walid, and S. Vishwanath, "Stability and scalability of blockchain systems," *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, vol. 4, no. 2, pp. 1–35, Jun. 2020.

[67] A. Chakravorty and C. Rong, "Ushare: User controlled social media based on blockchain," in *Proceedings of the 11th international conference on ubiquitous information management and communication*, ser. IMCOM '17, Beppu, Japan, Jan. 2017.

[68] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14 757–14 767, Jul. 2017.

[69] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A proof-of-trust consensus protocol for enhancing accountability in crowdsourcing services," *IEEE Transactions on Services Computing*, vol. 12, no. 3, pp. 429–445, May 2019.

[70] X. Liu, G. Zhao, X. Wang, Y. Lin, Z. Zhou, H. Tang, and B. Chen, "MDP-based quantitative analysis framework for proof of authority," in *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Guilin, China, Oct. 2019, pp. 227–236.

[71] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer pbft consensus for blockchain," *IEEE Transactions*

on Parallel and Distributed Systems, vol. 32, no. 5, pp. 1146–1160, 2021.

[72] W. Feng, Z. Yan, L. T. Yang, and Q. Zheng, "Anonymous authentication on trust in blockchain-based mobile crowdsourcing," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14 185–14 202, Aug. 2022.

[73] G. Liu, H. Dong, Z. Yan, X. Zhou, and S. Shimizu, "B4sdc: A blockchain system for security data collection in manets," *IEEE Transactions on Big Data*, vol. 8, no. 3, pp. 739–752, Jun. 2022.

[74] M. Abdel-Basset, N. Moustafa, and H. Hawash, "Privacy-preserved cyberattack detection in Industrial Edge of Things: A blockchain-orchestrated federated learning approach," *IEEE Transactions on Industrial Informatics*, pp. 1–1, Apr. 2022.

[75] Z. Chang, W. Guo, X. Guo, Z. Zhou, and T. Ristaniemi, "Incentive mechanism for edge-computing-based blockchain," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 11, pp. 7105–7114, Nov. 2020.

[76] W. Sun, J. Liu, Y. Yue, and P. Wang, "Joint resource allocation and incentive design for blockchain-based mobile edge computing," *IEEE Transactions on Wireless Communications*, vol. 19, no. 9, pp. 6050–6064, Sept. 2020.

[77] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2438–2455, Sept. 2021.

[78] V. Sharma, "An energy-efficient transaction model for the blockchain-enabled Internet of vehicles," *IEEE Communications Letters*, vol. 23, no. 2, pp. 246–249, Feb. 2019.

[79] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *19th International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, Korea (South), Feb. 2017, pp. 464–467.

[80] M. Moniruzzaman, S. Khezr, A. Yassine, and R. Benlamri, "Blockchain for smart homes: Review of current trends and research challenges," *Computers & Electrical Engineering*, vol. 83, p. 106585, May. 2020.

[81] L. Baird. The swirlds hashgraph consensus algorithm: Fair, fast, byzantine fault tolerance. [Online]. Available: https://hedera.com/learning/what-is-hedera-hashgraph

[82] S. Popov, "The tangle," *[Online]. Available: http://iotatoken.com/IOTA Whitepaper.pdf*, 2017.

[83] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. Weed Cocco, and J. Yellick, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proceedings of the thirteenth EuroSys conference*, New York, NY, Apr. 2018.

[84] S. Kumaraswamy. EOSIO - The most powerful infrastructure for decentralized applications. [Online]. Available: https://github.com/EOSIO/eos

[85] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-NG: A scalable blockchain protocol," in *13th Symposium on Networked Systems Design and Implementation (NSDI)*, Santa Clara, CA, Mar. 2016, pp. 45–59.

[86] P. Robinson, R. Ramesh, J. Brainard, and S. Johnson, "Atomic cross-chain transactions white paper," *arXiv preprint arXiv:2003.00903*, 2020.

[87] J. Feng, F. R. Yu, Q. Pei, J. Du, and L. Zhu, "Joint optimization of radio and computational resources allocation in blockchain-enabled mobile edge computing systems," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 4321–4334, Jun. 2020.

[88] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*. Tata McGraw-Hill Education, 2002.

[89] Y. Zhu, G. Zheng, and K.-K. Wong, "Stochastic geometry analysis of large intelligent surface-assisted millimeter wave networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 8, pp. 1749–1762, Aug. 2020.

[90] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and its applications*. John Wiley & Sons, 2013.

[91] D. Huang, X. Ma, and S. Zhang, "Performance analysis of the raft consensus algorithm for private blockchains," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 172–181, Jan. 2020.

[92] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer-to-Peer Networking and Applications*, vol. 9, no. 2, pp. 397–413, Apr. 2016.

[93] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu, "Direct acyclic graph-based ledger for Internet of things: Performance and security analysis," *IEEE/ACM Transactions on Networking*, vol. 28, no. 4, pp. 1643–1656, Aug. 2020.

[94] S. Dachian, N. Kordzakhia, Y. A. Kutoyants, and A. Novikov, "Estimation of cusp location of stochastic processes: a survey," *Statistical Inference for Stochastic Processes*, vol. 21, no. 2, pp. 345–362, 2018.

[95] M. Lei, Y. Shi, and L. Niu, "The applications of stochastic models in network embedding: A survey," in *IEEE/WIC/ACM International Conference on Web Intelligence (WI)*, Santiago, Chile, Dec. 2018, pp. 635–638.

