Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8038846, 15 pages
https://doi.org/10.1155/2022/8038846

Research Article

Differential Privacy-Based Double Auction for Data Market in Blockchain-Enhanced Internet of Things

Junhua Zhang and Caiming Zhong

College of Science and Technology, Ningbo University, Ningbo 315300, China

Correspondence should be addressed to Junhua Zhang; zhangjunhua@nbu.edu.cn

Received 18 March 2022; Revised 30 May 2022; Accepted 1 June 2022; Published 21 June 2022

Academic Editor: Huaming Wu

With the rapid development of the Internet of Things (IoT), large amounts of data are collected, which constitute a valuable business resource. Hence, a suitable IoT data market needs to be established, and the provision of safe and effective trading services for multiple buyers and sellers is required. This paper introduces an IoT data market framework supported by blockchain. It focuses on a transaction realization scheme for multiple buyers and sellers. In the scheme, the mechanisms are designed to determine the corresponding data providers and recipients for the buyers and sellers, respectively, and the transaction prices of both parties. When the data market runs, an inference attack will raise bid information leakage issues. We study a transaction scheme that enables differential privacy protection of bids based on an exponential mechanism. This paper theoretically proves the individual rationality, weak budget balance, and truthfulness of the normal transaction scheme and differential privacy-based transaction scheme. This paper also theoretically proves the effectiveness of the differential privacy protection for bids of transaction participants. Furthermore, this paper verifies the performances of the two schemes through digital simulation experiments. From the experiments, we can also prove that these schemes occupy reasonable social welfare and computational overhead.

1. Introduction

With the widespread use of the Internet of Things (IoT), large amounts of data are collected and stored [1]. These are shared such as with data analysts, IoT service providers, and artificial intelligence developers, who wish to maximize their benefits [2], which has given rise to the IoT data market [3, 4]. This is generally online, allowing buyers and sellers to enter at any time, and it satisfies properties such as individual rationality and balanced budgets [5].

Further analysis and decision-making based on the acquired data are needed to generate benefits for buyers. This requires the characteristics of data integrity, authenticity, and security. In addition, IoT data collection is often carried out by sensors at different locations, and data are stored nearby on a local edge server or base station. Therefore, distributed data transactions must conform to the characteristics of IoT data, in accordance with the characteristics of blockchain technology, and this has spurred interest in the research of blockchain-based IoT data market [6–9].

The key problem in the IoT data market is how to efficiently and reasonably determine transaction prices [10–12]. Liu et al. [13] studied the price optimization mechanism in the data market in the context of blockchain-enhanced IoT, where the abstract objects are multiple sellers and one buyer, and a two-stage Stackelberg game is used to solve the pricing and purchasing problem of the data consumer and market agency. However, there are always multiple sellers and buyers, whose efficient pricing and purchases are a more general problem, which this paper approaches with a double auction.

The current blockchain-based data market does not consider privacy leakage in transactions, which can easily lead to price information leakage under an inference attack

[5]. The differential privacy-based method shows promise to prevent such leakage while ensuring lower computation and communication overhead and good auction performance. We adopt differential privacy in auctions to protect the commercial interests of both parties in a transaction.

This paper addresses the above problems from three aspects:

(1) We describe the framework of a blockchain-enhanced IoT data market and propose a double-auction normal transaction method (DANTM) for multiple sellers and buyers

(2) To protect the price privacy of all parties, we upgrade DANTM to a double-auction transaction method based on differential privacy (DADPM). We demonstrate that our algorithms are individually rational, weakly budget-balanced, and truthful and prove that DADPM preserves the price privacy of buyers and sellers

(3) Simulations show that the proposed pricing schemes have the desired properties at a low time cost

The remainder of this paper is structured as follows. Section 2 reviews related research. Section 3 introduces a blockchain-enhanced IoT data market framework and a related data transaction model. Section 4 describes a double-auction scheme for data transactions in the IoT data market. Section 5 presents a differential privacy-based double-auction scheme. In Section 6, we evaluate our proposed schemes. We conclude our work in Section 7.

2. Related Work

With the development of the IoT, more and more data are collected from various IoT node devices, and these are important assets. IoT data have the requirements of real time and privacy, and related research of its market is proceeding [14, 15]. Blockchain, as an information infrastructure that provides transaction credibility and distribution, has been considered [16–19]. However, due to the limited resources of the IoT, related data markets supporting the application of blockchain technology are constructed by coordinating cloud and edge servers [13]. We present a data market framework and trading process in this context.

Much effort has been made to develop secure, efficient, pricing models of low complexity for the IoT data market [13, 20–22]. Wang et al. [20] presented two pricing models for data transactions in device-to-device communication networks: a Stackelberg game based on one buyer and multiple sellers, and an alternative ascending clock auction based on one seller and multiple buyers. Liu et al. [13] formulated a two-stage Stackelberg game to solve the pricing and purchasing problem of one buyer and multiple sellers, considered competition between sellers, and proposed a competition-enhanced pricing scheme. However, there are no pricing models for multiple sellers and buyers in the IoT data market, which is the more general case.

An auction market can be run fairly and efficiently via a trading process. A simple auction has one seller and multiple buyers, and a double auction has multiple sellers and buyers. From the perspective of resource trading, there is research on power and spectrum, adopting the pricing mode of an auction and sometimes considering the privacy protection of transaction information [5, 23]. Zhu and Shin [23] presented a differentially private and strategy-proof spectrum auction mechanism with approximate revenue maximization. Li et al. [5] proposed a differential privacy-based online double-auction scheme for energy trading in the smart grid, consisting of a Laplace-based winner determination rule and exponential-based allocation rule. There are certain differences between data and energy, as energy can only be consumed once, and data multiple times. There is no good or bad energy, but data have differences in quality. Our differential privacy-based double auction differs from previous schemes.

3. Framework, Model, and Desired Properties

3.1. Blockchain-Enhanced Data Market Framework for IoT. Figure 1 displays the system architecture of a blockchain-enhanced IoT data market, targeting the challenges of security and efficiency. The components are IoT sensors and an edge server, base station, cloud server, and data user. IoT sensors collect original data and upload them to the edge server, which refines them and uploads them to a nearby base station, where they are stored for selling. Base stations are always connected to a cloud server through wired networks. The formal public data trading platform is set up on the cloud server. Data users can buy IoT data using a web browser. We set up blockchain on the base station and cloud server, using consortium blockchain for efficiency and data protection [24].

In this system, base stations and cloud servers are the core part of the blockchain, in charge of commercial data storage and transactions. Base stations act as sellers, and users as buyers. Data trading rules are predefined in the blockchain as smart contracts. We design algorithms as data trading rules and protect the privacy of every participant. The IoT data market is a distributed system. Data can be sent from a base station directly to a buyer, which assures efficient trading. Blockchain records and stores transaction data and maintains the authenticity of transactions through its consensus mechanism. We adopt the proof-of-work (PoW) consensus protocol. Data transmission from seller to buyer can be assured by blockchain's key mechanisms. The process of blockchain-enhanced IoT data trading is presented in Figure 2.

We assume the following actions in Figure 2 occur in a time slot:

(1) Buyers (data users) and sellers (base stations) submit buying and selling requirements to the data trading platform (cloud server)

(2) The data trading platform runs data trading algorithms and decides on a trading scheme

(3) The first winning buyer (data user 1) and its data providers (base stations 1 and 2) are notified of the trading result

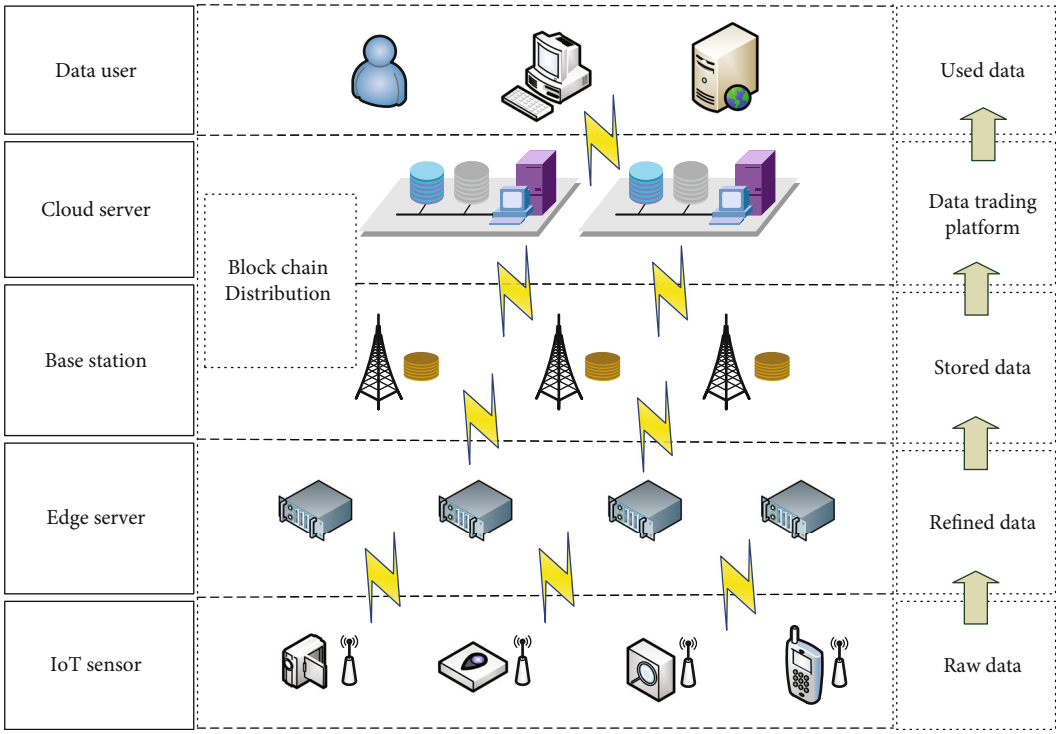

Figure 1: System architecture of blockchain-enhanced IoT data market.

