Integration of Blockchain and Edge Computing in Internet of Things: A Survey

He Xue, Dajiang Chen, *Member, IEEE,* Ning Zhang, *Senior Member, IEEE,* Hong-Ning Dai, *Senior Member, IEEE,* and Keping Yu, *Member, IEEE*

***Abstract*—As an important technology to ensure data security, consistency, traceability, *etc.*, blockchain has been increasingly used in Internet of Things (IoT) applications. The integration of blockchain and edge computing can further improve the resource utilization in terms of network, computing, storage, and security. This paper aims to present a survey on the integration of blockchain and edge computing. In particular, we first give an overview of blockchain and edge computing. We then present a general architecture of an integration of blockchain and edge computing system. We next study how to utilize blockchain to benefit edge computing, as well as how to use edge computing to benefit blockchain. We also discuss the issues brought by the integration of blockchain and edge computing system and solutions from perspectives of resource management, joint optimization, data management, computation offloading and security mechanism. Finally, we analyze and summarize the existing challenges posed by the integration of blockchain and edge computing system and the potential solutions in the future.**

***Index Terms*—Blockchain, Edge Computing, Internet of Things, Resource Management, Security and Privacy, Data Management**

I. Introduction

Traditional cloud computing has been used to achieve on-demand resource sharing because of its high flexibility and scalability. With the rapid development of Internet of Things (IoT) in recent years, however, the explosive growth of data has higher real-time requirements for data storage, data processing, and data exchange, which are far beyond the carrying capacity of traditional cloud computing. Specifically, in many IoT application scenarios, *e.g.*, Smart Grid and Internet of Vehicles (IoV), due to large scale data transmission between billions of devices and the data centres, high latency and bandwidth pressure limit the development of traditional cloud computing in IoT. According to the Telecommunications Industry Association (TIA), the number of connected devices on global network by 2022 will be 29 billion, and roughly 18 billion of them will be related to the IoT [1].

As an important complement to cloud computing, a new computing paradigm, named edge computing, has been proposed to expand both computing and storage capabilities from remote clouds to the edge of IoT. In this way, the resources of edge devices can be effectively used to alleviate computing, storage, and bandwidth burdens of traditional cloud computing. Edge computing can essentially offer distributed and low-latency computing services to smart cities, smart grid, smart healthcare, and other IoT scenarios [2]. Edge computing can offload computing tasks to edge devices, which are closer to data sources, thereby ensuring privacy preservation and data security [3]–[5]. However, due to the limited resources of edge devices, heterogeneity of networks, and highly dynamic environment, many existing data-security techniques cannot be fully utilized in the edge computing architecture [6].

As an alternative solution to improve the security level and efficiency of edge computing, blockchain has attracted enough attentions recently [7], [8]. Blockchain can be regarded as a decentralized ledger, which utilizes the technologies of peer-to-peer (P2P), cryptography, distributed storage, *etc.* to achieve the following properties: decentralization, transparency, traceability, security and immutability [9]. In essence, blockchain can enhance the security of edge nodes in edge computing by storing critical data at blockchain [10]. Moreover, blockchain can enable edge computing to implement security mechanisms, such as access control, authentication and privacy preservation, by using well-designed smart contracts [11]–[15]. Furthermore, blockchain can enable edge computing to orchestrate various edge resources through smart contract-based algorithms of resource allocation, task offloading and resource pricing [16], [17]. Edge computing, in turn, can support blockchain by providing enough computing resources for the mining tasks. For instance, when edge devices can provide idle resources as edge servers do, the resources will be allocated in the way of bidding and trading for blockchain.

The integration of blockchain and edge computing (IBEC) is a promising paradigm since both the two technologies can be complementary to construct frameworks to solve problems in several fields. For instance, in IoV and smart transportation, there exist challenges of insufficient on-board resources of most vehicles to support task processing and data storage, and difficulties in resources allocation brought by the mobility of vehicles [18]. To this end, the IBEC can serve IoV with collaborative management of computing and communication resources [19]–[22], data sharing and data management for automatic driving [23]–[25], collaborative identity authentication during consensus mechanism [26]–[29], *etc.* In Smart Grid, the IBEC is mainly applied to aspects of pricing and framework designing of energy trading [30]–[33], and trading security ensuring [34]–[36]. The IBEC can also benefit the other IoT scenarios, such as, Industrial Internet of Things (IIoT) [37]–[44], smart healthcare [45]–[52], edge intelligence and artificial intelligence (AI) [53]–[57], supply chain [58], [59], smart city [60]–[62], *etc.*

Moreover, other technologies (*e.g.*, cloud computing [63], fog computing [64], Software Defined Network (SDN) [65]–[67], Network Function Virtualization (NFV) [68]–[70], AI

[71]–[73]), are usually utilized in the architecture of IBEC, either to accomplish specific tasks like video stream processing and model training, or to design adaptable general frameworks for more practical and complicated networks and topologies. These studies aim to improve the processing performance of various tasks, to increase the resources utilization, and to enhance both network and data security in a more general and realistic environment.

This paper first discusses existing studies including blockchain-enabled edge computing, edge computing-enabled blockchain, and IBEC. Then the challenges and solutions including performance scalability, resource management, security and privacy computing, are summarized and discussed. Different from other similar studies which view the IBEC as a system [74] or pay attention to the solutions for edge intelligence and blockchain [75], this paper regards blockchain and edge computing as two complementary technologies and focuses on their integrations from the angle of existing issues. The other corresponding technologies are also discussed in this paper only if they contribute to the architecture design and problem solution of IBEC.

The remainder of this paper is structured as follows. In Section II, preliminaries of blockchain, edge computing and IBEC are first reviewed. Then, the issues brought by edge computing and blockchain-enabled solutions are discussed in Section III. Section IV next discusses the challenges of blockchain and the solutions brought by edge computing. After that, the general issues of the IBEC are studied in Section V. Finally, the challenges and solutions for IBEC are presented in Section VI, and the paper is concluded in Section VII.

II. An overview of Blockchain and Edge Computing

This section presents an overview on blockchain and edge computing technologies in Section II-A and Section II-B, respectively. We then discuss the opportunities brought by the IBEC in Section II-C.

A. Blockchain

Blockchain is a kind of chained data structure where data blocks are connected cryptographically and chronologically in sequence for immutability and unforgeability [76]. As shown in Fig. 1, each data block has block header and block body. The hash value of the previous block, timestamp of the block generating, version, *etc.* are recorded in the block header. Meanwhile, the transaction list is stored in the block body. Thus, blockchain can be seen as a distributed ledger [77]. Blockchain is able to carry valuable digital assets (*e.g.*, currency, copyrights, contracts, and notarization), and can be used to store or transfer the values of these assets by recording and backtracking because of its immutability and unforgeability. In other words, blockchain can deliver values. Public blockchains and private blockchains are two main types of blockchain systems [78]. A public blockchain allows any participant in the network to interact with the records on the chain, while a private blockchain requires only

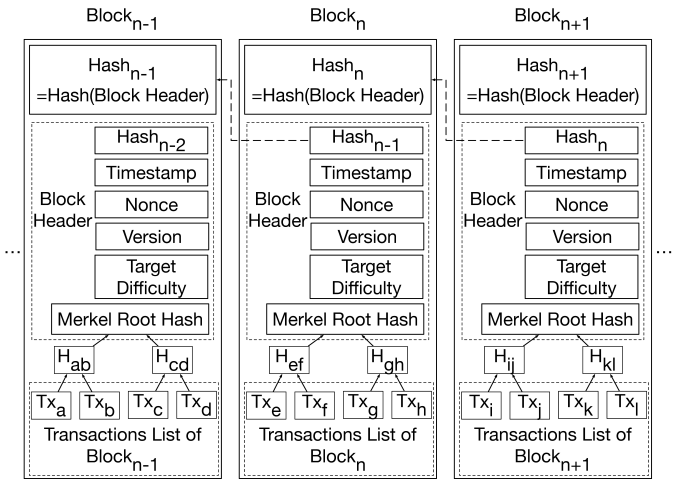

Fig. 1. Structure of Blockchain

authorized participants to perform corresponding operations. The characteristics of blockchain are summarized as follows.

- *Decentralization*: In blockchain, no organization or individual can control global data, and any node that stops working will not affect the overall operation of the system. This decentralized network will greatly improve data security [79], [80].
- *Tamper-proofing*: In blockchain, the encryption technologies are leveraged to protect data and distributed consensus algorithms are utilized to provide the consistency of data on chain. Moreover, it requires a large number of nodes (named miners) to participate in verifying transactions and generating blocks, and modifying any block of the chain requires changing at least half of nodes' subsequent blocks [81]; this is nearly impossible for a large scale blockchain network.
- *Transparency and Traceable*: The content in the block will be backed up to each node. All record information is public, and anyone can query the block data through the public interface. Each transaction is solidified into the block data through chain storage. All transaction records of all blocks are superimposed in form of hash digests through cryptographic algorithms, which can be traced back to any transaction history [82]–[84].

Blockchain is not a brand-new technology, yet a combined innovation that integrates multiple existing technologies as follows.

- *Consensus Mechanism*: The goals of consensus mechanism are to build trust among distrusted nodes and obtain rights of generating new blocks. It enables all honest nodes to maintain a consistent view of the blockchain while satisfying properties of consistency and effectiveness. Consistency means that the prefix part of the blockchain kept by all honest nodes is exactly the same. Effectiveness means the information released by an honest node will eventually be recorded in its own blockchain by all other honest nodes. The commonly-used consensus mechanisms mainly include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof

of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), *etc.*

- *Cryptography*: Cryptography [85] is one of the key technologies used in blockchains. Many classic modern cryptography algorithms are used in current blockchain applications, including hashing algorithms, symmetric encryption, asymmetric encryption, digital signatures, *etc.*
- *Distributed Storage*: Blockchain is a distributed ledger on P2P network [86]. Each participant will independently store and write block data. Different from traditional centralized storage, distributed storage has the following two advantages: each node backs up data information to avoid data loss due to single point of failure (SPoF); and data on each node is stored independently to avoid malicious tampering with historical data.
- *Smart Contract*: As a digital protocol to be executed on blockchain, smart contract allows traceable, irreversible and reliable trusted transactions with no third party intervention. It is essentially a code snippet that includes explicit functions and can be executed automatically when the conditions are met. Smart contract can be essentially used to enhance transaction security and reduce transaction costs, thereby improving end-to-end cooperation efficiency [87], [88].

B. Edge Computing

Cloud computing is struggling to deal with the data generated by massive devices in IoT due to high latency and bandwidth cost. Edge computing provides a nearby service computing paradigm that is close to objects or data sources, which can quickly respond to a variety of services and meet the basic requirements of the industry in real-time business, application intelligence, and security as well as privacy preservation [89], [90]. The characteristics of edge computing are summarized as follows.

- *Low Latency*: Edge computing provides computation resources close to the terminals physically and logically. Therefore, data generation, data processing and data usage all occur within a very close range from the data source, and the latency in receiving and responding to terminal requests is extremely low [91], [92].
- *Self-organization and High Reliability*: When network interruptions occur, edge severs can achieve local autonomy and self-recovery. With the assistance of edge severs, the central cloud only needs to perform dynamic computation offloading and schedule tasks to specific edge severs.
- *Heterogeneous and Scalability*: To fulfill the rising demands for IoT, there are a large number of heterogeneous and scalable edge devices [93]. Moreover, as a supplement of cloud computing, edge servers in edge computing environment can provide these nearby heterogeneous edge devices more efficient computing, storage and communication services; this means that the resources are moved down from cloud infrastructure to edge side, thus relieving the pressures of all aspects on the cloud layer.
- *Low Data Exposure*: Because edge devices can collect and process data locally, it is not necessary to transmit data to remote clouds. Therefore, most information, especially sensitive information, does not need to go through the network, thereby improving security to some extent.

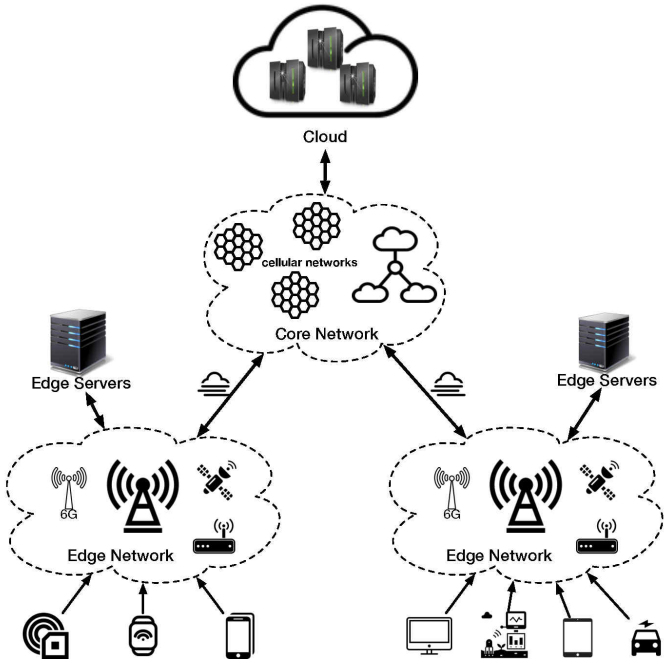

Fig. 2. Architecture of Edge Computing

As shown in Fig. 2, the entire framework of edge computing can be abstracted as a three-level hierarchical architecture as follows [7], [94]. From the edge to core are the device layer, edge layer and core infrastructure with the increased computing capability and storage capacity. The device layer is composed of large numbers of heterogeneous resource-limited IoT devices with low computing power, *e.g.*, sensors, Radio Frequency Identification (RFID) tags, cameras, vehicles, roadside units, *etc.*, which are used to achieve the functions of collecting, transmitting and uploading raw data. As the servers from the perspectives of computation, edge layer provides storage, computing and network resources to edge devices. Due to the dynamics of edge server resources and network topology, the computation offloading strategies of tasks and orchestration of corresponding resources are critical to the edge layer. The core infrastructure generally indicates the cloud layer, whose configurations are similar to cloud computing. The tasks that cannot be processed by the edge layer need to be completed in the cloud layer. Moreover, the cloud layer can also dynamically adjust the deployment strategies of the edge layer based on the dynamic allocation of edge resources.