[96] A. F. Karr, "Statistical models and methods in image analysis: A survey," in *Statistical Inference in Stochastic Processes*. CRC Press, 1991, pp. 1–34.

[97] A. Shakarami, M. Ghobaei-Arani, M. Masdari, and M. Hosseinzadeh, "A survey on the computation offloading approaches in mobile edge/cloud computing environment: a stochastic-based perspective," *Journal of Grid Computing*, vol. 18, no. 4, pp. 639–671, Aug. 2020.

[98] H. Kang, X. Chang, J. Mii, V. B. Mii, Y. Yao, and Z. Chen, "Stochastic modeling approaches for analyzing blockchain: A survey," *arXiv:2009.05945*, 2020.

[99] D. Fullmer and A. S. Morse, "Analysis of difficulty control in bitcoin and proof-of-work blockchains," in *IEEE Conference on Decision and Control (CDC)*, Miami, FL, Dec. 2018, pp. 5988–5992.

[100] H. Sukhwani, N. Wang, K. S. Trivedi, and A. Rindos, "Performance modeling of hyperledger fabric (permissioned blockchain network)," in *IEEE International Symposium on Network Computing and Applications (NCA)*, Cambridge, MA, Nov. 2018.

[101] N. Papadis, S. Borst, A. Walid, M. Grissa, and L. Tassiulas, "Stochastic models and wide-area network measurements for blockchain design and analysis," in *IEEE Conference on Computer Communications*, Honolulu, HI, Apr. 2018, pp. 2546–2554.

[102] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *2016 IEEE European Symposium on Security and Privacy (EuroS P)*. Saarbruecken, Germany: IEEE, May. 2016, pp. 305–320.

[103] Y. Li, B. Cao, L. Liang, D. Mao, and L. Zhang, "Block access control in wireless blockchain network: Design, modeling and analysis," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9258–9272, Jun. 2021.

[104] T. Meng, Y. Zhao, K. Wolter, and C.-Z. Xu, "On consortium blockchain consistency: A queueing network model approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 6, pp. 1369–1382, Jun. 2021.

[105] A. Asheralieva and D. Niyato, "Learning-based mobile edge computing resource management to support public blockchain networks," *IEEE Transactions on Mobile Computing*, vol. 20, no. 3, pp. 1092–1109, Dec. 2021.

[106] F.-Q. Ma, Q.-L. Li, Y.-H. Liu, and Y.-X. Chang, "Stochastic performance modeling for practical byzantine fault tolerance consensus in blockchain," *arXiv preprint arXiv:2107.00183*, 2021.

[107] K. Zheng, Y. Liu, C. Dai, Y. Duan, and X. Huang, "Model checking pbft consensus mechanism in healthcare blockchain network," in *IEEE International Conference on Information Technology in Medicine and Education (ITME)*, Hangzhou, China, Oct. 2018, pp. 877–881.

[108] H. Xu, L. Zhang, Y. Liu, and B. Cao, "Raft based wireless blockchain networks in the presence of malicious jamming," *IEEE Wireless Communications Letters*, vol. 9, no. 6, pp. 817–821, Jun. 2020.

[109] Y. Zhu, G. Zheng, and K.-K. Wong, "Blockchain-empowered decentralized storage in air-to-ground industrial networks," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3593–3601, Jun. 2019.

[110] Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao, and M. A. Imran, "Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5791–5802, Jun. 2019.

[111] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11 008–11 021, Nov. 2018.

[112] R. B. Myerson, *Game theory*. Harvard university press, 2013.

[113] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge university press, 2012.

[114] J. Nash, "Non-cooperative games," in *Annals of mathematics*. JSTOR, 1951, pp. 286–295.

[115] I. Eyal, "The miner's dilemma," in *IEEE Symposium on Security and Privacy*. San Jose, CA, USA: IEEE, May 2015, pp. 89–103.

[116] Y. Zhen, M. Yue, C. Zhong-yu, T. Chang-bing, and C. Xin, "Zero-determinant strategy for the algorithm optimize of blockchain pow consensus," in *Chinese Control Conference*. Dalian, China: IEEE, Jul. 2017, pp. 1441–1446.

[117] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 760–763, Oct. 2018.

[118] R. Xing, Z. Su, T. H. Luan, Q. Xu, Y. Wang, and R. Li, "UAVs-aided delay-tolerant blockchain secure offline transactions in post-disaster vehicular networks," *IEEE Transactions on Vehicular Technology*, pp. 1–14, Jun. 2022.

[119] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, H.-A. Pham, N. H. Tuong, and E. Dutkiewicz, "Blockchain-based secure platform for coalition loyalty program management," in *IEEE Wireless Communications and Networking Conference (WCNC)*, Nanjing, China, Mar. 2021, pp. 1–6.

[120] J. Li, T. Liu, D. Niyato, P. Wang, J. Li, and Z. Han, "Contract-theoretic pricing for security deposits in sharded blockchain with Internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 10 052–10 070, Jan. 2021.

[121] Y. Yang, Z. Liu, Z. Liu, Y. Xie, K. Y. Chan, and X. Guan, "Joint optimization of edge computing resource pricing and wireless caching for blockchain-driven networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 6, pp. 6661–6670, Jun. 2022.

[122] Y. Zuo, S. Jin, S. Zhang, Y. Han, and K.-K. Wong, "Delay-limited computation offloading for MEC-assisted mobile blockchain networks," *IEEE Transactions on Communications*, vol. 69, no. 12, pp. 8569–8584, Sept. 2021.

