IIoT Data Sharing Based on Blockchain: A Multileader Multifollower Stackelberg Game Approach

Yuna Jiang, *Graduate Student Member, IEEE*, Yi Zhong, *Member, IEEE*, and Xiaohu Ge, *Senior Member, IEEE*

***Abstract*—The evolution of the Industrial Internet of Things (IIoTs) greatly increases the volume of data generated by the connected IIoT devices. IIoT data are playing an increasingly important role in various industrial sectors. IIoT data sharing helps enterprises make better production decisions and respond to market changes timely. However, the distrust among IIoT entities and IIoT entities' distrust of data-sharing platforms may hinder the realization of data sharing. In this article, a decentralized IIoT data-sharing scheme based on blockchain and edge computing is proposed. A Proof of Storage and Transmission (PoST) consensus mechanism is proposed to meet data storage and transmission requirements of data owners in IIoT data-sharing networks. Based on the manufacture ties of data owners, shared data request probabilities are derived. The IIoT data sharing interactions between data owners and edge devices are modeled as a multiple-leader and multiple-follower Stackelberg game. The alternating direction method of multipliers (ADMMs) algorithm is used to obtain the optimal IIoT data sharing solutions in a distributed manner. Simulation results show that compared with the cooperative scheme, the total profit of edge devices is maximally increased by 59%, and the total utility of data owners is maximally increased by 52%.**

***Index Terms*—Alternating direction method of multipliers (ADMM) algorithm, blockchain, data sharing, Industrial Internet of Things (IIoTs), Stackelberg game.**

I. Introduction

ADVANCES in the Industrial Internet of Things (IIoTs) have contributed to the development of Industry 4.0. 5G IIoT focuses on the connectivity of intelligent devices in different industrial sectors, including manufacturing, agriculture, healthcare systems, oil and gas industries, etc., [1]. IIoT systems collect various types of industrial data that contain traffic records of freight transport systems, data generated during industrial processes, etc., [2]. The data generated in the industrial networks play a crucial role in industrial decision making [3]. In order to effectively use industrial data to drive the development of intelligent manufacturing, data sharing is proposed to enhance the potential value of data [4]–[6]. In the existing IIoT networks, the data collected by smart devices are usually transferred to a centralized cloud platform for processing [7]. Most enterprises only utilize their own data and have no access to data from other industrial entities. Although some centralized data sharing platforms, such as Factual, InfoChimps, etc., allow different entities to share data. Distrust between data owners and data-sharing platforms hinders the data sharing. A decentralized data sharing scheme is urgently needed to make the most of the potential value of IIoT data.

Blockchain has attracted widespread attention in recent years due to its decentralization, autonomy, immutability, and traceability. Structural data stored on the blockchain need to be maintained by the entire network, which promotes value transfer between nodes without trust [8]. Blockchain is considered as a critical technology for the decentralization of IIoT [9]. Bitcoin is the first application of blockchain that can only be used for digital currency transactions. Vitalik Buterin introduces smart contracts into the blockchain, which makes the application of blockchain more diversified. Access control of data sharing in IIoT networks can be realized based on blockchain and smart contracts, such as the access control of healthcare data [10], access control management of Internet of Things (IoTs) devices [11], and resource and data access control between IoT devices [12]. Although the blockchain solves the IIoT data-sharing challenge for decentralization, there are still many problems when directly applying blockchain to IIoT data-sharing networks. In the blockchain consensus mechanism, nodes participating in the consensus process are responsible for transaction validation, block validation, and consensus formation. The decentralized consensus and the distributed ledger storage of blockchain networks put forward higher requirements for the capabilities of nodes in blockchain networks. However, most low-power IIoT devices are unable to participate in the consensus process. For the IIoT data sharing in blockchain-enabled networks, the storage of shared data needs to be considered. Each full node in blockchain networks needs to store the full distributed ledger of the blockchain locally. The shared data stored in the distributed ledger of blockchain may cause a significant waste of storage resources, and the large amount of data contained in transactions may result in a negative effect on the performance of blockchain networks. Besides, frequently transmitting the shared data may increase the energy consumption of low-power IoT devices and

Manuscript received April 25, 2021; revised July 11, 2021; accepted August 4, 2021. Date of publication August 10, 2021; date of current version March 7, 2022. This work was supported by the National Natural Science Foundation of China under Grant U2001210. *(Corresponding author: Xiaohu Ge.)*

The authors are with the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan 430074, Hubei, China (e-mail: xhge@mail.hust.edu.cn).

Digital Object Identifier 10.1109/JIOT.2021.3103855

TABLE I
ANALYSIS OF RELATED WORKS ABOUT BLOCKCHAIN-ENABLED DATA SHARING

Related works	Related Technique	Advantages	Limitations
Cloud data sharing [22]	Data sharing incentives, shapley value	Fair incentive mechanism for cloud data sharing	Shared data is stored on blockchain
IIoT data collection and sharing [23]	Mobile crowdsensing, deep reinforcement learning	Joint data collection and sharing	Shared data is stored on blockchain
secureSVM: Smart city data sharing [24]	Paillier, support vector machine(SVM), gradient descent	IoT data sharing for privacy-preserving SVM training	Shared data is stored on blockchain
Data sharing in storage systems [25]	Interplanetary file system (IPFS), attributed-based encryption	Fine-grained shared data access control, decentralized storage	No incentives for IPFS storage systems
Electronic health records sharing [26]	Smart contract, IPFS	Trustworthy access control, decentralized storage	No incentives for IPFS storage systems
Electronic medical records sharing [27]	Attribute-based encryption system, IPFS	Data access control without affecting retrieval, decentralized storage	No incentives for IPFS storage systems

cause serious interference due to the massive access [13]. Edge computing is an auspicious solution to support the blockchain-enabled IIoT networks [14]. The consortium blockchain is a specific blockchain with multiple preselected nodes to establish the distributed ledger with moderate cost [15]. The trustworthy edge devices can be preselected to reach the consensus by using consortium blockchain. The integration of consortium blockchain and edge computing can enable reliable control of networks as well as distributed storage and computation at the edges [16]. How to incorporate the edge computing and consortium blockchain into IIoT data-sharing networks to realize the decentralized IIoT data sharing needs to be further studied.

Another problem related to IIoT data sharing is the manufacture ties embedded in the IIoT networks. Manufacture tie networks are defined as groups of IIoT individuals with some patterns of manufacture interactions, forming certain manufacture relationships. For example, air conditioner manufacturers and air conditioning accessories manufacturer may form a manufacture tie network. Manufacture tie networks can be considered as social IoT networks in the industrial production. The objective of social IoT networks is to build social collaborative networks for smart objects, which improves service discovery and resource visibility in IoT networks [17], [18]. Social IoT networks have been studied extensively in coastal monitoring [19], semantic virtual-object-enabled real-time management [20], intrusion detection [21], large-scale smart environment development [18], etc. Manufacture relationships between IIoT entities may influence data sharing, as IIoT entities tend to share data with manufacture related entities. However, the manufacture ties between IIoT entities in the blockchain-enabled IIoT data sharing networks have not been studied in the literature.

In this article, an IIoT data-sharing scheme is proposed based on consortium blockchain and edge computing. The data sharing interactions among data owners, data consumers, and edge devices are investigated. The main contributions of this article are summarized as follows.

1) Based on data storage and transmission demand of data owners in IIoT data-sharing networks, a Proof of Storage and Transmission (PoST) consensus mechanism is proposed. During each consensus period, the probability that consensus nodes obtains consensus rewards depends on the amount of shared data stored and transmitted.
2) The shared data request probability is derived based on the manufacture ties of data owners, in which node degree and local clustering coefficient are considered.
3) The interactions between data owners and edge devices for IIoT data sharing are modeled as a multiple-leader and multiple-follower Stackelberg game problem. Considering the high-dimensional strategy space of game players, the alternating direction method of multipliers (ADMMs) algorithm is used to obtain the optimized game solutions of IIoT data sharing.
4) Simulation results show that the proposed IIoT data-sharing scheme converges to the optimal results quickly. Both data owners and edge devices can achieve optimal solutions. Besides, the proposed IIoT data-sharing scheme is compared with the cooperative scheme. The results show that the total profit of edge devices is maximally increased by 59%, and the total utility of data owners is maximally increased by 52%.

The remainder of this article is organized as follows. Related works are presented in Section II. The system model of the proposed IIoT data-sharing scheme is presented in Section III. Problem formulation is presented in Section IV. Multileader multifollower Stackelberg game formulation is shown in Section V. The ADMM algorithm is used to solve the Stackelberg game in Section VI. Section VII shows simulation results. Finally, Section VIII concludes this article.

II. RELATED WORKS

The blockchain-enabled data sharing networks were investigated in [22]–[27]. The critical analysis about the related works is summarized in Table I. In [22], a reliable collaboration model based on blockchain and smart contracts was proposed to ensure the security of data sharing among multicloud platforms. Liu *et al.* [23] proposed an efficient data collection and sharing scheme based on blockchain. A reliable and secure environment was created by combining the

Ethereum blockchain and deep reinforcement learning. In [24], a data training scheme was proposed to protect data privacy in the IoT networks. A safe and reliable data-sharing platform among multiple data providers was built through blockchain. In the data-sharing schemes proposed in [22]–[24], data owners encrypt the data that needs to be shared, and store it on the blockchain. The distributed ledger of the blockchain is stored in each full node. If the shared data are stored on the blockchain, it will cause a significant waste of storage resources. Besides, the large size of transactions will add a negative impact on the performance of the entire blockchain network. Therefore, it is not a feasible scheme to store the shared data on blockchain. In some other blockchain-based data-sharing studies, an interplanetary file system (IPFS) was used for the storage of shared data [25]–[27]. Wang *et al.* [25] proposed a data storage and sharing architecture that combines IPFS, Ethereum, and attribute-based encryption. In [26], a new electronic medical data-sharing framework based on blockchain and IPFS was proposed, and a reliable access control mechanism was designed by using smart contracts. In [27], an attribute-based encryption scheme was proposed to achieve safe storage and efficient sharing of electronic medical records. IPFS was used to store the encrypted electronic medical data. IPFS is a decentralized storage protocol, which allocates a unique hash for each data packet. Only the hash values of data packets need to be stored on the blockchain with IPFS. However, the stable operation of IPFS networks requires users to contribute storage space and network bandwidth. If there is no appropriate incentive mechanism, it is difficult to maintain the ongoing operation of a network with huge storage resource overhead.