C. IBEC

The frameworks that integrate blockchain and edge computing have been applied to many IoT scenarios, such as IoV, Smart Grid, and IIoT [74], [95]–[97]. When blockchain meets edge computing, the privacy preservation, immutability and traceability of blockchain can be leveraged to improve the security of edge computing in IoT. On the other hand,

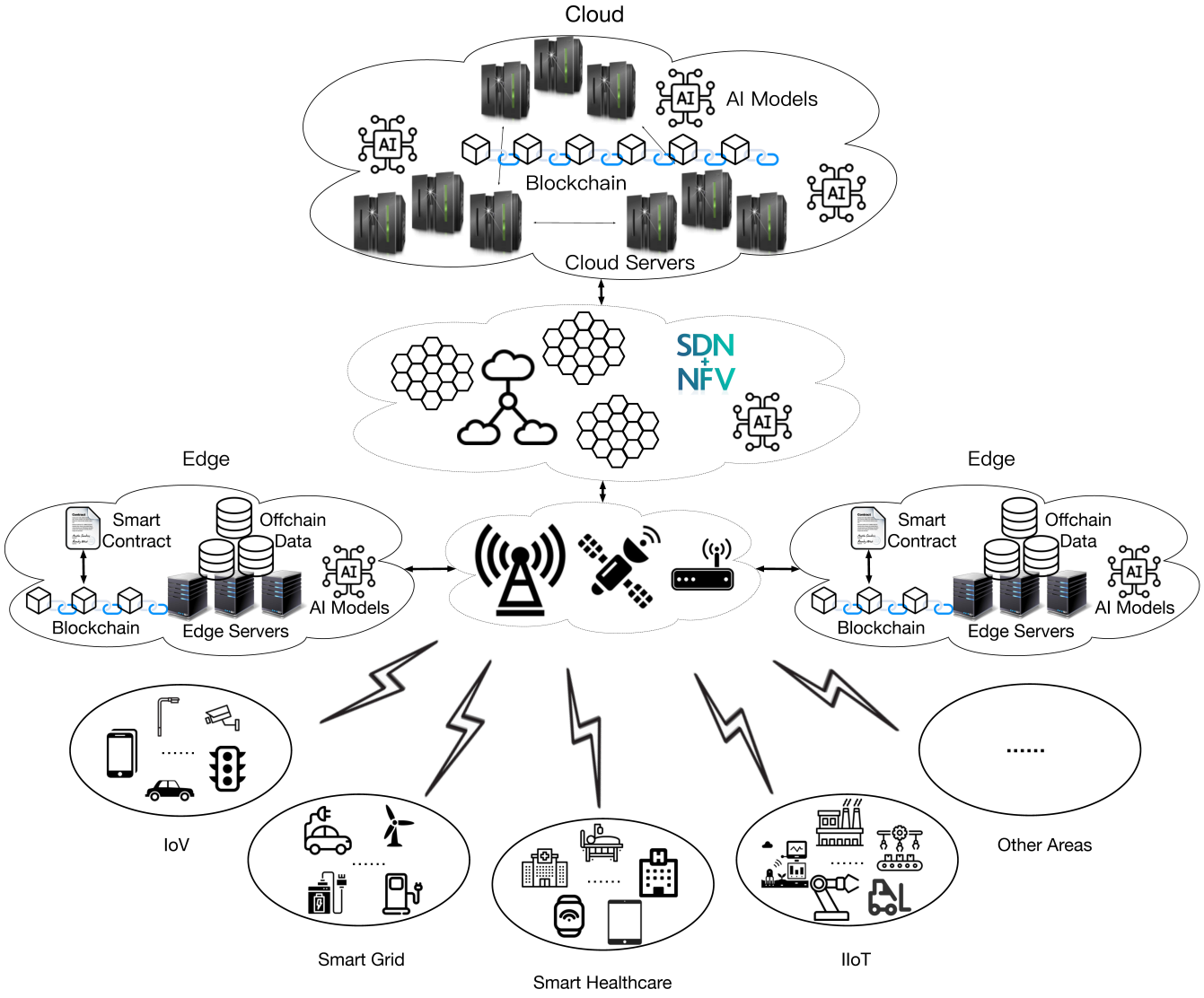

Fig. 3. Architecture of IBEC

edge computing can be utilized to provide large amount of resources for the high-performance operation of blockchain. The motivations for combining these two technologies are elaborated as follows.

- *Resource Enrichment*: The applications of blockchain in many IoT scenarios (*e.g.*, data sharing and resource management) require devices deployed on the IoT to perform consensus algorithms, broadcast or verify transactions, and record historical transactions on blockchain. It is a challenge for IoT devices with limited resources. Edge computing can provide rich storage, computing and communication resources for edge devices in these scenarios. For instance, the deployed edge servers can help the edge devices to process computation-intensive tasks [98]. Meanwhile, the storage capacity of edge servers can be used to maintain the blockchain for data sharing. Edge computing can also provide more powerful network support for edge devices.
- *Security and Privacy Assurance*: In edge computing, the dynamic topology of networks, and the mobility and heterogeneity of edge devices lead to security challenges [99], [100]. The blockchain can be used to ensure data consistency, traceability and tamper-proofing, and protect data privacy [101]. For example, with the effect of the consensus mechanism in blockchain, the participants can jointly maintain data security. Moreover, its decentralized architecture based on the P2P network fits the edge computing architecture in IoT.
- *Scalability Enhancement*: The IBEC enables resource-limited edge devices to participate in through certain design mechanisms, although edge servers can be used to assist for processing efficient tasks and maintaining blockchain. Actually, even resource-constrained edge devices can participate in mining tasks. For instance, the resource-constrained edge devices can share the collected data to obtain returns with an effective incentive mechanism in blockchain. Accordingly, the IBEC improves the scalability and flexibility of the entire system.

The architecture of IBEC is shown in Fig. 3. In this architecture, a variety of resource-limited edge devices connect to the edge network through various access ways, *e.g.*, 5G, Wi-Fi, and Bluetooth. The edge servers generally serve as blockchain nodes and miners, because the maintenance of blockchains requires sufficient storage, computing and network resources. For instance, in energy trading scenario of Smart Grid, edge servers are responsible for executing smart contracts for energy trading requesters. In data sharing scenario, edge servers train AI models in a distributed manner and finally update the AI models among all nodes through federated learning (FL) paradigm. On the top of the architecture is the cloud, which is used to deal with some highly complex tasks, which edge nodes cannot complete. For example, some raw data with high storage overhead (*e.g.*, X-ray image in healthcare) can be stored in the cloud, while their metadata is stored in blockchain.

III. Blockchain-Enabled Edge Computing

In this section, we will review the related studies of blockchain-enabled edge computing. We roughly categorize these studies into blockchain-based resource management for edge computing in Section III-A, blockchain-based security layer in Section III-B, blockchain-based data management for edge computing in Section III-C, and lightweight blockchain for resource-limited edge devices in Section III-D.

A. Blockchain-based Resource Management for Edge Computing

Resource management aims to integrate, allocate and utilize the resources (*e.g.*, computing, network and storage) in a rational, secure and efficient manner. An appropriate resource management architecture can largely improve the system performance, thereby enhancing the quality of service (QoS) and quality of experience (QoE) of users. With respect to edge computing, edge servers offer services for nearby resource-limited edge devices, which involve resource management issues such as resource allocation and computation offloading. Blockchain can enable edge computing to develop efficient resource management architectures, in which smart contracts can be used to implement specific functions, such as resource allocation, reputation establishment and resource trading.

There are several studies on blockchain-based resource management for edge computing. In [102], a resource management scheme, named BCEdge, is proposed, in which three smart contracts are designed to realize the functions of request submission, request response and optimal facility selection of tasks, respectively. Specifically, a proof-of-performance (PoP) consensus mechanism is presented in BCEdge to support the facility (*i.e.*, edge device) selection for a task. Based on the historical token exchange transaction and the contributions that a facility invested to the system, an optimal facility can be selected to process tasks in order to relieve the load of edge servers. Similarly, a blockchain-enabled device-to-device (D2D) edge computing and networks (D2D-ECN) framework is presented in [103] with a set of smart contracts for resource trading and task assignment. For low resource and energy consumption, a proof-of-reputation (PoR) consensus mechanism is proposed in [119]. Moreover, in [104], a fully decentralized resource trading market is designed, in which three smart contracts are designed to trade the fog / edge computing resources in a secure and efficient way.

To address the problem of spectrum contention access and utilize the idle spectrum in Cyber-Physical-Social-Systems (CPSSs), a blockchain and smart contract-based license-free spectrum resource management framework is proposed in [105] for processing non-real time data in edge / fog-enabled IoT network. In this framework, the mining-based and auction-based access mechanisms are designed to obtain the access license of spectrum. Moreover, in order to achieve better performance of the spectrum access, a key-micro blockchain protocol, named blockchain-KM protocol, is developed to generate two types of blocks. The key blocks are generated by PoS-after-PoW mechanism and used for recording data of spectrum owners, while micro blocks are generated by lower-PoW mechanism and used for recording transactions. Two kinds of blocks are connected into a multi-ring structure private blockchain using hash values to ensure that the data on the chain would not be tampered with.

Computation offloading algorithms can be implemented by smart contracts as well. Aiming at the coordination problem of computation offloading in mobile edge computing (MEC)-enabled ultra-dense wireless networks, a task-VM (*i.e.*, virtual machine) matching algorithm is introduced in [106] to match mobile users with suitable edge servers and implemented as a smart contract on blockchain to be performed automatically without trusted third parties. Considering both coverage of edge services and auditability during task offloading process, a private blockchain-based task offloading architecture is designed in [107] for drone-assisted MEC. In this proposed method, smart contracts with offloading policies are used to select MEC servers for task processing, in which both the process data and execution results are recorded in blockchain for auditing. To enhance the task offloading cooperation among edge servers, a blockchain-based decentralized platform in cooperative edge computing, named CoopEdge, is implemented in [108], where a reputation system based on historic task-processing performance of the edge servers is introduced to provide a trustworthy basis for the trustless task offloading environment. In CoopEdge, the incentive mechanism is employed to motivate more edge servers to participate in processing the peer-offloaded tasks, and a proof-of-edge-reputation (PoER) consensus mechanism is utilized such that the edge server with the highest reputation would be selected as a miner to add new blocks on blockchain. For the similar purpose, another blockchain-enabled incentive scheme for task sharing among edge servers in MEC environment is proposed in [109].

The above-mentioned studies on blockchain-based resource management for edge computing are summarized in Table I.

B. Blockchain-based Security Layer for Edge Computing

It is essential to ensure security and traceability in recording status data of resource management in a good resource

Table I
Blockchain-based Resource Management for Edge Computing

Refs.	Applications	Purposes	Contributions	Other Supporting Technologies
[102]	Resource Management	Improving utilization of computational resources and reducing its consumption.	Proposing a blockchain-based resource management framework named BCEdge and a PoP consensus mechanism.	No
[103]	Resource Management	Improving execution performance of time sensitive IoT applications.	Proposing a blockchain-enabled D2D-ECN framework and a PoR consensus mechanism.	No
[104]	Resource Management	Avoiding issues introduced by centralized paradigm.	Implementing a fully decentralized marketplace of fog / edge computing resources based on public blockchain network with functionalities realized by smart contracts.	No
[105]	Resource Management	Effectively managing the license-free spectrum resources in CPSSs.	Proposing a smart contract-based license-free spectrum resource management framework.	No
[106]	Computation Offloading	Addressing the coordination operations among mobile devices and edge servers in a decentralized and trusted manner.	Designing a blockchain-enabled computation offloading scheme by developing a smart contract-based task-virtual machine algorithm.	Deferred-acceptance algorithm
[107]	Computation Offloading	Achieving high-coverage and audibility of MEC services.	Proposing a private blockchain-based task offloading architecture and three smart contract-based offloading policies.	No
[108]	Computation Offloading	Enhancing cooperation among edge servers in task offloading.	Implementing a blockchain-based task processing platform with a reputation system and a PoER consensus mechanism.	No
[109]	Computation Offloading	Realizing secure task sharing in MEC.	Proposing a permissioned blockchain-based task sharing framework.	No

management architecture. Blockchain can be used in such architecture to provide a trustworthy environment and ensure data security. In [110], a blockchain-based management architecture is proposed to realize the systematically unified resource management and decentralized ecosystem construction during development and operations (DevOps) process, in which blockchain and smart contracts are deployed to provide trusted services without third party. Blockchain is also applied in [111] to guarantee the data integrity and traceability by recording the hash values of confidential data and providing the services of tracking data.

In order to help generating real-time optimal strategy to resist the uncertainties caused by resource conflict, service failure and performance degradation in the procedure of workflow scheduling in edge computing, a private blockchain is introduced in [112] to record and synchronize the data of real-time strategies and status data of edge nodes, thereby achieving secure and efficient strategies scheduling. Moreover, a non-dominated sorting genetic algorithm III (NSGA-III)-based method is designed to solve the formulated multi-objective optimization problem considering completion time and energy consumption. In [113], a blockchain-based approach is designed to ensure connectivity, availability, and survivability, which are fundamental in achieving ultra-reliable and low-latency communication in MEC.

Smart contracts in blockchain can also be used in edge computing to enhance its security [114]–[118]. In [114], a blockchain-powered trusted collaborative edge computing (CEC) service framework, named BlockEdge, is presented to enhance trustworthiness in CEC. In BlockEdge, a trust reputation system is constructed based on the deposit balances and verification results on-chain. In [115], a new blockchain, namely TrustChain, is proposed to establish a trust evaluation mechanism and realize privacy preservation for trust management and data security. Aiming to prevent attacks of selfish edge server and fake service record, a blockchain-based trust mechanism for offloading task processing in MEC is presented [116], where a blockchain is deployed to record and manage the trust information, and the consensus protocol combining PoW and PoS is developed. Two versions of edge server central processing unit (CPU) allocation and trust evaluation algorithms are designed by using reinforcement learning (RL) and deep reinforcement learning (DRL). Both the versions are used to reduce the computational consumption of edge servers by optimizing the number of CPUs and to evaluate the service reputation of edge servers using Bayesian inference. Moreover, the latter could further improve the computational performance by introducing modified Boltzmann distribution in achieving the optimal number of CPUs and applying convolutional neural networks (CNNs) to compress the state space. In [117], a consortium blockchain-enabled access control scheme in edge computing-based generic IoT environment (CBACS-EIoT) is proposed, which includes the access control phases between devices and gateway nodes as well as those between gateway nodes and edge servers, and the key management phase between edge servers and cloud servers. In [118], a security scheme for data storage and access is designed in a fully-decentralized architecture by combining blockchain and edge computing to resist the identity-revealing attack, session hijacking attack, relay attack and man-in-the-middle attack.

The above-mentioned studies on blockchain-based security layer for edge computing are summarized in Table II.