[123] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, "Blockchain mining games," in *Proceedings of the 2016 ACM Conference on Economics and Computation*, Boulder, CO, USA, Jul., pp. 365–382.

[124] W. Liu, B. Cao, L. Zhang, M. Peng, and M. Daneshmand, "A distributed game theoretic approach for blockchain-based offloading strategy," in *IEEE International Conference on Communications (ICC)*, Dublin, Ireland, Jun. 2020.

[125] M. E. Mkiramweni, C. Yang, J. Li, and W. Zhang, "A survey of game theory in unmanned aerial vehicles communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3386–3416, May. 2019.

[126] J. Pawlick, E. Colbert, and Q. Zhu, "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy," *ACM Computing Surveys (CSUR)*, vol. 52, no. 4, pp. 1–28, Aug. 2019.

[127] Q. Mao, F. Hu, and Q. Hao, "Deep learning for intelligent wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2595–2621, Fourthquarter 2018.

[128] J. Li, Y. Yuan, S. Wang, and F. Wang, "Transaction queuing game in bitcoin blockchain," in *IEEE Intelligent Vehicles Symposium (IV)*. Changshu, China: IEEE, Jun. 2018, pp. 114–119.

[129] Z. Yang, Y. Miao, C. Z., C. Tang, and X. Chen, "Zero-determinant strategy for the algorithm optimize of blockchain PoW consensus," in *Chinese Control Conference (CCC)*. Dalian, China: IEEE, Jul. 2017, pp. 1441–1446.

[130] C. Tang, C. Li, X. Yu, Z. Zheng, and Z. Chen, *IEEE transactions on cybernetics*, vol. 50, no. 10, pp. 4544–4549, Oct. 2020.

[131] S. Jiang and J. Wu, "Bitcoin mining with transaction fees: A game on the block size," in *2019 IEEE International Conference on Blockchain (Blockchain)*. Atlanta, GA, USA: IEEE, Jul. 2019, pp. 107–115.

[132] A. Taghizadeh, H. Kebriaei, and D. Niyato, "Mean field game for equilibrium analysis of mining computational power in blockchains," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7625–7635, Aug. 2020.

[133] C. Chen, X. Chen, J. Yu, W. Wu, and D. Wu, "Impact of temporary fork on the evolution of mining pools in blockchain networks: An evolutionary game analysis," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 400–418, Mar. 2021.

[134] S. Feng, Z. Xiong, D. Niyato, P. Wang, S. Wang, and Y. Zhang, "Cyber Risk Management with Risk Aware Cyber-Insurance in Blockchain Networks," in *IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, United Arab, Dec. 2018.

[135] S. Kim and S.-G. Hahn, "Mining Pool Manipulation in Blockchain Network Over Evolutionary Block Withholding Attack," *IEEE Access*, vol. 7, pp. 144 230–144 244, Oct. 2019.

[136] B. Li and J. Jiang, "Security analysis of paxos mechanism design based on game theory," in *2020 IEEE International Conference on Information Technology,Big Data and Artificial Intelligence (ICIBA)*. Chongqing, China: IEEE, Nov. 2020, pp. 59–66.

[137] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3602–3609, Jun. 2019.

[138] Y. Jiao, P. Wang, D. Niyato, and Z. Xiong, "Social welfare maximization auction in edge computing resource allocation for mobile blockchain," in *IEEE international conference on communications (ICC)*, Kansas City, MO, May. 2018.

[139] N. C. Luong, Z. Xiong, P. Wang, and D. Niyato, "Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach," in *IEEE International Conference on Communications (ICC)*, Kansas City, MO, May. 2018.

[140] D. Xu, L. Xiao, L. Sun, and M. Lei, "Game theoretic study on blockchain based secure edge networks," in *International Conference on Communications in China (ICCC)*, Qingdao, China, Oct. 2017.

[141] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, Aug. 2018.

[142] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4585–4600, Jun. 2019.

[143] J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim, "Incentivizing consensus propagation in Proof-of-Stake based consortium blockchain networks," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 157–160, Feb. 2019.

[144] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 451–466, Jan. 2020.

[145] S. Guo, Y. Dai, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: Stackelberg game and double auction based task offloading for mobile blockchain," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5549–5561, May. 2020.

[146] H. Hindi, "A tutorial on convex optimization II: duality and interior point methods," in *American Control Conference*. Minneapolis, MN, USA: IEEE, Jun. 2006, pp. 686–696.

[147] P. Berck and K. Sydsæter, "Linear and nonlinear programming," in *Economists' Mathematical Manual*. Springer, 1993, pp. 71–76.

[148] S. Boyd, N. Parikh, E. Chu, B. Peleato, J. Eckstein *et al.*, "Distributed optimization and statistical learning via the alternating direction method of multipliers," *Foundations and Trends in Machine learning*, vol. 3, no. 1, pp. 1–122, 2011.

[149] B. He, H. Yang, and S. Wang, "Alternating direction method with self-adaptive penalty parameters for monotone variational inequalities," *Journal of Optimization Theory and applications*, vol. 106, no. 2, pp. 337–356, Aug. 2000.

[150] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," in *Proceedings of the International Conference on Learning Representations*, Banff, Canada, Apr. 2014, pp. 1–15.

[151] J. Duchi, E. Hazan, and Y. Singer, "Adaptive subgradient methods for online learning and stochastic optimization." *Journal of machine learning research*, vol. 12, no. 7, pp. 2121–2159, Nov. 2011.