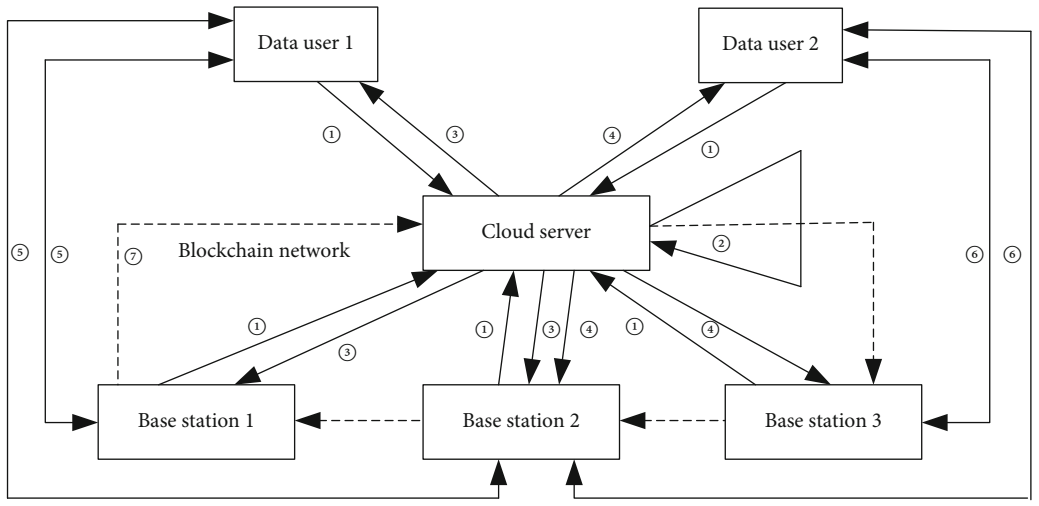

Figure 2: Trading process in IoT data market.

(4) The second winning buyer (data user 2) and its data providers (base stations 2 and 3) are notified of the trading result

(5) The first winning buyer (data user 1) and its data providers (base stations 1 and 2) directly implement data trading

(6) The second winning buyer (data user 2) and its data providers (base stations 2 and 3) directly implement data trading

(7) The blockchain network audits the transaction data

3.2. Designed Auction Model. n our data market, multiple buyers and sellers are involved in data transactions. A double-auction scheme is adopted to efficiently match the requirements of buyers and sellers. One trading process is finished in a time slot.

Buyers and sellers that need data transactions in a time slot are referred to as active buyers and sellers. A data buyer's bid information includes data kind, bid, data quality, and data

Table 1: Notation.

Symbol	Description
G, V	Sets of active buyers (G) and sellers (V) in slot t
g, v	An active buyer (g) and seller (v) in slot t
$C^{(g)}$, $P^{(v)}$	Sets of bids and asking prices
$c_i^{(g)}$, $p_i^{(v)}$	A bid and an asking price
$D^{(g)}$, $D^{(v)}$	The sets of data quality which are buyers' requirements and sellers' supply
$d_i^{(g)}$, $d_i^{(v)}$	Data quality, which is a buyer's requirement and a seller's supply
$E^{(g)}$, $E^{(v)}$	Sets of data quantity, which are buyers' requirements and sellers' supply
$e^{(g)}$, $e^{(v)}$	Data quantity, which is a buyer's requirement and a seller's supply
$S^{(g)}$, $S^{(v)}$	Sets of candidate buyers and sellers
$S_w^{(g)}$, $S_w^{(v)}$	Sets of winning buyers and sellers
$f^{(x)}(t)$	Valid price for buyers (when $x = g$) and sellers (when $x = v$) at slot t
B, S	Set of refined active buyers and sellers
$\bar{g}$	A winning buyer
$\bar{p}_t^{(g)}$, $\bar{p}_t^{(v)}$	Trading price of winning buyer g and winning seller v
DataTradingRecord	Data transaction result, including winning buyer $\bar{g}$, trading price of $\bar{g}$, data providers $S_w^{(v)}$, and whether requirement is satisfied ("yes" if $\sum_{v \in S_w^{(v)}} e^{(v)} - e^{(\bar{g})} \geq 0$), including winning sellers, trading prices, corresponding buyer, and amount of data provided
$q_i^{(g)}$, $q_i^{(v)}$	Quality value for candidate buyer i and seller i
$\Pr\left(q_i^{(g)}\right)$, $\Pr\left(q_i^{(v)}\right)$	Probability of being a winning buyer and seller

Input: active buyers and sellers (G, V) in slot t, and their bids (price, quality, and quantity) $(P^{(v)}, C^{(g)}, D^{(v)}, D^{(g)}, E^{(g)}, E^{(v)})$
Output: Data transaction result DataTradingRecord
//Initialization
$S^{(g)} \longleftarrow \varnothing$, $S^{(v)} \longleftarrow \varnothing$, $S_w^{(g)} \longleftarrow \varnothing$, DataTradingRecord $\longleftarrow \varnothing$
while $G - S_w^{(g)} \neq \varnothing$**do**
  $G \longleftarrow G - S_w^{(g)}$, $S_w^{(g)} \longleftarrow \varnothing$
  //Call Algorithm 2 to calculate valid price
  $f^x(t) = \text{CalcValidPrice}(G, V, C^{(g)}, P^{(v)}, D^{(g)}, D^{(v)})$
  $S^{(g)} = \{g : c^{(g)} \geq f^{(g)}(t), \forall g \in G\}$
  $S^{(v)} = \{v : p^{(v)} \leq f^{(v)}(t), \forall v \in V\}$
  $S^{(g)} \longleftarrow \text{sort}\, c^{(g)}$ in descending order, $g \in S^{(g)}$
  $S^{(v)} \longleftarrow \text{sort}\, p^{(v)}$ in ascending order, $v \in S^{(v)}$
  //Call Algorithm 3 (normal method) for data trading
  $(\text{DataTradingRecord+}, S_w^{(g)}) = \text{NormalTradeMethod}(S^{(g)}, S^{(v)}, C^{(g)}, P^{(v)}, E^{(g)}, E^{(v)})$
end

Algorithm 1: Double Auction with Valid Price Mechanism.

quantity. A data seller's asking information includes data kind, asking price, data quality, and data quantity.

We assume below that the data market will match the data kind through a smart contract in blockchain, allow buyers and sellers of the same data kind to meet, and start the process of a double auction. Table 1 lists the key notation used in our paper.

3.3. Desired Properties of Model

Definition 1. (Seller payoff). The payoff to the winning seller for time slot t is

$$U_t^{(v)} = \left(\bar{p}_t^{(v)} - p_t^{(v)}\right) \cdot e_t. \tag{1}$$

Input: price and data quality of active buyers and sellers $(G, V, C^{(g)}, P^{(x)}, D^{(g)}, D^{(v)})$ in slot t
Output: valid price $f^{(x)}(t)$ with $x = v$ or g for data trading in slot t
$m = |G|$; $n = |V|$
Sort prices of active buyers: $c_1^{(g)} > c_2^{(g)} > \cdots > c_m^{(g)}$
Sort prices of active sellers: $p_1^{(v)} < p_2^{(v)} < \cdots < p_n^{(v)}$
if $p_n^{(v)} \le c_m^{(g)}$ **then**
refine active buyers $B = \{1, 2, \cdots, ,m\}$
refine active sellers $S = \{1, 2, \cdots, n\}$
else if $c_l^{(g)} \ge p_k^{(v)} \ge c_{l+1}^{(g)}$ **then**
refine active buyers $B = \{1, 2, \cdots, l\}$, with $1 \le l \le m-1$
refine active sellers $S = \{1, 2, \cdots, k\}$, with $1 \le k \le n$
else if $p_{k+1}^{(v)} \ge c_r^{(g)} \ge p_k^{(v)}$ **then**
refine active buyers $B = \{1, 2, \cdots, r\}$, with $1 \le r \le m$
refine active sellers $S = \{1, 2, \cdots, k\}$, with $1 \le k \le n-1$
end
//Call function CalcValidPriceViaQuality to decide valid price
$f^x(t) = \text{CalcValidPriceViaQuality}(B, S, C^{(g)}, P^{(v)}, D^{(g)}, D^{(v)})$ **return** $f^{(x)}(t)$
The function CalcValidPriceViaQuality is as follows.
Function CalcValidPriceViaQuality
Input: price and data quality of refined active buyers and sellers $(B, S, C^{(g)}, P^{(v)}, D^{(g)}, D^{(v)})$ in slot t
Output: valid price $f^{(x)}(t)$ with $x = v$ or g for data trading in slot t
Sort quality of refined active buyers in B as $d_1^{(g)} < d_2^{(g)} < \cdots < d_{y^*}^{(g)}$, $y* = |B|$
Sort quality of refined active sellers in S as $d_1^{(v)} > d_2^{(v)} > \cdots > d_{s^*}^{(v)}$, $s* = |S|$
if $d_{s^*}^{(v)} \ge d_{y^*}^{(g)}$ **then**