Table II
Blockchain-based Security Layer for Edge Computing

Refs.	Applications	Purposes	Contributions	Other Supporting Technologies
[110]	Resource Management	Realizing a self-organizational, secure and rational Cloud / Edge ecosystem.	Analysing challenges, introducing ALLSTAR approach including four subsystems and designing business model to motivate the participants.	Machine Learning (ML),Cloud Computing
[111]	Resource Management	Facilitating deployment and management of IoT applications and monitoring resource in IoT.	Proposing a framework of integrating heterogeneous IoT-based systems to fog / cloud named FogBus with detailed modules and services and studying a use case of sleep apnea analysis.	Cloud Computing, Fog Computing
[112]	Resource Management	Solving the uncertainties caused by resource conflict, service failure and perform degradation in cloud computing.	Proposing a blockchain and edge computing-based resource provisioning method modelled by a multi-objective optimization problem and solved by NSGA-III for uncertainty-awareness in the workflow.	NSGA-III
[113]	Caching Management	Achieving ultra-reliability communications in MEC in terms of availability, connectivity, and survivability.	Using a neural network for a blockchain-based intelligent content transport mechanism and smart contracts for unmanned aerial vehicles (UAVs) caching functionalities.	Neural Network, UAV
[114]	Trust Mechanism	Guaranteeing trustworthiness in collaborative edge computing process.	Presenting a blockchain-enabled collaborative edge computing called BlockEdge with functionalities of distributed ledger, incentive scheme and reputation mechanism.	No
[115]	Trust Mechanism	Optimizing security issues, system delay and resource consumption of traditional blockchain.	Presenting an edge computing-enabled privacy preservation permissioned blockchain named Trustchain for decentralized security concerns.	No
[116]	Trust Mechanism	High processing performance and data security in MEC.	Formulating a blockchain-based trust mechanism to resist selfish edge attacks and faked service record attacks, and applying DRL for computational resource allocation decision.	DRL
[117]	Access Control	Achieving secure communication among various entities in edge-based IoT network.	Designing a consortium blockchain-based access control scheme to offer mutual authentication between different layers in edge-based IoT environment.	No
[118]	Authentication	Realizing privacy preservation and data security in edge computing.	Proposing a decentralized security scheme named DecChain for user authentication, data storage and data access.	No

C. Blockchain-based Data Management for Edge Computing

In edge computing, the operations of massive edge devices will generate a large amount of data, which can be further used for subsequent data analysis and data processing. The generated data needs to be stored and sometimes shared securely. The decentralization, immutability, and traceability of blockchain can enable edge computing to achieve secure data management. In [120], a blockchain-based trusted data management scheme in edge computing, named BlockTDM, is proposed. BlockTDM supports a range of functions, including mutual authentication for membership management and responsibility tracing, and multi-signature-based PBFT consensus and matrix-based multi-channel data segment for data privacy preservation. Moreover, user-defined sensitive data encryption, conditional access and decryption query of protected transactions are implemented in form of smart contracts.

Training by AI models, data can be transferred into valuable knowledge and data trading is equivalent to knowledge sharing to some extent. Knowledge sharing in edge computing can be enabled by blockchain [121]–[123].

In [121], a user-centric blockchain (UCB) framework is presented to deal with the security problems of weak copyright protection, untrusted accounting at edge and inefficient consensus in knowledge sharing. In UCB, a proof-of-popularity (PoP) consensus mechanism is proposed, which includes user-centric proposal value ranking and electing algorithm and security-aware block generating algorithm.

In [122], a blockchain-based knowledge trading market in edge-AI-enabled IoT is presented, in which a consortium blockchain is used to construct the market platform and smart contracts of both knowledge management and knowledge trading are designed to ensure the decentralization, tamper-proofing and confidentiality. Moreover, a proof-of-trading (PoT) consensus mechanism is proposed by combining PoW and PoS to reduce energy consumption. Moreover, optimal knowledge pricing strategy is derived as incentive mechanism through Karush-Kuhn-Tucker (KKT) condition that is based on game theory.

Similarly, in order to motivate content sharing in MEC, a blockchain-based solution is proposed [123], where base stations serve as edge servers and allocate computing power to run mining tasks to reward cache-enabled sharing mobile devices. By considering linear and nonlinear relationships

Table III
Blockchain-based Data Management for Edge Computing

Refs.	Applications	Purposes	Contributions	Other Supporting Technologies
[120]	Data Management	Solving the data security and privacy problems in edge computing environment.	A blockchain-based data management scheme with the functionalities of data isolation by multi-channel, on-chain data encryption and access control by smart contract.	No
[121]	Data Sharing	Solving resource limitations problems and guaranteeing data security of data sharing process in intelligent edge.	Designing an appropriate user-centric blockchain-enabled knowledge sharing framework with a PoP consensus for low energy and low latency.	AI
[122]	Data Sharing	Achieving data trading among heterogeneous edge-AI devices in IoT.	Implementing a knowledge trading market with a consortium blockchain as a ledger for secure and efficient transactions management, designing of digital coin and PoT consensus and noncooperative game-based pricing strategy.	AI
[123]	Incentive Mechanism	Encouraging content sharing among mobile devices in D2D network.	Developing two kinds of caching placement schemes considering relationships between allocated computing power and shared data size.	No
[124]	Communication	Guaranteeing the reliability of data transmission in the IoT.	Proposing a data transmission mechanism in edge computing environment based on an optimized blockchain where the edge servers maintain and update the full blockchain, and the general lightweight nodes utilize the data on the chain and the consensus mechanism is redesigned as PoR.	No

of computing power and shared data size, optimal caching schemes are developed to maximize total profit and solved respectively by KKT conditions-based solution and difference of convex (DC) programming algorithm.

In [124], a blockchain-based data transmission scheme is developed for D2D communication in edge computing, where a proof-of-reliability (PoR) consensus mechanism is designed such that the users with enough credit and supporters would be allowed to transmit data. The blockchain is introduced to ensure the tamper-proofing and traceability of data (*e.g.*, messages and behaviour data) in the IoT.

The above-mentioned studies on blockchain-based data management for edge computing are summarized in Table III.

D. Lightweight Blockchain for Resource-limited Edge Devices

When blockchain is used for resource management in edge computing, it requires a large amount of computation resources for consensus algorithms and enough storage resources for storing full blockchain. Thus, how to support the development of blockchain in edge computing is the priority issue in blockchain-based resource management.

There are a number of studies on redesigning lightweight blockchains [125]–[128]. In [125], a lightweight blockchain named LiTiChain is proposed to adapt to the edge-enabled IoT system. In LiTiChain, both transactions and blocks that have a time-limited characteristic are stored in the form of Endtime Ordering Graph (EOG, a data structure of tree in blockchain). The EOG is based on the order of the end time and an expired block would be deleted to save the storage resources on the edge nodes. Specific algorithms of k-height insertion and deletion / renewal of a block are designed to adjust the structure of EOG to maintain the order of blocks. In [126], a novel blockchain is redesigned to suit the edge computing environment, in which the optimal blocks storage allocation and recent blocks caching strategies are presented to achieve fair storage and quick efficient access of blocks. Moreover, an improved PoS consensus mechanism is designed for battery-limited edge devices to motivate the nodes to own more tokens and store more data.

An efficient consensus method is proposed in [127] to solve the mathematical puzzle of PoW consensus by using expectation maximization algorithm and polynomial matrix factorization. In [128], a proof-of-authentication (PoAh) consensus algorithm is presented, in which blocks could be packaging by all the nodes and signed by their private keys. In this proposed algorithm, the selected trusted nodes are responsible for verifying block validation by checking the Media Access Control (MAC) values with the corresponding public key.

The above-mentioned studies on lightweight blockchain for resource-limited edge devices are summarized in Table IV.

IV. Edge Computing-Enabled Blockchain

In this section, we will discuss how to use edge computing to benefit blockchain.

As a new computing paradigm, edge computing can provide sufficient resources for resource-limited edge devices to support blockchain. In other words, edge computing can be regarded as a resource enabler for blockchain. In [129], a MEC-enabled blockchain framework is proposed for IoT, in which mining as a service (MaaS) is designed for IoT devices to purchase computational resources in clouds. In [130], a blockchain-based resource allocation scheme is proposed in UAV-enabled edge computing environment, where the resources are allocated between edge computing stations (ECSs)

Table IV
Lightweight Blockchain for Resource-limited Edge Devices

Refs.	Applications	Purposes	Contributions	Other Supporting Technologies
[125]	Blockchain structure redesign	Designing appropriate blockchain for edge-based IoT.	Proposing a lightweight blockchain called LiTiChain using graphs and two algorithms of inserting a block and deleting / renewing a block.	No
[126]	Blockchain structure redesign	Designing appropriate blockchain and consensus mechanism for edge computing.	Proposing a redesigned blockchain with an improved PoS mechanism and a recent block storage allocation strategy.	No
[127]	Consensus Mechanism optimization	Achieving an efficient solution for PoW.	Designing an expectation maximization algorithm and polynomial matrix factorization-based approach for PoW.	Cloud Computing, Fog Computing
[128]	Consensus Mechanism optimization	Designing appropriate consensus mechanism for resource-limited edge devices.	Proposing a novel consensus algorithm called PoAh.	No

and UAVs, and all data related to the process of resource trading would be recorded in blockchain to achieve tamper-proofing and traceability. The Multi-leader Multi-follower game is utilized to formulate the interactions between ECSs and UAVs in resource trading process. The Lagrangian-based solution is designed to solve the profit-maximization problem of ECSs to obtain the optimal resource pricing, and the Bellman dynamic programming-based solutions under open loop situation and feedback situation are employed to address the differential game-based resource demands optimization problem.

Edge computing can be used to derive an optimal resource allocation scheme for blockchain mining tasks. In [131], a hierarchical Edge-Cloud computation offloading scheme is presented to obtain optimal resource pricing strategies by using game theory and RL technique. In [132], the Multi-leader Multi-follower game is used to formulate the interactions between miners and cloud / edge providers, and an Alternating Direction Method of Multipliers (ADMM) algorithm is adopted to cope with the standard Equilibrium Problem with Equilibrium Constraints (EPEC) challenge caused by the high dimensionality of each miner's strategy space, thereby obtaining the maximum profits of providers in consideration of utilities of miners. Moreover, a combinatorial double auction-based resource allocation scheme and a pricing strategy are designed to achieve budget balance, individual rationality and truthfulness in the auction process [133].

Non-mining-devices in IoT can also be considered as resource providers. In [134], a collaborative mining network (CMN) is constructed to realize collaborative mining between miners and idle IoT devices or between miners and resource-sufficient edge servers. The optimization problem between miners and non-mining-devices within a CMN is formulated as a double auction game to calculate the optimal auction price in order to maximize the whole utility of the two sides. The computation offloading model between edge servers and CMN nodes is formulated into a Stackelberg game to maximize the profits of edge servers, miners and idle IoT devices. In [135], two mining schemes: immediate reporting (IR) after successfully computing and strategically reporting (SR) after successfully computing are considered in order to obtain optimal profits of both miners and edge service providers in IR and SR schemes.

In [136], an edge computing-based parallel processing framework is designed to improve the scalability of blockchain, where the blockchain is deployed as a decentralized database to synchronize and store the activity data of IoT devices, and the edge nodes are configured to provide the validator service to perform the parallel processing algorithm.

The above-mentioned studies on edge computing-enabled blockchain are summarized in Table V.

V. Existing Issues and the Corresponding Solutions in IBEC

This section discusses research issues brought by the IBEC.

A. Resource Management for IBEC

The resource management is the key for integrating blockchain and edge computing to provide diversified services with high quality. In [137], a blockchain-based resource trading system is proposed for video transcoding and is delivered to satisfy various requirements of users in MEC. In this system, small base stations (SBSs) with MEC servers are regard as miners to generate and verify new blocks. Meanwhile, the video providers work on remote cloud networks and are responsible for video transcoding. Moreover, mobile users should pay for the services of transmission and transcoding to edge servers / SBSs and video providers. The whole resource trading process is self-organized by a series of smart contracts and is modelled into a three-stage Stackelberg game, and a resource allocation iteration algorithm is designed to solve the optimization problem. To improve the efficiency of video stream transcoding, a MEC and blockchain-enabled transcoding framework is proposed in [138], where the transcoding tasks are divided and offloaded to the nearby D2D nodes or small-cell base stations (SBSs). For the purpose of achieving maximum average profit of transcoding service, the ADMM-based solution is proposed in form of smart contracts

Table V
Edge Computing-enabled Blockchain

Refs.	Applications	Purposes	Contributions	Other Supporting Technologies
[129]	Resource Allocation	Solving PoW puzzles on edge nodes.	Reviewing MEC architectures and proposing an edge computing-enabled blockchain framework.	No
[130]	Resource Allocation	Optimal resource allocation between UAVs and edge computing servers for blockchain applications.	Proposing a resources pricing and trading scheme by using Stackelberg game.	Game Theory
[131]	Resource Pricing	Maximizing profits of both edge service providers and miners in the process of computation offloading.	Proposing a two-layer computational offloading paradigm and investigating two practical scenarios.	Game Theory
[132]	Resource Pricing	Achieving optimal utilities of miners and profits of resource providers.	Designing a resource trading scheme by formulating a Multi-leader Multi-follower-based problem and utilizing an ADMM algorithm to solve the problem.	Game Theory, ADMM algorithm
[133]	Computation Offloading	Offloading mining tasks to edge nodes.	Proposing a double auction-based resource allocation scheme for mining tasks and solving it by the step / smooth greedy algorithm-based solution.	No
[134]	Computation Offloading	Utilizing idle communication and computational resources on both non-mining-devices and edge clouds for mining tasks.	Proposing a resource trading scheme including double auction game-based task offloading to non-mining-devices and Stackelberg game-based task offloading to edge cloud operators.	Game Theory
[135]	Resource Pricing	Achieving optimal profits for both miners and edge service providers.	Proposing autofit strategies including IR and SR to obtain the maximum profit of the resource pricing problem based on the two-stage Stackelberg game.	Game Theory
[136]	Data Processing	Improving scalability of blockchain and data security in edge computing-based IoT network.	Implementing an edge computing-based parallel data processing architecture for blockchain mining tasks where blockchain ensures data security.	No

to obtain the optimal block size, offloading scheduling, and computation and spectrum resource allocation. To maximize the system efficiency of multi-task resource allocation with the constraints of individual rationality, truthfulness and budget balance, two smart contract-based incentive mechanisms are designed in the IBEC system [139]. Specifically, a double auction mechanism based on breakeven (DAMB) is proposed to satisfy constraints of all sellers and buyers, and a breakeven-free double auction mechanism (BFDA) is presented to handle more tasks for system efficiency further improvement with less buyers' truthfulness.