[152] L. Jiang, S. Xie, S. Maharjan, and Y. Zhang, "Joint transaction relaying and block verification optimization for blockchain empowered D2D communication," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 828–841, Jan. 2020.

[153] S. Sun, Z. Cao, H. Zhu, and J. Zhao, "A survey of optimization methods from a machine learning perspective," *IEEE Transactions on Cybernetics*, vol. 50, no. 8, pp. 3668–3681, Aug. 2020.

[154] G. Wu, R. Mallipeddi, and P. N. Suganthan, "Ensemble strategies for population-based optimization algorithms a survey," *Swarm and Evolutionary Computation*, vol. 44, pp. 695–711, Feb. 2019.

[155] D. K. Molzahn, F. Drfler, H. Sandberg, S. H. Low, S. Chakrabarti, R. Baldick, and J. Lavaei, "A survey of distributed optimization and control algorithms for electric power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2941–2962, Nov. 2017.

[156] T. Yang, X. Yi, J. Wu, Y. Yuan, D. Wu, Z. Meng, Y. Hong, H. Wang, Z. Lin, and K. H. Johansson, "A survey of distributed optimization," *Annual Reviews in Control*, vol. 47, pp. 278–305, May. 2019.

[157] O. Onireti, L. Zhang, and M. A. Imran, "On the viable area of wireless practical byzantine fault tolerance (PBFT) blockchain networks," in *IEEE Global Communications Conference (GLOBECOM)*, Waikoloa, HI, Dec. 2019.

[158] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled Internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906–2920, 2019.

[159] M. Saad, L. Njilla, C. Kamhoua, J. Kim, D. Nyang, and A. Mohaisen, "Mempool Optimization for Defending Against DDoS Attacks in PoW-based Blockchain Systems," in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. Seoul, Korea (South): IEEE, May. 2019, pp. 285–292.

[160] X. Cai, S. Geng, J. Zhang, D. Wu, Z. Cui, W. Zhang, and J. Chen, "A sharding scheme-based many-objective optimization algorithm for enhancing security in blockchain-enabled Industrial Internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7650–7658, Nov. 2021.

[161] J. Kang, Z. Xiong, D. Niyato, S. Xie, and D. I. Kim, "Securing data sharing from the sky: Integrating blockchains into drones in 5G and beyond," *IEEE Network*, vol. 35, no. 1, pp. 78–85, Feb. 2021.

[162] Y. Wu, J. Shi, X. Chen, K. Ni, L. Qian, and K. Zhang, "Optimal Multi-access Computation Offloading for Mobile Blockchain," in *IEEE International Conference on Communication Systems (ICCS)*, Chengdu, China, Dec. 2018, pp. 198–203.

[163] S. Fu, L. Zhao, X. Ling, and H. Zhang, "Maximizing the system energy efficiency in the blockchain based Internet of Things," in *IEEE International Conference on Communications (ICC)*, Shanghai, China, May. 2019.

[164] M. Wang, C. Xu, X. Chen, L. Zhong, Z. Wu, and D. O. Wu, "BC-MDC: A blockchain-based decentralized truthful framework for mobile device cloud," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1208–1219, Feb. 2021.

[165] Z. Xiong, J. Kang, D. Niyato, P. Wang, and H. V. Poor, "Cloud/edge computing service management in blockchain networks: Multi-leader multi-follower game-based admm for pricing," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 356–367, Apr. 2020.

[166] L. Saino, I. Psaras, E. Leonardi, and G. Pavlou, "Load imbalance and caching performance of sharded systems," *IEEE/ACM Transactions on Networking*, vol. 28, no. 1, pp. 112–125, Feb. 2020.

[167] Y. Zhang, D. Yang, and G. Xue, "Cheapay: An optimal algorithm for fee minimization in blockchain-based payment channel networks," in *IEEE International Conference on Communications (ICC)*, Shanghai, China, May. 2019.

[168] Z. Jin, R. Wu, X. Chen, and G. Li, "Charging guiding strategy for electric taxis based on consortium blockchain," *IEEE Access*, vol. 7, pp. 144 144–144 153, Oct. 2019.

[169] H. Zhu, C. Huang, and J. Zhou, "Edgechain: Blockchain-based multi-vendor mobile edge application placement," in *IEEE Conference on Network Softwarization and Workshops (NetSoft)*, Montreal, QC, Canada, Jun. 2018, pp. 222–226.

[170] T. O. Ayodele, *Introduction to machine learning*. InTech, 2010.

[171] P. Langley and H. A. Simon, "Applications of machine learning and rule induction," *Communications of the ACM*, vol. 38, no. 11, pp. 54–64, Nov. 1995.

[172] R. Saravanan and P. Sujatha, "A state of art techniques on machine learning algorithms: A perspective of supervised learning approaches in data classification," in *Second International Conference on Intelligent Computing and Control Systems (ICICCS)*. Madurai, India: IEEE, Jun. 2018, pp. 945–949.

[173] L. P. Kaelbling, M. L. Littman, and A. W. Moore, "Reinforcement learning: A survey," *Journal of artificial intelligence research*, vol. 4, pp. 237–285, 1996.

[174] M. Shen, J. Zhang, L. Zhu, K. Xu, and X. Tang, "Secure SVM training over vertically-partitioned datasets using consortium blockchain for vehicular social networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5773–5783, Dec. 2020.