$$f^{(x)}(t) \longleftarrow \begin{cases} \min\{c_1^{(g)}, \cdots, c_{y^*}^{(g)}\}, x = g \\ \max\{p_1^{(v)}, \cdots, p_{s^*}^{(v)}\}, x = v \end{cases}$$

else if $d_{w^*}^{(v)} \le d_{j*}^{(g)} \le d_{(w-1)^*}^{(v)}$ **then**

$$f^{(x)}(t) \longleftarrow \begin{cases} c_{j^*}^{(g)}, x = g \\ p_{(w-1)^*}^{(v)}, x = v \end{cases} \text{ with } j^* \in \{1, 2, \cdots, y^*\} \text{ and } w^* \in \{2, 3, \cdots, s^*\}$$

else if $d_{l^*}^{(g)} \le d_{k*}^{(v)} \le d_{(l+1)^*}^{(g)}$ **then**

$$f^{(x)}(t) \longleftarrow \begin{cases} c_{l^*}^{(g)}, x = g \\ p_{k^*}^{(v)}, x = v \end{cases} \text{ with } l^* \in \{1, 2, \cdots, (y-1)^*\} \text{ and } k^* \in \{1, 2, \cdots, s^*\}$$

endreturn $f^{(x)}(t)$

Algorithm 2: CalcValidPrice

Definition 2. (Buyer payoff). The payoff to the buyer in time slot t is

$$U_t^{(g)} = \left(c_t^{(g)} - \bar{p}_t^{(g)}\right) \cdot e_t. \tag{2}$$

Definition 3. (Social welfare). Social welfare in time slot t is

$$U_t^{\text{sw}} = \sum_{v=1}^{V} U_t^{(v)} + \sum_{g=1}^{G} U_t^{(g)}. \tag{3}$$

Social Welfare Maximization: in double-auction markets, the goal is to maximize the total social welfare, i.e.,

$$\begin{aligned} &\text{Maximize } U_t^{\text{sw}}, \\ &\text{subject to : } e_t \le e_t^{(v)}, \forall v \in V\,; e_t \le e_t^{(g)}, \forall g \in G. \end{aligned} \tag{4}$$

Individual Rationality: each seller and buyer must receive a nonnegative payoff, i.e.,

$$U_t^{(x)} \ge 0, \text{ where } x \text{ takes the value } v \text{ or } g. \tag{5}$$

Input: candidate buyers and sellers $(S^{(g)}, S^{(v)})$, data amounts $(E^{(g)}, E^{(v)})$, and prices of candidate buyers and sellers $(C^{(g)}, P^{(v)})$ in slot t
Output: data transaction result DataTradingRecord and winning buyer
//Initialization
DataTradingRecord $\longleftarrow \varnothing, S_w^{(v)} \longleftarrow \varnothing, S_w^{(g)} \longleftarrow \varnothing$
//Decide winning buyer
$\bar{g} \longleftarrow$ buyer with highest price in $S^{(g)}$
//Decide trading price of winning buyer
if $|S^{(g)}| > 1$**then**
  Find second-highest price from $C^{(g)}$ as trading price of $\bar{g}$
else
  Use price of $\bar{g}$ as trading price of $\bar{g}$
end
//Decide winning sellers providing data to winning buyer
while $\sum_{v \in S_w^{(v)}} e^{(v)} < e^{(\bar{g})}$**do**
  $S_w^{(v)} \longleftarrow S_w^{(v)} \cup \{v\}$
end
//Decide trading price of winning sellers
if $|S^{(v)}| - |S_w^{(v)}| > 0$**then**
  Trading price of sellers in $S_w^{(v)} \longleftarrow$ Price of first seller in $S^{(v)} - S_w^{(v)}$
else
  Trading price of sellers in $S_w^{(v)} \longleftarrow$ Price of last seller in $S_w^{(v)}$
end
//Record trading information of winning buyer
if $S_w^{(v)} \neq \varnothing$**then**
  $S_w^{(g)} \longleftarrow S_w^{(g)} \cup \{\bar{g}\}$
  DataTradingRecord $+= (\bar{g}$, trading price of $\bar{g}, S_w^{(v)}, \sum_{v \in S_w^{(v)}} e^{(v)} - e^{(\bar{g})})$
end
//Record trading information of winning sellers
for each $v \in S_w^{(v)}$**do**
  if $\sum_{v \in S_w^{(v)}} e^{(v)} - e^{(\bar{g})}$**then**
    DataTradingRecord $+= (v$, trading price of $v, \bar{g}, \sum_{v \in S_w^{(v)}} e^{(v)} - e^{(\bar{g})})$
  exit
  else
    DataTradingRecord $+= (v$, trading price of $v, \bar{g}, e^{(v)})$
  end
end
return $(\text{DataTradingRecord}, S_w^{(g)})$

Algorithm 3: NormalTradeMethod

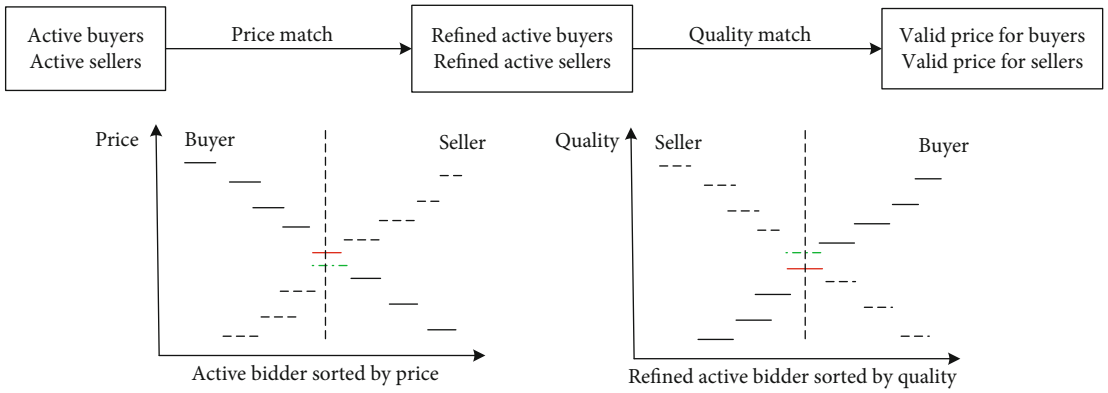

Figure 3: Interpretive explanation of valid price calculation.

In other words, a winning seller is not rewarded with less than its asking price $p_t^{(v)}$, and a winning buyer must not be charged more than its bid $c_t^{(g)}$.

Weak Budget Balance: for the data market in time slot t, if there exists

$$\sum_{g \in G} \bar{p}_t^{(g)} \cdot e_t^{(g)} - \sum_{v \in V} \bar{p}_t^{(v)} \cdot e_t^{(v)} \geq 0, \tag{6}$$

then the auction process satisfies the property of weak budget balance, which ensures that the auctioneer makes a tiny profit.

Truthfulness: an auction is truthful if and only if

$$U_t^{(x)}\left(\chi_t^{(x)}\right) \geq U_t^{(x)}\left(\vec{\chi}_t^{(x)}\right), \tag{7}$$

for each bidder i, whose true and false bids are $\chi_t^{(x)}$ and $\vec{\chi}_t^{(x)}$, respectively. This property ensures that bidders obtain their maximum payoff when and only when their truthful bids are reported.

4. DANTM

4.1. Double Auction with Valid Price Mechanism. We present the concept of a valid price.

Definition 4. (Valid Price). A valid price is a threshold value of a buyer's bid and a seller's asking price. It can determine whether a buyer or seller wins in an auction. A valid price is determined by bids, asking prices, and data quality of buyers and sellers.

In a double-auction data market, active buyers G and sellers V in slot t submit their bidding information to the data market administrator, which can be realized in a smart contract in blockchain. The data market administrator assigns each buyer with seller-provided data through Algorithms 1–3 (see below). The following information is obtained for buyers: the winning buyer $\bar{g}$ and its trading price, the data providers $S_w^{(v)}$, and whether its requirement is satisfied (i.e., whether $\sum_{v \in S_w^{(v)}} e^{(v)} - e^{(\bar{g})} \geq 0$). For sellers, the following information is obtained: the winning sellers, their trading price, the corresponding buyer, and the amount of data provided. The results are uniformly described by DataTradingRecord Algorithm 1 (DANTM) describing the auction scheme. We use Algorithm 2 to calculate the valid price for each active buyer and seller and use this to filter the active buyers G and sellers V to determine candidate participants $S^{(g)}$ and $S^{(v)}$. We sort the candidate buyers in descending bid order and candidate sellers by ascending asking prices. We call Algorithm 3 to obtain a winning buyer $\bar{g}$ (stored in $S_w^{(g)}$) and the related DataTradingRecord, delete that buyer from active buyers G, and serve the next active buyer.