In [140], a MEC-based blockchain-as-a-service (BaaS) system is proposed to realize efficient resource management and long-term reward in IoT networks, where UAVs are deployed as aerial base stations (BSs) and work with other terrestrial BSs in the MEC model. In this system, the interactions between BSs and blockchain nodes are formulated into a stochastic Stackelberg game with multi leaders / BSs and multi followers / blockchain nodes. The follower's action is regarded as partially observable Markov Decision Process (POMDP) and the leader's random state is modelled as a Markov Decision Process (MDP) according to the optimal responses from followers. An unsupervised polynomial-time Bayesian deep learning (BDL) algorithm is developed for followers to achieve optimal strategies and an unsupervised polynomial-time deep Q-learning (DQL) algorithm is designed correspondingly for leaders to maximize the expected long-term rewards. Another related work is [141], in which the resource management of both general computing tasks and mining tasks in IoT applications is studied in order to achieve both the optimal response strategies of miners and the optimal prices of service providers.

Besides computation resource, the allocation of caching and network resources is the key for high-quality services in the IBEC. In [142], a blockchain-based trustworthy edge caching scheme is proposed, in which smart contracts are used to record and maintain the transactions and payment information among edge nodes and mobile users. In this scheme, a pricing mechanism based on historical demands of mobile users for edge nodes, a gradient descent-based optimal caching demand seeking algorithm for mobile users, and a max-min-based fair caching resource allocation algorithm are designed as a trusted and efficient resource allocation solution to improve the QoE in mobile cyber-physical system (MCPS).

With the purpose of raising caching hit rate in edge computing environment, a blockchain-assisted compression algorithm of FL for content caching named CREAT is proposed in [143], which includes the FL-based proactive content caching algorithm (FPCC) and compression algorithm. The FPCC algorithm is designed for edge nodes to train the models using local data and predict caching contents according to the popularity and the trained models. The compression algorithm is applied in FPCC to improve communication efficiency of FL by compressing the uploaded gradients. Moreover, four smart contracts are designed to interact with the deployed blockchain to ensure data security. Based on Hyperledger Fabric, a multi-domain edge network resource management framework is implemented in [144], where service-level agreements (SLAs) are written in smart contracts and stored on blockchain. The data of escrow accounts, transaction number and domain

Table VI
Resource Management for IBEC

Refs.	Applications	Purposes	Contributions	Other Supporting Technologies
[137]	Resource Management	Realizing a secure and efficient video transcoding and delivery approach in distributed environment.	Presenting a smart contract-based MEC network architecture and video transcoding and delivery approach and designing an iteration algorithm as a systematic solution.	Game Theory
[138]	Resource Management	Efficient and high-yield video stream transcoding service.	Proposing a blockchain and MEC-enabled transcoding framework with an ADMM algorithm-based optimal resource allocation solution.	ADMM algorithm
[139]	Resource Management	Efficient and appropriate incentives for resource allocation.	Proposing a multi-task cross-server resource allocation framework using IBEC and designing DAMB and BFDA to maximize the system efficiency.	Game Theory
[140]	Resource Management	Adaptive and efficient communication resource management in blockchain-enabled MEC.	Proposing a service resource trading framework using blockchain and MEC, and respectively designing a hierarchical RL-based solution and an unsupervised hierarchical deep learning (DL) algorithm for complexity reducing and uncertainties prediction.	DL, RL, Game Theory
[141]	Resource Management	Adaptive and efficient computational resource management in blockchain-enabled MEC.	Developing a computational resource trading framework using blockchain and MEC, and designing a hierarchical RL-based interaction decision making approach.	DL, RL, Game Theory
[142]	Caching Management	Secure and efficient edge caching scheme for mobile edge users.	Proposing a blockchain-based edge caching scheme utilizing smart contracts to record and maintain transactions and designing a pricing mechanism for edge nodes, a gradient descent-based demands seeking algorithm and an optimal caching allocation algorithm for mobile users.	Gradient Decent algorithm
[143]	Resource Management	Improving cache hit rate in edge computing.	Designing a blockchain-enabled compressed algorithm of FL named CREAT for training model on decentralized edge nodes and reducing communication load in FL by compressing gradients.	FL
[144]	Network Management	Jointly satisfying the trusted and transparent requirements of QoS and optimizing network by resource allocation.	Implementing a Hyperledger Fabric-based multi-domain network management framework with end-to-end network slicing and service-level assurance providing.	5G, Network Slicing
[145]	Resource Management	Realizing trusted and transparent relationships, and seamless and dynamic resource exchange in current / future decentralized wireless network.	Foreseeing the integration of blockchain, edge computing and SDN for wireless network virtualization and presenting a corresponding architecture with the resistance of double spending attack without the usage of high-speed backhaul links.	SDN
[146]	Resource Management	Improving resource utilization and system flexibility and maintaining low latency.	Proposing a SDN-enabled IoT network architecture to integrate blockchain and edge computing with a task offloading algorithm to offload tasks to OpenFlow switches.	SDN, Fog Computing

edge orchestrator (DEO) ID is received by multi-domain edge orchestrator (MDEO) and recorded on blockchain, which not only supports network slicing resources provisioning algorithm to perform in a trustworthy and transparent manner, but also satisfies the SLAs, thus improving the QoS.

In [145], an architecture of fusion of blockchain, edge computing and SDN is presented to make a foreseeing on wireless network virtualization, where blockchain and edge computing are designed to resist the double-spending attack without the usage of the high-speed backhaul links. The architecture can be used to realize trusted yet transparent relationships, and resource exchange in current / future decentralized wireless network seamlessly and dynamically. In [146], edge / fog computing and SDN are introduced into the IoT network to develop a high flexible framework of IoT system, and blockchain is employed to ensure the reliability, availability and scalability of the overall system.

The above-mentioned studies on resource management for IBEC are summarized in Table VI.

B. Joint Optimization for IBEC

If the IBEC is regarded as an overall system and they are regarded as two subsystems, there exist joint optimizations for both subsystems. In [147], an allocation framework of radio spectrum and computational resources is proposed based on blockchain and MEC. The constraints of user association, data rate allocation, CPU-cycle frequencies of both offloading tasks and blockchain system, and block producer scheduling are jointly considered to obtain an optimal balance between the energy consumption of MEC and the delay / time to finality (DTF) of blockchain. The above optimization problem is formulated into a mixed-integer nonlinear programming (MINLP) problem. In [148], a resource allocation approach for wireless networks in blockchain-enabled mobile edge computing (B-MEC) framework is proposed, in which the consensus mechanism basing on PBFT is deployed. In this approach, by considering spectrum allocation, block size and the number of consecutive producing blocks per producer, a joint optimization problem is formulated as a MDP to simul-

Table VII
Joint Optimization for IBEC

Refs.	Applications	Purposes	Contributions	Other Supporting Technologies
[147]	Resource Management	Achieving optimal performance balancing between blockchain system and MEC system.	Formulating an optimization framework with IBEC by jointly considering user association, data rate allocation, block producer scheduling and CPU-cycle frequencies and designing corresponding algorithms for minimization of both energy consumption and delay / time.	No
[148]	Resource Management	Intelligent and secure resource management in future wireless network.	Proposing an integrated framework of blockchain and edge computing with PBFT and PoS-based consensus mechanisms and DRL-based solution for the optimization problem of system performance by jointly considering spectrum allocation, block size and the number of consecutive blocks.	Double-dueling DQN
[149]	Resource Management	Efficient integration of ML into edge computing-based IoT.	A collective learning approach by integrating DQL and blockchain and an improved consensus mechanism of PoL are jointly employed on solving resource allocation problems in networking integrated cloud-edge-end architecture.	DQL
[150]	Communication	Maintaining data transmission in a secure and reliable manner in damaged M2M communication networks.	Proposing a blockchain and edge computing-enabled M2M communication framework using UAVs for communication connectivity and designing a dueling DQN-based optimizing algorithm to improve data computation capacity and throughput of the blockchain.	Dueling DQN
[151]	Resource Management	Satisfying requirements of processing power, security and performance for delay-tolerant data in M2M communication networks.	Introducing a blockchain and edge computing-based system performance joint optimization framework and selecting dueling DQN as the solution of the formulated optimization problem by considering caching, computation and blockchain security.	Dueling DQN
[152]	Incentive Mechanism	Motivating users to participate in idle resource sharing.	Constructing a smart contract-based D2D cache and delivery market with pPBFT as the consensus approach and blockchain as the decentralized ledger and designing a DRL-based solution for caching placement and smart contract performing nodes selection.	DRL
[153]	Computation Offloading	Secure and efficient computation offloading and resource allocation schemes in MEC.	Proposing a blockchain-enabled resource managing joint optimizing framework with an asynchronous advantage actor-critic RL algorithm as the solution for maximizing computation rate of MEC system and transaction throughput of blockchain system.	DRL, RL

taneously obtain the optimal performance of both MEC and blockchain. The performance measurement indexes include average execution delay of MEC and the throughput and time to finality / confirmation latency of blockchain. A DRL-based algorithm is designed by using double-dueling deep Q-network (DQN) to solve the above-mentioned problem.

To solve the joint optimization problem of integrated networking and computing resource allocation, a blockchain-enabled DQL approach, named collective Q-learning (CQL), is proposed in [149]. In this approach, parts of the learning models are trained by the decentralized IoT nodes locally, and blockchain is used to record and share learning results in a secure, reliable and auditable manner. Instead of PoW, the designed proof-of-learning (PoL) consensus mechanism allows the nodes (who train the Deep Neural Network, namely DNN, with minimum reduced percentage of learning loss function) to generate the new blocks and even to trade these if they want. Utilizing the similar technologies, in [150], a resource allocation scheme is proposed for data transmission process in UAV-assisted machine-to-machine (M2M) communications to maximize the data computation capacity and throughput of blockchain. In this scheme, the blockchain is utilized to ensure data security and privacy, and the MEC is used to improve computing power. The optimization problem of resource allocation is formulated and solved by dueling DQN to achieve the optimal strategy including data transmission request, computing node selection, block size decision and block interval decision.

In [151], a blockchain and edge computing-enabled resource joint optimization framework is presented for delay-tolerant data in M2M communications, in which the data is transmitted periodically and can tolerate a relatively long latency. In order to solve the time-varying problem, the DQN-based approach is designed and the optimal selections and decisions on caching servers, computing servers and blockchain system are obtained to further satisfy the requirements of system rewards. Other related studies include cooperative computation offloading and resource allocation [153], and the D2D and MEC caching [152], in which DRL is used to develop solutions for the corresponding joint optimization problems. Moreover, in [152], the partial Practical Byzantine Fault Tolerance (pPBFT) consensus mechanism is proposed for smart contract execution nodes to decide whether or not to execute and push one transaction, and the integrated DPoS and aBFT mechanism is proposed to

reach the block producing consensus.

The above-mentioned studies on joint optimization for IBEC are summarized in Table VII.

C. Data Management Framework for IBEC

Different from resource management, data management focuses on the secure and efficient access, sharing, and tracing the data generated from edge computing-enabled IoT environment. Blockchain can provide a decentralized and third-party-free environment in edge computing based on the characteristics of the underlying P2P network. Accordingly, the decentralization and self-organization of a data management system can be guaranteed by using blockchain. In [154], a blockchain and AI-enabled edge computing platform, named Edgence, is proposed for intelligent management of massive decentralized applications (dApps) in IoT. In Edgence, a three-tier verification including smart contract verification is designed to provide different ways for various demands of IoT-based dApps. Moreover, decentralized crowdsourcing and decentralized AI training are integrated to realize intelligent management without data transmission to cloud to reduce latency and protect data privacy. To manage data generated by IoT devices, a three-layer data management architecture (*i.e.*, the device layer, fog layer and cloud layer) is proposed in [155], which combines blockchain, edge computing, SDN and NFV. The smart contract-based access management algorithm and orchestration management algorithm are designed to automatically handle requests from IoT devices without any third party, and the combination of NFV and SDN are used to optimize the performance of resource allocation.

Since a large amount of sensitive data is required to store in the IBEC system securely, secure storage is a key issue in data management. In [156], edge servers integrated with blockchain are utilized to provide large storage securely, in which the issues of integrity, adaptability and anonymity are addressed separately by Data Integrity Service (DIS), off-chain state channels (provided by Lightning networks or Raiden networks) and a hybrid cryptographic mechanism with linkable ring signature and zerocash techniques. In [157], a secure data storage scheme in edge computing is proposed by using blockchain and regeneration code to cope with the challenges brought by resource-limitations of sensors and data diversities. Specifically, based on the general three-tier edge computing architecture, a global blockchain is deployed at the cloud layer to store all the data, and regenerative code technology is integrated to provide data redundancy so as to improve data reliability. Moreover, a local lightweight blockchain is maintained by edge servers at the edge layer and is deployed on the IoT layer. The data transmission mechanisms between IoT devices and the local blockchain are designed to periodically synchronize data in order to ensure data integrity.

In the IBEC, blockchain can be used for data trading or sharing in a decentralized manner. This is mainly because the incentive mechanism in blockchain can motivate data producers to share high-quality data [158]–[160]. For instance, a four-layer data trading architecture, named EdgeBoT, is introduced in [158] for the IoT system by combining edge computing and Ethereum blockchain. In this architecture, edge gateways are designed to run AI algorithms, blockchain and smart contracts. Due to the built-in security mechanisms of blockchain, the architecture can be used to realize data processing and decision making locally, thereby reducing the bandwidth consumption of data uploading. In [160], a blockchain-enabled secure data aggregation strategy (BSDA) is proposed for edge computing-based IoT. In this method, a new block generation algorithm is designed to improve the throughput and reduce transaction latency. The labels of security level and task completion requirements are put into the block header to restrain the task receivers, *e.g.*, mobile data collectors (MDCs). Moreover, integrated with MDCs partition, sensitive task decomposition is adopted to preserve the privacy and to resist the collusion attack simultaneously. Besides, with the higher MDC configurations of security level and task completion conditions than those recorded in block header, a DRL-based self-adaptive double bootstrapped deep deterministic policy gradient (IDDPG) method is developed to achieve data aggregation with energy-efficiency.

The above-mentioned studies on data management framework for the IBEC are summarized in Table VIII.

