An Online Multi-Item Auction With Differential Privacy in Edge-Assisted Blockchains

Jianxiong Guo, Member, IEEE, Weili Wu, Senior Member, IEEE, Tian Wang, and Weijia Jia, Fellow, IEEE

Abstract—In recent years, the blockchain-based Internet of Things (IoT) has been widely studied and applied, and every IoT device can act as a node in the blockchain. However, these lightweight nodes usually do not have enough computing power to complete the consensus or other computing-required tasks. Edge computing network gives a platform to provide computing power to IoT devices. A fundamental problem is how to allocate limited edge servers to IoT devices in a highly untrusted environment. In a fair competitive environment, the allocation mechanism should be online, truthful, and privacy-preserved. In order to meet these three challenges, we propose an online multi-item double auction (MIDA) mechanism by means of auction theory, where IoT devices are buyers and edge servers are sellers. However, ensuring truthfulness is often contradictory to protecting users’ privacy. The participants’ private information is at risk of being exposed to inference attacks, which may lead to malicious manipulation of the market by adversaries. Thus, we enhance our MIDA mechanism with differential privacy (DP) to protect sensitive information from being leaked. It slightly interferes with the auction results in performance but guarantees privacy protection with high confidence. In addition, we upgrade our privacy-preserved MIDA mechanism such that it adapts to more complex and realistic scenarios. In the end, the effectiveness and correctness of algorithms are evaluated and verified by theoretical analysis and numerical simulations.

Index Terms—Blockchain, differential privacy (DP), inference attack, Internet of Things (IoT), online double auction, truthfulness.

I. INTRODUCTION

I N T HE last ten years, Internet of Things (IoT) gradually become a familiar concept, that involves connecting everyday physical objects, devices, and systems to the Internet, allowing them to collect and exchange data. These interconnected devices are embedded with sensors, software, and network connectivity, enabling them to interact with each other and the digital world. IoT has gained widespread adoption across various industries and applications due to its potential to enhance efficiency, productivity, and convenience, such as autonomous vehicles [1], remote healthcare [2], industrial automation [3], financial trading [4], and smart grids [5]. They require seamless and instant data processing and communication to function effectively and ensure safety, efficiency, and accuracy in their respective domains. However, the traditional architecture based on cloud computing cannot meet the needs of modern IoT applications, especially those that require high security and low latency. It faces the risk of a single point of failure, network congestion, waste of energy, privacy protection, and so on.

With the rapid development of 5G communication and edge computing, they complement each other, creating a powerful combination for applications that require low latency, high reliability, and real-time processing [6]. Together, they are driving innovations in real-time IoT-based applications with the potential to reshape industries. At the same time, the emergence of blockchain technology [7] helps avoid single points of failure and improves security with its decentralized nature. Therefore, an integrated environment of edge computing, blockchain, and IoT will ultimately lead us to next-generation IoT systems. Blockchain [7] is a public and decentralized database that is used to store real-time data generated by all valid participants in the system without a third-party platform. Because they do not trust each other, each newly generated data should be verified in a distributed manner before being added into a block, and then each newly generated block should be validated as well by the consensus process before being added into the blockchain in a permanent and tamper-resistant manner. At the same time, some cryptographic methods can guarantee the integrity of blocks in the blockchain, such as asymmetric encryption algorithms and digital signatures [8]. Moreover, each piece of data in the blockchain is traceable to all valid participants because of its chain-based structure. The security and reliability of blockchain-based systems are from their consensus mechanisms. Taking Proof of Work (PoW) [7, 9] as an example, each participant is required to solve a hash puzzle when competing with others to generate a new block, which is very computing-intensive and time-consuming.

An IoT system consists of many lightweight IoT devices, and it is difficult for the devices to participate in the consensus...
process due to a lack of sufficient computing power. Thus, such an IoT system is not enough to build a blockchain alone. Although we consider PoW in this article, it does not affect the generalization of our proposed model and algorithm because other consensus mechanisms also consume more or less computational resources. By integrating edge computing [10], edge servers at the network edge can provide computing power to their neighboring IoT devices, which is helpful for building a fully functional IoT system [11], [12], [13], [14], [15].

A reward mechanism in a blockchain system is a fundamental component designed to incentivize network participants to contribute their resources and efforts to the network’s operation and security. For example, mining rewards in PoW-based blockchain networks. Due to the reward, IoT devices are possible to be willing to consume computing power to compete with others. In addition, each IoT device may have its own specific computing tasks based on its applications. For example, they need to train their deep learning model according to real-time monitoring data. Whether participating in consensus or completing computing tasks, the lightweight IoT device has the expectation of obtaining enough computing power, thus buying computing power from nearby edge servers has become a feasible and effective solution. Now, the fundamental problem in this article, how to allocate limited edge servers to IoT devices in such an edge-assisted blockchain-based system is formulated. However, there are several challenges that are not concerned with existing mechanism designs [11], [12], [13], [14], [15]. In order to ensure the fairness and security of trading between IoT devices and edge servers, the allocation mechanism should be online, truthful, and privacy-preserved. To achieve it, we not only put forward a new allocation model but also our designs are based on addressing these three issues.

Because the consensus process in a blockchain system is executed round by round and edge servers run in a dynamic environment, the allocation mechanism must be online, which is executed round by round according to the real-time status of IoT devices and edge servers. However, in each round, the states of IoT devices and edge servers are changing. Besides, truthfulness is a very important property to design an incentive or allocation mechanism, which can prevent malicious users from manipulating the trading market by offering a misleading bid. The assurance of truthfulness not only ensures the fairness of trading but also ensures the security of the blockchain system by providing a reasonable resource allocation. Based on these two aspects, we propose an online seal-bid multi-item double auction (MIDA) mechanism to achieve resource allocation between IoT devices and edge servers. In the system, IoT devices are buyers and edge servers are sellers. The MIDA mechanism can give us a one-to-one mapping between IoT devices and edge servers, which is used as a special case to conduct theoretical analysis. We show that it is individually rational, budget balanced, computationally efficient, and truthful. Subsequently, we upgrade the MIDA to MIDA-General (MIDA-G) mechanism, establishing a many-to-one mapping between IoT devices and edge servers, which is more realistic.

In such an auction scenario, it exists a possible risk of privacy leakage in the multiple rounds of truthful bids given by buyers (truthful asks given by sellers), where the bids (asks) are the private information of buyers (sellers). As we know, the auction results could be altered by the change in a single bid (ask) [16], [17]. Thus, our MIDA mechanism is vulnerable to inference attack [18], [19], where adversaries could infer bids (asks) of other buyers (sellers) by comparing the auction results of multiple rounds. Thus, the adversary can make the auction result beneficial to itself by manipulating its own bid or ask. The differential privacy (DP) [20] is a promising technology to prevent the adversary from inferring other truthful bids or asks through the public auction results. Commonly used schemes of achieving DP with theoretical guarantee include the exponential mechanism and Laplace mechanism. Thus, another important part of this article is to design a scheme with differential private protection for our MIDA and MIDA-G mechanisms so as to achieve thorough privacy protection. Finally, the contribution of this article can be summarized as follows.

1) To achieve the decentralization and security guarantee, we introduce an edge-assisted blockchain-based IoT system and formulate it as a combinatorial optimization problem according to double auction theory.

2) We propose an online MIDA and MIDA-G mechanism to model the allocation of computing power between IoT devices and edge servers. By theoretical analysis, we show that our proposed mechanism is individually rational, budget balanced, computationally efficient, and truthful.

3) Considering the potential risk of privacy leakage because of inference attack, we enhance the MIDA and MIDA-G mechanisms with DP based on the Laplace mechanism, denoted by multi-item double auction with differential privacy (MIDA-DP) and MIDA-G-DP. They can effectively ensure privacy protection without affecting truthfulness.

4) We conduct intensive simulations to verify the feasibility and effectiveness of our proposed mechanisms. Simulation results show that our algorithms can achieve the design rationales, especially in privacy protection.

Organizations: In Section II, we discuss state-of-the-art work. In Section III, we introduce the system model and define our problem formally. In Section IV, we present our MIDA mechanism and theoretical analysis elaborately. In Section V, we achieve the differential private strategy for our MIDA mechanism. Then, the more general MIDA-G mechanism is shown in Section VI. Finally, we evaluate our algorithms by numerical simulations in Section VII and show the conclusions in Section VIII.

II. RELATED WORK

With the increasing development of blockchains, research on blockchain-based IoT systems has attracted more and more attention. They exploited the decentralization of blockchain to achieve security, interoperability, privacy, and traceability [21], [22]. For the resource allocation between IoT devices and edge servers, we summarize several classic articles here. Yao et al. [12] studied the resource management and pricing problem between miners and cloud servers by the Stackelberg game. Chang et al. [13] investigated how to encourage miners to purchase computing resources from edge
service providers and find the optimal solution through a two-stage Stackelberg game. Ding et al. [14], [15] attempted to build a secure blockchain-based IoT system by attracting more IoT devices to purchase computing power from edge servers and participate in the consensus process, where they adopted a multileader–multifollower Stackelberg game. Besides, some recent work has adopted reinforcement learning (RL) algorithms. Wang et al. [23] proposed a blockchain-enabled resource orchestration scheme for IoT by deep RL. Zhang et al. [24] designed a blockchain-empowered federated deep RL algorithm to address the secure and low-latency computation offloading problem in cloud–edge–end collaboration. However, truthfulness cannot be guaranteed by both Stackelberg game and RL method, which makes it hard to ensure fairness. Especially for RL-based algorithms, its convergence and robustness are poor, which makes it difficult to land.