4.2. Valid Price Algorithm. Algorithm 2 is used to calculate a valid price. We match the prices of active buyers and sellers in $(C^{(g)}, P^{(v)})$ to obtain the refined active buyers and sellers (B, S), and call CalcValidPriceViaQuality (see below) to match the data quality of (B, S) among $(D^{(g)}, D^{(v)})$, so as to select the proper prices of buyers and sellers and use them as valid price $f^{(x)}(t)$ for buyers (when $x = g$) and sellers (when $x = v$) at slot t.

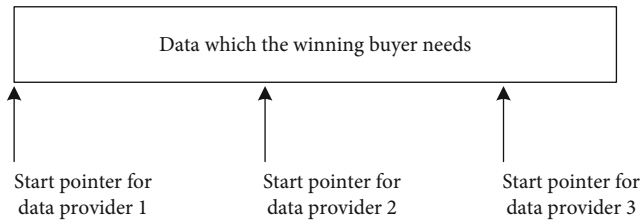

Figure 4: Data trading start pointer for data providers.

We provide an intuitive explanation of Algorithm 2 in Figure 3. To calculate the valid price, Algorithm 2 first ranks active buyers in descending order of price and active sellers in ascending order of price. On this basis, the prices of active buyers and active sellers are matched. As shown on the left of Figure 3, the buyer price (marked red) and the seller price (marked green) are the critical points, and the buyer and seller starting from the critical points to the left become refined active buyers and sellers. Next, refined active sellers are sorted in descending order of data quality and refined active buyers in ascending order of data quality. Then, the data quality of refined active buyers and refined active sellers are matched. As shown on the right of Figure 3, the buyer data quality (marked red) and the seller data quality (marked green) are the critical points, and we take the prices of the buyer and the seller located at the critical points as the corresponding valid price.

4.3. Normal Data Trading Method. We provide the normal data trading method as Algorithm 3. In the data trading process, we select the buyer with the highest price in $S^{(g)}$ as the winning buyer $\bar{g}$ and assign the trading price for the sellers providing data. We record the data trading information for the winning buyer $\bar{g}$ and for the sellers providing data (i.e., the winning sellers). The winning sellers provide data with all they can $(e^{(v)})$, except that the last winning seller needs to provide data with the one the winning buyer needs left $(\sum_{v \in S_w^{(v)}} e^{(v)} - e^{(\bar{g})})$, whose nonnegative value will indicate that the winning buyer has the enough data demanded.

As shown in Algorithm 3, when the number of candidate buyers exceeds 1, the trading price of the winning buyer $\bar{g}$ is equal to the second highest price among the bids of these candidate buyers. When only one candidate buyer exists, the trading price of the winning buyer $\bar{g}$ is equal to its bid. The former case follows the Vickrey-Clarke-Groves auction model [25] to ensure the truthfulness of our algorithm.

The elements in $S^{(v)} - S_w^{(v)}$ and $S_w^{(v)}$ are sorted according to their asking prices in a positive sequence, where $S_w^{(v)}$

represents the winning data sellers and $S^{(v)} - S_w^{(v)}$ represents the left sellers (nonwinning data providers). When there exist elements in $S^{(v)} - S_w^{(v)}$, we use the asking price of the first element in it as the trading price of all the sellers in $S_w^{(v)}$. When there are no elements in $S^{(v)} - S_w^{(v)}$, we use the asking price of the last element in $S_w^{(v)}$ as the trading price of all the sellers in $S_w^{(v)}$. In this pricing scheme, data provided to a buyer from different sellers are given the same price, reflecting the principle of fairness.

As shown in Figure 4, a data trading start pointer is adopted to indicate where a provider starts providing data. By default, the provider provides data starting from the l-ocation indicated by the pointer. Among those providing data to a buyer, data that can be provided by the last data provider may not be all that is required, so the cutoff point is recorded and fed back to the provider.

4.4. DANTM Scheme Analysis. We theoretically analyze the DANTM scheme properties.

Lemma 5. *The DANTM scheme is individually rational.*

Proof. For the buyer, the DANTM scheme considers two cases. First is $|S^{(g)}| > 1$, where winning buyer $\bar{g}$ is assigned trading price $\bar{p}_t^{(\bar{g})}$ as the second-highest bid $p_t^{(g')}$ from $C^{(g)}$. Since $\bar{p}_t^{(\bar{g})} = p_t^{(g')} < p_t^{(\bar{g})}$, there exists $p_t^{(\bar{g})} - \bar{p}_t^{(\bar{g})} > 0$. Second is $|S^{(g)}| = 1$, where winning buyer $\bar{g}$ is assigned trading price $\bar{p}_t^{(\bar{g})}$ as bid $p_t^{(\bar{g})}$ of itself, so $p_t^{(\bar{g})} - \bar{p}_t^{(\bar{g})} = 0$. Hence, the scheme is individually rational for buyers.

For the seller, trading price $\bar{p}_t^{(v)}$ of the winning sellers in $S_w^{(v)}$ is assigned as asking price $c_t^{(v')}$ of the first seller v' in $S^{(v)} - S_w^{(v)}$. Since the asking prices of sellers in $S^{(v)}$ are sorted in ascending order, $\bar{p}_t^{(v)} - c_t^{(v)} = c_t^{(v')} - c_t^{(v)} > 0$. Therefore, the scheme is individually rational for sellers. □

Lemma 6. *The DANTM scheme is weakly budget-balanced.*

Proof. A winning buyer $\bar{g}$ is provided data by a group of winning sellers $S_w^{(v)}$ with a single trading price. The data quantity is the same for both the buyer and sellers. To prove the lemma, we only need to show that $\bar{p}_t^{(\bar{g})} \geq \bar{p}_t^{(v)}$. From the DANTM scheme, winning buyers and sellers come from candidate buyers/sellers, and $p_t^{-(\bar{g})} \geq f^{(g)}(t) \geq f^{(v)}(t) \geq p_t^{-(v)}$. □

Lemma 7. *The DANTM scheme is truthful.*

Proof. We consider two cases for a buyer. First is $|S^{(g)}| = 1$. If the initial bid of the winning buyer is lower than its real value $p_t^{(g)}$, the buyer loses the opportunity to first become a candidate buyer and receives utility $U_t^{(g)} = 0$. If the initial bid is greater than $p_t^{(g)}$, a successful transaction may bring about negative utility $U_t^{(g)} < 0$ because the transaction price $\bar{p}_t^{(g)}$ is greater than $p_t^{(g)}$. In the second case, $|S^{(g)}| > 1$, the secondary bid is selected as $\bar{p}_t^{(g)}$, in accordance with the Vickrey second price auction rule, which is known to be truthful [25].

The DANTM scheme also considers two cases for a seller. First, only one qualified seller provides data to the buyer. A seller with an asking price greater than its real value $c_t^{(v)}$ loses the opportunity to become a winning seller and receives utility $U_t^{(v)} = 0$. If the asking price is less than $c_t^{(v)}$, a successful transaction may have utility $U_t^{(v)} < 0$ because $\bar{p}_t^{(v)}$ is less than $c_t^{(v)}$. Second, multiple qualified sellers provide data to the same purchaser. Among them, the offer with the highest asking price, following the Vickrey second price auction rule, guarantees a truthful ask [25], and other winning sellers will not get more utility. A seller whose asking price exceeds $c_t^{(v)}$ loses the opportunity to become a winning seller, and $U_t^{(v)} = 0$, or becomes the last winning one, which maybe provide limited data $\sum_{v \in S_w^{(v)}} e^{(v)} - e^{(\bar{g})}$ when $\sum_{v \in S_w^{(v)}} e^{(v)} - e^{(\bar{g})} > 0$, and impact its utility $U_t^{(v)}$. If a seller gives an asking price below its real value $c_t^{(v)}$, its utility $U_t^{(v)}$ is not affected. □

Theorem 8. *The DANTM scheme is individually rational, truthful, and weakly budget-balanced.*

5. DADPM

5.1. Differential Privacy Data Trading Method. An inference attack can exist in a double auction [5], and when it works, data buyers or sellers can infer the bidding information of other buyers or sellers, which compromises their privacy. To protect privacy requires an obstacle to prevent the guessing of original bids from data trading results, in which case differential privacy is used. If two nearly identical inputs are input to a function, the probability distribution of their outputs is limited, which is the effect of differential privacy, which we define as follows.

Definition 9 (Differential Privacy). A function f has ε-differential privacy ((ε, δ)-differential privacy) if, for any two input sets A and B with a single input difference, the outputs are within a fixed range R,

$$\Pr[f(A) \in R] \leq \exp(\varepsilon) \times \Pr[f(B) \in R](+\delta), \tag{8}$$

where ε and δ are small positive values.