D. Computation Offloading for IBEC

Computation offloading refers to transferring the entire or part of a task to nearby edge servers to execute for resource-constrained edge devices. During the transferring process, data about the tasks is vulnerable to be attacked in the sophisticated environment. In this regard, blockchain can be used as a ledger to ensure data consistency and integrity by recording the status data of resource allocation and task offloading on-chain.

In [161], a blockchain-enabled edge computing system, named DeTEC, is designed by utilizing the idle computing resources for task offloading in a decentralized and trusted manner. Taking capacity and fairness of the edge servers into consideration, the optimal task allocation problem is proposed in order to minimize the total latency, and is solved by the heuristic allocation (Heu-Alloc) algorithm. Specifically, when the task requests from IoT devices are collected, the Heu-Alloc algorithm is run to generate a scheduling scheme, which is sent to the smart domain name server (DNS). The appropriate edge server is selected to process the corresponding tasks and return the results to IoT devices. Moreover, two verification schemes are designed to improve the verification speed. In DeTEC, blockchain serves as a distributed ledger to record the contributions of edge servers so as to reward them for their computations.

In [162], a blockchain-enabled computation offloading scheme named BeCome is proposed for IoT in MEC to obtain the optimal offloading scheme. In this scheme, VM instances are used for provisioning physical resources in IoT, and a VM allocation ledger updating algorithm is presented to monitor resource utilization. Considering the modelled total time consumption, total energy consumption and the level of load balance, a candidate computation offloading strategy generating algorithm is designed using NSGA-III. Moreover, a

Table VIII
Data Management Framework for IBEC

Refs.	Applications	Purposes	Contributions	Other Supporting Technologies
[154]	Data and Resource Management	Efficient, intelligent and cost-cutting management of heterogeneous decentralized applications in IoT jointly using edge clouds and blockchain.	Proposing a dApps management platform with three-tier validation for better demand satisfaction and AI training based on blockchain and edge computing.	DL
[155]	Data and Resource Management	Convenient and efficient access, managing and processing mass IoT data and secure resource management.	Proposing a hybrid architecture using blockchain, edge computing, cloud computing, SDN and NFV together and designing the corresponding algorithms.	SDN, NFV
[156]	Data Management	Achieving a secure and practical decentralized data storage solution in edge computing.	Proposing a solution framework for anonymity, integrity and adaptability of data storage by reviewing the challenges and requirements of deployment of blockchain and edge computing in IoT systems and implementing a system prototype utilizing Ethereum's JavaScript API.	No
[157]	Data Management	Solving security of data stored in edge computing environment.	Proposing a storage architecture with global blockchain deployed on the cloud layer and local lightweight blockchain running on IoT devices for storage of data hashes.	No
[158]	Data Management	Secure and efficient data trading environment in IoT.	Presenting a data trading platform using Ethereum with consensus of proof-of-concept (PoC).	No
[159]	Data Management	Security and privacy-assured data management framework for privacy-critical systems.	Implementing a private Ethereum blockchain-based edge computing architecture using AI for data analysis on edge nodes locally and the learned data is shared by smart contracts.	Ethereum, AI
[160]	Data Management	Secure and efficient data sharing in edge-enabled IoT.	Developing a blockchain-based data aggregation strategy and designing a DRL-based self-adaptive double bootstrapped deep deterministic policy gradient solution.	DRL

simple additive weighting method and a multi-criteria decision making method are employed to calculate the highest utility value of the strategies; this means obtaining the optimal scheme among the candidates. Blockchain is used in this scheme as a dynamic VM allocation ledger to record the resource utilization data of edge devices and the unoccupied VM instances in order to provide the integrity of data. For edge computing in 5G environment, the same problem is also raised and solved with a blockchain-based solution in the same way [163].

To minimize the total cost of the mobile equipment (ME) in edge computing, a blockchain-based joint computation offloading and coin loaning system is proposed in [164]. In this system, the problem that the ME either chooses to loan from banks and pay for task offloading to edge servers, or chooses to compute locally is formulated as a noncooperative game. The developed smart contracts on computing resource trading and coin loaning are deployed and run in an on-chain manner. Subsequently, the performance and QoE of users are improved by a series of optimizations as mentioned in [165], which include a consortium blockchain-based edge computing system with a group-agent strategy for trust computing, a task sorting mechanism for resource allocation improvement, and a content search model based on popularity for search optimization.

In [166], a MEC-enabled PoW task offloading scheme is proposed by redesigning a micro-blockchain for high offloading performance. In this scheme, only the block headers are stored an on-chain way, and a lightweight account tree structure is illustrated and put into the block header to record and update account balances of mobile users. Moreover, a DL-based block data offloading (BDO) algorithm is designed to achieve optimal offloading schedule in order to maximize the utility of users. Furthermore, the adopted neural network model is trained to optimize its weights and biases by minimizing a loss function. In [167], an online DRL-based computation offloading approach is designed to achieve policy self-adjustment and system long-term performance in a highly dynamic and complexity environment of blockchain-enabled MEC. In this approach, the computation offloading problem is formulated as a MDP to obtain the optimal strategy for executing the mining and computational tasks. Moreover, the adaptive genetic algorithm (AGA) is applied in the proposed approach to avoid useless exploration and improve convergence speed.

The above-mentioned studies on computation offloading for IBEC are summarized in Table IX.

E. Security Strategies for IBEC

Besides the characteristics of transparency, traceability and tamper-proofing of blockchain, the functions of access control and identity authentication can be implemented in form of smart contracts to achieve security and privacy in the IBEC system.

In [168], a trust management architecture is proposed by using smart contracts and smart oracles to provide security services across the Edge-Fog-Cloud computing continuum to support development and operation of smart applications. In this architecture, the smart oracles are used to assess and provide specific metrics for smart contracts, which are

Table IX
Computation Offloading for IBEC

Refs.	Applications	Purposes	Contributions	Other Supporting Technologies
[161]	Computation Offloading	Secure, efficient and rewarding tasks allocation system with low latency.	Devising a task allocation platform called DeTEC with heuristic algorithm be the allocating solution and centralized / decentralized verification schemes.	Heu-Alloc algorithm
[162]	Computation Offloading	Reducing time and energy costs and achieving data integrity of task offloading process.	Proposing a blockchain-enabled computation offloading method named BeCome and employing NSGA-III to achieve optimal offloading strategy.	NSGA-III
[163]	Computation Offloading	Guaranteeing integral operating performance and data integrity for computation offloading.	Designing a computation offloading method including a blockchain-based edge computing framework and NSGA-III enabled optimal offloading strategy.	NSGA-III, 5G
[164]	Computation Offloading	Optimizing the total cost of all mobile devices and ensuring each device to participate in computation offloading successfully if it needs.	Jointly studying the computation offloading and coin loaning problems in blockchain-enabled MEC.	No
[165]	Computation Offloading	Improving system performance and QoE of users.	Proposing a consortium blockchain-based edge computing system with a group-agent strategy, a task sorting algorithm and a content search scheme.	No
[166]	Computation Offloading	Improving mining task offloading performance.	Proposing a MEC-enabled mining task offloading scheme for a redesigned lightweight blockchain and designing a DL-based BDO solution.	DL
[167]	Computation Offloading	Improving comprehensive performance of computational offloading in mobile edge computing.	Proposing an adaptive genetic algorithm-enabled DRL solution for high performance of online computation offloading in blockchain-enabled MEC by taking both mining tasks and data processing tasks into consideration.	Genetic algorithm, DRL

implemented to monitor off-chain data and to select optimal fog nodes to reduce the cost and to improve QoS of the whole system.

In order to achieve secure authentication and collaborative sharing, a distributed and trusted authentication system is developed in [169] by combining blockchain and edge computing, in which an optimized PBFT consensus algorithm is proposed to help store authentication data and logs on blockchain. Moreover, a domain name system (DNS)-based dynamic name resolution strategy is designed to provide authentication and data synchronization services for terminals, and an elliptic curve cryptography (ECC)-based cryptographic algorithm is designed to ensure anonymity and communication security between terminals and edge nodes. Furthermore, content caching strategy based on belief propagation (BP) algorithm is utilized to improve the downloading efficiency by cooperation.

To preserve network topology privacy, a consortium blockchain-based trusted MEC multi-domain collaboration architecture named BlockTC is proposed in [170], where SDN controllers of all domains are authenticated to own credible access identities, and are responsible to perform the routing verification consensus and maintain the blockchain. Specifically, in order to balance radio resources, optical resources and edge servers' resources, a MEC collaboration routing algorithm is designed in BlockTC for SDN controllers to calculate the weights of links and servers and to choose the minimum routing link.

To protect the privacy of cross-domain routing in multi-domain MEC network, a consortium blockchain-based routing verification scheme, a network-driven collaboration routing verification (ND-CRV) scheme and a cloud-driven CRV (CD-CRV) scheme, are proposed in [171] by using the blooming filter to generate new requests for the subsequent SDN controllers without exposing topology privacy. Moreover, to simultaneously achieve confidentiality and transparency, an ECC-based privacy-enhancement scheme (PES) in the IBEC environment is developed, which includes public key random generation and digital signature generation.

In [172], a data anonymous storage and transaction protocol is proposed by utilizing blockchain and edge computing to achieve the anonymity during processes of data storing and trading. In the stage of data anonymous storage, the edge nodes generate pseudo identities for the collected data from IoT devices, encrypt the data using symmetric key, then store the data to the distributed hash table (DHT) and finally obtain the addresses. In the stage of data anonymous transactions, the edge devices first register on blockchain and serve as data sellers; when data buyer requests the transaction and sends a digital cheque, the seller delivers the encrypted data and a bank transfers money with the cheque, where the information of requests and cheques are recorded on blockchain.

For the purpose of achieving secure and efficient messaging in the IBEC, a messaging model is developed in [173]. The private blockchain and public blockchain are together utilized in the messaging model to respectively support the communications within an edge group and in the whole network. Sequentially, a hybrid messaging method is proposed in [174] by integrating the Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), in which the less power-consuming CoAP protocol is used for resource-limited terminals to communicate with their edge

Table X
Security Strategies for IBEC

Refs.	Applications	Purposes	Contributions	Other Supporting Technologies
[168]	Security and Privacy	Achieving trust of data, software and infrastructure management among multi-parties in decentralized scenarios .	Studying vital attributes of trust, introducing a blockchain-enabled trust management system and implementing PoC.	No
[169]	Security and Privacy	High-efficient and secure authentication of IoT data access and data sharing.	Proposing a decentralized and trusted authentication system based on blockchain and edge computing for IoT data storing and sharing.	No
[170]	Security and Privacy	Achieving privacy preservation of network topology in heterogeneous MEC system.	Designing a blockchain-based MEC system which implements multiplex mutual trust networking and collaborative routing verification using the blooming filter.	5G
[171]	Security and Privacy	Simultaneously achieving confidentiality and transparency in the IBEC.	Proposing an ECC-based privacy-enhancement scheme (PES).	No
[172]	Security and Privacy	Secure data storing and data sharing.	Proposing an anonymous data storage and transaction protocol, which generates ElGamal cryptosystem-based pseudo identities and blinding signature-based electronic cheques.	No
[173]	Security and Privacy	Optimizing security and performance of M2M communication in IoT environment.	Establishing a hybrid messaging model where the IoT devices layer maintains multi-group private blockchains and edge servers layer maintains a public blockchain.	No
[174]	Security and Privacy	Designing a messaging protocol that fits the IBEC.	Comparing and analysing the MQTT and CoAP messaging protocols in IoT network and proposing a novel one by combining the two protocols.	No
[175]	Security and Privacy	Achieving high-quality and high-reliability in MEC communication service.	Proposing a digital twin-enabled edge computing for network optimizing and asynchronous aggregation-based resource allocation scheme with blockchain for communication security and data privacy.	FL, Digital Twin
[176]	Security and Privacy	Improving security of LoRa technology-based communication in IoT.	Implementing a prototype LoRa system using edge computing and blockchain and analysing four security issues.	LoRa
[177]	Security and Privacy	Addressing the security and privacy challenges of resource allocation.	Reviewing challenges for computation resource lending, discussing the corresponding security and privacy technologies and proposing to use unidirectional payment channels for addressing the challenges.	No

servers, while the MQTT protocol is utilized for communication between edge / fog nodes. To be closer to the practical edge networks with complexities and heterogeneity, the digital twin technology is introduced in edge networks [175], where the permissioned blockchain-enabled FL scheme is proposed to enhance the communication security and data privacy. In this method, the asynchronous model update and aggregation algorithm is adopted to reduce the delay of users, and a RL-based solution is designed to train the digital twin-enabled policy DNN to finally optimize user scheduling and bandwidth allocation.

As one of the low-power wide-area (LPWA) technologies, long-range (LoRa) has been widely applied in IoT environment to provide energy-efficient communications, although it is challenging to guarantee its security and efficiency. In [176], two blockchain ledgers are deployed in the proposed LoRa system, where LoRa gateways are responsible for constructing blocks using the Merkle tree and executing root value generation algorithms to maintain the network ledger. Another blockchain is regarded as application ledger that could only be accessed by authorized application servers. The security issues of application-layer, including denial-of-service (DoS) attack, SPOF, malicious LoRa gateway and malicious network server, are analyzed and demonstrated to be mitigated or eliminated in the proposed LoRa system.

Different from the above software-based security solutions, a hardware-based solution for the blockchain-enabled edge computing architecture is proposed in [177] by using Intel Software Guard Extension (SGX) to realize data privacy, task and code tamper-proofing, incentive mechanism and execution in a sandboxed environment.

The above-mentioned studies on security strategies for IBEC are summarized in Table X.

VI. Challenges and Solutions

This section presents the challenges and the potential solutions of the IBEC.

A. Performance Scalability

Performance scalability is one of the biggest challenges in blockchain application. For instance, in Bitcoin ledger, blockchain is explicitly stipulated on its block size, consensus mechanism, broadcasting algorithm, *etc.* for its decentralization and security. However, when the number of users surges, these regulations lead to a decrease in Bitcoin's throughput,

e.g., Bitcoin can only process 3 to 7 transactions per second simultaneously.

With respect to the IBEC, energy trading or knowledge trading are two major application scenarios in recent years. One of the important functions of these two scenarios is to optimize the performance of public blockchains. For instance, designing a novel lightweight blockchain or proposing a novel consensus mechanism to fulfill the specific demands. However, these solutions do not meet the rapid growth of verification demands for blockchain transactions especially in IoT applications, which combine blockchain and edge computing. Moreover, there is an urgent need of intelligent autonomy for the distributed networks of air-space-ground-sea integration areas in 6G and beyond context. These emerging domains require blockchain-based solutions and also pose higher demands for the performance of underlying blockchains. In other words, large volumes of data and huge numbers of devices in 6G context will pose a great challenge on existing blockchain systems in terms of performance scalability. As a result, the performance scalability of the IBEC remains to be improved due to the performance scalability issue of blockchain. Accordingly, how to improve the performance scalability of blockchain is a challenge, especially for the IBEC.