Some other studies focus on the consensus mechanisms of blockchain networks [28]–[31]. The consensus mechanism is critical for blockchain networks. Both Bitcoin and Ethereum adopt the Proof-of-Work (PoW) algorithm that is strongly dependent on computation [28]. It is hard for low-power IoT devices to operate the PoW consensus mechanism. Hyperledger Fabric adopts the traditional practical Byzantine fault tolerance (PBFT) algorithm [29]. The PBFT algorithm effectively solves the low-efficiency problem of the original Byzantine fault-tolerant algorithm. The algorithm complexity is reduced from exponential to polynomial, making the Byzantine fault-tolerant algorithm feasible in practical applications. However, in IIoT networks with a large number of nodes, the communication complexity of PBFT will increase significantly. For the decentralized data storage, FileCoin proposed the PoS consensus mechanism that includes the proof of data possession (PDP) and Proof of Retrievability (PoR) [30], [31]. Compared with the PoW consensus mechanism, consensus nodes that participate in the PoS consensus mechanism do not need to waste a large amount of computing power on hash computation. Consensus nodes can increase their probabilities of getting consensus rewards by providing more storage space for other devices. In the research of blockchain-based IIoT data sharing, data sharing requirements and consensus mechanism design should be considered jointly to achieve efficient data sharing among multiple IoT entities.

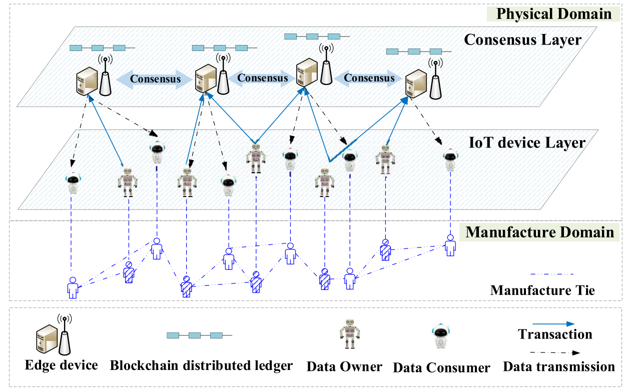

Fig. 1. System framework.

III. System Model

A. System Framework

In the consortium blockchain-enabled IIoT data-sharing networks, the edge computing is introduced to support the distributed consensus of blockchain networks due to the incapabilities of IIoT devices. Fig. 1 shows the IIoT data-sharing system framework. The physical domain contains the block consensus layer and IIoT device layer. Individuals in the manufacture domain correspond to IIoT devices in the IIoT device layer. There are manufacture ties between IIoT devices, and device pairs with manufacture ties are interested in the same data type. The block consensus layer and IIoT device layer in the physical domain are introduced as follows.

1) *Block Consensus Layer:* In the block consensus layer, edge devices with strong hardware capabilities can be admitted to join the consensus process of blockchain networks. As consensus nodes of the blockchain networks, edge devices are responsible for the block consensus, verification, and packaging of data-sharing transactions, etc. The edge device set is $\mathbb{D} = \{D_1, \ldots, D_d, \ldots, D_{N_D}\}$, and $N_D = |\mathbb{D}|$. The consensus mechanism among edge devices is PoST. During each consensus period, the probabilities that the edge devices receive the consensus reward depend on the amount of shared data they stored or transmitted. Edge devices participating in the consensus process form a distributed storage network. IIoT data owners can store the shared data in the distributed storage network. Meanwhile, the address of data storage is recorded on the blockchain distributed ledger.
2) *IIoT Devices Layer:* In the IIoT devices layer, IIoT devices can be data owners or data consumers. Data owners collect data from IIoT networks and share the collected data by sending transactions to blockchain networks. The data owner set is $\mathbb{O} = \{O_1, O_2, \ldots, O_i, \ldots, O_{N_O}\}$, and $N_O = |\mathbb{O}|$. The set of data packets shared by data owners is $\mathbb{F} = \{F_1, F_2, \ldots, F_i, \ldots, F_{N_O}\}$. Data consumers request the interested data from blockchain networks. The data consumer set is $\mathbb{C} = \{C_1, \ldots, C_j, \ldots, C_{N_C}\}$, and $N_C = |\mathbb{C}|$.

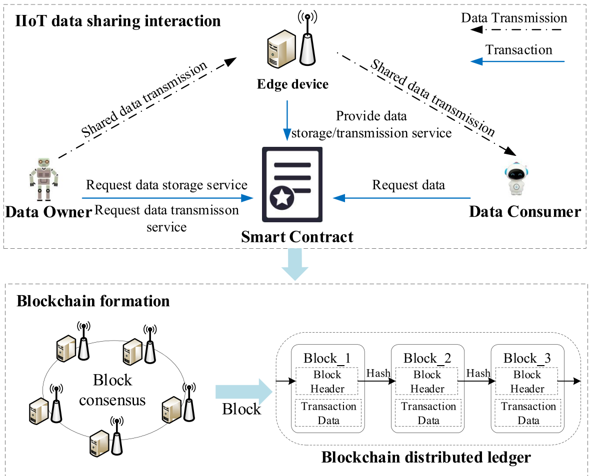

Fig. 2. IIoT data-sharing process.

B. IIoT Data-Sharing Process

The process of data sharing between IIoT devices through blockchain networks is shown in Fig. 2. In the IIoT data-sharing interaction stage, when the data owner O_i wants to share data F_i, O_i first requests data storage services by calling functions written in the smart contract. The shared data of O_i are stored in the distributed storage networks when the edge devices provide the storage service for O_i. The address of shared data stored by the data owner O_i is recorded on the blockchain distributed ledger. When the data consumer C_j requests data through the smart contract. If the data requested by C_j exist in blockchain networks, such as the data stored on the edge device D_d by O_i, O_i would send data transmission transactions to request data transmission service from D_d. Then, D_d transmits the requested data to C_j. If the data requested by C_j does not exist in blockchain networks, C_j needs to wait for the data owners with the related requested data to store the data in the distributed storage networks. After the data consumer C_j gets the requested data from data owners, such as O_i, C_j would share the quality information of the shared data to other data consumers with manufacture ties. If the data quality of O_i is high, then more data consumers who have manufacture ties with O_i would request data from O_i. The interaction processes among data owners, data consumers, and edge devices are operated automatically through smart contracts without relying on third-party platforms. In the blockchain formation stage, edge devices that are consensus nodes reach consensus based on the PoST mechanism. Then, the selected block that includes the block header and transaction data is added into the blockchain distributed ledger to form the traceability of shared data.

C. IIoT Data-Sharing Smart Contracts

Smart contracts are modular, reusable, and automatically executed scripts that run on the blockchain. Smart contracts are stored on the blockchain distributed ledger, so each node can execute functions written in smart contracts, and check the logs of interactions with smart contracts [32]. In the blockchain-enabled IIoT data-sharing networks, the interaction principles among data owners, data consumers, and edge devices, including the shared data storage and transmission principles among data owners and edge devices, and the data-sharing principles among data owners and data consumers, are recorded on the blockchain. Any IIoT entity can call functions written in smart contracts by sending transactions to blockchain networks, and then, the corresponding principles can be realized automatically. The proposed IIoT data-sharing scheme mainly contains the following smart contracts.

1) *Data Storage and Transmission Service Smart Contract:* Shared data storage and transmission principles among data owners and edge devices are written in the data storage and transmission service smart contract. By calling data storage functions in the smart contract, data owners can request storage services from edge devices. The storage time for one storage service request is set as a constant in the smart contract. The shared data of data owners are stored on the edge devices for the set time when the edge devices provide the storage services through blockchain. The stored data are deleted by the edge devices when the storage time exceeds the set time. Meanwhile, the addresses of data storage are recorded on the blockchain distributed ledger. When data consumers send data request transactions to blockchain networks, data owners would call the data transmission function in the smart contract. Then, the edge devices that stored the requested data will transmit the data to data consumers. After above transactions are verified and recorded on blockchain, edge devices will receive data storage and transmission service charges from data owners.
2) *Data-Sharing Smart Contract:* Data-sharing principles among data owners and data consumers are written in the data-sharing smart contract. Data consumers can request data from data owners by calling functions in the data-sharing smart contract. Data owners who own the requested data would call the data transmission function in the data storage and transmission service smart contract. Then, edge devices that stored the requested data will transmit the data to data consumers. After data consumers receive the requested data successfully, the data owners who provide the shared data will receive payoffs from data consumers.

D. Consensus Mechanism

In the consortium blockchain-enabled IIoT data-sharing networks, it is hard for low-power IIoT devices to maintain stable blockchain networks, as the consensus process is computing intensive or storage intensive. Edge devices with strong hardware capabilities can support the IIoT blockchain networks and join the block distributed consensus process. In the proposed IIoT data sharing scheme, edge devices need to provide storage service for IIoT data owners. Besides, edge devices need to transmit the requested data to data consumers who get data access permissions from data owners. The amount of IIoT data that edge devices stored and transmitted can both indicate the contributions of edge devices to data-sharing networks. Therefore, a Proof-of storage and transmission consensus mechanism is proposed in this article. During each consensus period, whether edge devices can obtain the consensus reward depends on the amount of shared data stored and transmitted. During the consensus period T, the amount of shared data storage in edge device D_d ($D_d \in \mathbb{D}$) is denoted as Data_S$_d$, and the amount of shared data transmission in D_d is denoted as Data_T$_d$. The probability that D_d gets the consensus reward is

$$P_d = \frac{\text{Data\_S}_d + \text{Data\_T}_d}{\sum_{d=1}^{N_D} (\text{Data\_S}_d + \text{Data\_T}_d)}. \tag{1}$$

IV. Problem Formulation

In the proposed IIoT data-sharing scheme, the positivity of edge devices to join the consensus process of blockchain networks and the enthusiasm of data owners to share data are the main focus to ensure the stable operation of IIoT data-sharing networks. Both edge devices and data owners might be willing to participate in data-sharing networks if they can obtain payoffs. In this section, the shared data request probability based on manufacture ties is analyzed. Then, the utility function of data owners and the profit function of edge devices are derived.

A. Data Request Probability Based on Manufacture Ties

When data owners share data with data consumers, data owners need to request data storage and transmission service from edge devices through blockchain networks. Based on the shared data storage service, data owners can store the shared data in edge devices. Based on the shared data transmission service, data consumers can get the requested data from edge devices with data owners' permissions. The probability is that the shared data requested by data consumers depend on the manufacture ties of data owners.