Auction theory has been considered a feasible solution in many different systems, such as mobile crowdsensing [25], [26], mobile cloud/edge computing [27], [28], and energy trading [29], [30]. Here, we only focus on the MIDA. Yang et al. [31] studied a cooperative communication scene by proposing a double auction mechanism, where they first got a mapping from buyer to seller through assignment algorithms and then used McAfree auction [32] to determine winners and clearing prices. Jin et al. [27], [28] considered a resource allocation problem by designing a truthful double auction mechanism for the resource trading between users and cloudlet, but it is only one-to-one mapping. Guo et al. [33] proposed a secure and efficient charging scheduling system based on DAG-blockchain and double auction mechanism. However, these existing auction-based algorithms cannot be directly migrated to solve our problem because of online execution, double sides, multi-item, and resource-constrained edge servers.

In a fair auction platform, the auction results have to be public, which leads to the sensitive information of participants being at risk of being exposed. The theories and applications of privacy protection were investigated in [34] and [35]. Dwork [20] first put forward the concept of DP, and then it can be applied to double auction mechanisms for protecting players’ privacy. Chen et al. [17] combined the DP with a double spectrum auction design in order to maximize social welfare approximately. Li et al. [36] proposed an online double auction scheme that combined with DP to build a secure market among electric vehicles. Besides, a variety of schemes based on DP have been used to design double auction systems in [37], [38], and [39]. However, because our proposed auction model is different from the previous ones, how to integrate DP to achieve privacy protection has become a new problem. Thus, we need to redesign according to the structure of our own algorithm. Actually, our scheme with DP is more simple and more effective than the above works.

III. MODELS AND PRELIMINARIES

In this section, we introduce the basic model of an edge-assisted blockchain-based IoT system. Then, we show the definition of adversary attacks and the formulation of double auction and DP.

A. System Model

Fig. 1 illustrates the basic usage scenario that we consider in this article. A typical instance of the blockchain-based IoT system is a network composed of many lightweight IoT devices that are used to perform some tasks such as environmental monitoring, where each IoT device can be considered as a node in the blockchain system. We assume that this blockchain system adopts a PoW consensus mechanism. Stimulated by the reward from participating in the consensus process of the blockchain system, part of IoT devices would like to be miners. Then, they would compete with other miners for the right to generate the next block by solving a hash puzzle, which has been adopted widely in the Bitcoin system [7]. The block in the blockchain system consists of transactions stored in a Merkle tree structure and a block header that contains the hash value of its previous block. In the PoW consensus mechanism, the mining process is executed by miners to find a nonce such that

$$\text{Hash(Transactions, Header, Nonce)} \leq D$$

where $D$ is a 256-bit binary number assigned by the platform to control the rate of block generation.

However, such a blockchain is limited by its high requirement for computing power because its consensus mechanism is based on solving a hash puzzle, thereby it cannot be applied to lightweight IoT devices with limited power directly. At this time, these IoT devices will attempt to purchase computing power from one or more edge servers around them and offload their mining tasks to their assigned edge servers. The number of edge servers is limited and each IoT device may only offload its tasks to a few edge servers nearby. Thus, a natural question is how to allocate limited edge servers to IoT devices.

B. Problem Formulation

As shown in Fig. 1, the dashed lines that connect an IoT device to several edge servers indicate the mining task of this
device can only be offloaded to one of the edge servers that it connects to because of space limitation and bandwidth limitations. Therefore, we propose an online sealed-bid MIDA mechanism to model the competition among IoT devices in the blockchain system and edge servers. There are three kinds of players involved in such an auction: 1) auctioneer; 2) buyers; and 3) sellers. In the system, the centralized cloud server acts as the auctioneer, IoT devices that plan to purchase computing power act as buyers, and edge servers that can provide computing power act as sellers. The transactions between IoT devices and edge servers are established on the wireless infrastructure, which is the reason why the tasks of an IoT device may only be assigned to a finite number of edge servers near it. Otherwise, the communication overhead will increase dramatically. Nevertheless, each IoT device has different preferences for different edge servers in line with the quality of service they provide, such as geographical locations, response speeds, credit scores, and other factors. This causes an IoT device to have different valuations for different edge servers in our model.

In the system, we denote by the set of IoT devices (buyers) \( D = \{d_1, d_2, \ldots, d_n\} \) who pay for purchase computing power and the set of edge servers (sellers) \( S = \{s_1, s_2, \ldots, s_m\} \) who get a reward for providing computing power. It formulates a bipartite graph \( G = (D, S, E) \) like Fig. 1, where \( \{d_i, s_j\} \in E \) if IoT device \( d_i \) can be assigned to edge server \( s_j \). As we know, the PoW consensus mechanism is executed round by round, where each round happens in a time slot. We consider a time interval \( I \), which can be discretized into time slots as \( I = \{1, 2, \ldots, T\} \). In each slot \( t \in I \), a round of consensus will be carried out, in other words, a round of auction will be carried out. Let us consider a special case first in which each edge server can serve at most one IoT device in a slot. Therefore, for each slot \( t \in I \), it is similar to finding a maximum weight matching in the bipartite graph \( G \) according to the bids of buyers and asks of sellers.

In a time slot \( t \in I \), we define the notations in our auction as follows. For each buyer \( d_i \in D \), its bid can be given by \( b_i^t = (t_i^t, r_i^t) \). Here, \( t_i^t = (t_i^{t,1}, t_i^{t,2}, \ldots, t_i^{t,m}) \) is its bid vector, where \( t_i^{t,j} \in b_i^t \) (\( b_i^t \in [b_{\text{min}}, b_{\text{max}}] \)) is the unit bid (maximum buying price) per unit computing power of purchasing from the seller \( s_j \in S \) and \( r_i^t \) is the amount of computing power it needs to buy. According to our scenario, we have \( b_i^{t,j} = 0 \) if \( \{d_i, s_j\} \notin E \). For each seller \( s_j \in S \), its ask information can be given by \( A_j = (a_j, q_j) \). Here, \( a_j \in [a_{\text{min}}, a_{\text{max}}] \) is the unit ask (minimum selling price) per unit computing power and \( q_j \) is the maximum amount of computing power it can provide. Based on the above definitions, a buyer gives different unit bids to different sellers, but a seller gives the same ask to different buyers since it only cares about the payment charged from buyers. The bid information of buyers and ask information of sellers are submitted to the auctioneer, thereby our auction can be defined on \( \Omega^t = (\{b_i^t\}_{d_i \in D}, \{A_j\}_{s_j \in S}) \).

Given the \( \Omega^t \) in the slot \( t \), the auctioneer not only determines a winning buyer set \( D^t_w \subseteq D \) and a winning seller set \( S^t_w \subseteq S \), but also determines a bijective function \( \sigma^t \) mapping from \( D^t_w \) to \( S^t_w \), where \( \sigma^t(d_i) = s_j \) implies the computing task of IoT device \( d_i \in D^t_w \) is offloaded to edge server \( s_j \in S^t_w \). In the auction, we can say “IoT device \( d_i \) is assigned to edge server \( s_j \)”.

We define the unit price \( p_i^t \) charged to buyer \( d_i \in D^t_w \) and the unit payment \( \bar{p}_j^t \) rewarded to seller \( s_j \in S^t_w \). Besides, the valuation vector of each buyer \( d_i \in D \) is \( v_i^t = (v_i^{t,1}, v_i^{t,2}, \ldots, v_i^{t,m}) \), where \( v_i^{t,j} \in v_i^t \) is the unit valuation per unit computing power of purchasing from the seller \( s_j \in S \) and the unit cost per computing power of each seller \( s_j \in S \) is \( c_j^t \). According to the valuation vectors of buyers and costs of sellers, the utility \( \tilde{u}_i^t \) of buyer \( d_i \in D \) and utility \( \tilde{u}_j^t \) of seller \( s_j \in S \) can be defined. For each winning buyer \( d_i \in D^t_w \) and winning seller \( s_j \in S^t_w \), we have

\[
\tilde{u}_i^t = \left( v_i^{t,\sigma^t(d_i)} - \bar{p}_i^t \right) \cdot r_i^t 
\]

\[
\tilde{u}_j^t = \left( \bar{p}_j^t - c_j^t \right) \cdot r_{\sigma^t^{-1}(s_j)}^t
\]

where \( \sigma^{-1}(s_j) = d_i \) means that \( \sigma(d_i) = s_j \). Otherwise, we have \( \tilde{u}_i^t = 0 \) for each losing buyer \( d_i \in D \setminus D^t_w \) and \( \tilde{u}_j^t = 0 \) for each losing seller \( s_j \in S \setminus S^t_w \). The utilities are characterized by the difference between charge (reward) and valuation (cost), which reflects their satisfaction with the current auction result.