To maintain the privacy of bids for both winning buyers and sellers, we randomly select them from candidate buyers and sellers, while preserving some valuable properties. We present an exponential-based privacy preserving mechanism to choose winning buyers and sellers.

We calculate the quality value for candidate buyers and determine the probability distribution of winning

Input: candidate buyers and sellers $(S^{(g)}, S^{(v)})$, data amounts $(E^{(g)}, E^{(v)})$, prices of candidate buyers and sellers $(C^{(g)}, P^{(v)})$, valid price $f^{(x)}(t)$ in slot t, and differential privacy-related parameters ε_1 and ε_2.
Output: data transaction result DataTradingRecord and winning buyer
//Initialization
DataTradingRecord $\longleftarrow \varnothing$, $S_w^{(v)} \longleftarrow \varnothing$, $S_w^{(g)} \longleftarrow \varnothing$
//Determine winning buyer
for $i = 1$ to $|S^{(g)}|$**do**
  $q_i^{(g)} \longleftarrow c_i^{(g)}/c_1^{(g)}$
end
for $i = 1$ to $|S^{(g)}|$**do**
$\Pr(c_i^{(g)}) = \exp(\varepsilon_1 \cdot q_i^{(g)}))/\sum_{s_j^{(g)} \in S^{(g)}} \exp(\varepsilon_1 \cdot q_j^{(g)})$
end
Select data buyer $\bar{g} \in S^{(g)}$ according to probability distribution $\Pr(c_i^{(g)})$
//Determine trading price for winning buyer
Use $f^{(g)}(t)$ as trading price of $\bar{g}$
//Calculate probability to be a winning seller
for $i = 1$ to $|S^{(v)}|$**do**
  $q_i^{(v)} \longleftarrow p_1^{(v)}/p_i^{(v)}$
end
for $i = 1$ to $|S^{(v)}|$**do**
  $\Pr(p_i^{(v)}) = \exp(\varepsilon_2 \cdot q_i^{(v)}))/\sum_{j=1}^{n} \exp(\varepsilon_2 \cdot q_j^{(v)}))$
end
while $S^{(v)} \neq \varnothing$**do**
  //Select a winning seller for the winning buyer
  Select seller $v \in S^{(v)}$ according to probability distribution $\Pr(p_i^{(v)})$
  $S_w^{(v)} \longleftarrow S_w^{(v)} \cup \{v\}$
  Use $f^{(v)}(t)$ as trading price of v
  //Record trading information of seller
  if$\sum_{v \in S_w^{(v)}} e^{(v)} \geq e^{(\bar{g})}$**then**
    DataTradingRecord + =(v, the trading price of v, $\bar{g}$, $\sum_{v \in S_w^{(v)}} e^{(v)} - e^{(\bar{g})}$)
    exit
  else
    DataTradingRecord + =(v, the trading price of v, $\bar{g}$, $e^{(v)}$)
    $S^{(v)} \longleftarrow S^{(v)} - \{v\}$
  end
end
//Record trading information of buyer
if $S_w^{(v)} \neq \varnothing$**then**
  $S_w^{(g)} \longleftarrow S_w^{(g)} \cup \{\bar{g}\}$
  DataTradingRecord + =($\bar{g}$, the trading price of $\bar{g}$, $S_w^{(v)}$, $\sum_{v \in S_w^{(v)}} e^{(v)} - e^{(\bar{g})}$)
end
return (DataTradingRecord, $S_w^{(g)}$)

Algorithm 4: DPTradeMethod

buyers. We want the buyer with a higher bid to be the winning buyer with priority. As the bids $C^{(g)}$ of candidate buyers are arranged in descending order, $c_1^{(g)}$ is the highest bid. We set the quality value of buyers as

$$q_i^{(g)} \longleftarrow \frac{c_i^{(g)}}{c_1^{(g)}}, \tag{9}$$

determine the probability distribution of winning buyers,

$$\Pr\left(c_i^{(g)}\right) = \frac{\exp\left(\varepsilon_1 \cdot q_i^{(g)}\right)}{\sum_{s_j^{(g)} \in S^{(g)}} \exp\left(\varepsilon_1 \cdot q_j^{(g)}\right)}, \tag{10}$$

where $S^{(g)}$ is the set of candidate buyers, and choose a winning buyer.

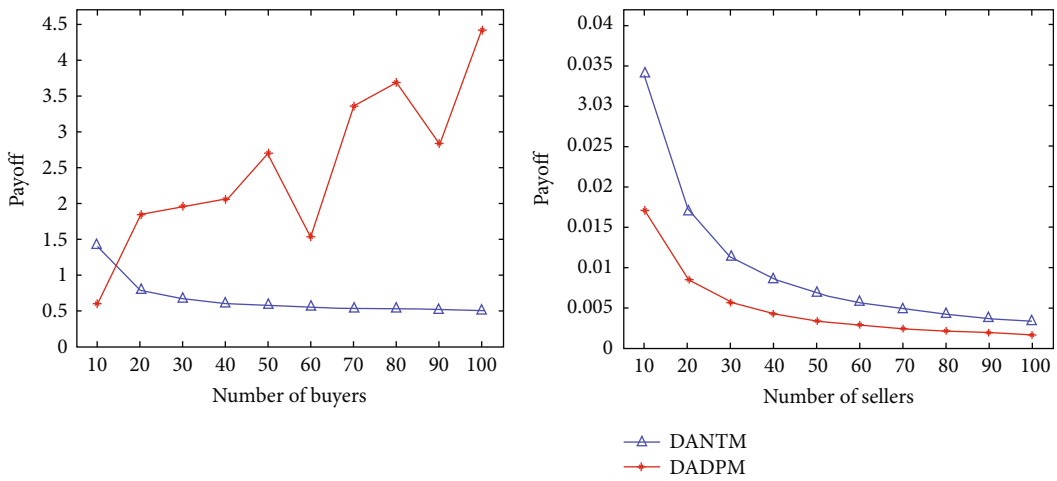

Figure 5: Payoff for (a) buyers and (b) sellers.

We choose a method to calculate the quality value for sellers. We want a seller with a lower asking price to be the winning seller with priority. The asking prices $P^{(v)}$ of candidate sellers are arranged in ascending order, so $p_1^{(v)}$ is the lowest asking price. The quality value of a seller is

$$q_i^{(v)} \longleftarrow \frac{p_1^{(v)}}{p_i^{(v)}}. \tag{11}$$

We calculate the probability distribution of winning sellers among n candidate sellers

$$\Pr\left(p_i^{(v)}\right) = \frac{\exp\left(\varepsilon_2 \cdot q_i^{(v)}\right)}{\sum_{j=1}^{n} \exp\left(\varepsilon_2 \cdot f\left(q_j^{(v)}\right)\right)}, \tag{12}$$

and choose a winning seller.

We assume that the quality function of buyer (seller) i is bounded by $[q_{\min}, q_{\max}]$, and the difference between maximum and minimum value of the quality function of buyers (sellers) is $\triangle_1$ ($\triangle_2$).

According to Theorem 9.36 in [25], while a mechanism is truthful, there is a critical value such that if a buyer's bid is higher than the critical value, the buyer's trading price is equal to the value; if a buyer's bid is less than the value, the buyer will lose in the transaction. In our situation, we can conclude that the bid threshold is just our valid price $f^{(g)}(t)$, and this is the trading price of the winning buyer. We similarly use valid price $f^{(v)}(t)$ as the trading price of the winning seller.

Algorithm 4 presents the implementation of data transaction preserving differential privacy, using **DPTrade Method** instead of **NormalTradeMethod** defined in Algorithm 1:

$$\left(\text{DataTradingRecord+}, S_w^{(g)}\right) = \text{DPTradeMethod}\left(S^{(g)}, S^{(v)}, C^{(g)}, P^{(v)}, E^{(g)}, E^{(v)}, f^{(x)}(t), \text{DP parameters}\right). \tag{13}$$

We define Algorithm 4 using differential privacy method as DADPM. To call DPTradeMethod, we add an input parameter, valid price $f^{(x)}(t)$, and differential privacy-related parameters ε_1 and ε_2.

To achieve differential privacy, we calculate the quality value $q_i^{(g)}$ and probability distribution $\Pr(c_i^{(g)})$ for each candidate buyer and select a data buyer $\bar{g}$ according to this distribution, with trading price $f^{(g)}(t)$ as the trading price of $\bar{g}$.