IIoT devices with manufacture ties are interested in the same data type, and share data or data quality information. The manufacture ties between data owners and data consumers mean that data consumers would request data from data owners. The manufacture ties between data consumers mean that data consumers would share the data quality information. The manufacture ties between IIoT devices are represented by a graph $G = (V, E)$, and $V = \{v_1, v_2, \ldots, v_n\}$ is the set of vertices and $E = \{e_{ab} : (a, b) \subset [1, \ldots, n]^2\}$ is the set of edges between vertices, e_{ab} is the edge connecting vertex v_a and v_b. The existence of e_{ab} represents that v_a and v_b have a manufacture tie, namely, v_a and v_b are interested in the same data type. The node degree and clustering coefficient have been widely studied as the critical indicators of social networks [33]. In an undirected and unweighted network, the node degree is the number of neighbor nodes. The neighbor nodes of v_a are nodes who are connected with v_a. The neighbor node set of v_a is $\Lambda_a = \{v_b : e_{ab} \in E\}$, and the number of elements in Λ_a is M_a. Thus, the node degree of v_a is M_a. The clustering coefficient of v_a denotes the degree of interconnection among neighbor nodes of v_a. A larger cluster coefficient of v_a indicates that the neighbor nodes of v_a are connected with a greater probability [34]. The local clustering coefficient of v_a is

$$CC_a = \frac{2|\{e_{ab} : v_a, v_b \in \Lambda_a, e_{ab} \in E\}|}{M_a(M_a - 1)}. \tag{2}$$

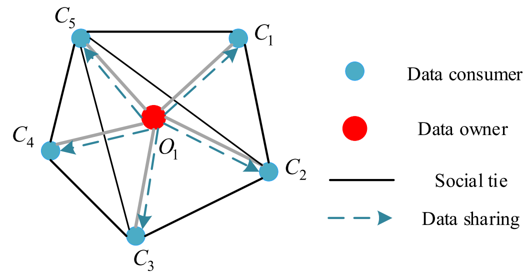

Fig. 3. Manufacture tie network of IoT devices.

In IIoT data-sharing networks, the node degree of data owner O_i ($O_i \in \mathbb{O}$) represents the number of IIoT devices that have manufacture ties with O_i. The local clustering coefficient of O_i represents the probability that IIoT devices who are connected with O_i have manufacture ties with each other. The node degree and local clustering coefficient of O_i can both evaluate the manufacture ties of O_i. In order to better understand the manufacture ties between IIoT entities, we set an example. As shown in Fig. 3, data owner O_1 has manufacture ties with data consumer C_1, C_2, C_3, C_4, and C_5. The node degree of O_1 is 5, and the local clustering coefficient of O_1 is 0.7. Assume that O_1 shares the high-quality data through blockchain networks. When C_1 gets the high quality data F_1 from O_1, C_1 would share the data quality information of F_1 with nodes who have manufacture ties with O_1, such as data consumer C_2 and C_5. Then, C_2 and C_5 would prefer to request F_1 from O_1. After C_5 gets the data F_1, C_5 would continue to share data quality information of F_1 to C_3 and C_4, which urges C_3 and C_4 to request F_1. In IIoT data-sharing networks, O_i with more manufacture ties would receive more data requests from data consumers.

The manufacture tie factor of the data owner O_i is derived based on the node degree and local clustering coefficient. The manufacture tie factor of O_i is

$$SI_{O_i} = \varepsilon CC_{O_i} \times M_{O_i} \tag{3}$$

where CC_{O_i} is the local clustering coefficient of O_i and M_{O_i} is the node degree of O_i. ε is the positive proportional coefficient. The request probability of data shared by O_i is

$$f_{O_i} = \frac{SI_{O_i}}{\sum_{m=1}^{N_O} SI_{O_m}}. \tag{4}$$

When the data owner O_i shares data, O_i will request data storage and transmission service from different edge devices. The shared data storage service requesting by O_i from edge devices $\mathbb{D}$ is denoted as $x_i^s = \{x_{i1}^s, \ldots, x_{id}^s, \ldots, x_{iN_D}^s\}$. The shared data transmission service requesting by O_i from edge devices $\mathbb{D}$ is denoted as $x_i^t = \{x_{i1}^t, \ldots, x_{id}^t, \ldots, x_{iN_D}^t\}$. $X^s = \{x_1^s, \ldots, x_i^s, \ldots, x_{N_O}^s\}$ represents the storage service demand of all data owners, and X_{-i}^s represents the storage service demand of data owners other than O_i. $X^t = \{x_1^t, \ldots, x_i^t, \ldots, x_{N_O}^t\}$ represents the transmission service demand of all data owners, and X_{-i}^t represents the transmission service demand of data owners other than O_i. The total amount of data storage service provided by edge device D_d is

$$x_{D_d}^{s,\text{total}} = \sum_{i=1}^{N_O} w_{id} x_{id}^s. \tag{5}$$

The total amount of data transmission service provided by the edge device D_d is

$$x_{D_d}^{t,\text{total}} = \sum_{i=1}^{N_O} w_{id} x_{id}^t \tag{6}$$

where w_{id} is the probability that the data owner O_i chooses the edge device D_d.

The shared data transmission service demand of O_i depends on the shared data storage service demand and the request probability of the stored data F_i. Assume that the number of data request at the edge device D_d follows the Poisson distribution with parameter λ. During the consensus period T, the total number of data requests at D_d is $T\lambda$, and the number of data requests for the data packet F_i is $f_{O_i}T\lambda$. The amount of data transmission service requested by O_i at D_d is

$$x_{id}^t = x_{id}^s f_{O_i} T\lambda. \tag{7}$$

Assume that the number of data requests at each edge device all follows the Poisson distribution with parameter λ. Then, the total amount of data transmission service requested by O_i during T is

$$x_{O_i}^{t,\text{total}} = \sum_{d=1}^{N_D} x_{id}^s f_{O_i} T\lambda. \tag{8}$$

B. Profit Function of Edge Devices

In the proposed IIoT data-sharing scheme, the consensus mechanism executed by edge devices is PoST. During each consensus period, the probability that edge devices get the consensus reward depends on the amount of shared data stored and transmitted. In order to get the consensus reward, edge devices would try their best to provide shared data storage and transmission service. The probability that the edge device D_d gets the consensus reward is

$$\begin{aligned} P_d\left(x_i^s, X_{-i}^s\right) &= \frac{x_{D_d}^{s,\text{total}} + x_{D_d}^{t,\text{total}}}{\sum_{d=1}^{N_D}\left(x_{D_d}^{s,\text{total}} + x_{D_d}^{t,\text{total}}\right)} \\ &= \frac{\sum_{i=1}^{N_O} w_{id}x_{id}^s + \sum_{i=1}^{N_O} w_{id}x_{id}^s f_{O_i}T\lambda}{\sum_{d=1}^{N_D}\left(\sum_{i=1}^{N_O} w_{id}x_{id}^s + \sum_{i=1}^{N_O} w_{id}x_{id}^s f_{O_i}T\lambda\right)}. \end{aligned} \tag{9}$$

In addition to the consensus reward, the edge device D_d can also obtain service profits from data owners. Besides, D_d needs to pay for the storage and transmission expenditures. The service prices that D_d sets for data owners $\mathbb{O}$ is denoted as $p_d = \{p_{1,d}, \ldots, p_{i,d}, \ldots, p_{N_o,d}\}$. The profit function of edge device D_d is expressed as follows:

$$\begin{aligned} U_{D_d} = &\, RP_d\left(x_i^s, X_{-i}^s\right) + \sum_{i=1}^{N_o} w_{id}\left(x_{id}^s + \delta x_{id}^t\right)p_{i,d} \\ &- \sum_{i=1}^{N_o} w_{id}x_{id}^s c_s - \sum_{i=1}^{N_o} w_{id}x_{id}^t c_t \end{aligned} \tag{10}$$

where the first part is the consensus reward, the second part is the profits of data storage and transmission services that D_d charges from data owners, the third part is the storage expenditure of D_d, and the last part is the transmission expenditure of D_d. c_s is the storage expenditure coefficient of edge devices. c_t is the transmission expenditure coefficient of edge devices. δ_i is the pricing factor of the data transmission services provided by edge devices, which is related to the data request probability of data owners. δ_i is expressed as

$$\delta_i = 1 - \frac{f_{O_i}}{f_{O,\max}}. \tag{11}$$

In (11), δ_i is inversely proportional to f_{O_i}, which means that edge devices prefer to provide services for data owners whose shared data have a higher request probability.

C. Utility Function of Data Owners

Based on edge devices' pricing scheme, data owners will decide the amount of data shared through edge devices to maximize their utilities. The utility function of data owners is constituted by three parts. The first part is the utility obtained by storing the shared data in edge devices. The second part is the utility obtained by sharing data with data consumers. The last part is the service expenses paid to edge devices. The total amount of data shared by the data owner O_i with the aid of edge devices $\mathbb{D}$ is expressed as $x_{O_i}^{t,\text{total}} = \sum_{d=1}^{N_D} w_{id}x_{id}^t$. The utilities that data owners receive by storing shared data in edge devices and sharing data with data consumers are represented by the logarithmic function, whose marginal utility is diminishing [35], [36]. The utility of data owner O_i increases by increasing the amount of data stored $x_{O_i}^{s,\text{total}}$ and the amount of data shared $x_{O_i}^{t,\text{total}}$. But the increase of utility becomes lower when $x_{O_i}^{s,\text{total}}$ and $x_{O_i}^{t,\text{total}}$ are larger. The utility function of the data owner O_i is

$$\begin{aligned} U_{O_i} = &\, \varpi_1 \sum_{d=1}^{N_D} w_{id}\log\left(1 + x_{id}^s\right) \\ &+ \varpi_2 \sum_{d=1}^{N_D} w_{id}\log\left(1 + f_{O_i}T\lambda x_{id}^s\right) \\ &- \varpi_3 \sum_{d=1}^{N_D} w_{id}x_{id}^s\left(1 + \delta f_{O_i}T\lambda\right)p_{i,d} \end{aligned} \tag{12}$$

where ϖ_1 is the utility coefficient of data storage, ϖ_2 is the utility coefficient of data sharing, and ϖ_3 is the expense coefficient of data owners.

In this article, the incentive mechanism in [37] is adopted to define the probability that the data owner O_i chooses the edge device D_d to provide service, and w_{id} is expressed as

$$w_{id} = \frac{p_{\max} - p_{i,d}}{\sum_{k=1}^{N_D}\left(p_{\max} - p_{i,k}\right)} \tag{13}$$

where the numerator represents the difference between the maximum value of service price $p_{\max}$ and the service price of edge device D_d. The value of w_{id} becomes larger, when $p_{i,d}$ is lower, which is an incentive for edge devices to lower their prices.