For convenience, the allocation result determined by the auctioneer in the slot \( t \) can be denoted by a matrix \( X_t = \{x_{i,j}\}_{d_i \in D, s_j \in S} \), where we have

\[
x_{i,j} = \begin{cases} 1, & \text{if buyer } d_i \text{ is assigned to seller } s_j \\ 0, & \text{otherwise} \end{cases} 
\]

where \( x_{i,j} \) indicates whether the buyer \( d_i \) is assigned to the seller \( s_j \) in the slot \( t \).

In the slot \( t \), the social welfare maximization (SWM) problem is formulated

\[
\max \sum_{d_i \in D} \sum_{s_j \in S} x_{i,j} \cdot r_i^t \cdot \left( b_i^{t,j} - a_j^t \right)
\]

s. t. \( \sum_{d_i \in D} x_{i,j} \leq 1 \quad \forall s_j \in S \) \hspace{1cm} (5a)

\( \sum_{s_j \in S} x_{i,j} \leq 1 \quad \forall d_i \in D \) \hspace{1cm} (5b)

\( \sum_{d_i \in D} r_i^t \cdot x_{i,j} \leq q_j^t \quad \forall s_j \in S \) \hspace{1cm} (5c)

\( \sum_{d_i \in D} r_i^t \cdot x_{i,j} \leq \theta(D, S) \quad \forall d_i \in D \) \hspace{1cm} (5d)

\( x_{i,j} = 0 \quad \forall \{d_i, s_j\} \notin E \) \hspace{1cm} (5e)

\( x_{i,j} \in \{0, 1\} \quad \forall d_i \in D \quad \forall s_j \in S \) \hspace{1cm} (5f)

As shown in (5), the SWM problem illustrates all the constraints we give in our online double auction mechanism. Equations (5a) and (5b) express the bijection relationship between winning buyer set \( D^t_w \) and winning seller set \( S^t_w \); Equation (5c) implies the amount of computing power that \( d_i \) buy from \( s_j \) must be less than the amount of computing power that \( s_j \) can provide if buyer \( d_i \) is assigned to seller \( s_j \); Equation (5d) shows that the total computing resource that buyer \( d_i \) purchases in the time interval \( I \) cannot exceed a threshold \( \theta(D, S) \), which depends on the number of IoT devices.
devices and edge servers in the system. It aims to prevent an IoT device from owning too much computing power to undermine the security of the blockchain system; and Equations (5e) and (5f) mean that an IoT device can only be assigned to its permitted edge servers. Actually, maximizing social welfare is just an idealized situation, and we usually need to sacrifice part of social welfare to ensure the truthfulness of the auction mechanism.

C. Potential Information Leakage

For a justifiable auction platform, the auctioneer should announce the auction result in each slot $t$. The auction result refers to $X^t$ (including $D^t_w$, $S^t_w$, and $\sigma^t$), the amount of computing power $\{r^t_i\}_{i \in D^t_w}$ and $\{q^t_i\}_{i \in S^t_w}$, and clearing unit price $\{\hat{p}^t_i\}_{i \in D^t_w}$ and $\{\hat{p}^t_i\}_{i \in S^t_w}$ to all players so as to make sure the fairness and verifiability of this auction. The reason to publish the amount of computing power is to let other players check (5c) and (5d). Through this, the players avoid being cheated by the auctioneer because it cannot fabricate auction results for benefit. However, adversaries can use these public auction results to infer other players’ private information and lead to privacy leakage.

In our proposed auction mechanism, private information contains the unit bids of buyers $\{b^t_i\}_{i \in D^t_w}$ and unit asks of sellers $\{a^t_i\}_{i \in S^t_w}$. Even though adversaries cannot get in touch with other players’ private information, they can make inferences from these known auction results, which is called inference attack [18], [19]. Thus, we consider two kinds of privacy preservation (inference attack) in our mechanism design: 1) the adversary (some seller) infers the unit asks of other sellers and 2) the adversary (some buyer) infers the unit bids of other buyers. This is because of the competitive relationship among buyers (or sellers). The inference attack will not only lead to the privacy leakage of players but also make the auction unfair. We assume that all players have known how the auction operates in the beginning. By inferring other players’ bids or asks, the adversary can change its strategy to increase its benefit strategically. Therefore, protecting privacy is a challenge that we must face in mechanism design.

IV. ONLINE DOUBLE AUCTION DESIGN

In this section, we introduce several design rationales, a truthful double auction mechanism, and an example to explain the reason why private information is leaked.

A. Design Rationales

The online double auction in the time slot $t \in I$ has been defined as $\Omega^t$. A desired double auction mechanism should satisfy individual rationality, budget balance, computational efficiency, and truthfulness.

Definition 1 (Individual Rationality): The utility for each buyer should be larger than or equal to zero. In our auction $\Omega^t$, we have $\hat{u}^t_i(\Omega^t) \geq 0$ for each buyer $d_i \in D^t_w$ and $\hat{u}^t_j(\Omega^t) \geq 0$ for each seller $s_j \in S^t_w$.

Definition 2 (Budget Balance): The auctioneer should be profitable to operate this auction. Thus, we have

\[
\sum_{d_i \in D^t_w} \hat{p}^t_i \cdot r^t_i - \sum_{s_j \in S^t_w} \hat{p}^t_j \sum_{r^t_k \in S^t_w} r^t_k \cdot x^t_{i,j} \geq 0. \tag{6}
\]

Definition 3 (Computational Efficiency): The auction results defined in Section III-C can be obtained in polynomial time by the auction mechanism.

Definition 4 (Truthfulness): Every buyer (seller) bids (asks) truthfully is one of its dominant strategies, which maximizes its utility definitely. Thus, we have $\hat{u}^t_i((w^t_i, r^t_i), \Omega^t_i) \geq \hat{u}^t_i((b^t_i, r^t_i), \Omega^t_i)$ for each buyer $d_i \in D^t_w$ and $\hat{u}^t_j((l^t_j, q^t_j), \Omega^t_j) \geq \hat{u}^t_j((a^t_j, q^t_j), \Omega^t_j)$ for each seller $s_j \in S^t_w$, where $\Omega^t_i$ is the strategy collection of players except buyer $d_i$ (seller $s_j$). If an auction is truthful, there is no buyer improving its utility by giving a bid vector different from its valuation vector and no seller improving its utility by giving an ask different from its cost.

When we consider the truthfulness, we suppose that the amount of computing power $r^t_i$ (or $q^t_j$) submitted by the buyer (seller) is authentic and public since it can be monitored and must be executed once assigned. Because of the truthfulness, no player has the motivation to change its strategy for obtaining more benefits, which makes the strategic decision of players easier and guarantees a fair competitive environment.

B. Algorithm Design

Here, we propose an MIDA mechanism that attempts to maximize the social welfare but ensure the truthfulness. It is shown in Algorithm 1, which consists of two parts, winning candidate determination (MIDA-WCD) shown in Algorithm 2 and assignment and pricing (MIDA-AP) shown in Algorithm 3.

As shown in Algorithm 2, we construct a set of buyer–seller pairs $D^t_w$ first where each pair $d^t_{k,l} \in D^t_w$ if

\[
d_k \in D^t_w, s_j \in S^t_w, \{d_k, s_j\} \in E, b^t_{k,l} > 0, r^t_k \leq q^t_l \tag{7}
\]

\[
\sum_{r^t_k \in S^t_w} r^t_k \cdot x^t_{k,l} + r^t_k \leq \theta(D, S). \tag{8}
\]

It can be denoted by $D^t_w = \{d^t_{k,l} : d^t_{k,l} \text{ satisfies (7) and (8)}\}$, which means that the buyer $d_k$ is feasible to be assigned to the seller $s_j$ in the slot $t$. Then, we sort the sellers based on their asks in ascending order and select the median $d^t_{k,l}$ as a threshold to balance the number of winning buyer candidates and winning seller candidates. For each pair $d^t_{k,l} \in D^t_w$, it will be a winning buyer candidate if its bid $b^t_{k,l}$ is not less than $a^t_{l}$ and the ask of its corresponding seller $d^t_{k,l}$ is less than $d^t_{l}$. At the same time, seller $s_j$ will be a winning seller candidate if there is at least one winning buyer candidate $d^t_{k,l} \in D^t_w$ existing that bids for it.
Algorithm 2 MIDA-WCD (Ω′)

Input: Ω′ = {⟨Bj⟩i∈D: {Aj}j∈S}
Output: D′c, S′c, a′jo
1: D′c ← \emptyset, S′c ← \emptyset
2: Construct a set D′c = {d′c,k : d′c,k satisfies (7) (8)}
3: Sort the sellers such that S′c = \langle s′c,1, s′c,2, ..., s′c,m \rangle where \begin{align*} &d′c,1 \leq d′c,2 \leq \cdots \leq d′c,m \end{align*}
4: Find the median ask a′jo of S′c, \phi = \left\lceil \frac{m+1}{2} \right\rceil
5: for each d′c,k ∈ D′c do
6: if b′c,k ≥ a′jo and a′jo < d′c,k then
7: D′c ← D′c ∪ {d′c,k}
8: if s′c ⫅ S′c then
9: S′c ← S′c ∪ \{s′c\}
10: end if
11: end if
12: end for
13: return (D′c, S′c, a′jo)