The solutions of blockchain expansion are fully summarized in [178]–[182]. These solutions mainly concentrate on on-chain expansions, off-chain expansions and the zero's layer ones. On-chain expansions refer to the improvements of basic protocols on the data layer, consensus layer and network layer. The improvements of protocols including block size increment, the delay reduction of block broadcasting and gaining consensus, *etc.* Omnilegder [183], Bitcoin-Cash [184], Spectre [185], PBFT [186] and DPoS [187] are the typical cases of on-chain expansions.

Off-chain expansions mainly lie in the improvements of the application layer. These countermeasures include state channel, side-chain, cross-chain and off-chain computation. Lightning Network [188], Raiden Network [189], Plasma [190] and Cosmos [191] are the typical cases of off-chain expansions.

The zero's layer expansions improve the performance scalability by optimizing the underlying data transfer protocols of blockchain, *e.g.*, Blockchain Distribution Network (BDN) utilized by bloXroute [192]. However, due to the fact that the IBEC has the massively dispersed and small pieces of resources, it is challenging to fulfill the rising demands of IoT. In the future, being empowered by AI algorithms, lightweight and flexible blockchain expansion schemes for the resource-limited and heterogeneous edge devices should be designed to improve the performance scalability.

B. Resource Management

In the IBEC, a large number of heterogeneous edge devices can collaborate with edge servers to serve nearby devices when they are idle. Moreover, most edge devices are really resource-limited devices, which need to resort to the resources provided by edge servers or other devices to complete corresponding tasks. These cases will occur more commonly in 6G and beyond context, in which the global deep fusion of air, space, ground and sea networks will involve much more related networks, network carrying equipment and heterogeneous accessing devices. This will inevitably pose a new challenge for resource management for the IBEC. Furthermore, many application scenarios of the IBEC focus on data sharing and knowledge discovery; this requires ML or other technologies to perform a lot of computation-intensive tasks. In addition, maintaining the blockchain itself requires huge computational resources. Therefore, resource management is a key requirement in the IBEC.

With the rapid development of Internet of Everything [193], more devices and facilities will be connected to the network. The proliferation and heterogeneity of devices, and frequent online and offline of IoT devices increase the difficulty of resource integration and management. Therefore, how to optimize resource management and improve the QoS of the IBEC is the key challenge. An alternative solution is to design a more reasonable, practical and efficient bidding and pricing mechanism under a more realistic trading model, which can encourage devices to participate in the exchange of resources. Moreover, an AI-based edge intelligent resource management system with adaptive integration and allocation of resources should be proposed by utilizing emerging technologies (*e.g.*, FL) to cope with the highly dynamic and complexity of the IBEC.

C. Security

The IBEC brings security challenges, which exhibit in two aspects: (1) how to realize the security of smart contract; and (2) how to achieve efficient identification of edge devices.

The IBEC puts forth specific functions, such as resource allocation, identity authentication and access control, which are generally implemented in the form of smart contracts. Despite the merits such as high efficiency, customization, flexibility, automation, *etc.*, smart contracts cause large economic accidents due to their security vulnerabilities, inalterable error codes, and malicious codes [194]–[196]. Moreover, there is no effective legal supervision of smart contracts. Therefore, it is a challenge to ensure that smart contracts are completely correct and effective, especially in the IBEC. One solution is to strengthen the security analysis of smart contracts by designing practical privacy preservation encrypted traffic inspection scheme on blockchains. With this scheme, the abnormal and suspicious codes of smart contracts can be detected while preserving the privacy of smart contracts.

The identification of edge devices is another key issue to establish trust among devices or cross systems. Since a large number of heterogeneous devices need to be authenticated in order to join various networks to participate in activities, thereby posing huge computing pressure on the edge side. Moreover, there are diverse authentication standards. Accordingly, it is still a challenge to design a lightweight, fast and consistent authentication mechanism. The above issue may be potentially solved by designing a distributed IoT device identification mechanism, as well as promoting the standardizations of IoT device identification protocol.

D. Privacy Computing

Data sharing and knowledge discovery are the basic requirements in many application scenarios (such as, IoV, IIoT, and smart healthcare) of the IBEC. For example, knowledge discovery requires a comprehensive analysis of a large number of patient records. Meanwhile, sharing the GPS positioning data corrects errors in assisted automatic driving. Especially in future generation network environment, data generated by more equipment and devices will be more scattered, and the increasing number of stakeholders drives the great demand of data sharing. Privacy preservation of the data in the IBEC system is important, as a large amount of personally sensitive data is stored in the system. However, existing works usually focus on the security of data, which is nevertheless limited by the underlying security mechanism of blockchains. Moreover, traditional privacy preservation mechanisms are not suitable for edge devices due to the complexities. Therefore, how to protect data privacy in the computing process is the key to widen the applications of the IBEC.

At this stage, technologies related to data privacy computing include privacy-enhanced computing (PEC), multi-party secure computing (MPSC), *etc.* To apply these technologies efficiently in the IBEC, it is necessary to consider issues of limited resources on edge devices and huge demands for computing offloading. Therefore, lightweight, parallel and modular optimizations on PEC algorithms, MPSC algorithms or others that can protect data computing privacy may be new trends to improve the applicability and scalability of the IBEC system.

VII. Conclusion

As two crucial technologies for IoT, both blockchain and edge computing have been used to realize secure and efficient resource management, computation offloading and data sharing. This survey starts with a brief introduction of blockchain and edge computing and then presents the architecture of an IBEC system in IoT application scenarios. We next classify and discuss the corresponding research issues and existing solutions, in perspectives of resource management, data management, computation offloading, security and privacy, which have attracted most attentions in the areas of IoV, Smart Grid, smart healthcare, IIoT, *etc*. Finally, we summarize research challenges, which have hindered the further large-scale deployments. We also discuss performance optimization for the IBEC, in terms of performance scalability, resource management, security, and privacy computing.

References

[1] https://tiaonline.org/industry-priorities/transforming-infrastructure/edge-data-centers-cloud/, accessed February, 2020.

[2] I. Sittón-Candanedo, "Edge computing: A review of application scenarios," in International Symposium on Distributed Computing and Artificial Intelligence. Springer, 2019, pp. 197–200.

[3] D. Chen, N. Zhang, Z. Qin, X. Mao, Z. Qin, X. Shen, and X.-Y. Li, "S2m: A lightweight acoustic fingerprints-based wireless device authentication protocol," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 88–100, 2016.

[4] D. Chen, N. Zhang, R. Lu, N. Cheng, K. Zhang, and Z. Qin, "Channel precoding based message authentication in wireless networks: Challenges and solutions," IEEE Network, vol. 33, no. 1, pp. 99–105, 2018.

[5] D. Chen, N. Zhang, N. Cheng, K. Zhang, Z. Qin, and X. Shen, "Physical layer based message authentication with secure channel codes," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 5, pp. 1079–1093, 2018.

[6] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," Proceedings of the IEEE, vol. 107, no. 8, pp. 1608–1631, 2019.

[7] I. Sittón-Candanedo, R. S. Alonso, J. M. Corchado, S. Rodríguez-González, and R. Casado-Vara, "A review of edge computing reference architectures and a new global edge proposal," Future Generation Computer Systems, vol. 99, pp. 278–294, 2019.

[8] Y. Wu, H. N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable iiot critical infrastructures in industry 4.0," IEEE Internet of Things Journal, vol. PP, no. 99, 2020.

[9] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for internet of things," Computer Communications, vol. 136, pp. 10–29, 2019.

[10] G. Luo, H. Zhou, N. Cheng, Q. Yuan, J. Li, F. Yang, and X. S. Shen, "Software defined cooperative data sharing in edge computing assisted 5g-vanet," IEEE Transactions on Mobile Computing, 2019.

[11] 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, 2018.

[12] H. Tan and I. Chung, "Secure authentication and key management with blockchain in vanets," IEEE Access, vol. 8, pp. 2482–2498, 2019.

[13] S. Guo, X. Hu, Z. Zhou, X. Wang, F. Qi, and L. Gao, "Trust access authentication in vehicular network based on blockchain," China Communications, vol. 16, no. 6, pp. 18–30, 2019.

[14] L. Nkenyereye, B. Adhi Tama, M. K. Shahzad, and Y.-H. Choi, "Secure and blockchain-based emergency driven message protocol for 5g enabled vehicular edge computing," Sensors, vol. 20, no. 1, p. 154, 2020.

[15] Y. Xiao, Y. Liu, and T. Li, "Edge computing and blockchain for quick fake news detection in iov," Sensors, vol. 20, no. 16, p. 4360, 2020.

[16] J. Liu, X. Zhang, Y. Li, Q. Cui, and X. Tao, "Blockchain-empowered content cache system for vehicle edge computing networks," in International Conference on Blockchain and Trustworthy Systems. Springer, 2019, pp. 410–421.

[17] S. Wang, X. Huang, R. Yu, Y. Zhang, and E. Hossain, "Permissioned blockchain for efficient and secure resource sharing in vehicular edge computing," arXiv preprint arXiv:1906.06319, 2019.

[18] K. Xiao, W. Shi, Z. Gao, C. Yao, and X. Qiu, "Daer: A resource pre-allocation algorithm of edge computing server by using blockchain in intelligent driving," IEEE Internet of Things Journal, 2020.

[19] X. Lin, J. Wu, S. Mumtaz, S. Garg, J. Li, and M. Guizani, "Blockchain-based on-demand computing resource trading in iov-assisted smart city," IEEE Transactions on Emerging Topics in Computing, 2020.

[20] S. Wang, D. Ye, X. Huang, R. Yu, Y. Wang, and Y. Zhang, "Consortium blockchain for secure resource sharing in vehicular edge computing: A contract-based approach," IEEE Transactions on Network Science and Engineering, 2020.

[21] A. Hammoud, H. Sami, A. Mourad, H. Otrok, R. Mizouni, and J. Bentahar, "Ai, blockchain, and vehicular edge computing for smart and secure iov: Challenges and directions," IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 68–73, 2020.

[22] Y. Dai, D. Xu, K. Zhang, S. Maharjan, and Y. Zhang, "Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks," IEEE Transactions on Vehicular Technology, vol. 69, no. 4, pp. 4312–4324, 2020.

[23] C. Li, Y. Fu, F. R. Yu, T. H. Luan, and Y. Zhang, "Vehicle position correction: A vehicular blockchain networks-based gps error sharing framework," IEEE Transactions on Intelligent Transportation Systems, 2020.

[24] G. Singh, A. Singh, M. Singh, S. Sharma, N. Kumar, and K.-K. R. Choo, "Blocked: Blockchain-based secure data processing framework in edge envisioned v2x environment," IEEE Transactions on Vehicular Technology, 2020.

[25] L. Cui, Z. Chen, S. Yang, Z. Ming, Q. Li, Y. Zhou, S. Chen, and Q. Lu, "A blockchain-based containerized edge computing platform for the internet of vehicles," IEEE Internet of Things Journal, 2020.

[26] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, "A proof-of-quality-factor (poqf) based blockchain and edge computing for vehicular message dissemination," IEEE Internet of Things Journal, 2020.

[27] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5g-enabled vehicular networks," IEEE Network, vol. 34, no. 2, pp. 37–45, 2020.

[28] A. Yang, J. Weng, K. Yang, C. Huang, and X. Shen, "Delegating authentication to edge: A decentralized authentication architecture for vehicular networks," IEEE Transactions on Intelligent Transportation Systems, 2020.

[29] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, and Y. Zhang, "Blockchain empowered cooperative authentication with data traceability in vehicular edge computing," IEEE Transactions on Vehicular Technology, vol. 69, no. 4, pp. 4221–4232, 2020.

[30] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, pp. 43–57, 2019.

[31] A. Jindal, G. S. Aujla, and N. Kumar, "Survivor: A blockchain based edge-as-a-service framework for secure energy trading in sdn-enabled vehicle-to-grid environment," Computer Networks, vol. 153, pp. 36–48, 2019.

[32] M. Stübs, W. Posdorfer, and S. Momeni, "Blockchain-based multi-tier double auctions for smart energy distribution grids," in 2020 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, 2020, pp. 1–6.

[33] S. Chen, Y. Bai, Y. Zhang, X. Liu, J. Zhang, T. Gao, Z. Fang, and Y. Dai, "A framework of decentralized electricity market based on the collaborative mechanism of blockchain and edge computing," in 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI). IEEE, 2019, pp. 219–223.

[34] Y. Ren, Q. Zhao, H. Guan, and Z. Lin, "A novel authentication scheme based on edge computing for blockchain-based distributed energy trading system," EURASIP Journal on Wireless Communications and Networking, vol. 2020, no. 1, pp. 1–15, 2020.

[35] J. Wang, L. Wu, K.-K. R. Choo, and D. He, "Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1984–1992, 2019.

[36] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7992–8004, 2019.

[37] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge intelligence and blockchain empowered 5g beyond for the industrial internet of things," IEEE Network, vol. 33, no. 5, pp. 12–19, 2019.

[38] W. Chen, Z. Zhang, Z. Hong, C. Chen, J. Wu, S. Maharjan, Z. Zheng, and Y. Zhang, "Cooperative and distributed computation offloading for blockchain-empowered industrial internet of things," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8433–8446, 2019.

[39] C. K. Lee, Y. Huo, S. Zhang, and K. Ng, "Design of a smart manufacturing system with the application of multi-access edge computing and blockchain technology," IEEE Access, vol. 8, pp. 28 659–28 667, 2020.

[40] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential privacy-based blockchain for industrial internet-of-things," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4156–4165, 2019.

[41] Y. Ren, F. Zhu, J. Qi, J. Wang, and A. K. Sangaiah, "Identity management and access control based on blockchain under edge computing for the industrial internet of things," Applied Sciences, vol. 9, no. 10, p. 2058, 2019.

[42] J. Xu, S. Wang, B. K. Bhargava, and F. Yang, "A blockchain-enabled trustless crowd-intelligence ecosystem on mobile edge computing," IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3538–3547, 2019.

[43] J. P. Queralta, L. Qingqing, Z. Zou, and T. Westerlund, "Enhancing autonomy with blockchain and multi-access edge computing in distributed robotic systems," in 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC). IEEE, 2020, pp. 180–187.