V. Multileader Multifollower Stackelberg Game Formulation

Game theory is a powerful tool to study the distributed decision making of strategic agents [38]. In this section, the interactions between edge devices $\mathbb{D}$ and data owners $\mathbb{O}$ are modeled as a multileader and multifollower Stackelberg game. Stackelberg game is a two-stage complete information dynamic game that describes sequential interactions between strategy players. In stage I, the edge devices act as leaders to set the prices of data services. In stage II, the data owners act as followers of the game to decide the amount of data stored and transmitted. In this article, the amount of data transmission can be represented by the amount of data storage requested by data owners $\mathbb{O}$. The price of data transmission services can be represented by the price of data storage services provided by edge devices $\mathbb{D}$. Therefore, we only need to study the amount of data storage requested by data owners $\mathbb{O}$ and the price of data storage services provided by edge devices $\mathbb{D}$.

A. Data Owners' Service Demand in Stage II

In stage II, the pricing scheme of edge devices is given as $P = \{p_1, \ldots, p_d, \ldots, p_{N_d}\}$, and $p_d = [p_{i,d}](0 \leq p_{i,d} \leq p_{\max}, 1 \leq i \leq N_O)$. The data storage strategy of data owners except for data owner O_i is obtained as X^s_{-i}. The data owner O_i decides its data storage demand $x^{s,\text{total}}_{O_i}$ by optimizing the following objective function:

$$\begin{aligned}U_{O_i}\left(x_i^s, X_{-i}^s, P\right) = \varpi_1 \sum_{d=1}^{N_D} w_{id} \log\left(1 + x_{id}^s\right)\\ + \varpi_2 \sum_{d=1}^{N_D} w_{id} \log\left(1 + f_{O_i} T\lambda x_{id}^s\right)\\ - \varpi_3 \sum_{d=1}^{N_D} w_{id} x_{id}^s \left(1 + \delta f_{O_i} T\lambda\right) p_{i,d}. \quad (14)\end{aligned}$$

The subgame of the data owner O_i is formulated as follows:

$$\begin{aligned}\max_{x_i^s}\ & U_{O_i}\left(x_i^s, X_{-i}^s, P\right)\\ \text{s.t.}\ & x_{id}^s \geq 0\\ & \sum_{d=1}^{N_D} x_{id}^s \leq S_{\max} \quad (15)\end{aligned}$$

where $S_{\max}$ is the maximum amount of data stored by each data owner. Considering the privacy problem, data owners will not increase the amount of shared data indefinitely.

B. Edge Devices' Pricing Strategy in Stage I

In stage I, based on data owners' data storage demand X^s, and the pricing scheme of other edge devices except for edge device D_d that is P_{-d}, each edge device determines the price of its data storage services to maximize profit. The objective function for the edge device D_d is

$$\begin{aligned}U_{D_d}\left(p_d, P_{-d}, X^s\right) = R \frac{\sum_{i=1}^{N_O} w_{id} x_{id}^s \left(1 + f_{O_i} T\lambda\right)}{\sum_{d=1}^{N_D} \sum_{i=1}^{N_O} w_{id} x_{id}^s \left(1 + f_{O_i} T\lambda\right)}\\ + \sum_{i=1}^{N_o} w_{id} x_{id}^s \left(1 + \delta f_{O_i} T\lambda\right) p_{i,d}\\ - \sum_{i=1}^{N_o} w_{id} x_{id}^s \left(c_s + f_{O_i} T\lambda c_t\right). \quad (16)\end{aligned}$$

The subgame of the edge device D_d is formulated as follows:

$$\begin{aligned}\max_{p_d}\ & U_{D_d}\left(p_d, P_{-d}, X^s\right)\\ \text{s.t.}\ & 0 \leq p_{i,d} \leq p_{\max}. \quad (17)\end{aligned}$$

The difficulty in solving the multileader and multifollower game problem proposed in this article lies in the high-dimensional strategy space of each data owner. The traditional backward compatible method is no longer suitable. The ADMM optimization algorithm is adopted to solve the optimal solution of the Stackelberg game between edge devices and data owners.

VI. Optimization of Utility and Profit Based on ADMM Algorithm

In the blockchain-enabled IIoT data-sharing networks, both edge devices and data owners are rational agents who want to maximize their payoffs. However, maximizing the profit of the edge device D_d will affect the payoffs of other edge devices and all data owners. Maximizing the utility of the data owner O_i will affect the payoffs of other data owners and all edge devices. The ADMM algorithm can decompose a complex optimization problem into multiple subproblems to deal with distributed multiparameter convex optimization problems in the scenarios with large scale. Besides, the ADMM algorithm has good convergence. The ADMM algorithm is feasible to the distributed blockchain-enabled IIoT data-sharing system constituted by multiple edge devices and multiple data owners. In this article, the ADMM algorithm is adopted to solve the multileader multifollower Stackelberg game problem in the proposed IIoT data-sharing networks.

The multileader multifollower Stackelberg game problem proposed in this article contains two-level iterations. In the inner loop, based on the service pricing scheme P given by edge devices, data owners employ the ADMM algorithm to obtain the optimal amount of data storage X^s that maximize their utilities. In the outer loop, edge devices act as leaders to give the pricing scheme P that maximize edge devices' profits. Data owners act as followers and update their shared data storage strategy X^s based on the pricing scheme updated by edge devices.

The iterative optimization problem between data owners and edge devices is shown as follows.

A. Inner Loop

In the inner loop, the ADMM algorithm is used to solve the optimal strategies of data owners in the qth outer loop, where q is the number of outer loop iterations. The utility optimization of data owners is shown in (15), which has inequality constraints. To use the ADMM algorithm to solve the problem, we first need to transform the inequality-constrained optimization problem into an equality-constrained optimization problem. The transformed problem is

$$\begin{aligned} \max_{x_i^s} \;& U_{O_i}\left(x_i^s, X_{-i}^s, P\right) \\ \text{s.t. } & f_{id}\left(x_{id}^s\right) = 0 \\ & g_i\left(x_i^s\right) = 0 \end{aligned} \tag{18}$$

where $f_{id}(x_{id}^s) = \max\{0, -x_{id}\}^2$, and $g_i(x_i^s) = \max\{0, \sum_{d=1}^{N_D} x_{id}^s - S_{\max}\}^2$ [39], [40].

The number of the inner loop is denoted as t, and the process of solving the optimal solution based on the ADMM algorithm in the inner loop is shown as follows. For the utility function of the data owner O_i shown in (14), its augmented Lagrangian function is

$$\begin{aligned} L&\left(x_i^s, \eta_i, \mu_i\right) \\ &= U_{O_i} + \eta_i^T \sum_{d=1}^{N_D} f_{id}\left(x_{id}^s\right) + \frac{\rho}{2}\left\|\sum_{d=1}^{N_D} f_i\left(x_{id}^s\right)\right\|_2^2 \\ &\quad + \mu_i^T g_i\left(x_i^s\right) + \frac{\rho}{2}\left\|g_i\left(x_i^s\right)\right\|_2^2 \end{aligned} \tag{19}$$

where η_i and μ_i are dual variables. The variable x_i^s is decomposed and updated based on the scale-form solution of the ADMM algorithm. The strategy update steps are shown in

$$\begin{aligned} &\left(x_{id}^s\right)^q(t+1) \\ &= \underset{x_{id}^s}{\operatorname{argmax}}\left(U_{O_i}\right) + \frac{\rho}{2}\left\|f_{id}\left(x_{id}^s\right)^q(t+1) + \gamma_i^t\right\|_2^2 \\ &\quad + \frac{\rho}{2}\left\|g_{id}\left(x_{id}^s\right)^q(t+1) + v_i^t\right\|_2^2 \end{aligned} \tag{20}$$

$$\begin{aligned} &g_{id}\left(x_{id}^s\right)^q(t+1) \\ &= \max\left\{0, \begin{array}{l} \sum\limits_{k=1}^{d-1}\left(x_{ik}^s\right)^q(t+1) + \left(x_{id}^s\right)^q \\ + \sum\limits_{k'=d+1}^{N_D}\left(x_{ik'}^s\right)^q(t) - S_{\max} \end{array}\right\}^2 \end{aligned} \tag{21}$$

where γ_i and v_i are scale-form dual variables, and are expressed as

$$\gamma_i = \frac{\eta_i}{\rho} \tag{22}$$

$$v_i = \frac{u_i}{\rho}. \tag{23}$$

The update step of γ_i is shown as

$$\gamma_i^{t+1} = \gamma_i^t + \max\left\{0, -(x_i)^q(t+1)\right\}^2. \tag{24}$$

The update step of v_i is shown as

$$v_i^{t+1} = v_i^t + \max\left\{0, \sum_{d=1}^{N_D}(x_{id})^q(t+1) - S_{\max}\right\}^2 \tag{25}$$

where $\rho > 0$ is a damping factor. Data owners' strategy $x_i^s (1 \le i \le N_O)$ is updated based on the above iterative steps until x_i^s, γ_i, and v_i no longer change significantly. In the iterative update process of x_{id}^s, the bisection method is used to get the optimal value of x_{id}^s that maximizes U_{O_i}.

Algorithm 1 IIoT Data-Sharing Strategy Game Optimization Algorithm

Input: $p_{i,d} \in \left[0, p_{\max}\right]$, where $d = 1, 2, \cdots, N_D, i = 1, 2, \cdots, N_O$, Ξ, $q = 1$;
Output: Optimal storage strategy of data owners $\left(x_{id}^s\right)^*$;
Optimal pricing strategy of edge devices $\left(p_{i,d}\right)^*$;
While $\left\|U_{D_d}\left(p_{i,d}\right)^q - U_{D_d}\left(p_{i,d}\right)^{q-1}\right\| \le \Xi$

1: Inner loop: Based on the pricing strategy given by edge devices $p_{i,d}$, data owners iteratively update the storage strategy based on the ADMM algorithm to obtain the optimal amount of data storage $\left(x_{id}^s\right)^q$ that maximizes U_{O_i};
2: Outer loop: Based on the storage strategy given by data owners, the edge devices get the optimal value of $\left(p_{i,d}\right)^q$ that maximizes U_{D_d} with the bisection method;
3: $q = q + 1$
4: Result:Optimal storage strategy of data owners $\left(x_{id}^s\right)^*$;
Optimal pricing strategy of edge devices $\left(p_{i,d}\right)^*$;

B. Outer Loop

In the outer loop, when edge devices get the strategies $X^s = \{x_1^s, \ldots, x_i^s, \ldots, x_{N_O}^s\}$ of data owners in the qth outer loop, each edge device adjusts its pricing strategy to maximize the profit. The iterative steps for the edge device D_d to adjust its pricing strategy are shown as follows:

$$\left(p_{i,d}\right)^q(t+1) = \arg\max_{p_{i,d}}\left(U_{D_d}\left(p_{i,d}\right)^q\right). \tag{26}$$

Each edge device gradually updates its service pricing strategy $p_d = \{p_{1,d}, \ldots, p_{i,d}, \ldots, p_{N_o,d}\}$ based on the above iterative steps. After all edge devices update the pricing strategy, they will notify the data owners of the updated pricing strategies. Then, the q + 1th outer loop starts. The outer loop of the algorithm is formed. The condition under which the outer loop ends is shown as follows:

$$\left\|U_{D_d}\left(p_{i,d}\right)^q - U_{D_d}\left(p_{i,d}\right)^{q-1}\right\| \le \Xi \tag{27}$$

where $1 \le i \le N_O$, $1 \le d \le N_D$, Ξ is the predefined threshold. During the iteration of pricing strategies given by edge devices, the optimal strategy $(p_{i,d})^q$ that maximizes $U_{D_d}(p_{i,d})^q$ needs to be solved. Considering the complexity of the profit function of edge devices, the bisection method is used to get the optimal value of $p_{i,d}$ that maximizes $U_{D_d}(p_{i,d})^q$.