Algorithm 3 MIDA-AP (Ω′, D′c, S′c, d′jo)

Input: Ω′, D′c, S′c, a′jo
Output: D′w, S′w, σ′, Pt′w, Pt′w
1: D′w ← \emptyset, S′w ← \emptyset, Pt′w ← \emptyset, Pt′w ← \emptyset
2: Create a sorted list Q′w = \langle d′w,k : d′w,k ∈ D′c \rangle for each s′j ∈ S′c such that b′w,k1 ⋅ r′k1 ≥ b′w,k2 ⋅ r′k2 ≥ \cdots
3: for each s′j ∈ S′c do
4: d′w,k1 ← Q′w[1] // The first price in Q′w
5: if d′w,k1 ∉ D′w then
6: D′w ← D′w ∪ \{d′w,k1\}
7: end if
8: if |Q′w| = 1 then
9: \begin{align*} &\tilde{p}_{k1} = a′jo \end{align*}
10: end if
11: else
12: \begin{align*} &\tilde{p}_{k1} = \max(a′jo, b′w,k1 ⋅ (r′k2/r′k1)) \end{align*}
13: end if
14: end for
15: for each d′j,k ∈ D′w do
16: H′k = \{ s′j : s′j ∈ S′c, Q′w[1] = d′w,k1 \}
17: Find s′j = arg max s′j∈H′k \{(b′j,k1 − \tilde{p}_{k1}) ⋅ r′k1\}
18: σ′(d′j,k) = s′j
19: S′w ← S′w ∪ \{s′j\}
20: \begin{align*} &\tilde{p}_{k} = \tilde{p}_{k,1}, \tilde{p}_{w} \leftarrow a′jo \end{align*}
21: \begin{align*} &\tilde{p}_{w} ← \tilde{p}_{w} \cup (\tilde{p}_{k}, \tilde{p}_{w} ← \tilde{p}_{w} \cup (\tilde{p}_{k}w) \end{align*}
22: end for
23: return (D′w, S′w, σ′, Pt′w, Pt′w)

As shown in Algorithm 3, we create a sorted list Q′w for each winning seller candidate s′j ∈ S′c that contains all winning buyer candidates {d′j,k : d′j,k ∈ D′c} bidding for it and is sorted according to the total bid a′jo ⋅ r′k. The total bid equals the unit bid multiplied by the amount of computing power. From lines 3 to 14 in Algorithm 3, it determines the target (buyer) of providing service for each winning seller candidate and the corresponding unit price charged to the target. For each sj ∈ S′c, its target is buyer dk1 where the d′k1 is the first part in Q′w and \tilde{p}_{k1} is the unit price charged to buyer dk1 if the dk1 will be assigned to sj next. From lines 15 to 22 in Algorithm 3, for each winning buyer dk ∈ D′c, it is assigned to the seller sj that can obtain its maximum utility, thus we have b′k,1 − \tilde{p}_{k1} ≥ b′k,1 − \tilde{p}_{k1} for each sj ∈ H′k. Then, sj is selected as a winning buyer, and we have \tilde{p}_{k} = \tilde{p}_{k,1} as well as \tilde{p}_{w} = a′jo.

C. Theoretical Analysis of MIDA

Next, we validate that our MIDA as shown in Algorithm 1 satisfies the above four design rationales.

Lemma 1: The MIDA is individually rational.

Proof: For each winning buyer dk ∈ D′c, the unit price \tilde{p}_{k} charged to it is either a′jo or b′k,σ(k) ⋅ (r′k2/r′k1), where we have d′k,σ(k) = Q′w[1]. We have known that b′k,σ(k) ≥ a′jo or b′k,σ(k) ⋅ r′k1 ≥ b′k,σ(k) ⋅ r′k2 since k = Q′w[1]. Thus, we have b′k,σ(k) ≥ \tilde{p}_{k} and \tilde{u}_{k}(Ω′) ≥ 0. For each winning seller sj ∈ S′c, we have \tilde{p}_{j} = a′jo > a′jo and \tilde{u}_{j}(Ω′) ≥ 0. Thus, the MIDA is individually rational since both buyers and sellers are individually rational.

Lemma 2: The MIDA is budget balanced.

Proof: This is a bijection by the winning buyer set \tilde{D}_{w} and the winning seller set S_{w}. Thus, (6) can be written as
\begin{align*} \sum_{s′j ∈ S′w} \left( \tilde{p}_{k} - \tilde{p}_{w,σ(k)} \right) ⋅ r′k &\geq 0 \end{align*}

since we have \tilde{p}_{k} ≥ a′jo and \tilde{p}_{w,σ(k)} < a′jo according to Lemma 1. Thus, the MIDA is budget balanced.

Lemma 3: The MIDA is computationally efficient.

Proof: Let us look at Algorithm 2 first. Sorting the sellers takes O(m log(m)) time and there are at most |E| pairs in D_{w}. From this, the running time of Algorithm 2 is bounded by O(m log(m) + |E|). Then, let us look at Algorithm 3, it takes at most O(φ ⋅ n log(n)) time to construct the Q′w for each seller candidate sj ∈ S′c. Other steps in Algorithm 3 can be complete by a constant time. The running time of Algorithm 3 is bounded by O(φ ⋅ n log(n)). Therefore, it is obvious that the MIDA can be completed in polynomial time, which is computationally efficient.

Lemma 4: The MIDA is truthful.

Proof: For each buyer dk ∈ D, we need to judge whether \tilde{u}_{w}'(v_{k}, r_{k}, Ω_{k}) ≥ \tilde{u}_{w}'(b_{k}, r_{k}, Ω_{k}).
1) The dk ∈ D, if it bids truthfully: Based on Algorithm 3, we have σ′(dk) = arg max s′j∈H′k \{(b′j,k1 − \tilde{p}_{k1}) ⋅ r′k1\} such that each seller sj ∈ H′k, we denote by \tilde{u}_{k1}' = (v_{k1} − \tilde{p}_{k1}) ⋅ r_{k1}' otherwise, \tilde{u}_{k1}' = 0. For convenience, any notations \tilde{z}_{k} and \tilde{a}_{k} refer to the concepts given by truthful bid v_{k} and untruthful bid b_{k}. For each seller sj ∈ H′k, we consider the following two subcases,
   1a) b_{k1} > v_{k1}': The price \tilde{p}_{k1}' charged to dk is equal to \tilde{p}_{k1}' because the d′k1 has been the first pair in Q′w when bidding truthfully. Thus, we have \tilde{u}_{k1}' = \tilde{u}_{k1}'.
   1b) b_{k1} < v_{k1}': The price \tilde{p}_{k1}' charged to dk is equal to \tilde{p}_{k1}' if the d′k1 is still the first pair in Q′w when

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
Therefore, the utility cannot be improved by bidding untruthfully ($b_{k,l}^i \geq \tilde{p}_{k,l}^i$). Thus, we have $\tilde{u}_{k,l}^i = \tilde{u}_{k,l}^i$. If $b_{k,l}^i < \tilde{p}_{k,l}^i$, we have $s_l \notin H_k^i$ and $\tilde{u}_{k,l}^i = 0$. Thus, we have $\tilde{u}_{k,l}^i = 0 < \tilde{u}_{k,l}^i$.

Therefore, both buyers and sellers are truthful, which leads to the MIDA being truthful.

| $b_{k,l}^i$ | $s_1$ | $s_2$ | $s_3$ | $s_4$ | $s_5$ | $s_6$ | $s_7$ | $r_k^i$ |
|----------------|-------|-------|-------|-------|-------|-------|-------|-------|
| $d_1$ | 0 | 4 | 0 | 5 | 2 | 0 | 0 | 5 |
| $d_2$ | 2 | 0 | 0 | 0 | 5 | 1 | 0 | 2 |
| $d_3$ | 7 | 0 | 5 | 0 | 0 | 4 | 0 | 6 |
| $d_4$ | 0 | 6 | 4 | 0 | 6 | 0 | 0 | 4 |
| $d_5$ | 0 | 0 | 0 | 2 | 0 | 4 | 5 | 3 |

### Table 1

**Walk-Through Example with Five Buyers and Seven Sellers**

*Theorem 1:* The MIDA is individually rational, budget balanced, computationally efficient, and truthful.

*Proof:* It can be derived from Lemmas 1 to 4.