[44] Y. Gao, Y. Chen, X. Hu, H. Lin, Y. Liu, and L. Nie, "Blockchain based iiot data sharing framework for sdn-enabled pervasive edge computing," IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 5041–5049, 2020.

[45] A. Srivastava, P. Jain, B. Hazela, P. Asthana, and S. W. A. Rizvi, "Application of fog computing, internet of things, and blockchain technology in healthcare industry," in Fog Computing for Healthcare 4.0 Environments. Springer, pp. 563–591.

[46] W. Tang, K. Zhang, D. Zhang, J. Ren, Y. Zhang, and X. Shen, "Fog-enabled smart health: toward cooperative and secure healthcare service provision," IEEE Communications Magazine, vol. 57, no. 5, pp. 42–48, 2019.

[47] R. Akkaoui, X. Hei, and W. Cheng, "Edgemedichain: A hybrid edge blockchain-based framework for health data exchange," IEEE Access, vol. 8, pp. 113 467–113 486, 2020.

[48] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain and edge computing for decentralized emrs sharing in federated healthcare," in GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, 2020, pp. 1–6.

[49] A. A. Abdellatif, L. Samara, A. Mohamed, A. Erbad, C. F. Chiasserini, M. Guizani, M. D. O'Connor, and J. Laughton, "Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange," IEEE Internet of Things Journal, 2021.

[50] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," in 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019, pp. 44–51.

[51] W. Wang, H. Huang, L. Xue, Q. Li, R. Malekian, and Y. Zhang, "Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environment," Journal of Systems Architecture, vol. 115, p. 102024, 2021.

[52] A. Islam and S. Y. Shin, "Bhmus: blockchain based secure outdoor health monitoring scheme using uav in smart city," in 2019 7th International Conference on Information and Communication Technology (ICoICT). IEEE, 2019, pp. 1–6.

[53] V. C. Leung, X. Wang, F. R. Yu, D. Niyato, T. Taleb, and S. Pack, "Guest editorial: Special issue on blockchain and edge computing techniques for emerging iot applications," IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2082–2086, 2021.

[54] 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, 2021.

[55] M. H. ur Rehman, K. Salah, E. Damiani, and D. Svetinovic, "Towards blockchain-based reputation-aware federated learning," in IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2020, pp. 183–188.

[56] Q. Wang, Y. Guo, X. Wang, T. Ji, L. Yu, and P. Li, "Ai at the edge: Blockchain-empowered secure multiparty learning with heterogeneous models," IEEE Internet of Things Journal, 2020.

[57] Y. Zhao, J. Zhao, L. Jiang, R. Tan, D. Niyato, Z. Li, L. Lyu, and Y. Liu, "Privacy-preserving blockchain-based federated learning for iot devices," IEEE Internet of Things Journal, 2020.

[58] S. Hu, S. Huang, J. Huang, and J. Su, "Blockchain and edge computing technology enabling organic agricultural supply chain: a framework solution to trust crisis," Computers & Industrial Engineering, vol. 153, p. 107079, 2021.

[59] H. Zhang, S. Li, W. Yan, Z. Jiang, and W. Wei, "A knowledge sharing framework for green supply chain management based on blockchain and edge computing," in International Conference on Sustainable Design and Manufacturing. Springer, 2019, pp. 413–420.

[60] A. Fitwi, Y. Chen, and S. Zhu, "A lightweight blockchain-based privacy protection for smart surveillance at the edge," in 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019, pp. 552–555.

[61] R. Xu, S. Y. Nikouei, Y. Chen, E. Blasch, and A. Aved, "Blendmas: A blockchain-enabled decentralized microservices architecture for smart public safety," in 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019, pp. 564–571.

[62] V. Hassija, V. Chamola, D. N. G. Krishna, N. Kumar, and M. Guizani, "A blockchain and edge computing-based secure framework for government tender allocation," IEEE Internet of Things Journal, 2020.

[63] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[64] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in Internet of everything. Springer, 2018, pp. 103–130.

[65] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. S. Shen, "Cooperative spectrum access towards secure information transfer for crns," IEEE Journal on Selected Areas in Communications, vol. 31, no. 11, pp. 2453–2464, 2013.

[66] N. Zhang, N. Cheng, N. Lu, H. Zhou, J. W. Mark, and X. S. Shen, "Risk-aware cooperative spectrum access for multi-channel cognitive radio networks," IEEE Journal on Selected Areas in Communications, vol. 32, no. 3, pp. 516–527, 2014.

[67] N. Cheng, N. Zhang, N. Lu, X. Shen, J. W. Mark, and F. Liu, "Opportunistic spectrum access for cr-vanets: A game-theoretic approach,"

IEEE Transactions on Vehicular Technology, vol. 63, no. 1, pp. 237–251, 2013.

[68] N. Zhang, P. Yang, J. Ren, D. Chen, L. Yu, and X. Shen, "Synergy of big data and 5g wireless networks: opportunities, approaches, and challenges," IEEE Wireless Communications, vol. 25, no. 1, pp. 12–18, 2018.

[69] J. Ren, Y. Zhang, N. Zhang, D. Zhang, and X. Shen, "Dynamic channel access to improve energy efficiency in cognitive radio sensor networks," IEEE Transactions on Wireless Communications, vol. 15, no. 5, pp. 3143–3156, 2016.

[70] N. Zhang, H. Liang, N. Cheng, Y. Tang, J. W. Mark, and X. S. Shen, "Dynamic spectrum access in multi-channel cognitive radio networks," IEEE Journal on Selected Areas in Communications, vol. 32, no. 11, pp. 2053–2064, 2014.

[71] D. Chen, Z. Zhao, X. Qin, Y. Luo, M. Cao, H. Xu, and A. Liu, "Magleak: A learning-based side-channel attack for password recognition with multiple sensors in iiot environment," IEEE Transactions on Industrial Informatics, 2020.

[72] L. Ale, N. Zhang, H. Wu, D. Chen, and T. Han, "Online proactive caching in mobile edge computing using bidirectional deep recurrent neural network," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5520–5530, 2019.

[73] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, and Z. Qin, "Deepedn: a deep-learning-based image encryption and decryption network for internet of medical things," IEEE Internet of Things Journal, vol. 8, no. 3, pp. 1504–1518, 2020.

[74] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1508–1532, 2019.

[75] X. Wang, X. Ren, C. Qiu, Z. Xiong, H. Yao, and V. C. Leung, "Synergy of Edge Intelligence and Blockchain: A Comprehensive Survey," 6 2021. [Online]. Available: https://www.techrxiv.org/articles/preprint/Synergy_of_Edge_Intelligence_and_Blockchain_A_Comprehensive_Survey/14724360

[76] Y. Zhang, C. Xu, H. Li, H. Yang, and X. Shen, "Chronos: Secure and accurate time-stamping scheme for digital files via blockchain," in ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019, pp. 1–6.

[77] D. Liu, J. Ni, C. Huang, X. Lin, and X. S. Shen, "Secure and efficient distributed network provenance for iot: A blockchain-based approach," IEEE Internet of Things Journal, vol. 7, no. 8, pp. 7564–7574, 2020.

[78] Y. Zhang, C. Xu, X. Lin, and X. S. Shen, "Blockchain-based public integrity verification for cloud storage against procrastinating auditors," IEEE Transactions on Cloud Computing, 2019.

[79] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5g beyond," IEEE Network, vol. 33, no. 3, pp. 10–17, 2019.

[80] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges," IEEE Communications Surveys and Tutorials, vol. 21, no. 2, pp. 1508–1532, 2019.

[81] 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, 2019.

[82] D. Liu, J. Ni, X. Lin, and X. Shen, "Transparent and accountable vehicular local advertising with practical blockchain designs," IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15 694–15 705, 2020.

[83] M. He, J. Ni, D. Liu, H. Yang, and X. Shen, "Private, fair, and verifiable aggregate statistics for mobile crowdsensing in blockchain era," in 2020 IEEE/CIC International Conference on Communications in China (ICCC). IEEE, 2020, pp. 160–165.

[84] Y. Zhang, C. Xu, J. Ni, H. Li, and X. S. Shen, "Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage," IEEE Transactions on Cloud Computing, 2019.

[85] D. Liu, C. Huang, J. Ni, X. Lin, and X. S. Shen, "Blockchain-based smart advertising network with privacy-preserving accountability," IEEE Transactions on Network Science and Engineering, 2020.

[86] Z. Guan, X. Lu, N. Wang, J. Wu, X. Du, and M. Guizani, "Towards secure and efficient energy trading in iiot-enabled energy internet: A blockchain approach," Future Generation Computer Systems, vol. 110, pp. 686–695, 2020.

[87] Y. Lu, "The blockchain: State-of-the-art and research challenges," Journal of Industrial Information Integration, vol. 15, pp. 80–90, 2019.

[88] A. Miglani, N. Kumar, V. Chamola, and S. Zeadally, "Blockchain for internet of energy management: Review, solutions, and challenges," Computer Communications, vol. 151, pp. 395–418, 2020.

[89] J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted internet of things: From security and efficiency perspectives," IEEE Network, vol. 33, no. 2, pp. 50–57, 2019.

[90] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," Future Generation Computer Systems, vol. 97, pp. 219–235, 2019.

[91] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE internet of things journal, vol. 3, no. 5, pp. 637–646, 2016.

[92] X. Ma, S. Wang, S. Zhang, P. Yang, C. Lin, and X. S. Shen, "Cost-efficient resource provisioning for dynamic requests in cloud assisted mobile edge computing," IEEE Transactions on Cloud Computing, pp. 1–1, 2019.

[93] Y. Chen, Y. Zhang, Y. Wu, L. Qi, and X. Shen, "Joint task scheduling and energy management for heterogeneous mobile edge computing with hybrid energy supply," IEEE Internet of Things Journal, vol. PP, no. 99, pp. 1–1, 2020.

[94] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," IEEE Access, vol. 6, pp. 18 209–18 237, 2018.

[95] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards next generation teaching, learning, and context-aware applications for higher education: A review on blockchain, iot, fog and edge computing enabled smart campuses and universities," Applied Sciences, vol. 9, no. 21, p. 4479, 2019.

[96] C. Luo, L. Xu, D. Li, and W. Wu, "Edge computing integrated with blockchain technologies," in Complexity and Approximation. Springer, 2020, pp. 268–288.

[97] S. Desai and S. Padhi, "Measuring performance of blockchain enabled iot over edge computing system."

[98] I. Sittón-Candanedo, "A new approach: Edge computing and blockchain for industry 4.0," in International Symposium on Distributed Computing and Artificial Intelligence. Springer, 2019, pp. 201–204.

[99] D. Wang, J. Ren, C. Xu, J. Liu, and X. Shen, "Privstream: Enabling privacy-preserving inferences on iot data stream at the edge," in 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2019.

[100] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5g beyond," IEEE Network, vol. 33, no. 3, pp. 10–17, 2019.

[101] 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, 2018.

[102] A. Zhou, Q. Sun, and J. Li, "Bcedge: Blockchain-based resource management in d2d-assisted mobile edge computing," Software: Practice and Experience, 2019.

[103] G. Qiao, S. Leng, H. Chai, A. Asadi, and Y. Zhang, "Blockchain empowered resource trading in mobile edge computing and networks," in ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019, pp. 1–6.

[104] M. Pincheira, M. Vecchio, and R. Giaffreda, "Rationale and practical assessment of a fully distributed blockchain-based marketplace of fog/edge computing resources," in 2020 Seventh International Conference on Software Defined Systems (SDS). IEEE, 2020, pp. 165–170.

[105] X. Fan and Y. Huo, "Blockchain based dynamic spectrum access of non-real-time data in cyber-physical-social systems," IEEE Access, vol. 8, pp. 64 486–64 498, 2020.

[106] S. Seng, C. Luo, X. Li, H. Zhang, and H. Ji, "User matching on blockchain for computation offloading in ultra-dense wireless networks," IEEE Transactions on Network Science and Engineering, 2020.

[107] S. Luo, H. Li, Z. Wen, B. Qian, G. Morgan, A. Longo, O. Rana, and R. Ranjan, "Blockchain-based task offloading in drone-aided mobile edge computing," IEEE Network, vol. 35, no. 1, pp. 124–129, 2021.

[108] L. Yuan, Q. He, S. Tan, B. Li, J. Yu, F. Chen, H. Jin, and Y. Yang, "Coopedge: A decentralized blockchain-based platform for cooperative edge computing," in Proceedings of the Web Conference 2021, 2021, pp. 2245–2257.

[109] A. V. Rivera, A. Refaey, and E. Hossain, "A blockchain framework for secure task sharing in multi-access edge computing," IEEE Network, 2020.

[110] H. Zhou, X. Ouyang, and Z. Zhao, "Allstar: a blockchain based decentralized ecosystem for cloud and edge computing," in 2020 IEEE International Conference on Joint Cloud Computing. IEEE, 2020, pp. 55–62.

[111] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, "Fogbus: A blockchain-based lightweight framework for edge and fog computing," Journal of Systems and Software, vol. 154, pp. 22–36, 2019.

[112] X. Xu, Q. Geng, H. Cao, R. Mo, S. Wan, L. Qi, and H. Wang, "Blockchain-powered service migration for uncertainty-aware workflows in edge computing," in International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications. Springer, 2019, pp. 217–230.

[113] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K.-K. R. Choo, "Neural-blockchain-based ultrareliable caching for edge-enabled uav networks," IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5723–5736, 2019.

[114] B. Wu, K. Xu, Q. Li, S. Ren, Z. Liu, and Z. Zhang, "Toward blockchain-powered trusted collaborative services for edge-centric networks," IEEE Network, vol. 34, no. 2, pp. 30–36, 2020.

[115] U. Jayasinghe, G. M. Lee, Á. MacDermott, and W. S. Rhee, "Trustchain: a privacy preserving blockchain with edge computing," Wireless Communications and Mobile Computing, vol. 2019, 2019.

[116] L. Xiao, Y. Ding, D. Jiang, J. Huang, D. Wang, J. Li, and H. V. Poor, "A reinforcement learning and blockchain-based trust mechanism for edge networks," IEEE Transactions on Communications, 2020.

[117] S. Saha, D. Chattaraj, B. Bera, and A. Kumar Das, "Consortium blockchain-enabled access control mechanism in edge computing based generic internet of things environment," Transactions on Emerging Telecommunications Technologies, p. e3995, 2020.

[118] E. Bonnah and J. Shiguang, "Decchain: A decentralized security approach in edge computing based on blockchain," Future Generation Computer Systems, vol. 113, pp. 363–379, 2020.