[175] H. J. Singh and A. S. Hafid, "Transaction confirmation time prediction in ethereum blockchain using machine learning," *arXiv preprint arXiv:1911.11592*, 2019.

[176] I. Arel, D. C. Rose, and T. P. Karnowski, "Deep machine learning-a new frontier in artificial intelligence research," *IEEE computational intelligence magazine*, vol. 5, no. 4, pp. 13–18, 2010.

[177] L. Deng, "A tutorial survey of architectures, algorithms, and applications for deep learning," *APSIPA Transactions on Signal and Information Processing*, vol. 3, Jan. 2014.

[178] B. Waske and J. A. Benediktsson, "Fusion of support vector machines for classification of multisensor data," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 45, no. 12, pp. 3858–3866, Nov. 2007.

[179] L. Breiman, "Random forests," *Machine Learning*, vol. 43, no. 1, pp. 5–32, Oct. 2001.

[180] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–44, May. 2015.

[181] G. Litjens, T. Kooi, B. E. B., A. A. A. Setio, F. Ciompi, M. Ghafoorian, J. A. W. M. Laak, B. Ginneken, and C. I. Snchez, "A survey on deep learning in medical image analysis," *Medical Image Analysis*, vol. 42, pp. 60–88, Dec. 2017.

[182] H.-T. Cheng, L. Koc, J. Harmsen, T. Shaked, T. Chandra, H. Aradhye, G. Anderson, G. Corrado, W. Chai, M. Ispir, R. Anil, Z. Haque, L. Hong, V. Jain, X. Liu, and H. Shah, "Wide & deep learning for recommender systems," in *Proceedings of the 1st workshop on deep learning for recommender systems*, Boston, MA, Sept. 2016, pp. 7–10.

[183] N. Kumar, A. Singh, A. Handa, and S. K. Shukla, "Detecting malicious accounts on the ethereum blockchain with supervised learning," in *International Symposium on Cyber Security Cryptography and Machine Learning*. Be'er Sheva, Israel: Springer, Jul. 2020, pp. 94–109.

[184] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 55–68, Jun. 2022.

[185] N. Sundareswaran and S. Sasirekha, "Packet filtering mechanism to defend against DDoS attack in blockchain network," in *Evolutionary Computing and Mobile Sustainable Networks*, V. Suma, X. Fernando, K.-L. Du, and H. Wang, Eds. Singapore: Springer Singapore, 2022, pp. 201–214.

[186] M. U. Hassan, M. H. Rehmani, and J. Chen, "Anomaly detection in blockchain networks: A comprehensive survey," *arXiv preprint arXiv:2112.06089*, 2021.

[187] C. Bishop, *Pattern Recognition and Machine Learning (Information Science and Statistics)*. Springer-Verlag, Berlin, 2006.

[188] G. Nguyen, S. Dlugolinsky, M. Bobak, V. Tran, A. Lopez Garcia, I. Heredia, P. Malk, and L. Hluch, "Machine learning and deep learning frameworks and libraries for large-scale data mining: a survey," *Artificial Intelligence Review*, vol. 52, pp. 77–124, Jun. 2019.

[189] G. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Capkun, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Transactions on Information and System Security*, vol. 18, pp. 1–32, May. 2015.

[190] S. Dey, "Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work," in *Computer science and electronic engineering (CEEC)*. Colchester, UK: IEEE, Sept. 2018, pp. 7–10.

[191] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction, 2nd Edition*. Bradford Books, 2018.

[192] C. Szepesvri, "Reinforcement learning algorithms for mdps," *Morgan and Claypool Publishers*, Jun. 2010.

[193] H. Kim, J. Park, M. Bennis, and S.-L. Kim, "Blockchained on-device federated learning," *IEEE Communications Letters*, vol. 24, no. 6, pp. 1279–1283, Jun. 2020.

[194] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*. Ft. Lauderdale, FL, USA: PMLR, Apr. 2017, pp. 1273–1282.

[195] M. Cao, L. Zhang, and B. Cao, "Toward on-device federated learning: A direct acyclic graph-based blockchain approach," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–15, Aug. 2021.

[196] T. Baltruaitis, C. Ahuja, and L.-P. Morency, "Multimodal machine learning: A survey and taxonomy," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 41, no. 2, pp. 423–443, Feb. 2019.

[197] F. O. Olowononi, D. B. Rawat, and C. Liu, "Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 524–552, Firstquarter 2021.

[198] N. C. Luong, D. T. Hoang, S. Gong, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "Applications of deep reinforcement learning in communications and networking: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3133–3174, Fourthquarter 2019.

[199] E. Bout, V. Loscri, and A. Gallais, "How machine learning changes the nature of cyberattacks on iot networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 248–279, Firstquarter 2022.

[200] Y. Wu, Z. Wang, Y. Ma, and V. C. Leung, "Deep reinforcement learning for blockchain in industrial iot: A survey," *Computer Networks*, vol. 191, p. 108004, May. 2021.

[201] M. Dibaei, X. Zheng, Y. Xia, X. Xu, A. Jolfaei, A. K. Bashir, U. Tariq, D. Yu, and A. V. Vasilakos, "Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–18, Aug. 2021.

[202] D. C. Nguyen, M. Ding, Q.-V. Pham, P. N. Pathirana, L. B. Le, A. Seneviratne, J. Li, D. Niyato, and H. V. Poor, "Federated learning meets blockchain in edge computing: Opportunities and challenges," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12 806–12 825, Aug. 2021.