We calculate the quality value $q_i^{(v)}$ for each candidate seller and obtain probability distribution $\Pr(p_i^{(v)})$, selecting

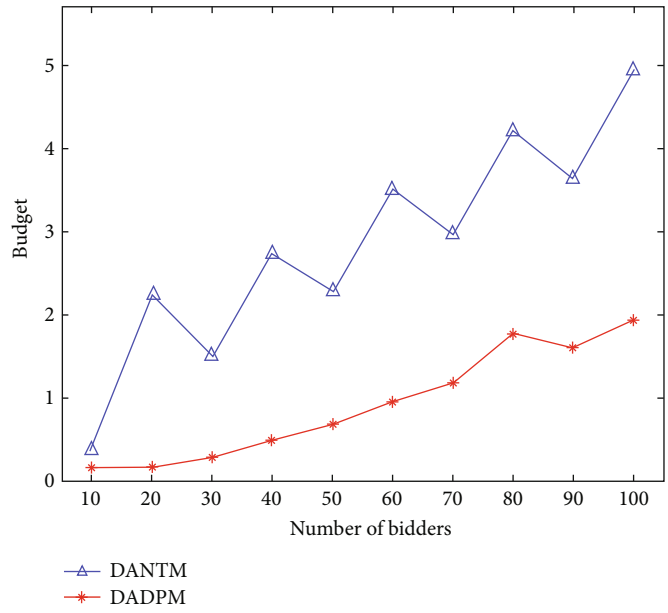

Figure 6: Budget of data market.

sellers according to this distribution to provide data for $\bar{g}$. We use $f^{(v)}(t)$ as the trading price of sellers. Similar to the normal trade method, we record and return (DataTradingRecord, $S_w^{(g)}$) and adopt a data trading start pointer in Algorithm 4 as Algorithm 3.

5.2. DADPM Analysis. We theoretically analyze DADPM.

Lemma 10. *The DADPM scheme is individually rational.*

Proof. The winning buyer $\bar{g}$ is assigned trading price $\bar{p}_t^{(\bar{g})}$ as valid price $f^{(g)}(t)$. From the calculation of the active buyers $S^{(g)}$ (Algorithm 1), $p_t^{(\bar{g})} \geq f^{(g)}(t)$ So, $p_t^{(\bar{g})} - \bar{p}_t^{(\bar{g})} = p_t^{(\bar{g})} - f^{(g)}(t) \geq 0$. Therefore, DADPM is individually rational for buyers.

The trading price $\bar{p}_t^{(v)}$ of the winning sellers in $S_w^{(v)}$ is assigned as valid price $f^{(v)}(t)$. From the calculation of the active sellers $S^{(v)}$ (Algorithm 1), $c_t^{(v)} \leq f^{(v)}(t)$. So, $\bar{p}_t^{(v)} - c_t^{(v)} = f^{(v)}(t) - c_t^{(v)} \geq 0$. Therefore, DADPM is individually rational for sellers.

With a proof similar to that of the DANTM scheme, we can conclude Lemma 11. □

Lemma 11. *The DADPM scheme is weakly budget-balanced.*

Lemma 12. *The DADPM scheme is truthful.*

Proof. For buyers, we can prove the conclusion directly using Theorem 9.36 in [25], according to which, if there is a critical trading price for buyers, the scheme is truthful. From Algorithm 1, $S^{(g)}$ is obtained by sorting $c^{(g)}$ in descending order, so the elements in $S^{(g)}$ are monotone in $c^{(g)}$. Also from Algorithm 1, $S^{(g)}$ is obtained by filtering buyers with $c^{(g)} \geq f^{(g)}(t)$. So, there exists a critical value $f^{(g)}(t)$.

Recall that Vazirani et al. [25] discussed the situation of a simple auction, with one seller and multiple buyers. We discuss a double auction, with multiple sellers and buyers. A buyer's bid is a preference to choose a buyer, and an asking price is a preference to choose a seller. Then, if there is a critical value of a trading price for sellers, the scheme is truthful.

Based on the above discussion, we can prove that the DADPM scheme is truthful for sellers. From Algorithm 1, $S^{(v)}$ is obtained by sorting $p^{(v)}$ in ascending order, so the elements in $S^{(v)}$ are monotone in $p^{(v)}$, and $S^{(v)}$ is obtained by filtering sellers with $p^{(v)} \leq f^{(v)}(t)$. So, there exists a critical value $f^{(v)}(t)$. □

Theorem 13. *The DADPM scheme is individually rational, truthful, and weakly budget-balanced.*

Now, we prove that DADPM preserves the data buyer's valuation privacy.

Theorem 14. *For data buyers, DADPM preserves* $(\varepsilon_1(e-1)\Delta_1 \ln(e/\delta), \delta)$ *differential privacy for bidders' quality values when* $\delta \leq 1/2$.

Proof. We can prove our conclusions using a proof method similar to Theorem 8 in [23]. Let Q and Q' be vectors of a quality function that differ for a single bidder, and let $C^{(g)}$ and $C'^{(g)}$ be corresponding bid vectors. We show that DADPM can preserve bid privacy even if the order of winning bidders is revealed. Assume we get an arbitrary sequence of winning buyers $W = W'(= \{w_1, w_2, \cdots, w_l\})$ with length l. The relative probability of obtaining the sequences

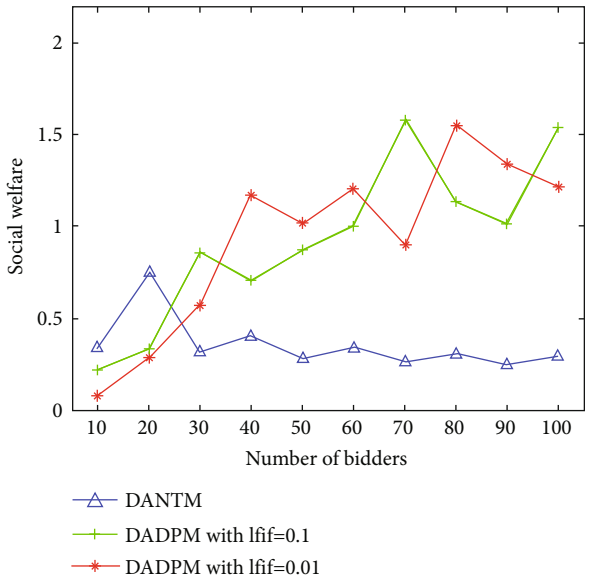

Figure 7: Social welfare of data market.

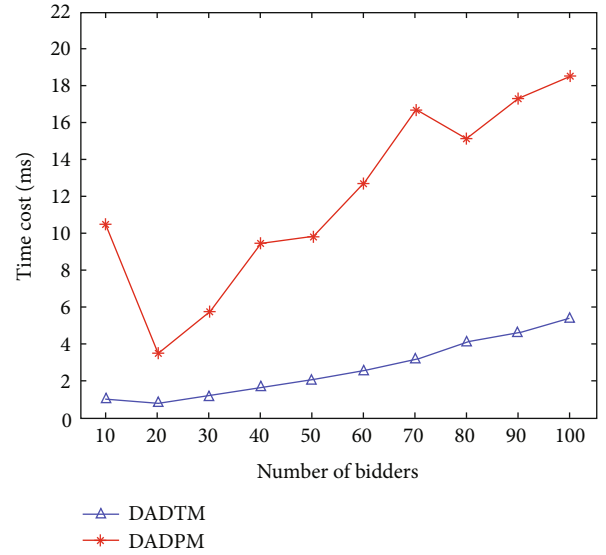

Figure 8: Time cost of data trading.

for given vectors of quality function Q and Q' is

$$\frac{\Pr[W=\{w_1,w_2,\cdots,w_l\}]}{\Pr\left[W'=\{w_1,w_2,\cdots,w_l\}\right]}=\prod_{i=1}^{l}\left(\frac{\exp\left(\varepsilon_1\cdot q_i^{(g)}\right)/\sum_{s_j^{(g)}\in S^{(g)}}\exp\left(\varepsilon_1\cdot q_{ij}^{(g)}\right)}{\exp\left(\varepsilon_1\cdot q'^{(g)}_i\right)/\sum_{s_j^{(g)}\in S^{(g)}}\exp\left(\varepsilon_1\cdot q'^{(g)}_{ij}\right)}\right)$$
$$=\prod_{i=1}^{l}\exp\left(\varepsilon_1\cdot\left(q_i^{(g)}-q'^{(g)}_i\right)\right)\times\prod_{i=1}^{l}\frac{\sum_{s_j^{(g)}\in S^{(g)}}\exp\left(\varepsilon_1\cdot q'^{(g)}_{ij}\right)}{\sum_{s_j^{(g)}\in S^{(g)}}\exp\left(\varepsilon_1\cdot q_{ij}^{(g)}\right)},\tag{14}$$

if $q_i^{(g)}>q'^{(g)}_i$, $\exp(\varepsilon_1\cdot(q_i^{(g)}-q'^{(g)}_i))\le\exp(\varepsilon_1\cdot\Delta_1)$, and the second product is less than 1. Therefore,

$$\frac{\Pr[W=\{w_1,w_2,\cdots,w_l\}]}{\Pr\left[W'=\{w_1,w_2,\cdots,w_l\}\right]}\le\exp(\varepsilon_1\cdot\Delta_1),\tag{15}$$