### D. Walk-Through Example and Inference Attack

We give a walk-through example to demonstrate how our MIDA mechanism works. The bid information of buyers and ask information of sellers are shown in Table 1. In the time slot $t$, we assume each buyer satisfies (5d) and each player bids (asks) truthfully. In the MIDA-WCD process, the threshold is $d^o_{t-1} = 3^t = 4$, thereby we have $S^o = \{s_2, s_5, s_6\}$ and $D^o = \{d_{t-2}, d_{t-4}, d_{t-5}, d_{t-6}, d_{t-7}\}$. In the MIDA-AP process, for each winning seller candidate, we have $Q^b = \{d_{t-2}, d_{t-4}, d_{t-5}\}$ and $Q^w = \{d_{t-6}, d_{t-7}\}$. The prices charged to them should be $\hat{p}^b_{t-2} = \max(\{d_{t-2}, d_{t-4}, d_{t-5}\}) = 5$, $\hat{p}^w_{t-6} = \max(\{d_{t-6}, d_{t-7}\}) = 4$, and $\hat{p}^w_{t-7} = \max(\{d_{t-6}, d_{t-7}\}) = 4$. For buyer $d_4$, we have $\hat{p}^w_{t-7} = (\hat{p}^b_{t-2} - \hat{p}^w_{t-6}) = 4$ and $\hat{p}^w_{t-6} = (\hat{p}^b_{t-2} - \hat{p}^w_{t-7}) = 4$. To maximize its utility, buyer $d_4$ is assigned to seller $s_5$. The published auction result is $D_w^o = \{d_3, d_4\}$, $S_w^o = \{s_5, s_6\}$, $\sigma(d_3) = s_5$, $\sigma(d_4) = s_5$, $\hat{p}^w_w = (\hat{p}^b_{t-2} - \hat{p}^w_{t-6}) = \{4, 4\}$, and $\hat{p}^w_w = (\hat{p}^b_{t-2} - \hat{p}^w_{t-7}) = \{4, 4\}$ and $(\sigma^+, r^+_6) = (6, 4)$. The social welfare can be written as

$$\sum_{d_k \in D^o_w} (b_{k, \sigma(d_k)} - \sigma^+(\sigma(d_k))) \cdot r_k = 24.$$  (10)

**Case 1:** As mentioned before, there are two kinds of inference attacks. First, we consider a seller adversary infers the unit asks of other sellers in the time slot $t + 1$. We assume that seller $s_3$ is the adversary who gives an untruthful ask $d^+_3 = 2$ and other players remain the same as the last slot. Now, we have $d^+_3 = 3$ and $\sigma^+(d_3) = \{s_2, s_3, s_6\}$. The published auction result will be $D^+_w = \{d_3, d_4\}$, $S_w^o = \{s_5\}$, $\sigma^+(d_3) = s_3$, $\sigma^+(d_4) = s_5$, $\hat{p}^w_w = (\hat{p}^b_{t-2} - \hat{p}^w_{t-6}) = \{4, 5\}$, and $\hat{p}^w_w = (\hat{p}^b_{t-2} - \hat{p}^w_{t-7}) = \{4, 4\}$ and $(\sigma^+, r^+_6) = (6, 4)$.

Now, we can observe that the seller $s_5$ is not a winning seller. Besides, the seller $s_5$ is not in the current seller candidate set $S^o_t$ because buyer $d_4$ will be assigned to it if $s_5 \in S^o_t$ based on the result of last slot. Since seller $s_3$ decreases its ask, seller $s_5$ is removed from the seller candidate set. According to the current threshold payment to sellers, it is easy to infer
that $d'_{i+1} - d'_{0} = 3$. Then, the privacy of seller $s_5$ has been threatened.

Case 2: Next, we consider a buyer adversary infers the unit bids of other buyers in the time slot $i + 1$. We assume that buyer $d_1$ is the adversary who gives an untruthful bid $b'_{i+1} = 6$ and other players remain the same as the last slot. Now, we have $d'_{i+1} = d_{0} = 4$, $s'_{i+1} = \{s_2, s_5, s_6\}$, and $D'_{i+1} = \{d'_{1,2}, d'_{1,3}, d'_{1,6}, d'_{1,8}, d'_{1,9}\}$. The published auction result will be $D''_{i+1} = \{d_1, d_3, d_4\}$, $s''_{i+1} = \{s_2, s_5, s_6\}$, $\sigma'_{i+1}(d_1) = s_5$, $\sigma'_{i+1}(d_3) = s_6$, $\sigma'_{i+1}(d_4) = s_2$, $\hat{P}'_{w} = \{\tilde{p}'_{1, i}, \tilde{p}'_{2, i}, \tilde{p}'_{4, i}\} = \{(4.4, 4.5), \hat{P}'_{w} = \{\tilde{p}'_{2, i}, \tilde{p}'_{5, i}, \tilde{p}'_{6, i}\} = \{(4.4, 4.4), \mathcal{D}'_{i+1} = \{s_1, s_2, s_3, s_4\}$, and $\{r'_{1, i}, r'_{2, i}, r'_{3, i}\} = \{5, 6, 4\}$. Now, we can observe that buyer $d_4$ is assigned to seller $s_2$ instead of $s_5$. Thus, buyer $d_1$ replaces the top position of $d'_{i+1}$ in the sorted list $O'_{i+1}$. According to the price charged to $d_1$, we have $\hat{p}'_{1, i} = \tilde{p}'_{1, i} = b'_{i+1} = 6$. Then, the privacy of buyer $d_4$ has been threatened.

V. ONLINE DOUBLE AUCTION DESIGN WITH DIFFERENTIAL PRIVACY

To protect the privacy of both buyers and sellers, we enhance our MIDA mechanism by using the technology of DP. We first introduce several important concepts about DP and then formulate our algorithms on them.

A. Differential Privacy

DP [20] is a technology to guarantee that an adversary is not capable of distinguishing between two neighboring inputs with high probability. The neighboring databases means two data sets $O = \{\omega_1, \omega_2, \ldots, \omega_\phi\}$ and $O' = \{\omega'_1, \omega'_2, \ldots, \omega'\phi\}$ which have exactly one different element. In differentially private protection, it is possible that two neighboring inputs have the same or similar output. Thus, adversaries are hard to infer other private inputs according to public query results. Let us look at its definition.

Definition 5 (DP): An algorithm (query function) $f$ gives $\varepsilon$-DP if and only if, for any two neighboring inputs $O$ and $O'$, we have

$$\Pr[f(O) \in R] \leq \exp(\varepsilon) \cdot \Pr[f(O') \in R]$$

(11)

where $R$ is a fixed range such that $R \subseteq \text{Range}(f)$ and $\varepsilon$ is called privacy budget.

The privacy budget is a parameter used to control the degree of privacy protection that an algorithm gives. Usually, a smaller privacy budget implies stronger privacy protection. The sensitivity of an algorithm $f$ quantifies the magnitude of the noise that is needed to protect the data from adversaries.

Definition 6 (Sensitivity): The $\ell_1$-sensitivity of an algorithm $f$ is defined as

$$\Delta f = \max_{O, O' \in \text{dom}(f)} ||f(O) - f(O')||_1.$$  (12)

Based on this definition, the sensitivity is an upper bound we need to perturb the output of $f$ to protect privacy. The noise is generally sampled from a Laplace distribution. A random variable $X$ subjected to Laplace distribution, denoted by $X \sim \text{Lap}(\mu, b)$, has a probability density function

$$\text{Lap}(x | \mu, b) = \frac{1}{2b} \exp\left(\frac{-|x - \mu|}{b}\right)$$

(13)

where $\mu$ is the center point, and $b$ is the scaling factor [40]. Now, we can define the Laplace mechanism. The Laplace mechanism runs an algorithm $f$ directly and then adds a Laplace noise sampled from the Laplace distribution.

Definition 7 (Laplace Mechanism): Given an algorithm (query function) $f : \text{dom}(f) \rightarrow \mathbb{R}$, the Laplace mechanism $\mathcal{M}_L(x, f, \varepsilon)$ can be defined as

$$\mathcal{M}_L(x, f, \varepsilon) = f(x) + \text{Lap}(0, \Delta f / \varepsilon)$$

(14)

where $x \in \text{dom}(f)$ and $\text{Lap}(\Delta f / \varepsilon)$ is a random noise sampled from the Laplace distribution.

B. Algorithm Design

Here, we make some minor changes to the MIDA mechanism to ensure the private security of both buyers and sellers. The MIDA-DP mechanism is shown in Algorithm 4, whose winning candidate determination part (MIDA-WCD-AP) is shown in Algorithm 5. As shown in Algorithm 5, we select the median $d'_{i,j}$ as a threshold first and add a Laplace noise sampled from the Laplace distribution $\text{Lap}(0, \Delta_1 / \varepsilon)$ to get an updated threshold $\tilde{d}'_{i,j}$. Then, we use the updated threshold to select the candidate winning buyer and seller set.

**Algorithm 4 MIDA-DP ($\Omega_2$)**

**Input:** $\Omega' = \{\{B_i\}_{i \in D}, \{A_i\}_{i \in S}, \varepsilon\}$

**Output:** $D'_w, S'_w, \sigma'_i, \hat{P}'_{w}$

1: $(D'_i, S'_i, \tilde{d}'_{i,j}) \leftarrow \text{MIDA-WCD-AP} (\Omega_0, \varepsilon)$

2: $(D'_w, S'_w, \sigma'_i, \hat{P}'_{w}, \hat{P}'_{w}) \leftarrow \text{MIDA-AP} (\Omega_2, \hat{D}'_w, \hat{S}'_w, \hat{d}'_{i,j})$

3: return $(D'_w, S'_w, \sigma'_i, \hat{P}'_{w}, \hat{P}'_{w})$
C. Theoretical Analysis and Privacy Protection

First, we give an analysis of privacy protection in our MIDA-DP mechanism.