[203] H. Tang, Y. Jiao, B. Huang, C. Lin, S. Goyal, and B. Wang, "Learning to classify blockchain peers according to their behavior sequences," *IEEE Access*, vol. 6, pp. 71 208–71 215, Nov. 2018.

[204] S. Sayadi, S. B. Rejeb, and Z. Choukair, "Anomaly Detection Model Over Blockchain Electronic Transactions," in *International Wireless Communications & Mobile Computing Conference (IWCMC)*. Tangier, Morocco: IEEE, Jun. 2019, pp. 895–900.

[205] T. Pham and S. Lee, "Anomaly detection in bitcoin network using unsupervised learning methods," *arXiv preprint arXiv:1611.03941*, 2016.

[206] M. Shin, U. Baek, K. Shim, J. Park, S. Yoon, and M. Kim, "Block analysis in bitcoin system using clustering with dimension reduction," in *Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Matsue, Japan, Sept. 2019.

[207] M. A. Khan, S. Abbas, A. Rehman, Y. Saeed, A. Zeb, M. I. Uddin, N. Nasser, and A. Ali, "A machine learning approach for blockchain-based smart home networks security," *IEEE Network*, vol. 35, no. 3, pp. 223–229, May. 2021.

[208] H. Liu, S. Zhang, P. Zhang, X. Zhou, X. Shao, G. Pu, and Y. Zhang, "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6073–6084, Jun. 2021.

[209] A. Bugday, A. Ozsoy, and H. Sever, "Securing Blockchain Shards By Using Learning Based Reputation and Verifiable Random Functions," in *International Symposium on Networks, Computers and Communications (ISNCC)*, Istanbul, Turkey, Jun. 2019.

[210] M. Liu, Y. Teng, F. R. Yu, V. C. M. Leung, and M. Song, "Deep reinforcement learning based performance optimization in blockchain-enabled Internet of vehicle," in *IEEE International Conference on Communications (ICC)*, Shanghai, China, May. 2019.

[211] W. Hao, J. Zeng, X. Dai, J. Xiao, Q. Hua, H. Chen, K. Li, and H. Jin, "Towards a trust-enhanced blockchain P2P topology for enabling fast and reliable broadcast," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 904–917, Jue. 2020.

[212] S. Hu, Y.-C. Liang, Z. Xiong, and D. Niyato, "Blockchain and artificial intelligence for dynamic resource sharing in 6G and beyond," *IEEE Wireless Communications*, vol. 28, no. 4, pp. 145–151, Aug. 2021.

[213] J. Kang, Z. Xiong, X. Li, Y. Zhang, D. Niyato, C. Leung, and C. Miao, "Optimizing task assignment for reliable blockchain-empowered federated edge learning," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1910–1923, Feb. 2021.

[214] Z. Li, M. Xu, J. Nie, J. Kang, W. Chen, and S. Xie, "Noma-enabled cooperative computation offloading for blockchain-empowered Internet of things: A learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2364–2378, Aug. 2021.

[215] Z. Xiong, Y. Zhang, N. C. Luong, D. Niyato, P. Wang, and N. Guizani, "The best of both worlds: A general architecture for data management in blockchain-enabled Internet-of-Things," *IEEE Network*, vol. 34, no. 1, pp. 166–173, Feb. 2020.

[216] T. Idé, "Collaborative anomaly detection on blockchain from noisy sensor data," in *IEEE International Conference on Data Mining Workshops (ICDMW)*, Singapore, Nov. 2018, pp. 120–127.

[217] N. C. Luong, T. T. Anh, H. T. T. Binh, D. Niyato, D. I. Kim, and Y. Liang, "Joint transaction transmission and channel selection in cognitive radio based blockchain networks: A deep reinforcement learning approach," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. Brighton, UK: IEEE, May. 2019, pp. 8409–8413.

[218] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, "A blockchained federated learning framework for cognitive computing in industry 4.0 networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2964–2973, Apr. 2021.

[219] Y. He, Y. Wang, C. Qiu, Q. Lin, J. Li, and Z. Ming, "Blockchain-based edge computing resource allocation in iot: A deep reinforcement learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2226–2237, Feb. 2021.

[220] C. Qiu, X. Wang, H. Yao, J. Du, F. R. Yu, and S. Guo, "Networking integrated cloudedgeend in iot: A blockchain-assisted collective q-learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12 694–12 704, Aug. 2021.

[221] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1285–1297, Nov. 2020.

[222] F. Jamil, N. Iqbal, Imran, S. Ahmad, and D. Kim, "Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid," *IEEE Access*, vol. 9, pp. 39 193–39 217, Feb. 2021.

[223] Y. Lalle, L. C. Fourati, M. Fourati, and J. P. Barraca, "A privacy-protection scheme for smart water grid based on blockchain and machine learning," in *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, Porto, Portugal, Jul. 2020.

[224] C. Dai, X. Xiao, Y. Ding, L. Xiao, Y. Tang, and S. Zhou, "Learning Based Security for VANET with Blockchain," in *IEEE International Conference on Communication Systems (ICCS)*, Chengdu, China, Dec. 2018, pp. 210–215.

[225] H. Liao, Y. Mu, Z. Zhou, M. Sun, Z. Wang, and C. Pan, "Blockchain and learning-based secure and intelligent task offloading for vehicular fog computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4051–4063, Jul. 2021.