if $q_i^{(g)}<q'^{(g)}_i$, the first product is less than 1; therefore,

$$\frac{\Pr[W=\{w_1,w_2,\cdots,w_l\}]}{\Pr\left[W'=\{w_1,w_2,\cdots,w_l\}\right]}\le\prod_{i=1}^{l}\frac{\sum_{s_j^{(g)}\in S^{(g)}}\exp\left(\varepsilon_1\cdot q'^{(g)}_{ij}\right)}{\sum_{s_j^{(g)}\in S^{(g)}}\exp\left(\varepsilon_1\cdot q_{ij}^{(g)}\right)}$$
$$=\prod_{i=1}^{l}\frac{\sum_{s_j^{(g)}\in S^{(g)}}\exp\left(\varepsilon_1\cdot\beta_{ij}\right)\cdot\exp\left(\varepsilon_1\cdot q_{ij}^{(g)}\right)}{\sum_{s_j^{(g)}\in S^{(g)}}\exp\left(\varepsilon_1\cdot q_{ij}^{(g)}\right)}$$
$$=\prod_{i=1}^{l}E_i[\exp(\varepsilon_1\cdot\beta_i)],\tag{16}$$

where $\beta_{ij}=q'^{(g)}_{ij}-q_{ij}^{(g)}$, and the expectation is taken over the probability distribution about the quality values of $S^{(g)}$ at the time slot. Note that $S^{(g)}$ is adjusted dynamically in DADPM, and $q_{ij}^{(g)}$ is the value of $q_j^{(g)}$ to calculate $\Pr(c_i^{(g)})$ when winning buyer i is selected. For all $\alpha\le1$, $e^\alpha\le1+(e-1)\cdot\alpha$. Therefore, for all $\varepsilon_1\le1$, we have

$$\prod_{i=1}^{l}E_i[\exp(\varepsilon_1\cdot\beta_i)]\le\prod_{i=1}^{l}E_i[1+(e-1)\varepsilon_1\cdot\beta_i]$$
$$\le\exp\left((e-1)\varepsilon_1\prod_{i=1}^{l}E_i[\beta_i]\right).\tag{17}$$

Since δ is a small positive value ($\delta\le1/2$), by Lemma B.2 in [26], we have $\prod_{i=1}^{l}E_i[\beta_i]\le\Delta_1\ln(e\delta^{-1})$.

So, there exists

$$\frac{\Pr[W=\{w_1,w_2,\cdots,w_l\}]}{\Pr\left[W'=\{w_1,w_2,\cdots,w_l\}\right]}\le\exp\left(\varepsilon_1\cdot\Delta_1\cdot(e-1)\cdot\ln\left(e\delta^{-1}\right)\right).\tag{18}$$

Similar to the proof of Theorem 14, we can conclude that DADPM preserves sellers' valuation privacy. □

Theorem 15. *For data sellers, DADPM preserves $(\varepsilon_2(e-1)\Delta_2\ln(e/\delta),\delta)$ differential privacy for bidders' quality values when $\delta\le1/2$.*

5.3. Design Rationale Discussion. Two popular mechanisms to ensure differential privacy are the exponential mechanism and Gaussian mechanism. The exponential mechanism protects the privacy of the input by randomly selecting the output result via probability in a set. It is commonly used for a one-sided auction. Problems with lower social welfare and satisfaction ratio may occur when it is used for a double auction [5]. The Gaussian mechanism protects the privacy of the input by calculating the output results after adding

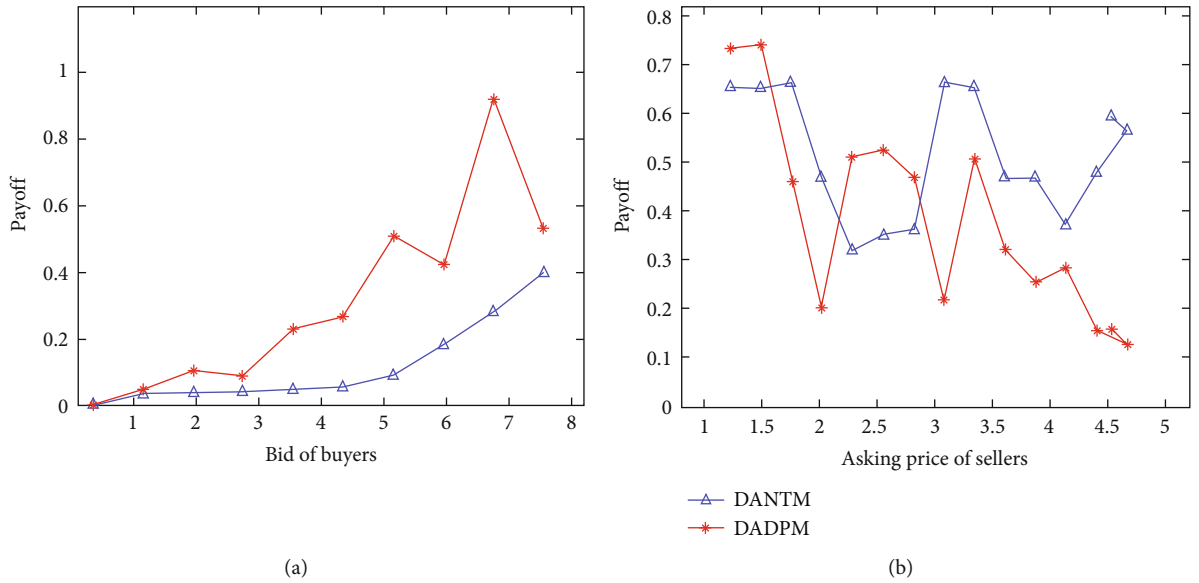

Figure 9: Payoff change impacted by (a) bids and (b) asking prices.

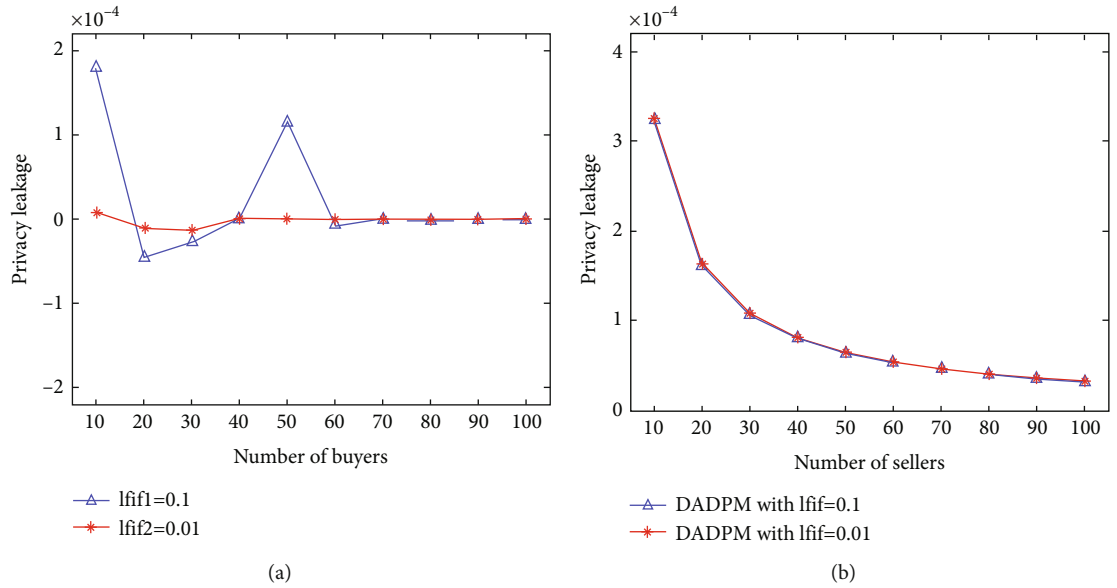

Figure 10: Privacy leakage: (a) buyers; (b) sellers.

Gaussian noise to the input. The disadvantage of this method is the difficulty in determining the size of the noise to achieve a balance between the protection of privacy and the auction performance.

Researchers who used the above mechanisms include Zhu and Shin [23] and Li et al. [5]. Zhu and Shin [23] used the exponential mechanism to solve the one-side auction for spectrum with approximate revenue maximization and achieved good results. Li et al. [5] solved the double auction for smart grid, where the Gaussian mechanism was adopted for the privacy protection of bidders' valuation, while the exponential mechanism was adopted for the protection of transaction volume.

To the best of our knowledge, prior to our paper, there was no double-auction study on data and no differential privacy protection solution on this basis. Given the apparent shortcomings of the Gaussian mechanism, our work employs an exponential mechanism to protect price privacy.

Our work for data double auction is different from the traditional sense of resource double auction, because the resource (such as the above spectrum and power) is unique; a resource in a slot can only match and provide to a unique buyer, and the data are repeatable, i.e., a seller of data in a slot can match and provide them to multiple different buyers, not a one-to-one matching relationship. Therefore, our work adopts the exponential mechanism for double

auction, which theoretically has no problem, and will not encounter the low auction performance mentioned by Li et al. [5]. Later performance evaluations also demonstrate this.

In addition, our work focuses on the single core element of the bid of the auction, which is different from [5] to protect valuation and transaction volume, making the background of using the exponential mechanism different from [5] at this point.

6. Performance Evaluation

As there is no existing scheme for data double auction as far as we know, we directly evaluate the effectiveness of DANTM and DADPM, considering the auction process in a slot. We assume uniformly distributed bids, asking prices, and demand and supply volumes of bidders. We further assume substantial matches of data quality between providers and purchasers. We set ε_1 and ε_2 to 0.1. Unless otherwise stated, simulation results are based on these settings.