C. Convergence Analysis

The framework of the Stackelberg game-based optimization algorithm is shown in Algorithm 1. From [41]–[43], it has been shown that the ADMM converges to the stable optimal solutions when the minimum objective function is separable and convex. After checking the utility function of data owners $U_{O_i}(x_i^s, X_{-i}^s, P)$, we have the following proposition.

Proposition 1: The utility function of each data owner $U_{O_i}(x_i^s, X_{-i}^s, P)$ is strictly concave.

Proof: See Appendix A. ■

We will further give the convergence analysis of the ADMM algorithm used in the inner loop. Based on the concave of data owners utility function, the convergence of the ADMM algorithm in the inner loop is analyzed as follows. The Lagrangian function of problem (18) is given as follows:

$$L_0\left(x_i^s, \eta_i, \mu_i\right) = U_{O_i} + \eta_i^T \sum_{d=1}^{N_D} f_{id}\left(x_{id}^s\right) + \mu_i^T g_i\left(x_i^s\right). \quad (28)$$

Based on the dual theory, we can get that for all $x_i^s \in X^s$, there is

$$L_0\left(x_i^{s*}, \eta_i^*, \mu_i{}^*\right) \geq L_0\left(x_i^s, \eta_i^*, \mu_i{}^*\right) \quad (29)$$

where x_i^{s*}, γ_i^*, and $\mu_i{}^*$ are optimal primal and dual variables. The Lagrangian function is identical to the augmented Lagrangian function with $\rho = 0$. Considering that the strong duality holds, the optimal solution of problem (18) is the same as the optimal solution of the Lagrangian dual. The optimal function value is defined as $U_{O_i}^*$, and the residuals of the equality constraints are defined as $r_{g_i}^t = g_i(x_i^s)^t$ and $r_{f_i}^t = f_i(x_i^s)^t$, respectively. Then, we have the following theorem.

Theorem 1: The ADMM algorithm used in the inner loop satisfies the following convergence.

1) *Convergence of the Residuals:* When $t \to \infty$, we get $r_{g_i}^t \to 0$, $r_{f_i}^t \to 0$.
2) *Convergence of the Optimal Function Value:* When $t \to \infty$, the function value will approach the optimal function value, $U_{O_i} \to U_{O_i}^*$.

The proof of Theorem 1 can be found in [40]. The convergence of the inner loop is proved. For the outer loop, we need to prove the concave of the profit function $U_{D_d}(p_d, P_{-d}, X^s)$. We have the following proposition.

Proposition 2: The profit function of each edge device $U_{D_d}(p_d, P_{-d}, X^s)$ is strictly concave.

Proof: See Appendix B. ■

Based on the above analysis, we can get that the proposed IIoT data-sharing strategy game optimization algorithm is convergent.

D. Computation Complexity

In the proposed IIoT data-sharing strategy game optimization algorithm, each data owner decides its storage strategy based on the ADMM algorithm. The complexity of the ADMM algorithm is $O(1/\Xi^2)$, where Ξ is the predefined tolerance or convergence index of the ADMM algorithm [44]. Since there are N_O data owners, the time required for the inner loop is $O(N_O/\Xi^2)$. Then, the edge devices give the pricing strategy for each data owner. The complexity of the outer loop is $O(N_O N_D)$. Besides, the number of iterations required for the convergence of the algorithm is $O((N_O N_D)/\Xi)$. Therefore, the total computation complexity of the proposed scheme is $O([N_O N_D/\Xi]([N_O/\Xi^2] + N_O N_D))$.

E. Communication Overhead

The communication overhead can be described by the number of scalars exchanged by edge devices and data owners. At the end of the inner loop, each data owner needs to send its storage strategy to edge devices. The total number of scalars sent to the edge devices is equal to $N_O N_D$. Then, the edge devices announce the pricing strategy to each data owner. The number of transmitted scalars is $N_O N_D$. The total number of iterations required for convergence is $O(N_O N_D/\Xi)$, and when the convergence is reached, the edge devices announce the optimal pricing strategy to each data owner. Therefore, the total number of scalars transmitted, that is, the communication overhead, is $2O((N_O N_D)/\Xi)(N_O N_D) + N_O N_D$.

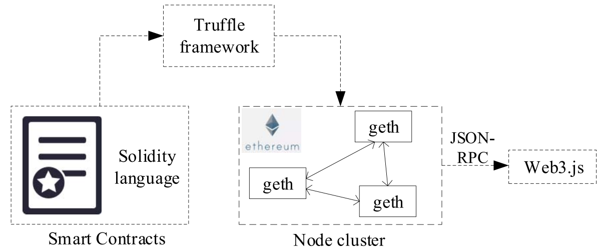

Fig. 4. Implementation of smart contracts.

VII. Implementation and Simulation Analysis

In this article, the designed smart contracts are implemented and tested on the Ethereum blockchain platform. The implementation process is shown in Fig. 4. The Solidity language is used to write the smart contracts. The blockchain node cluster that includes the data owner, data consumer, and edge device is built based on go-ethereum (geth). The configuration file for the genesis block is defined, including the blockchain network ID, gas limit, etc. Each geth node can open a Javascript Console, where the built-in objects can execute certain operations. The designed smart contracts are compiled and deployed on the blockchain node cluster based on the truffle framework. Then, each blockchain node can interact with the smart contracts. In the following, the shared data request probability based on manufacture tie networks is first analyzed. Then, the convergence of the ADMM algorithm based on the Stackelberg game is analyzed. The performance of the multileader and multifollower data-sharing scheme proposed in this article is compared with the cooperative scheme. Without specific explanation, the simulation parameters of this article are set as follows $T = 20$, $R = 5000$, $\lambda = 30$, $\Xi = 0.01$, $\varpi_1 = 5$, $\varpi_2 = 5$, $\varpi_3 = 0.1$, $p_{\max} = 20$, and $S_{\max} = 300$.

A. Simulation Analysis of Data Request Probability

In this section, the data request probability of data owners based on manufacture tie networks is analyzed. The manufacture tie network between IIoT devices is formed based on the NW model and Octopus model. The NW model is a small world model proposed in [45]. The NW network model starts with the vertex ring, and edges are randomly added between pairs of selected vertices. The Octopus model is proposed based on small-world and scale-free network model [46]. In the Octopus model, nodes are allowed to have a random number of long-range contacts, and a threshold is set for nodes to form short-range contacts. The manufacture ties between IIoT devices include long-range contacts and short-range contacts, representing far and close social connections, respectively. The number of short-range contacts for each IIoT device is equal

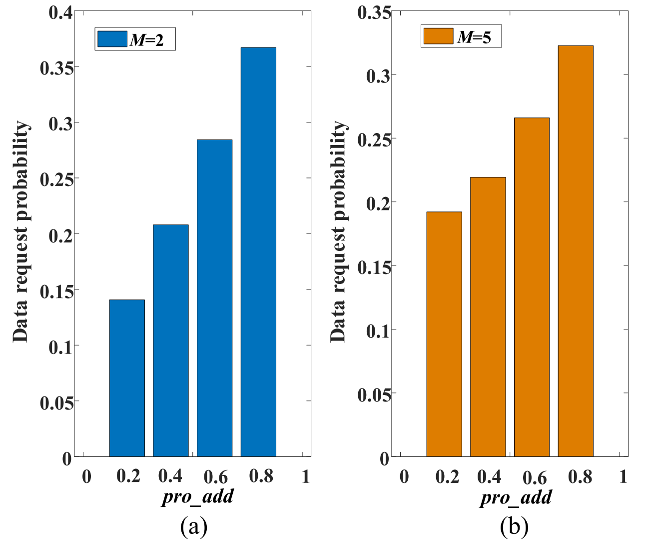

Fig. 5. Data request probability of data owners. (a) Data request probability (M=2). (b) Data request probability (M=5).

to the initialized node degree. The long-range contacts are randomly added between IIoT devices with a probability *pro_add*. In the simulation environment, the initialized node degree of IIoT devices is M, and the number of data owners is N_O. For each data owner, edges are randomly added between data owners and other unconnected IoT devices with a probability *pro_add*, which are long-range contacts of data owners. The data request probability of data owners can be obtained based on the formed manufacture tie network. In this section, the number of data owners is 4, and the values of *pro_add* for four data owners are 0.2, 0.4, 0.6, and 0.8, respectively.

Fig. 5 shows the data request probability of data owners with different *pro_add*. As shown in Fig. 5, when the initialized node degree M is fixed, the data request probability of data owners grows with the increase of *pro_add*. Besides, with the increase of M, the difference in the data request probability among data owners decreases. As the increase of M mitigates the impact of local clustering coefficient on the data request probability.

B. Simulation Analysis of Stackelberg Game-Based IIoT Data Sharing

In this section, the multileader multifollower Stackelberg game-based IIoT data sharing is simulated and analyzed. First, the convergence of the data-sharing strategy game optimization algorithm is shown. Then, numerical results about the performance of the proposed data-sharing scheme are shown. Finally, the proposed IIoT data-sharing scheme is compared with the cooperative scheme.