[226] J. Li, T. Liu, D. Niyato, P. Wang, J. Li, and Z. Han, "Contract-theoretic pricing for security deposits in sharded blockchain with Internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 10 052–10 070, Jun. 2021.

[227] K.-A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577–601, Firstquarter 2016.

[228] T. M. Fernndez-Carams, "From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the Internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, Jul. 2020.

[229] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of Network and Computer Applications*, vol. 126, pp. 45–58, Jan. 2019.

[230] M. Li, J. Weng, A. Yang, J. Liu, and X. Lin, "Toward Blockchain-Based Fair and Anonymous Ad Dissemination in Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11 248–11 259, Nov. 2019.

[231] M. D. Noel, O. V. Waziri, M. S. Abdulhamid, and A. J. Ojeniyi, "Stateful hash-based digital signature schemes for bitcoin cryptocurrency," in *International Conference on Electronics, Computer and Computation (ICECCO)*, Abuja, Nigeria, Dec. 2019.

[232] K. Chalkias, J. Brown, M. Hearn, T. Lillehagen, I. Nitto, and T. Schroeter, "Blockchained post-quantum signatures," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, Aug. 2018, pp. 1196–1203.

[233] M. Sato and S. Matsuo, "Long-term public blockchain: Resilience against compromise of underlying cryptography," in *International Conference on Computer Communication and Networks (ICCCN)*, Vancouver, BC, Canada, Aug. 2017.

[234] S. Yaji, K. Bangera, and B. Neelima, "Privacy preserving in blockchain based on partial homomorphic encryption system for AI applications," in *IEEE 25th International Conference on High Performance Computing Workshops (HiPCW)*, Bengaluru, India, Dec. 2018, pp. 81–85.

[235] P. Zhong, Q. Zhong, H. Mi, S. Zhang, and Y. Xiang, "Privacy-Protected Blockchain System," in *IEEE International Conference on Mobile Data Management (MDM)*, Hong Kong, China, Jun. 2019, pp. 457–461.

[236] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Bhubaneswar, India, Dec. 2017.

[237] M. Zhang, S. Wang, P. Zhang, L. He, X. Li, and S. Zhou, "Protecting Data Privacy for Permissioned Blockchains using Identity-Based Encryption," in *IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Chengdu, China, Mar. 2019, pp. 602–605.

[238] M. Harikrishnan and K. V. Lakshmy, "Secure Digital Service Payments using Zero Knowledge Proof in Distributed Network," in *International Conference on Advanced Computing & Communication Systems (ICACCS)*. Coimbatore, India: IEEE, Mar. 2019, pp. 307–312.

[239] M. H. Murtaza, Z. A. Alizai, and Z. Iqbal, "Blockchain Based Anonymous Voting System Using zkSNARKs," in *International Conference on Applied and Engineering Mathematics (ICAEM)*. Taxila, Pakistan: IEEE, Aug. 2019, pp. 209–214.

[240] D. Ding, K. Li, L. Jia, Z. Li, J. Li, and Y. Sun, "Privacy protection for blockchains with account and multi-asset model," *China Communications*, vol. 16, no. 6, pp. 69–79, Jun. 2019.
[241] Y. C. Tsai, R. Tso, Z. Liu, and K. Chen, "An improved non-interactive zero-knowledge range proof for decentralized applications," in *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)*. Newark, CA, USA: IEEE, Apr. 2019, pp. 129–134.
[242] A. S. Sani, D. Yuan, W. Bao, P. L. Yeoh, Z. Y. Dong, B. Vucetic, and E. Bertino, "Xyreum: A high-performance and scalable blockchain for iiot security and privacy," in *IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, Dallas, TX, Jul. 2019, pp. 1920–1930.
[243] S. Zhu, H. Hu, Y. Li, and W. Li, "Hybrid blockchain design for privacy preserving crowdsourcing platform," in *IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, Jul. 2019, pp. 26–33.
[244] Z. Wan, Z. Guan, Y. Zhou, and K. Ren, "zk-authfeed: How to feed authenticated data into smart contract with zero knowledge," in *IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, Jul. 2019, pp. 83–90.
[245] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, "NormaChain: A blockchain-based normalized autonomous transaction settlement system for IoT-based E-commerce," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4680–4693, Jun. 2018.
[246] H. Kang, T. Dai, N. Jean-Louis, S. Tao, and X. Gu, "FabZK: Supporting Privacy-Preserving, Auditable Smart Contracts in Hyperledger Fabric," in *Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Portland, OR, Jun. 2019, pp. 543–555.
[247] J. Fan , X. Li, T. Nie, and Y. Ge, "Survey on Smart Contract Based on Blockchain System," *Computer Science*, vol. 46, no. 11, pp. 1–10, Mar. 2019.
[248] W. Kenton. Killer application. website. Accessed 2018. [Online]. Available: https://www.investopedia.com/terms/k/killerapplication.asp
[249] China Academy of Information and Communications Technology. Blockchain white paper (2020). Accessed 2020. [Online]. Available: http://www.caict.ac.cn/kxyj/qwfb/bps/202012/t20201230_367315.htm