We evaluate the characteristics of DANTM and DADPM, including individual rationality, weak budget balance, and truthfulness, and their comprehensive performance, including social welfare, time cost, and privacy leakage.

We ran simulations on a PC with a 1.80 GHz Intel Core i7-8565U CPU and 16 GB RAM under Windows 10. Results were averaged over 100 runs to obtain fair and credible results.

6.1. Evaluation of Basic Characteristics for DANTM and DADPM

6.1.1. Individual Rationality. Figure 5 shows payoffs for buyers and sellers using DANTM and DADPM. We can see that every payoff is positive, which satisfies the principle of individual rationality for buyers and sellers.

6.1.2. Weak Budget Balance. Figure 6 displays the relationship between the number of bidders and the average budget (defined in (6)) obtained with DANTM and DADPM. Half the bidders are buyers, and half are sellers; the same setting is used while the horizontal axis represents the number of bidders in Figures 7 and 8. The results show positive budgets in DANTM and DADPM; hence, a weak budget balance is reached.

6.1.3. Truthfulness. To verify truthfulness using DANTM and DADPM, we need to observe how the bid/asking price impacts the payoff for buyers/sellers. Figure 9 shows the experimental results. In Figure 9(a), the payoff generally decreases with decreasing bids, which means that a lower bid does not help buyers obtain a higher payoff. In Figure 9(b), the payoff does not increase when sellers ask a higher price.

6.2. Evaluation of Comprehensive Performance for DANTM and DADPM

6.2.1. Social Welfare. Figure 7 shows the average social welfare for a bidder with different numbers of bidders. We can see that the average social welfare in DADPM is higher than in DANTM in most cases, which is due to different transaction pricing mechanisms. For convenience, we replace ε with Ifif in Figures 7 and 10 (note that ε represents ε_1 and ε_2).

6.2.2. Privacy Leakage

Definition 16 (Privacy Leakage). Assume Q_1 and Q_2 are neighboring databases that differ only in a single datum. We use W as the output of some algorithm $M()$ on input Q_1 and Q_2, and W^+ is the set of outputs W. Pr is the probability distribution about $M(Q_i) = W$ with $i = 1$ and 2. The privacy leakage (Pl) between two neighboring databases is derived as [5]

$$\mathrm{Pl} = \sum_{W \in W^+} \Pr[M(Q_1) = W] \ln \left(\frac{\Pr[M(Q_1) = W]}{\Pr[M(Q_2) = W]} \right). \quad (19)$$

From the definition, we can see that privacy leakage indicates how we can distinguish the input when the generated output is the same. The less the privacy leakage, the better the privacy protection.

In our situation, we change one bid in a group of bidders, with the winning bidders unchanged, to obtain the privacy leakage results in Figure 10. In Figure 10(a), the privacy leakage is limited between −0.0002 and 0.0002. In Figure 10(b), it is limited between 0 and 0.0004. Based on these results, it is almost impossible to distinguish or infer the bidding information and threaten bidder privacy.

6.2.3. Time Cost. Figure 8 shows the time cost of data trading as the number of bidders changes from 10 to 100. In most cases, the time cost increases with the number of bidders. As the computing process is more complex in DADPM than in DANTM, its time cost is higher. The highest time cost is less than 20 ms, which indicates the effectiveness of our schemes.

7. Conclusion

We described a blockchain-supported IoT data market framework and focused on data trading of multiple buyers and sellers. We presented a data trading scheme, based directly on the bid information of participants, to determine the winning sellers and buyers at auction and the amount and trading price. To protect participant bid information, we leveraged the data transaction scheme based on differential privacy, with the properties of individual rationality, weak budget balance, and truthfulness, and with good privacy protection based on an exponential mechanism. A performance evaluation demonstrated the effectiveness of the schemes. Experimental results confirmed the above properties, along with good performance in terms of social welfare and computational overhead.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the Natural Scientific Foundation of China (grant no. 62172242) and sponsored by the K. C. Wong Magna Fund in Ningbo University.

References

[1] 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.

[2] K. Figueredo, D. Seed, and C. Wang, "A scalable, standards-based approach for IoT data sharing and eco-system monetization," *IEEE Internet of Things Journal*, vol. 9, pp. 5645–5652, 2020.

[3] K. Mišura and M. Žagar, "Data marketplace for Internet of Things," in *2016 International Conference on Smart Systems and Technologies (SST)*, pp. 255–260, Osijek, Croatia, 2016.

[4] L. G. Pitta and M. Endler, "Market design for IoT data and services the emergent 21st century commodities," in *2018 IEEE Symposium on Computers and Communications (ISCC)*, pp. 410–415, Natal, Brazil, 2018.

[5] D. Li, Q. Yang, W. Yu, D. An, Y. Zhang, and W. Zhao, "Towards differential privacy-based online double auction for smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 971–986, 2020.

[6] P. Cui, U. Guin, A. Skjellum, and D. Umphress, "Blockchain in IoT: current trends, challenges, and future roadmap," *Journal of Hardware and Systems Security*, vol. 3, no. 4, pp. 338–364, 2019.

[7] O. Novo, "Blockchain meets IoT: an architecture for scalable access management in IoT," *IEEE Internet Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.

[8] D. Nguyen and M. I. Ali, "Enabling on-demand decentralized IoT collectability marketplace using blockchain and crowdsensing," in *2019 Global IoT Summit (GIoTS)*, pp. 1–6, Aarhus, Denmark, 2019.

[9] W. Badreddine, K. Zhang, and C. Talhi, "Monetization using blockchains for IoT data marketplace," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–9, Toronto, ON, Canada, 2020.

[10] Y. Jiao, P. Wang, S. Feng, and D. Niyato, "Profit maximization mechanism and data management for data analytics services," *IEEE Internet Things Journal*, vol. 5, no. 3, pp. 2001–2014, 2018.

[11] W. Mao, Z. Zheng, and F. Wu, "Pricing for revenue maximization in IoT data markets: an information design perspective," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, pp. 1837–1845, Paris, France, 2019.

[12] H. Oh, S. Park, G. M. Lee, H. Heo, and J. K. Choi, "Personal data trading scheme for data brokers in IoT data marketplaces," *IEEE Access*, vol. 7, pp. 40120–40132, 2019.

[13] K. Liu, X. Qiu, W. Chen, X. Chen, and Z. Zheng, "Optimal pricing mechanism for data market in blockchain-enhanced internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9748–9761, 2019.

[14] Z. Zheng, W. Mao, F. Wu, and G. Chen, "Challenges and opportunities in IoT data markets," in *SocialSense'19: Proceedings of the Fourth International Workshop on Social Sensing*, pp. 1-2, Montreal, QC, Canada, 2019.

[15] Y. Na, Y. Joo, H. Lee et al., "Enhancing the reliability of IoT data marketplaces through security validation of IoT devices," in *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 265–272, Marina del Rey, CA, USA, 2020.

[16] J. Meijers, G. Dharma Putra, G. Kotsialou, S. S. Kanhere, and A. Veneris, "Cost-effective blockchain-based IoT data marketplaces with a credit invariant," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1–9, Sydney, Australia, 2021.

[17] L. D. Nguyen, I. Leyva-Mayorga, A. N. Lewis, and P. Popovski, "Modeling and analysis of data trading on blockchain-based market in IoT networks," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6487–6497, 2021.

[18] P. Gupta, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "Towards a blockchain powered IoT data marketplace," in *2021 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pp. 366–368, Bangalore, India, 2021.

[19] G. Ishmaev, "The ethical limits of blockchain-enabled markets for private IoT data," *Philosophy & Technology*, vol. 33, no. 3, pp. 411–432, 2020.

[20] J. Wang, C. Jiang, Z. Bie, T. Q. S. Quek, and Y. Ren, "Mobile data transactions in device-to-device communication networks: pricing and auction," *IEEE Wireless Communications Letters*, vol. 5, no. 3, pp. 300–303, 2016.

[21] H. Oh, S. Park, G. M. Lee, J. K. Choi, and S. Noh, "Competitive data trading model with privacy valuation for multiple stakeholders in IoT data markets," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3623–3639, 2020.

[22] Z. Xiao, D. He, and J. Du, "A Stackelberg game pricing through balancing trilateral profits in big data market," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12658–12668, 2021.

[23] R. Zhu and K. G. Shin, "Differentially private and strategy-proof spectrum auction with approximate revenue maximization," 2014, https://www.dropbox.com/s/z50284bvbgp2vrf/pass.pdf.

[24] H. G. Do and W. K. Ng, "Blockchain-based system for secure data storage with private keyword search," in *2017 IEEE World Congress on Services (SERVICES)*, pp. 90–93, Honolulu, HI, USA, 2017.

[25] V. V. Vazirani, N. Nisan, T. Roughgarden, and E. Tardos, *Algorithmic Game Theory*, Cambridge University Press, Cambridge, UK, 2007.

[26] A. Gupta, K. Ligett, F. McSherry, A. Roth, and K. Talwar, "Differentially private combinatorial optimization," in *Proceedings of the 2010 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pp. 1106–1125, Austin, Texas, USA, 2010.