Fig. 6 shows the convergence of the data-sharing strategy game optimization algorithm. We consider four data owners and three edge devices, and the data request probabilities of data owners can be obtained from above simulation results, which are 0.1398, 0.2075, 0.2890, and 0.3637, respectively. The value of c_s is 1, 5, and 10 for each edge device. The value of c_t is 1, 5, and 10 for each edge device, and $\lambda = 6$. From Fig. 6, we can get that the utilities of data owners and profits of

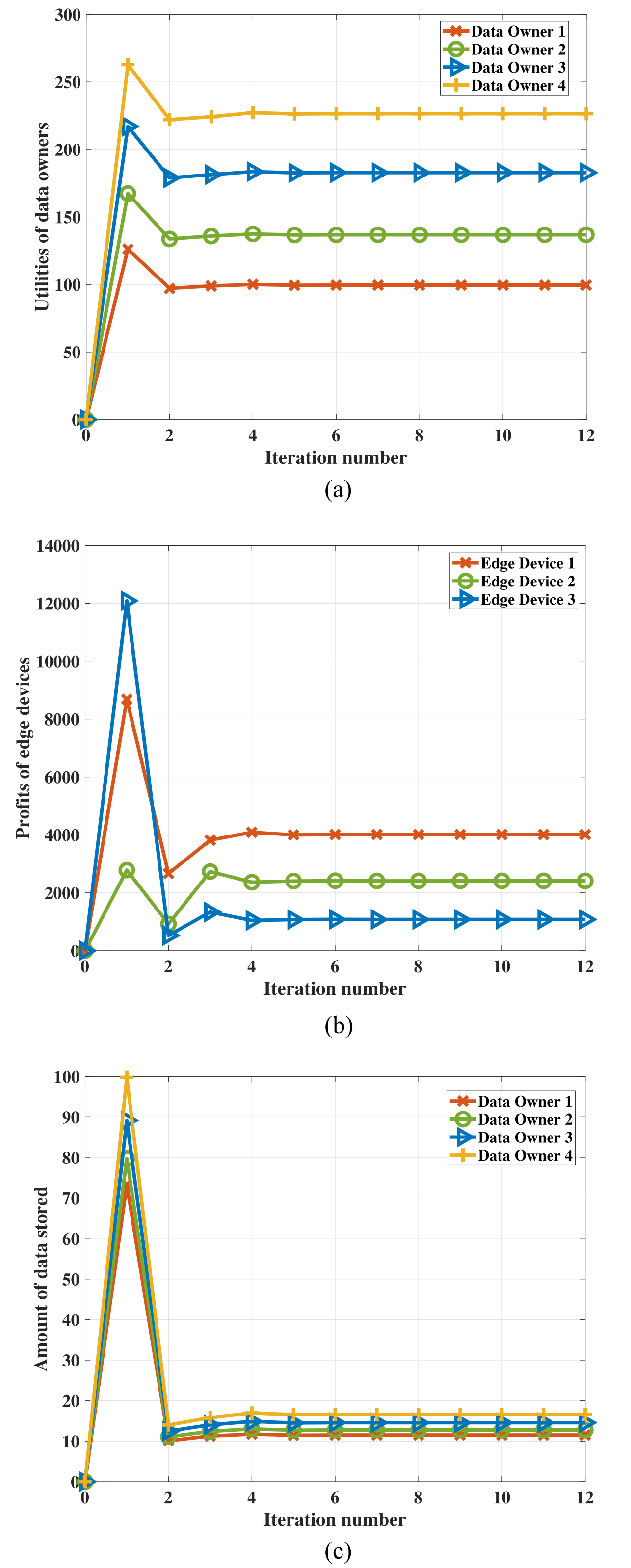

Fig. 6. Convergence among data owners and edge devices to get the optimum results. (a) Utilities of data owners versus iteration number. (b) Profits of edge devices versus iteration number. (c) Amount of data stored versus Iiteration number.

edge devices all converge quickly. As shown in Fig. 6(a), the utility of data owner 4 is maximum while the utility of data owner 1 is minimum. We can get that with the increase of

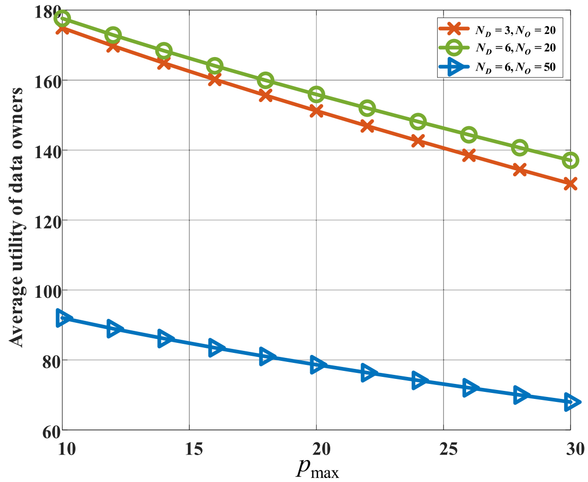

Fig. 7. Average utility of data owners as function of $p_{\max}$ ($c_s = c_t = 1$).

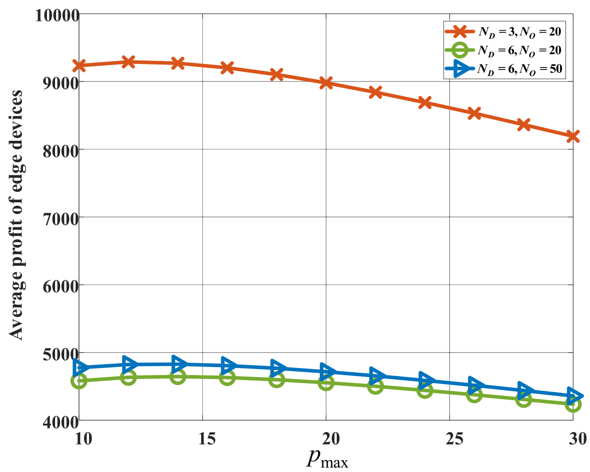

Fig. 8. Average profit of edge devices as function of $p_{\max}$ ($c_s = c_t = 1$).

data request probability, the utilities of data owners increase. From Fig. 6(b), the profit of edge device 1 is maximum, as the data storage and transmission overhead of edge device 1 are minimum. From Fig. 6(c), the amount of data stored by data owner 4 is higher than other three data owners, as the data owner 4 has the highest data request probability.

Fig. 7 shows the average utility of data owners as function of $p_{\max}$. The data request probability for each data owner is equal. As shown in Fig. 7, the average utility of data owners declines with the increase of $p_{\max}$. When the number of data owners is fixed, the growth in the number of edge devices increases the average utility of data owners. The reason is that a significant number of edge devices increase the competitiveness among edge devices, which impels edge devices to decrease the service price. When the number of edge devices is fixed, the increase in the number of data owners reduces the average utility of data owners. Because when the number of data owners increases, the data request probability for each data owner decreases, which makes the average utility of data owners reduced.

Fig. 8 shows the average profit of edge devices as the function of $p_{\max}$.The data request probability for each data owner

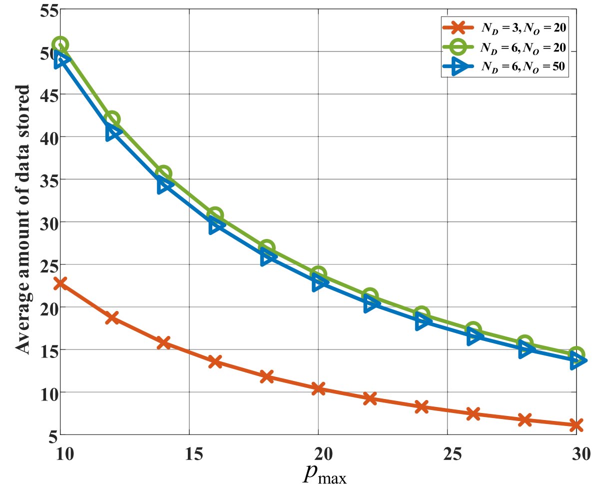

Fig. 9. Average amount of data stored as function of $p_{\max}$ ($c_s = c_t = 1$).

is equal. As shown in Fig. 8, the increase of $p_{\max}$ makes the average profit of edge devices grow to a maximum value first and then decrease. Due to the fact that the growth of $p_{\max}$ will increase the average profit of edge devices at first. As $p_{\max}$ continues to increase, the probability that the edge device is selected by data owners for data storage and transmission will decrease, so the income of the edge device will show a decreasing trend. When the number of data owners is fixed, the increase in the number of edge devices will decrease the average profit of edge devices substantially. On the one hand, the increase in the number of edge devices reduces the probability of edge devices obtaining the consensus reward, which leads to the decrease in average profit. On the other hand, a higher number of edge devices increase the competitiveness among edge devices, which impels edge devices to decrease the price. So the average profit of edge devices decreases. When the number of edge devices is fixed, the increase in the number of data owners increases the average profit of edge devices slightly. The reason is that the increase in the number of data owners increases the total amount of shared data, which increases the average profit of edge devices.

Fig. 9 shows the average amount of data stored by data owners as the function of $p_{\max}$. From Fig. 9, we can observe that the average amount of data stored by data owners declines with the increase of $p_{\max}$. As the number of edge devices increases, the average amount of data storage increases. The growth in the number of data owners makes the average amount of data stored reduce slightly.

Fig. 10 shows the total payoffs as the function of the consensus reward R. As shown in Fig. 10, when λ is fixed, the total utility of data owners and total profit of edge devices grow linearly with the increase of R. When R is fixed, the total utility of data owners and total profit of edge devices increase with the increase of λ.

Next, the IIoT data-sharing scheme proposed in this article is compared with the cooperative scheme. Under the cooperative scheme, edge devices cooperate with each other to provide data storage and transmission services for data owners. So there is no competitiveness among edge devices. The service price is $p_{\max}$ for each edge device. For the cooperative

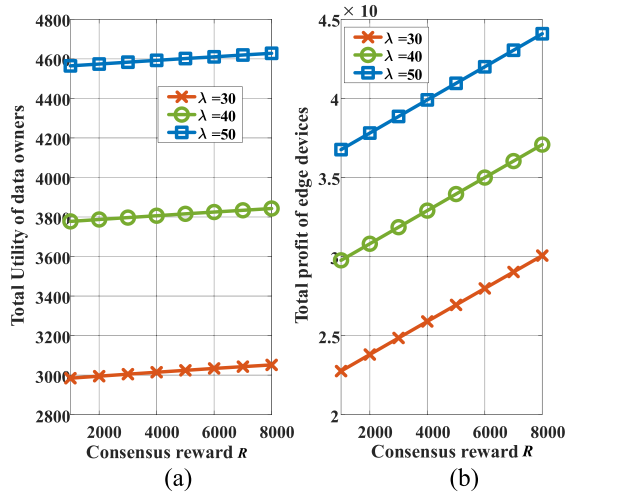

Fig. 10. Total payoffs as function of consensus reward R. (a) Consensus reward R. (b) Consensus reward R.