[119] F. Gai, B. Wang, W. Deng, and W. Peng, "Proof of reputation: A reputation-based consensus protocol for peer-to-peer network," in International Conference on Database Systems for Advanced Applications. Springer, 2018, pp. 666–681.

[120] M. Zhaofeng, W. Xiaochang, D. K. Jain, H. Khan, G. Hongmin, and W. Zhen, "A blockchain-based trusted data management scheme in edge computing," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2013–2021, 2019.

[121] G. Li, M. Dong, L. T. Yang, K. Ota, J. Wu, and J. Li, "Preserving edge knowledge sharing among iot services: A blockchain-based approach," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 4, no. 5, pp. 653–665, 2020.

[122] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-ai enabled iot: A consortium blockchain-based efficient and incentive approach," IEEE Transactions on Industrial Informatics, vol. 15, no. 12, pp. 6367–6378, 2019.

[123] H. Cui, Z. Chen, N. Liu, and B. Xia, "Blockchain-driven contents sharing strategy for wireless cache-enabled d2d networks," in 2019 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, 2019, pp. 1–5.

[124] P. Zhang, X. Pang, N. Kumar, G. S. Aujla, and H. Cao, "A reliable data-transmission mechanism using blockchain in edge computing scenarios," IEEE Internet of Things Journal, 2020.

[125] C. K. Pyoung and S. J. Baek, "Blockchain of finite-lifetime blocks with applications to edge-based iot," IEEE Internet of Things Journal, vol. 7, no. 3, pp. 2102–2116, 2019.

[126] Y. Huang, J. Zhang, J. Duan, B. Xiao, F. Ye, and Y. Yang, "Resource allocation and consensus on edge blockchain in pervasive edge computing environments," in 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2019, pp. 1476–1486.

[127] G. Kumar, R. Saha, M. K. Rai, R. Thomas, and T.-H. Kim, "Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6835–6842, 2019.

[128] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-authentication for scalable blockchain in resource-constrained distributed systems," in 2019 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2019, pp. 1–5.

[129] P. Bhattacharya, S. Tanwar, R. Shah, and A. Ladha, "Mobile edge computing-enabled blockchain framework—a survey," in Proceedings of ICRIC 2019. Springer, 2020, pp. 797–809.

[130] H. Xu, W. Huang, Y. Zhou, D. Yang, M. Li, and Z. Han, "Edge computing resource allocation for unmanned aerial vehicle assisted mobile network with blockchain applications," IEEE Transactions on Wireless Communications, vol. 20, no. 5, pp. 3107–3121, 2021.

[131] S. Jiang, X. Li, and J. Wu, "Hierarchical edge-cloud computing for mobile blockchain mining game," in 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2019, pp. 1327–1336.

[132] 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, 2019.

[133] X. Liu, J. Wu, L. Chen, and C. Xia, "Efficient auction mechanism for edge computing resource allocation in mobile blockchain," in 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). IEEE, 2019, pp. 871–876.

[134] 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, 2020.

[135] Z. Chang, W. Guo, X. Guo, Z. Zhou, and T. Ristaniemi, "Incentive mechanism for edge computing-based blockchain," IEEE Transactions on Industrial Informatics, 2020.

[136] A. O. G. Rivera, D. K. Tosh, and L. Njilla, "Scalable blockchain implementation for edge-based internet of things platform," in MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM). IEEE, 2019, pp. 1–6.

[137] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, "Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing," IEEE Transactions on Vehicular Technology, vol. 68, no. 11, pp. 11 169–11 185, 2019.

[138] M. Liu, Y. Teng, F. R. Yu, V. C. Leung, and M. Song, "A mobile edge computing (mec)-enabled transcoding framework for blockchain-based video streaming," IEEE Wireless Communications, vol. 27, no. 2, pp. 81–87, 2020.

[139] 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, 2020.

[140] A. Asheralieva and D. Niyato, "Distributed dynamic resource management and pricing in the iot systems with blockchain-as-a-service and uav-enabled mobile edge computing," IEEE Internet of Things Journal, vol. 7, no. 3, pp. 1974–1993, 2019.

[141] ——, "Learning-based mobile edge computing resource management to support public blockchain networks," IEEE Transactions on Mobile Computing, 2019.

[142] Q. Xu, Z. Su, and Q. Yang, "Blockchain-based trustworthy edge caching scheme for mobile cyber-physical system," IEEE Internet of Things Journal, vol. 7, no. 2, pp. 1098–1110, 2019.

[143] L. Cui, X. Su, Z. Ming, Z. Chen, S. Yang, Y. Zhou, and W. Xiao, "Creat: Blockchain-assisted compression algorithm of federated learning for content caching in edge computing," IEEE Internet of Things Journal, 2020.

[144] V. K. Rathi, V. Chaudhary, N. K. Rajput, B. Ahuja, A. K. Jaiswal, D. Gupta, M. Elhoseny, and M. Hammoudeh, "A blockchain-enabled multi domain edge computing orchestrator," IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 30–36, 2020.

[145] D. B. Rawat, "Fusion of software defined networking, edge computing, and blockchain technology for wireless network virtualization," IEEE Communications Magazine, vol. 57, no. 10, pp. 50–55, 2019.

[146] A. Muthanna, A. A Ateya, A. Khakimov, I. Gudkova, A. Abuarqoub, K. Samouylov, and A. Koucheryavy, "Secure and reliable iot networks using fog computing with software-defined networking and blockchain," Journal of Sensor and Actuator Networks, vol. 8, no. 1, p. 15, 2019.

[147] 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, 2020.

[148] F. Guo, F. R. Yu, H. Zhang, H. Ji, M. Liu, and V. C. Leung, "Adaptive resource allocation in future wireless networks with blockchain and mobile edge computing," IEEE Transactions on Wireless Communications, vol. 19, no. 3, pp. 1689–1703, 2019.

[149] C. Qiu, X. Wang, H. Yao, J. Du, F. R. Yu, and S. Guo, "Networking integrated cloud-edge-end in iot: A blockchain-assisted collective q-learning approach," IEEE Internet of Things Journal, 2020.

[150] M. Li, F. R. Yu, P. Si, R. Yang, Z. Wang, and Y. Zhang, "Uav-assisted data transmission in blockchain-enabled m2m communications with mobile edge computing," IEEE Network, 2020.

[151] M. Li, F. R. Yu, P. Si, W. Wu, and Y. Zhang, "Resource optimization for delay-tolerant data in blockchain-enabled iot with edge computing: A deep reinforcement learning approach," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9399–9412, 2020.

[152] R. Zhang, F. R. Yu, J. Liu, T. Huang, and Y. Liu, "Deep reinforcement learning (drl)-based device-to-device (d2d) caching with blockchain and mobile edge computing," IEEE Transactions on Wireless Communications, vol. 19, no. 10, pp. 6469–6485, 2020.

[153] J. Feng, F. R. Yu, Q. Pei, X. Chu, J. Du, and L. Zhu, "Cooperative computation offloading and resource allocation for blockchain-enabled mobile edge computing: A deep reinforcement learning approach," IEEE Internet of Things Journal, 2019.

[154] J. Xu, S. Wang, A. Zhou, and F. Yang, "Edgence: A blockchain-enabled edge-computing platform for intelligent iot-based dapps," China Communications, vol. 17, no. 4, pp. 78–87, 2020.

[155] S. El Kafhali, C. Chahir, M. Hanini, and K. Salah, "Architecture to manage internet of things data using blockchain and fog computing," in Proceedings of the 4th International Conference on Big Data and Internet of Things, 2019, pp. 1–8.

[156] B. W. Nyamtiga, J. C. S. Sicato, S. Rathore, Y. Sung, and J. H. Park, "Blockchain-based secure storage management with edge computing for iot," Electronics, vol. 8, no. 8, p. 828, 2019.

[157] Y. Ren, Y. Leng, Y. Cheng, and J. Wang, "Secure data storage based on blockchain and coding in edge computing," Math. Biosci. Eng, vol. 16, no. 4, pp. 1874–1892, 2019.

[158] A. Nawaz, J. Peña Queralta, J. Guan, M. Awais, T. N. Gia, A. K. Bashir, H. Kan, and T. Westerlund, "Edge computing to secure iot data ownership and trade with the ethereum blockchain," Sensors, vol. 20, no. 14, p. 3965, 2020.

[159] A. Nawaz, T. N. Gia, J. P. Queralta, and T. Westerlund, "Edge ai and blockchain for privacy-critical and data-sensitive applications," in 2019 Twelfth International Conference on Mobile Computing and Ubiquitous Network (ICMU). IEEE, 2019, pp. 1–2.

[160] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu, and M. S. Hossain, "A secure data aggregation strategy in edge computing and blockchain empowered internet of things," IEEE Internet of Things Journal, 2020.

[161] L. Cui, S. Yang, Z. Chen, Y. Pan, Z. Ming, and M. Xu, "A decentralized and trusted edge computing platform for internet of things," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3910–3922, 2019.

[162] X. Xu, X. Zhang, H. Gao, Y. Xue, L. Qi, and W. Dou, "Become: Blockchain-enabled computation offloading for iot in mobile edge computing," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4187–4195, 2019.

[163] X. Xu, Y. Chen, X. Zhang, Q. Liu, X. Liu, and L. Qi, "A blockchain-based computation offloading method for edge computing in 5g networks," Software: Practice and Experience, 2019.

[164] Z. Zhang, Z. Hong, W. Chen, Z. Zheng, and X. Chen, "Joint computation offloading and coin loaning for blockchain-empowered mobile-edge computing," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9934–9950, 2019.

[165] L. Zhang, Y. Zou, W. Wang, Z. Jin, Y. Su, and H. Chen, "Resource allocation and trust computing for blockchain-enabled edge computing system," Computers & Security, vol. 105, p. 102249, 2021.

[166] C.-H. Chu, "Task offloading based on deep learning for blockchain in mobile edge computing," Wireless Networks, vol. 27, no. 1, pp. 117–127, 2021.

[167] X. Qiu, L. Liu, W. Chen, Z. Hong, and Z. Zheng, "Online deep reinforcement learning for computation offloading in blockchain-empowered mobile edge computing," IEEE Transactions on Vehicular Technology, vol. 68, no. 8, pp. 8050–8062, 2019.

[168] P. Kochovski, S. Gec, V. Stankovski, M. Bajec, and P. D. Drobintsev, "Trust management in a blockchain based fog computing platform with trustless smart oracles," Future Generation Computer Systems, vol. 101, pp. 747–759, 2019.

[169] 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, 2019.

[170] H. Yang, Y. Liang, J. Yuan, Q. Yao, A. Yu, and J. Zhang, "Distributed blockchain-based trusted multi-domain collaboration for mobile edge computing in 5g and beyond," IEEE Transactions on Industrial Informatics, 2020.

[171] B. Ernest and J. Shiguang, "Privacy enhancement scheme (pes) in a blockchain-edge computing environment," IEEE Access, vol. 8, pp. 25 863–25 876, 2020.

[172] Z. Qiao, C. Zhu, Z. Wang, and N. Yang, "Anonymous iot data storage and transaction protocol based on blockchain and edge computing," in International Conference on Science of Cyber Security. Springer, 2019, pp. 181–189.

[173] Y. Jiang, H. Bai, and H. Yang, "The messaging model design based blockchain and edge computing for the internet of things," in 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS). IEEE, 2019, pp. 604–608.

[174] H. Bai, Y. Jiang, H. Yang, and G. Xia, "The messaging protocols analysis of integrating blockchain and edge computing for iot," in 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS). IEEE, 2019, pp. 99–102.

[175] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Communication-efficient federated learning and permissioned blockchain for digital twin edge networks," IEEE Internet of Things Journal, 2020.

[176] L. Hou, K. Zheng, Z. Liu, X. Xu, and T. Wu, "Design and prototype implementation of a blockchain-enabled lora system with edge computing," IEEE Internet of Things Journal, 2020.

[177] P. Mendki, "Blockchain enabled iot edge computing: Addressing privacy, security and other challenges," in Proceedings of the 2020 The 2nd International Conference on Blockchain Technology, 2020, pp. 63–67.

[178] A. I. Sanka and R. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," Journal of Network and Computer Applications, p. 103232, 2021.

[179] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," Applied Sciences, vol. 11, no. 20, p. 9372, 2021.

[180] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," IEEE Access, vol. 8, pp. 16 440–16 455, 2020.

[181] G. Kaur and C. Gandhi, "Scalability in blockchain: Challenges and solutions," in Handbook of Research on Blockchain Technology. Elsevier, 2020, pp. 373–406.

[182] L. Yang, M. Jinbao, Y. Han, W. Sining, and F. Jingang, "Overview of blockchain capacity expansion technology," Electric Power Information and Communication Technology, vol. 18, pp. 1–9, 2020.

[183] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018, pp. 583–598.

[184] Y. Kwon, H. Kim, J. Shin, and Y. Kim, "Bitcoin vs. bitcoin cash: Coexistence or downfall of bitcoin cash?" in 2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019, pp. 935–951.

[185] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, "Spectre: a fast and scalable cryptocurrency protocol." IACR Cryptol. ePrint Arch., vol. 2016, no. 1159, 2016.

[186] 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, 2020.

[187] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE international congress on big data (BigData congress). IEEE, 2017, pp. 557–564.

[188] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016.

[189] H. Hees, "Raiden network: Off-chain state network for fast dapps," in Devcon Two. Ethereum Foundation, 2016.

[190] J. Poon and V. Buterin, "Plasma: Scalable autonomous smart contracts," White paper, pp. 1–47, 2017.

[191] J. Kwon and E. Buchman, "Cosmos whitepaper," 2019.

[192] U. Klarman, S. Basu, A. Kuzmanovic, and E. G. Sirer, "bloxroute: A scalable trustless blockchain distribution network whitepaper," IEEE Internet of Things Journal, 2018.

[193] Y. Liu, H. N. Dai, Q. Wang, M. K. Shukla, and M. Imran, "Unmanned aerial vehicle for internet of everything: Opportunities and challenges," Computer Communications, vol. 155, pp. 66–83, 2020.

[194] A. Vacca, A. Di Sorbo, C. A. Visaggio, and G. Canfora, "A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges," Journal of Systems and Software, vol. 174, p. 110891, 2021.

[195] P. Tolmach, Y. Li, S.-W. Lin, Y. Liu, and Z. Li, "A survey of smart contract formal specification and verification," ACM Computing Surveys (CSUR), vol. 54, no. 7, pp. 1–38, 2021.
[196] Z. Zheng, S. Xie, H. N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," 2019.