**Lemma 5**: The MIDA-DP gives $\varepsilon$-DP for the asks of sellers.

**Proof**: The process of MIDA-WCD-DP as shown in Algorithm 5 can be regarded as an algorithm $f:[a_{\text{min}}, a_{\text{max}}]^m \rightarrow [a_{\text{min}}, a_{\text{max}}]^m$ where the input is the asks of sellers $a^t = (a^t_1, a^t_2, \ldots, a^t_m) \in [a_{\text{min}}, a_{\text{max}}]^m$ and the output is the threshold $a^t_{\phi} \in [a_{\text{min}}, a_{\text{max}}]$ in the time slot $t$. Let us consider two neighboring inputs $a^t$ and $a^t'$ that have exactly one different ask. For any value $a^t_{j_{\phi}} \in \mathbb{R}$, we have

$$\Pr\left[\mathcal{M}_t(a^t, f, \varepsilon) = a^t_{j_{\phi}}\right] = \frac{\exp(-\varepsilon|f(a^t) - a^t_{j_{\phi}}|/\Delta t)}{\exp(-\varepsilon|f(a^t') - a^t_{j_{\phi}}|/\Delta t)}$$

because we have known $|f(a^t) - f(a^t')| \leq \Delta t$. By symmetry, we have $\Pr\left[\mathcal{M}_t(a^t', f, \varepsilon) = a^t_{j_{\phi}}\right]/\Pr\left[\mathcal{M}_t(a^t, f, \varepsilon) = a^t_{j_{\phi}}\right] \geq \exp(-\varepsilon)$ easily.

Then, we give the qualitative analysis of privacy protection based on the aforementioned two cases of inference attack discussed in Section IV-D. For case 1, even though it can infer that the seller $s_5$ is not in the current winning seller candidate set, the adversary cannot conclude with high confidence that $a^t_5$ is the maximum one higher than or equal to the threshold. Besides, the threshold $a^t_{j_{\phi}}$ has been perturbed. Even though $a^t_5$ is the maximum one higher than or equal to the threshold, the adversary cannot know what $a^t_5$ is. For case 2, because of the uncertainty of threshold $a^t_{j_{\phi}}$ and $a^t_5$, the adversary cannot make sure that $a^t_{j_{\phi}}$ is in current winning buyer candidate set. Thus, it is hard to infer that $\tilde{P}^{t+1}_{4,5} = \psi_4^{t+1} / \psi_4^{t+1}$. The adversary cannot know what the $\psi_4^{t+1}$ is. The privacy security of both buyers and sellers has been guaranteed.

**Theorem 2**: The MIDA-DP is individually rational, budget balanced, computationally efficient, and truthful. Moreover, it protects the privacy of buyers and sellers.

**Proof**: The MIDA-DP satisfies the design rationales from Definitions 1 to 4 by similar proofs from Lemmas 5 to 4. According to Lemma 5, it gives $\varepsilon$-DP to the sellers. Because the winning buyers and their charged prices are dependent on the winning seller candidate set, the privacy of buyers would be protected as well.

VI. PROBLEM EXTENSION

For the previous problem defined in Section III-B, it is just a special case where each edge server (seller) can serve at most one IoT device in a slot. Actually, an edge server could serve more than one IoT device. Thus, in a more general scenario, (5a) should be removed, and thus, the function $\sigma^t$ from $D^t_\omega$ to $S^t_\omega$ is not a bijection, but a many-to-one mapping. To distinguish from the MIDA mechanism, the algorithm to solve this general case is named as MIDA-G mechanism shown in Algorithm 6. Its winning candidate determination is the same as MIDA-WCD shown in Algorithm 2, but its assignment and price (MIDA-G-AP) is shown in Algorithm 7. There exists a tentative set $Q^t_j$ for each $s_j \in S^t_\omega$, where each buyer in $Q^t_j$ could be assigned to seller $s_j$. Naturally, we have $\sum_{d_i \in Q^t_j} c_i \leq q^t_j$. The charged price given in lines 9 and 17 is used to guarantee truthfulness.

By similar induction as the MIDA mechanism, we also have that the MIDA-G mechanism is individually rational, budget balanced, computationally efficient, and truthful. The differentially private strategy shown in Section V can be used in our MIDA-G mechanism to protect the privacy of buyers and sellers for the same reason. Thus, the MIDG-G-DP mechanism can be formulized by replacing MIDA-WCD in Algorithm 6 with MIDA-WCD-DP as shown in Algorithm 5.

VII. NUMERICAL SIMULATIONS

In this section, we construct a virtual scenario to simulate an edge-assisted blockchain-based IoT system. Then, we evaluate our MIDA mechanism with or without DP in detail. Here, we focus on verifying that the mechanism satisfies our desired properties, such as truthfulness, and observe how these mechanisms with DP affect social welfare and protect users’ privacy in real simulations.

A. Simulation Setup

We hypothesize an area with $a \times a$ km$^2$, where there are $n$ IoT devices (blockchain nodes and buyers) and $m$ edge servers (sellers). We default by $n = m$ and they are distributed uniformly in this area. Given an IoT device $d_i \in D$ and an edge server $s_j \in S$, their coordinates in this area are denoted by $(x_i, y_i)$ and $(x_j, y_j)$, which implies their positions. The distance between IoT device $d_i$ and edge server $s_j$ can be defined as $\text{Dist}(d_i, s_j)$. We have

$$\text{Dist}(d_i, s_j) = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}. \quad (15)$$

Here, we give a parameter $\gamma$ such that $\{d_i, s_j\} \in E$ if $\text{Dist}(d_i, s_j) \leq \gamma$; otherwise, $\{d_i, s_j\} \notin E$. According to the definitions in Section III-B, in the time slot $t \in I$, we assume the unit cost $c^t_j$ of each seller $s_j \in S$ is distributed uniformly in interval $[0, 1]$. Similarly, the unit valuation $v^t_{i,j}$ is also distributed uniformly in interval $[0, 1]$ if $\text{Dist}(d_i, s_j) \leq \gamma$ and

---

**Algorithm 6 MIDA-G ($\Omega^t$)**

**Input**: $\Omega^t = (\{D^t_i\}_{d_i \in D}, \{A^t_j\}_{s_j \in S})$

**Output**: $\mathcal{D}_w^t, S^t_\omega, \sigma^t, \tilde{P}_w^t$

1: $(D^t_i, S^t_\omega, t_{i,j}) \leftarrow \text{MIDA-WCD (} \Omega^t \}$
2: $(D^t_i, S^t_\omega, t_{i,j}, \tilde{P}_w^t) \leftarrow \text{MIDA-G-AP (} \Omega^t, D^t_i, S^t_\omega, t_{i,j} \}$
3: return $(\mathcal{D}_w^t, S^t_\omega, \sigma^t, \tilde{P}_w^t)$
Algorithm 7 MIDA-G-AP ($\Omega^i$, $D^i_w$, $S^i$, $d^j_o$)

Input: $\Omega^i$, $D^i_w$, $S^i$, $d^j_o$

Output: $D^i_w$, $S^i$, $\sigma^i$, $\hat{p}^i_w$, $\hat{p}^i_w$

1: $D^i_w \leftarrow \emptyset$, $S^i \leftarrow \emptyset$, $\hat{p}^i_w \leftarrow \emptyset$, $\hat{p}^i_w \leftarrow \emptyset$
2: Create a sorted list $Q^i = \{d^i_k \in D^i_c\}$ for each $s^i_j \in S^i_c$
3: for each $s^i_j \in S^i_c$ do
4: if $\sum_{d^i_k \in Q^i} r^i_k \leq q^i_l$ then
5: for each $d^i_k \in Q^i$ do
6: if $d^i_k \in D^i_w$ then
7: $D^i_w \leftarrow D^i_w \cup \{d^i_k\}$
8: end if
9: $\hat{p}^i_k \leftarrow d^i_j$
10: end for
11: else
12: Let $k_m$ be the maximum value such that it satisfies the constraint $\sum_{d^i_k \in Q^i} r^i_k \leq q^i_l$
13: for each $d^i_k \in Q^i[1, \ldots, k_m]$ do
14: if $d^i_k \in D^i_w$ then
15: $D^i_w \leftarrow D^i_w \cup \{d^i_k\}$
16: end if
17: $\hat{p}^i_k \leftarrow \max\{d^i_j, b^i_{km+1,j} \cdot (r^i_{km+1}/r^i_k)\}$
18: end for
19: $Q^i_l \leftarrow Q^i[1, \ldots, k_m]$
20: end if
21: end for
22: for each $d^i_k \in D^i_w$ do
23: $H^i_k = \{s^i_j \in S^i, d^i_k \in Q^i\}$
24: Find $s^i_f \leftarrow \max_{s^i_j \in H^i_k} \{b^i_{km+1,j} \cdot (r^i_{km+1}/r^i_k)\}$
25: $\sigma^i(d^i_k) \leftarrow s^i_f$
26: $\hat{p}^i_k \leftarrow \hat{p}^i_f$, $\hat{p}^i_w \leftarrow \hat{p}^i_w \cup \{\hat{p}^i_k\}$
27: if $s^i_f \notin S^i_w$ then
28: $S^i_w \leftarrow S^i_w \cup \{s^i_f\}$
29: $\hat{p}^i_f \leftarrow d^i_j$, $\hat{p}^i_w \leftarrow \hat{p}^i_w \cup \{\hat{p}^i_f\}$
30: end if
31: end for
32: return $(D^i_w, S^i, \sigma^i, \hat{p}^i_w, \hat{p}^i_w)$

$v^i_{j,o} = 0$ if $\text{Dist}(d^i_o, s^i_j) > \gamma$. The settings of computing power $r^i_k$ requested by buyer $d^i_k \in D$ and computing power $g^i_j$ provided by seller $s^i_j \in S$ will be introduced later.