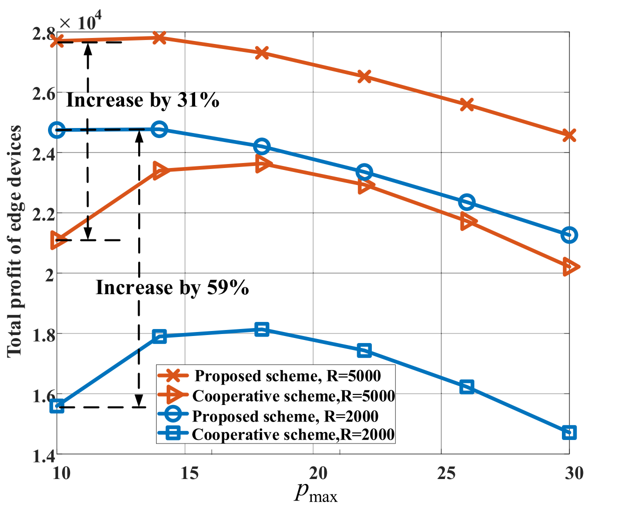

Fig. 11. Total profit of edge devices as function of $p_{\max}$ considering different schemes ($N_O = 20$, $N_D = 3$).

scheme, the computation complexity is $O([N_O/\Xi^2])$, and the communication overhead is $2N_ON_D + N_D(N_D - 1)$. Although the computation complexity and communication overhead of the cooperative scheme are lower than those of the proposed scheme, we show that the payoffs of both data owners and edge devices under the proposed scheme are higher than those under the cooperative scheme.

Fig. 11 shows the total profit of edge devices as function of $p_{\max}$ considering different schemes. When $p_{\max}$ is fixed, the difference of edge devices total profit between the proposed scheme and cooperative scheme becomes higher when the consensus reward R decreases. Compared with the cooperative scheme, the simulation results show that the total profit of edge devices has been maximally increased by 59%. Fig. 12 shows the total utility of data owners as function of $p_{\max}$ considering different schemes. We can observe from Fig. 12 that the data owners' total utility decreases linearly as $p_{\max}$ increases. The consensus reward R does not affect the data owners' total utility under the cooperative scheme. Compared

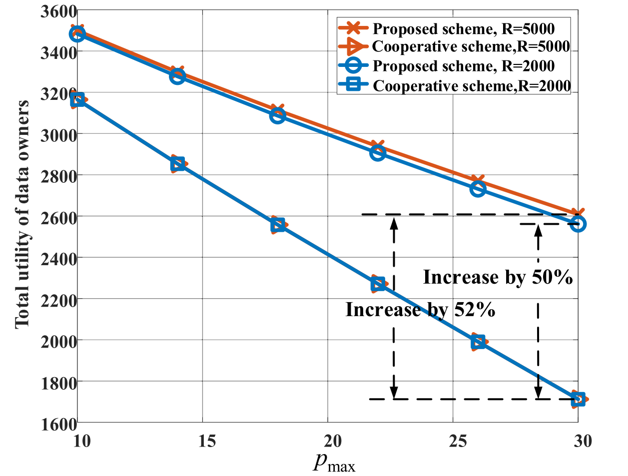

Fig. 12. Total utility of data owners as function of $p_{\max}$ considering different schemes ($N_O = 20$ and $N_D = 3$).

with the cooperative scheme, the total utility of data owners has been maximally increased by 52%. The reason is that under the cooperative scheme, edge devices do not compete with each other and the price is $p_{\max}$, which discourages data owners from sharing data. Then, both the total profit of edge devices and total utility of data owners decrease compared with the proposed scheme.

VIII. Conclusion

In this article, a decentralized data-sharing solution for IIoT networks based on blockchain and edge computing was proposed. With the aid of edge computing, the distributed consensus of blockchain networks and the decentralized storage of shared data are realized at the edge of IIoT networks. A PoST consensus mechanism was proposed, in which edge devices struggle for the consensus reward by contributing to the data sharing in IIoT networks. Based on the manufacture ties of data owners, the shared data request probability was derived. Then, the interactions between data owners and edge devices, including data storage and transmission service interactions, were modeled as a multiple-leader and multiple-follower Stackelberg game problem. Finally, the optimal solutions for both data owners and edge devices were obtained based on the ADMM algorithm. Simulation results show that with the proposed IIoT data-sharing scheme, the total profit of edge devices is maximally increased by 59%, and the total utility of data owners is maximally increased by 52%. In future works, the impact of wireless transmission on blockchain-based IIoT data sharing will be further investigated.

Appendix A
Proof of Proposition 1

First, we prove that the utility function of data owners $U_{O_i}(x_i^s, X_{-i}^s, P)$ is concave. The first derivative of $U_{O_i}(x_i^s, X_{-i}^s, P)$ is

$$\frac{\partial U_{O_i}}{\partial x_{id}^s} = \frac{\varpi_1 w_{id}}{1 + x_{id}^s} + \frac{\varpi_2 w_{id} f_{O_i} T\lambda}{1 + x_{id}^s} - \varpi_3 w_{id}\big(1 + \delta f_{O_i} T\lambda\big) p_{i,d}. \quad (30)$$

The second derivative of $U_{O_i}(x_i^s, X_{-i}^s, P)$ is

$$\frac{\partial^2 U_{O_i}}{\partial {x_{id}^s}^2} = \frac{-\varpi_1 w_{id} - \varpi_2 w_{id} f_{O_i} T\lambda}{\left(1 + x_{id}^s\right)^2} < 0. \tag{31}$$

So $U_{O_i}(x_i^s, X_{-i}^s, P)$ is a convex function.

Appendix B
Proof of Proposition 2

Then, we prove that the profit function of edge devices $U_{D_d}(p_d, P_{-d}, X^s)$ is concave. For $U_{D_d}(p_d, P_{-d}, X^s)$ shown in (16), w_{id} in (16) is expressed as

$$\begin{aligned} w_{id} &= \frac{p_{\max} - p_{i,d}}{\sum_{k=1}^{N_D}\left(p_{\max} - p_{i,k}\right)} \\ &= \frac{p_{\max} - p_{i,d}}{\sum_{k\neq d}^{N_D}\left(p_{\max} - p_{i,k}\right) + \left(p_{\max} - p_{i,d}\right)}. \end{aligned} \tag{32}$$

The first derivative of w_{id} is

$$\frac{\partial w_{id}}{\partial p_{i,d}} = \frac{-\left[\sum_{k\neq d}\left(p_{\max} - p_{i,k}\right)\right]}{\left[\sum_{k\neq d}\left(p_{\max} - p_{i,k}\right) + \left(p_{\max} - p_{i,d}\right)\right]^2} < 0. \tag{33}$$

$$\frac{\partial^2 w_{id}}{\partial p_{i,d}^2} = \frac{-2 \times \left[\sum_{k\neq d}\left(p_{\max} - p_{i,k}\right) + \left(p_{\max} - p_{i,d}\right)\right] \times \left[\sum_{k\neq d}\left(p_{\max} - p_{i,k}\right)\right]}{\left[\sum_{k\neq d}\left(p_{\max} - p_{i,k}\right) + \left(p_{\max} - p_{i,d}\right)\right]^4} < 0 \tag{34}$$

$$\begin{aligned} A_1 &= \frac{\sum_{i=1}^{N_O} w_{id} x_{id}^s\left(1 + f_{O_i} T\lambda\right)}{\sum_{d=1}^{N_D}\sum_{i=1}^{N_O} w_{id} x_{id}^s\left(1 + f_{O_i} T\lambda\right)} \\ &= \frac{w_{id} x_{id}^s\left(1 + f_{O_i} T\lambda\right) + \sum_{m\neq i}^{N_O} w_{md} x_{md}^s\left(1 + f_{O_m} T\lambda\right)}{w_{id} x_{id}^s\left(1 + f_{O_i} T\lambda\right) + \sum_{k\neq d}^{N_D}\sum_{m\neq i}^{N_O} w_{mk} x_{mk}^s\left(1 + f_{O_m} T\lambda\right)} \\ &= \frac{w_{id} x_{id}^s\left(1 + f_{O_i} T\lambda\right) + B_1}{w_{id} x_{id}^s\left(1 + f_{O_i} T\lambda\right) + B_2} \end{aligned} \tag{35}$$

$$\begin{aligned} A_2 &= \sum_{i=1}^{N_o} w_{id}\left[x_{id}^s\left(1 + \delta f_{O_i} T\lambda\right) p_{i,d} - x_{id}^s\left(c_s + f_{O_i} T\lambda c_t\right)\right] \\ &= \sum_{m\neq i}^{N_o} w_{md}\left[x_{md}^s\left(1 + \delta f_{O_m} T\lambda\right) p_{m.d} - x_{md}^s\left(c_s + f_{O_m} T\lambda c_t\right)\right] + w_{id}\left[x_{id}^s\left(1 + \delta f_{O_i} T\lambda\right) p_{i,d} - x_{id}^s\left(c_s + f_{O_i} T\lambda c_t\right)\right] \end{aligned} \tag{36}$$

$$\frac{\partial A_1}{\partial p_{i,d}} = \frac{\frac{\partial w_{id}}{\partial p_{i,d}} x_{id}^s\left(1 + f_{O_i} T\lambda\right)(B_2 - B_1)}{\left[B_2 + w_{id} x_{id}^s\left(1 + f_{O_i} T\lambda\right)\right]^2} \tag{37}$$

$$\frac{\partial^2 A_1}{\partial p_{i,d}^2} = \frac{\begin{array}{c}\frac{\partial^2 w_{id}}{\partial p_{i,d}^2} x_{id}^s\left(1 + f_{O_i} T\lambda\right)(B_2 - B_1)\left[B_2 + w_{id} x_{id}^s\left(1 + f_{O_i} T\lambda\right)\right]^2 \\ -2\left(\frac{\partial w_{id}}{\partial p_{i,d}} x_{id}^s\left(1 + f_{O_i} T\lambda\right)\right)^2\left[B_2 + w_{id} x_{id}^s\left(1 + f_{O_i} T\lambda\right)\right](B_2 - B_1)\end{array}}{\left[B_2 + \sum_{i=1}^{N_O} w_{id} x_{id}^s\left(1 + f_{O_i} T\lambda\right)\right]^4} \tag{38}$$

$$\frac{\partial A_2}{\partial p_{i,d}} = \frac{\partial w_{id}}{\partial p_{i,d}} \times \left[p_{i,d} x_{id}^s\left(1 + \delta f_{O_i} T\lambda\right) - x_{id}^s\left(c_s + f_{O_i} T\lambda c_t\right)\right] + w_{id} x_{id}^s\left(1 + \delta f_{O_i} T\lambda\right) \tag{39}$$

$$\frac{\partial^2 A_2}{\partial p_{i,d}^2} = \frac{\partial^2 w_{id}}{\partial p_{i,d}^2} \times \left[p_{i,d} x_{id}^s\left(1 + \delta f_{O_i} T\lambda\right) - x_{id}^s\left(c_s + f_{O_i} T\lambda c_t\right)\right] + 2\frac{\partial w_{id}}{\partial p_{i,d}} x_{id}^s\left(1 + \delta f_{O_i} T\lambda\right) \tag{40}$$

The second derivative of w_{id} is shown in (34), at the bottom of the previous page. To simplize the analysis of U_{D_d}, we transform the expression of U_{D_d} as $U_{D_d}(p_d, P_{-d}, X^s) = RA_1 + A_2$, and A_1 is shown in (35), at the bottom of the previous page. In (35), $B_1 = \sum_{m\neq i}^{N_O} w_{md}x_{md}^s(1 + f_{O_m}T\lambda)$ and $B_2 = \sum_{k\neq d}^{N_D}\sum_{m\neq i}^{N_O} w_{mk}x_{mk}^s(1 + f_{O_m}T\lambda)$. A_2 is shown in (36), at the bottom of the previous page.