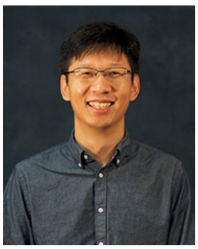
Bin Cao is an associate professor in the state key laboratory of network and switching technology at Beijing University of Posts and Telecommunications (BUPT). He received his Ph.D. degree (Honors) in communication and information systems from the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China (UESTC) in 2014. From April to December in 2012, he was an international visitor at the Institute for Infocomm Research (I2R), Singapore. He was a research fellow at the National University of Singapore from July 2015 to July 2016. He is an Associate Editor of IEEE Transactions on Mobile Computing, a Lead Guest Editor of IEEE Internet of Things Journal for Special Issue on Blockchain-enabled Internet of Things, and a cochair for big data track of IEEE Globecom 2022. He also served as Guest Editor of IEEE Sensors Journal, IEEE Transactions on Industrial Informatics, as well as symposium cochair for IEEE ICNC 2018, blockchain workshop cochair for CyberC 2019, IEEE Blockchain 2020 and TPC member for numerous conferences. He is the Founding Vice Chair of Special Interest Group on Wireless Blockchain Networks in IEEE Cognitive Networks Technical Committee. He received IEEE Outstanding Leadership Award 2020 and IEEE Broadcast Technology Society 2021 Best Paper Award. His research interests include blockchain system, internet of things and mobile edge computing, and he has extensive publications in IEEE/ACM Transactions on Networking, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Mobile Computing, IEEE Transactions on Multimedia, IEEE Transactions on Vehicular Technology, IEEE Transactions on Industrial Informatics, IEEE Transactions on Could Computing, IEEE Internet of Things Journal, IEEE Sensors Journal, IEEE Communications Magazine, IEEE Wireless Communications, and IEEE Network, and three of them are ESI Hot/Highly Cited Papers.

Zixin Wang received the M.E degree in information and communication engineering from Chongqing University of Posts and Telecommunications, Chongqing, China, in 2020. She currently is pursuing her Ph.D. degree in the State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China. Her research interests include blockchain and Internet of Things.

Long Zhang received the M.E degree in information and communication engineering from Chongqing University of Posts and Telecommunications, Chongqing, China, in 2019. He currently is pursuing his Ph.D. degree at the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu, China. His research areas include next generation mobile networks and Internet of Things.

Daquan Feng received the Ph.D. degree in information engineering from the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu, China, in 2015. From 2011 to 2014, he was a visiting student with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA. After graduation, he was a Research Staff with State Radio Monitoring Center, Beijing, China, and then a Postdoctoral Research Fellow with the Singapore University of Technology and Design, Singapore. Since 2016, he has been with the College of Electronics and Information Engineering, Shenzhen University, as an Assistant Professor and then Associate Professor. His research interests include URLLC communications, MEC, and massive IoT networks. Dr. Feng is an Associate Editor of IEEE Communications Letters, Digital Communications and Networks, and ICT Express.

Mugen Peng received the Ph.D. degree in communication and information systems from the Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2005. Afterward, he joined BUPT, where he has been a Full Professor with the School of Information and Communication Engineering since 2012. In 2014, he was an Academic Visiting Fellow with Princeton University, Princeton, NJ, USA. He leads a Research Group focusing on wireless transmission and networking technologies with the State Key Laboratory of Networking and Switching Technology, BUPT. He has authored/coauthored over 100 refereed IEEE journal papers and over 300 conference proceeding papers. Dr. Peng was a recipient of the 2018 Heinrich Hertz Prize Paper Award, the 2014 IEEE ComSoc AP Outstanding Young Researcher Award, and the Best Paper Award in the JCN 2016 and IEEE WCNC 2015. He is on the Editorial/Associate Editorial Board of the IEEE Communications Magazine, the IEEE Internet of Things Journal, and IEEE Access.



Lei Zhang is a Professor of Trustworthy Systems at the University of Glasgow. He has academia and industry combined research experience on wireless communications and networks, and distributed systems for IoT, blockchain, autonomous systems. His 20 patents are granted/filed in 30+ countries/regions. He published 3 books, and 150+ papers in peer-reviewed journals, conferences and edited books. Dr. Zhang is an associate editor of IoT Journal, IEEE Wireless Communications Letters and Digital Communications and Networks, and a guest editor of IEEE JSAC. He received the IEEE ComSoc TAOS Technical Committee Best Paper Award 2019 and IEEE ICEICT'21 Best Paper Award. Dr. Zhang is the founding Chair of IEEE Special Interest Group on Wireless Blockchain Networks in IEEE Cognitive Networks Technical Committee (TCCN). He delivered tutorials in IEEE ICC'20, IEEE PIMRC'20, IEEE Globecom'21, IEEE VTC'21 Fall, IEEE ICBC'21 and EUSIPCO'21.

Zhu Han (S'01M'04-SM'09-F'14) received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively.

From 2000 to 2002, he was an R&D Engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an assistant professor at Boise State University, Idaho. Currently, he is a John and Rebecca Moores Professor in the Electrical and Computer Engineering Department as well as in the Computer Science Department at the University of Houston, Texas. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid. Dr. Han received an NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the Journal on Advances in Signal Processing in 2015, IEEE Leonard G. Abraham Prize in the field of Communications Systems (best paper award in IEEE JSAC) in 2016, and several best paper awards in IEEE conferences. Dr. Han was an IEEE Communications Society Distinguished Lecturer from 2015-2018, AAAS fellow since 2019, and ACM distinguished Member since 2019. Dr. Han is a 1% highly cited researcher since 2017 according to Web of Science. Dr. Han is also the winner of the 2021 IEEE Kiyo Tomiyasu Award, for outstanding early to mid-career contributions to technologies holding the promise of innovative applications, with the following citation: "for contributions to game theory and distributed management of autonomous communication networks."