B. Simulation Results and Analysis

Part 1: We consider a static MIDA mechanism in any time slot $t \in I$ based on the above settings, where we assume that $\text{Dist}(d^i_o, s^i_j) \leq \gamma$ and $r^i_k \leq g^i_j$ for any $d^i_k \in D$ and $s^i_j \in S$. Here, the $r^i_k$ is distributed uniformly in interval $[0, 10]$. Moreover, (8) has been satisfied. Here, we give $\alpha = 10$ and $n = m = 10$. Thus, we have $D = \{d^i_1, d^i_2, \ldots, d^i_{10}\}$ and $S = \{s^i_1, s^i_2, \ldots, s^i_{10}\}$. We use this simplified scene to evaluate whether it satisfies individual rationality, budget balance, and truthfulness.

1.a) Individual Rationality and Budget Balance: Fig. 2 shows the auction results and their individual rationality, where the $d^i_0(S^i)$ means $\sigma^i(d^i_0) = s^i_7$. As shown in Fig. 2, we have $D^i_w = \{d^i_9, d^i_2, d^i_{10}, d^i_3\}$ and $S^i_w = \{s^i_7, s^i_4, s^i_9, s^i_3\}$. The price charged to each winning buyer is less than its bid and the payment rewarded to each winning seller is more than its ask. Thus, individual rationality can be held. According to the definition of budget balance shown as (9), the budget balance can be held obviously.

1.b) Truthfulness: Fig. 3 shows the truthfulness of buyers and sellers in MIDA. (a) Buyer $d^i_2 \in D^i_w$. (b) Buyer $d^i_7 \notin D^i_w$, (c) Seller $s^i_7 \in S^i_w$. (d) Seller $s^i_1 \notin S^i_w$. As shown in Fig. 3(a), each $b^i_{2,j}$ changes from 0 to 1. At this time, other unit bids except for $b^i_{2,j}$ are equal to their corresponding valuations. For buyer $d^i_2$, its utility is $u^i_2 = 0.695$ when giving the truthful bid. We can see that it cannot improve its utility by giving an untruthful bid $b^i_{2,j}$, which even reduces its utility to a negative value. For buyer $d^i_7$, its utility is $u^i_7 = 0$ when giving the truthful bid. As shown in Fig. 3(b), it cannot improve its maximum utility by giving an untruthful bid as well. As shown in Fig. 3(c) and (d), it is obvious that sellers obtain their maximum utilities.
by giving truthful asks. Therefore, the truthfulness of buyers and sellers can be held definitely.

Part 2: We consider a static MIDA-DP mechanism in any time slot \( t \in I \) based on the above settings, where we give \( \alpha = 1000, n = m = 1000 \), and \( \gamma = 50 \). Here, \( r_i' \) is distributed uniformly in interval \([0, 10] \), \( r_i' \leq g_j' \) for any \( d_i \in D \) and \( s_j \in S \), and (8) has been satisfied. Then, we consider the online MIDA and MIDA-DP mechanisms in time interval \( I \), where we give \( \theta = 30 \). Thus, (8) should be checked in each time slot. We use these two scenes to evaluate the performance of DP and online mechanisms.

2.a) DP: Fig. 4(a) shows the social welfare of a given time slot obtained by MIDA and MIDA-DP with the different privacy budget \( \varepsilon \), where we run the MIDA-DP mechanism 100 times and take the average of them. As shown in Fig. 4(a), we can observe that the expected social welfare of MIDA-DP increases and approaches the social welfare of MIDA (without DP) gradually as its privacy budget increases. As we know, the larger the privacy budget is, the weaker the privacy protection is. Thus, we need to tradeoff the performance of social welfare and the degree of privacy protection.

2.b) Online Mechanisms: Fig. 4(b) shows the social welfare of each time slot obtained by online MIDA and MIDA-DP, where the time interval is \( I = \{1, 2, \ldots, 50\} \). As shown in Fig. 4(b), the social welfare decreases gradually as the time slot increases. This is due to the constraint of \( \theta \), and the permitted total computing resources in this time interval for some IoT devices have been used up. Besides, we can see that the fluctuation of social welfare is larger when the privacy budget is smaller.

Part 3: We evaluate the MIDA-G mechanism where there is more than one IoT device can be assigned to an edge server. Thus, we give that the \( g_j' \) is distributed in interval \([50, 100]\). Similar to Part 2, we first consider a static MIDA-G-DP mechanism in any time slot \( t \in I \) and then consider the online MIDA-G and MIDA-G-DP mechanisms in time interval \( I \). The process is similar to the process in Part 2, which should be easier to understand.

3.a) DP: Fig. 5(a) shows the social welfare of a given time slot obtained by MIDA-G and MIDA-G-DP with the different privacy budget \( \varepsilon \), where we run the MIDP-G-DP mechanism 100 times and take the average of them. According to our settings, we have \( r_i' < (1/5) \cdot g_j' \) for any \( d_i \in D \) and \( s_j \in S \). Thus, there are at least five IoT devices can be assigned to an edge server. As shown in Fig. 5(a), it demonstrates a similar trend to the MIDA-DP mechanism shown in Fig. 4(a). However, the social welfare of MIDA-G has been improved significantly.

3.b) Online Mechanisms: Fig. 5(b) shows the social welfare of each time slot obtained by online MIDA-G and MIDA-G-DP, where the time interval is \( I = \{1, 2, \ldots, 50\} \). As shown in Fig. 5(b), it also demonstrates a similar trend to MIDA and MIDA-DP shown in Fig. 4(b). Besides, the MIDA-G converges to zero more rapidly than the MIDA since many more IoT devices can be assigned in earlier time slots, thus faster to reach (8).

Part 4: We conduct the experiment to evaluate the impact of the increasing or decreasing number of edge servers or IoT devices. The parameter setting is similar to Part 2 and the comparison experiment can be divided into two groups: 1) fix \( n = 1000 \) and increase \( m \) from 200 to 1000 and 2) fix \( m = 1000 \) and increase \( n \) from 200 to 1000.

4.a) MIDA/MIDA-DP: Fig. 6 shows the total social welfare within a time interval \( I \) under the different number of edges or IoT obtained by MIDA and MIDA-DP. (a) \( n = 1000, \varepsilon = 5 \), (b) \( m = 1000, \varepsilon = 5 \).
they have more candidates to serve, thus the transaction unit price will be higher. In addition, we find that when the number of IoT devices is more than 600, the welfare is very close to that obtained with the number of IoT devices is 1000 since the service capacity of edge servers has approached saturation under the current constraints.

4.b) MIDA-G/MIDA-G-DP: Fig. 7 shows the total social welfare with a time interval \( I = \{1, 2, \ldots, 50\} \) obtained by MIDA-G and MIDA-G-DP, where the privacy budget of MIDA-G-DP is \( \varepsilon = 5 \). As shown in Fig. 7, the welfare is higher than that shown in Fig. 6 under the same state. This is because an edge server can serve more than one IoT device now, thus the service capacity has increased significantly. The rest of the conclusions and laws are similar to 4.a).

From these three aspects, our proposed mechanisms under special or general cases, with or without DP, have been thoroughly validated.

### VIII. Conclusion

In this article, we discussed a typical system model for integrating blockchain and edge computing in IoT systems. First, we formulated the problem mathematically and modeled it by an online MIDA mechanism. We designed an MIDA mechanism for a simplified special case and proved that it is individually rational, budget balanced, computationally efficient, and truthful. Then, we analyzed system security and used DP to enhance security and privacy protection in order to prevent inference attacks. Next, we proposed an MIDA-G mechanism changing our allocation from bijection to many-to-one, which is more general and realistic. Finally, we constructed a virtual scenario to test our mechanism by numerical simulations, which indicates the effectiveness and correctness of our auction algorithms and privacy protection.

In the future, this problem is worth further discussion. The design of the business scenario and auction mechanism in this article is more complicated than the existing work, thereby how to design a satisfactory DP mechanism based on this model is challenging. Here, we just add disturbance in an intuitive way, which can guarantee privacy protection for sellers. This is far from enough. Besides, we also hope to balance the contradiction between privacy protection and social welfare, then extend to a more generalized mechanism design based on DP.