Then, $(\partial A_1/\partial p_{i,d})$ and $(\partial^2 A_1/\partial p_{i,d}^2)$ are derived. $(\partial A_1/\partial p_{i,d})$ is expressed in (37), shown at the bottom of the previous page. $(\partial^2 A_1/\partial p_{i,d}^2)$ is expressed in (38), shown at the bottom of the previous page. Because $(\partial w_{id}/\partial p_{i,d}) < 0$, $(\partial^2 w_{id}/\partial p_{i,d}^2) < 0$, $B_2 - B_1 > 0$, so we can get $(\partial^2 A_1/\partial p_{i,d}^2) < 0$. Finally, $(\partial A_2/\partial p_{i,d})$ and $(\partial^2 A_2/\partial p_{i,d}^2)$ are derived. $(\partial A_2/\partial p_{i,d})$ is expressed in (39), shown at the bottom of the previous page. $(\partial^2 A_2/\partial p_{i,d}^2)$ is expressed in (40), shown at the bottom of the previous page. Because $(\partial^2 A_1/\partial p_{i,d}^2) < 0$ and $(\partial^2 A_2/\partial p_{i,d}^2) < 0$, we can get that $(\partial^2 U_{D_d}/\partial p_{i,d}^2) < 0$, so function $U_{D_d}(p_d, P_{-d}, X^s)$ is concave.

REFERENCES

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

[2] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, pp. 968–979, May 2020.

[3] G. Dartmann, H. Song, and A. Schmeink, *Big Data Analytics for Cyber-Physical Systems: Machine Learning for the Internet of Things*. Amsterdam, The Netherlands: Elsevier, 2019.

[4] F. Liang, W. Yu, D. An, Q. Yang, X. Fu, and W. Zhao, "A survey on big data market: Pricing, trading and protection," *IEEE Access*, vol. 6, pp. 15132–15154, 2018.

[5] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled Internet of Vehicles: Optimizing Consensus management using reputation and contract theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019.

[6] J. Kang, Z. Xiong, D. Niyato, S. Xie, and J. Zhang, "Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10700–10714, Dec. 2019.

[7] R. Li, C. Shen, H. He, X. Gu, Z. Xu, and C.-Z. Xu, "A lightweight secure data sharing scheme for mobile cloud computing," *IEEE Trans. Cloud Comput.*, vol. 6, no. 2, pp. 344–357, Apr./Jun. 2018.

[8] H. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[9] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.

[10] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, "A smart-contract-based access control framework for cloud smart healthcare system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5914–5925, Apr. 2021.

[11] O. Novo, "Scalable access management in IoT using blockchain: A performance evaluation," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4694–4701, Jun. 2019.

[12] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1594–1605, Apr. 2019.

[13] Y. Zhong, G. Mao, X. Ge, and F.-C. Zheng, "Spatio-temporal modeling for massive and sporadic access," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 3, pp. 638–651, Mar. 2021

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

[15] J. Kang *et al.*, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.

[16] 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 Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.

[17] C.-H. Wang, J.-J. Kuo, D.-N. Yang, and W.-T. Chen, "Collaborative social Internet of Things in mobile edge networks," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11473–11491, Dec. 2020.

[18] F. Cicirelli *et al.*, "Edge computing and social Internet of Things for large-scale smart environments development," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2557–2571, Aug. 2018.

[19] R. Girau *et al.*, "Coastal monitoring system based on social Internet of Things platform," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1260–1272, Feb. 2020.

[20] Z. U. Shamszaman and M. I. Ali, "Toward a smart society through semantic virtual-object enabled real-time management framework in the social Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2572–2579, Aug. 2018.

[21] L. Nie *et al.*, "Intrusion detection for secure social Internet of Things based on collaborative edge computing: A generative adversarial network-based approach," *IEEE Trans. Comput. Soc. Syst.*, early access, Mar. 22, 2021, doi: 10.1109/TCSS.2021.3063538.

[22] M. Shen, J. Duan, L. Zhu, J. Zhang, X. Du, and M. Guizani, "Blockchain-based incentives for secure and collaborative data sharing in multiple clouds," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1229–1241, Jun. 2020.

[23] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3516–3526, Jun. 2019.

[24] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019.

[25] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018.

[26] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based E-Health systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019.

[27] J. Sun, X. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records in IPFS," *IEEE Access*, vol. 8, pp. 59389–59401, 2020.

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

[29] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, pp. 398–461, Nov. 2002.

[30] A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in *Proc. 14th ACM Conf. Comput. Commun. Security*, New York, NY, USA, Oct. 2007, pp. 584–597.

[31] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security*. 2008, pp. 90–107.

[32] Y. Jiang, Y. Zhong, and X. Ge, "Smart contract-based data commodity transactions for industrial Internet of Things," *IEEE Access*, vol. 7, pp. 180856–180866, 2019.

[33] C.-H. Zeng and K.-C. Chen, "Social network analysis facilitates cognition in large wireless networks: Clustering coefficient aided geographical routing," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 3, pp. 618–634, Sep. 2018.

[34] Y. Jiang, X. Ge, Y. Zhong, G. Mao, and Y. Li, "A new small-world IoT routing mechanism based on Cayley graphs," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10384–10395, Dec. 2019.

[35] T. D. Tran and L. B. Le, "Resource allocation for multi-tenant network slicing: A multi-leader multi-follower Stackelberg game approach," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8886–8899, Aug. 2020.

[36] L. Duan, J. Huang, and B. Shou, "Duopoly competition in dynamic spectrum leasing and pricing," *IEEE Trans. Mobile Comput.*, vol. 11, no. 11, pp. 1706–1719, Nov. 2012.

[37] 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 Trans. Services Comput.*, vol. 13, no. 2, pp. 356–367, 1 Mar./Apr. 2020.

[38] J. Nie, J. Luo, Z. Xiong, D. Niyato, P. Wang, and H. V. Poor, "A multi-leader multi-follower game-based analysis for incentive mechanisms in socially-aware mobile crowdsensing," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1457–1471, Mar. 2021.

[39] J. Giesen and S. Laue, "Combining ADMM and the augmented Lagrangian method for efficiently handling many constraints," in *Proc. 28th Int. Joint Conf. Artif. Intell. (IJCAI)*, 2019, pp. 4525–4531.

[40] J. Giesen and S. Laue, "Distributed convex optimization with many convex constraints," 2016. [Online]. Available: arXiv:1610.02967.

[41] N. Raveendran, H. Zhang, Z. Zheng, L. Song and Z. Han, "Large-scale fog computing optimization using equilibrium problem with equilibrium constraints," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Singapore, 2017, pp. 1–6.

[42] Z. Zheng, L. Song, Z. Han, G. Y. Li, and H. V. Poor, "A Stackelberg game approach to proactive caching in large-scale mobile edge networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 8, pp. 5198–5211, Aug. 2018.

[43] Z. Xiong, J. Zhao, D. Niyato, R. Deng, and J. Zhang, "Reward optimization for content providers with mobile data subsidization: A hierarchical game approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 4, pp. 2363–2377, Oct.–Dec. 2020.

[44] P. K. Bishoyi and S. Misra, "Enabling green mobile edge computing for 5G-based healthcare applications," *IEEE Trans. Green Commun. Netw.*, early access, Apr. 26, 2021, doi: 10.1109/TGCN.2021.3075903.

[45] M. E. J. Newman and D. J. Watts, "Renormalization group analysis of the small-world network model," *Phys. Lett. A*, vol. 263, pp. 341–346, Dec. 1999.

[46] H. Inaltekin, M. Chiang, and H. V. Poor, "Average message delivery time for small-world networks in the continuum limit," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4447–4470, Sep. 2010.

Yuna Jiang (Graduate Student Member, IEEE) received the B.E. degree in communications engineering from the China University of Mining and Technology, Xuzhou, China, in 2017. She is currently pursuing the Ph.D. degree with the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan, China.

Her research interests are Internet of Things and blockchain.

Yi Zhong (Member, IEEE) received the B.S. and Ph.D. degrees in electronic engineering from the University of Science and Technology of China, Hefei, China, in 2010 and 2015, respectively.

From August 2012 to December 2012, he was a visiting student with the Prof. Martin Haenggi's Group, University of Notre Dame, Notre Dame, IN, USA. From July to October 2013, he was a research intern of Corporate Research and Development with Qualcomm Incorporated, Beijing, China. From July 2015 to December 2016, he was a Postdoctoral Research Fellow with the Wireless Networks and Decision Systems Group, Singapore University of Technology and Design, Singapore, led by Prof. Tony Q. S. Quek. He is currently an Assistant Professor with the School of Electronic Information and Communications, Huazhong University of Science and Technology, Wuhan, China. His main research interests include heterogeneous and femtocell-overlaid cellular networks, wireless *ad hoc* networks, stochastic geometry, and point process theory.

Xiaohu Ge (Senior Member, IEEE) received the Ph.D. degree in communication and information engineering from the Huazhong University of Science and Technology (HUST), Wuhan, China, in 2003.

He is currently a Full Professor with the School of Electronic Information and Communications, HUST. He is an Adjunct Professor with the Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW, Australia. He has been worked with HUST, since November 2005. Prior to that, he worked as a Researcher with Ajou University, Suwon, South Korea, and the Politecnico Di Torino, Turin, Italy, from January 2004 to October 2005. He has published more than 200 papers in refereed journals and conference proceedings and has been granted about 50 patents in China. His research interests are in the area of mobile communications, traffic modeling in wireless networks, green communications, and interference modeling in wireless communications.

Prof. Ge received the Best Paper Awards from IEEE Globecom 2010. He serves as an Associate Editor for IEEE WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and IEEE ACCESS. He served as the General Chair for the 2015 IEEE International Conference on Green Computing and Communications (IEEE GreenCom 2015). He served as the China Representative for international federation for information processing.