### References

[1] S. Hakak et al., “Autonomous vehicles in 5G and beyond: A survey,” Veh. Commun., vol. 39, Feb. 2022, Art. no. 100551.

[2] B. Damak, M. Turki, S. Cheikhouhou, M. Baklouti, R. Mars, and A. Dhabhi, “IoRachaincare: An IoT architecture integrating blockchain and IoRa network for personal health care data monitoring,” Sensors, vol. 22, no. 4, p. 1497, 2022.

[3] G. Hampel, C. Li, and J. Li, “5G ultra-reliable low-latency communications in factory automation leveraging licensed and unlicensed bands,” IEEE Wireless Commun. Mag., vol. 57, no. 5, pp. 117–123, May 2019.

[4] W. X. Wang, Y. Chen, J. Guo, and W. Jia, “Improving stock trend prediction with multi-granularity denoising contrastive learning,” in Proc. Int. Joint Conf. Neural Netw. (IJCNN), 2023, pp. 1–10.

[5] H. Hui, J. Grant, K. McLaughlin, D. Laverty, and S. Sezer, “Secure real-time industrial IoT communications in smart grids using named data networking,” in Proc. IEEE 21st Int. Conf. Ind. Informat. (INDIN), 2023, pp. 1–6.

[6] R. W. L. Coutinho and A. Boukerche, “Design of edge computing for 5G-enabled tackle Internet-based industrial applications,” IEEE Commun. Mag., vol. 60, no. 1, pp. 60–66, Jan. 2022.

[7] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Bitcoin, Las Vegas, NV, USA, 2008.

[8] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital signature algorithm (ECDSA),” Int. J. Inf. Security, vol. 1, no. 1, pp. 36–63, 2001.

[9] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum, Zug, Switzerland, Yellow Paper, 2014.

[10] C. Feng, P. Han, X. Zhang, B. Yang, Y. Liu, and L. Guo, “Computation offloading in mobile edge computing networks: A survey,” J. Netw. Comput. Appl., vol. 202, Jun. 2022, Art. no. 103366.

[11] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, “EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts,” IEEE Internet Things J., vol. 6, no. 3, pp. 4719–4732, Jun. 2019.

[12] 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.

[13] Z. Chang, W. Guo, X. Guo, Z. Zhou, and T. Ristantemi, “Incentive mechanism for edge computing-based blockchain,” IEEE Trans. Ind. Informat., vol. 16, no. 11, pp. 7105–7114, Nov. 2020.

[14] X. Ding, J. Guo, D. Li, and W. Wu, “An incentive mechanism for building a secure blockchain-based Internet of Things,” IEEE Trans. Netw. Sci. Eng., vol. 8, no. 1, pp. 477–487, Jan.–Mar. 2021.

[15] X. Ding, J. Guo, D. Li, and W. Wu, “Pricing and budget allocation for IoT blockchain with edge computing,” IEEE Trans. Cloud Comput., vol. 11, no. 2, pp. 1608–1621, Apr.–Jun. 2023.

[16] H. Jin, L. Su, B. Ding, K. Nahrstedt, and N. Borisov, “Enabling privacy-preserving incentives for mobile crowd sensing systems,” in Proc. IEEE 36th Int. Conf. Distrib. Comput. Syst. (ICDCS), 2016, pp. 344–353.

[17] Z. Chen, T. Ni, H. Zhong, S. Zhang, and J. Cui, “Differentially private double spectrum auction with approximate social welfare maximization,” IEEE Trans. Inf. Forensics Security, vol. 14, pp. 2805–2818, 2019.

[18] R. Zh. Zhu, Z. Li, F. Wu, K. Shin, and G. Chen, “Differentially private spectrum auction with approximate revenue maximization,” in Proc. 15th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2014, pp. 185–194.

[19] R. Zh. Zhu and K. G. Shin, “Differentially private and strategy-proof spectrum auction with approximate revenue maximization,” in Proc. IEEE Conf. Comput. Commun. (INFOCOM), 2015, pp. 918–926.

[20] C. Dwork, “Differential privacy: A survey of results,” in Proc. Int. Conf. Theory Appl. Models Comput., 2008, pp. 1–19.

[21] H.-N. 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.

[22] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, “A comprehensive survey of blockchain: From theory to IoT applications and beyond,” IEEE Internet Things J., vol. 6, no. 5, pp. 8114–8154, Oct. 2019.

[23] C. Wang, C. Jiang, J. Wang, S. Shen, S. Guo, and P. Zhang, “Blockchain-aided network resource orchestration in intelligent Internet of Things,” IEEE Internet Things J., vol. 10, no. 7, pp. 6151–6163, Apr. 2023.

[24] Z. Zhang et al., “Blockchain and federated deep reinforcement learning based secure cloud-edge-end collaboration in power IoT,” IEEE Wireless Commun., vol. 29, no. 2, pp. 84–91, Apr. 2022.
D. Yang, X. Fang, and J. Tang, “Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones,” IEEE/ACM Trans. Netw., vol. 24, no. 3, pp. 1732–1744, Jun. 2016.

J. Guo, X. Ding, and W. Wu, “Reliable traffic monitoring mechanisms based on blockchain in vehicular networks,” IEEE Trans. Rel., vol. 71, no. 3, pp. 1219–1229, Sep. 2022.

A.-L. Jin, W. Song, and W. Zhuang, “Auction-based resource allocation for sharing cloudlets in mobile cloud computing,” IEEE Trans. Emerg. Topics Comput., vol. 6, no. 1, pp. 45–57, Jan.–Mar. 2018.

A.-L. Jin, W. Song, P. Wang, D. Niyato, and P. Ju, “Auction mechanisms toward efficient resource sharing for cloudlets in mobile cloud computing,” IEEE Trans. Services Comput., vol. 9, no. 6, pp. 895–909, Nov./Dec. 2015.

W. Wang, B. Liang, and B. Li, “Designing truthful spectrum double auctions with local markets,” IEEE Trans. Mobile Comput., vol. 13, no. 1, pp. 75–88, Jan. 2014.

A. Yassine, M. S. Hossain, G. Muhammad, and M. Guizani, “Double auction mechanisms for dynamic autonomous electric vehicles energy trading,” IEEE Trans. Veh. Technol., vol. 68, no. 8, pp. 7466–7476, Aug. 2019.

D. Yang, X. Fang, and G. Xue, “Truthful auction for cooperative communications,” in Proc. 12th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2011, pp. 1–10.

R. P. McAfee, “A dominant strategy double auction,” J. Econ. Theory, vol. 56, no. 2, pp. 434–450, 1990.

J. Guo, X. Ding, and W. Wu, “A double auction for charging scheduling among vehicles using DAG-blockchains,” 2020, arXiv:2010.01436.

X. Yang, T. Wang, X. Ren, and W. Yu, “Survey on improving data utility in differentially private sequential data publishing,” IEEE Trans. Big Data, vol. 7, no. 4, pp. 729–749, Oct. 2021.

M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, “A systematic review of data protection and privacy preservation schemes for smart grid communications,” Sustain. Cities Soc., vol. 38, pp. 806–835, Apr. 2018.

D. Li, Q. Yang, W. Yu, D. An, Y. Zhang, and W. Zhao, “Towards differential privacy-based online double auction for smart grid,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 971–986, 2019.

M. U. Hassan, M. H. Rehmani, and J. Chen, “DEAL: Differentially private auction for blockchain-based microgrids energy trading,” IEEE Trans. Services Comput., vol. 13, no. 2, pp. 263–275, Mar./Apr. 2020.

Y. Li, H. C. Ng, L. Zhang, and B. Li, “Online cooperative resource allocation at the edge: A privacy-preserving approach,” in Proc. IEEE 28th Int. Conf. Netw. Protocols (ICNP), 2020, pp. 1–11.

T. Ni, Z. Chen, L. Chen, S. Zhang, X. Xu, and H. Zhong, “Differentially private combinatorial cloud auction,” IEEE Trans. Cloud Comput., vol. 11, no. 1, pp. 412–425, Jan.–Mar. 2023.

T. Zhu, G. Li, W. Zhou, and P. S. Yu, “Preliminary of differential privacy,” in Differential Privacy and Applications. Cham, Switzerland: Springer, 2017, pp. 7–16.

Jianxiong Guo (Member, IEEE) received the B.E. degree from the School of Chemistry and Chemical Engineering, South China University of Technology, Guangzhou, China, in 2015, and the Ph.D. degree from the Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA, in 2021. He is currently an Assistant Professor with the Advanced Institute of Natural Sciences, Beijing Normal University, Zhuhai, China, and also with the Guangdong Key Laboratory of AI and Multi-Modal Data Processing, BNU-HKBU United International College, Zhuhai. He has published more than 50 papers and been a reviewer in famous international journals/conferences. His research interests include social networks, algorithm design, data mining, IoT applications, blockchain, and combinatorial optimization. Dr. Guo is a member of ACM and CCF.